ISSN 1060-992X, Optical Memory and Neural Networks, 2020, Vol. 29, No. 4, pp. 336–353. © Allerton Press, Inc., 2020.

An Effective and Secure Data Sharing in P2P Network Using Biased Contribution Index Based Rumour Riding Protocol (BCIRR)

Dharmendra Kumar[a], * and Mayank Pandey[b]

[a]*Dr. A.P. J Abdul Kalam Technical University, Lucknow, Uttar Pradesh, India*

[b]*Motilal Nehru National Institute of Technology, Teliarganj, Prayagraj, Uttar Pradesh, India*

**e-mail: kumar.dharmendra@rediffmail.com*

Received November 11, 2019; revised May 14, 2020; accepted May 27, 2020

Abstract—Data sharing in the Peer to Peer (P2P) networks became an important function in the trustworthy computing. Secure and load balancing control in file sharing is vital to enhance the overall performance of P2P file sharing system. In literature many methods of load balancing control and security control have been used but it is not able to attain the best results in P2P networks. Hence, in this paper, Biased Contribution Index Based Rumour Riding Protocol (BCIRR) is developed to attain the load balancing control and security enhancement of P2P networks. The proposed method is concentrated to achieve two main objective function such as load balancing control and security enhancement. The proposed protocol is a combination of Biased Contribution Index (BCI) and Enhanced Rumour Riding protocol (ERR). Here, load balancing control of the P2P network is attained with the utilization of the BCI and security enhancement of the P2P network is attained with the utilization of the ERR. The proposed protocol will be implemented in the Matlab platform and the performance of the proposed protocol is analysed with different performance metrics such as Packet loss, Delivery ratio, Average end to end delay and Throughput. To analysis the effectiveness of proposed method, it will be compared with the existing method of Catching Algorithms (CA).

Keywords: P2P networks, BCI, ERR, BCIRR, load balancing, and security enhancement

DOI: 10.3103/S1060992X20040104

1. INTRODUCTION

Nowadays, the P2P network can be a popular architecture and it used for diverse applications of different services such as file sharing, content distribution, backup storage, communication of voice, instant messages and multicast, etc. [1]. Additionally, the P2P network able to share files and content distribution without a client-server model. The P2P network, the computers are acting as the client and server model for sharing the data resources and files, etc. [2]. For example, a file transfer request which is sent computer A to computer B. In the above file sending process, the A computer act as a client and computer B acts as the server model in the computer. Based on the request to sharing the file, the client and server role changes in the network [3]. This process able to reduce the work of the server model and enhance the general performance of the network. The file-sharing application is very popular and it is presently used in P2P networks. The P2P network tries to control the limitations of client/server architecture [4].

The P2P networks are fault-tolerant, self-organizing, security, load balancing and scalable assurances on a number of hops to solution a query. Additionally, P2P systems are popular due to the many advantages such as the ability to pool together and harness huge volumes of resources, availability through massive replication [5]. Without need of powerful and expensive server, P2P networks can be able to do the file sharing with bandwidth and storage, distribute the main cost of sharing data and across all the peers in the network. P2P networks basically come in three types; (1) centralized P2P networks such as Napster, (2) decentralized unstructured networks such as Gnutella and Kazaa and 3) decentralized structured networks such as Content-Addressable Network (CAN) and Chord [6]. P2P networks are getting more significant and popular over internet-based applications. Despite, P2P networks have many strengths, however P2P networks also present many challenges that are presently obstacles to their widespread acceptance and usage such as efficiency, load balancing security and performance guarantees like transactional semantics and atomicity [7].

To attain efficient operation of P2P networks, Load balancing and security are critical issues. Many methods are developed by the researcher to enhance the data sharing in the P2P networks such as ID Management Algorithm, Intra-Cluster, and Inter-Cluster Load Balancing and Load Balancing Algorithm in Dynamic Structured P2P Systems using Directories [8], etc. ID management algorithm is used to data and execution balancing in P2P networks. This algorithm gathers statistics of overlay link usage while normal operation and uses this information to supply suitable ID to joining peers [9]. However, the response time of peers is changed. Additionally, many factors affecting the security of P2P networks. Open P2P networks are insecure because users can join without authentication of their identity. So anyone can access data without authentication, it can be lead the security problem in the P2P networks. Many methods earlier developed for meeting security in P2P network, of tens or hundreds of servers may no longer apply [10]. So new techniques are required to meet the load balancing control and security enhancement in P2P systems.

Contribution of the Paper

In this paper, we present a BCIRR method to provide data balancing and security in the P2P networks. The proposed system includes the following contributions,

—The proposed technique is developed to achieve security with data balancing control in the P2P networks.

—The proposed system is concentrated on two main objectives such as enhancement of security and load balancing control in P2P networks.

—The data balancing control of the P2P network is enhanced with the help of the BCI computation and BCI should balance the download and upload amount of resources at each peer.

—The security of the P2P network is achieved with the use of the ERR and it is identify the attacker node, avoid the viruses and enhance the security of the system.

—The proposed method for security enhancement and load balancing control is evaluated using MATLAB and its performance is validated based on the Packet loss, Delivery ratio, Average end to end delay, Throughput, encryption time, decryption time, and it is compared with the CA.

The remaining part of the paper organized as follows, the section 2 reviewed the recent works related to our research study. The section 3 describes the detail information of the BCIRR method for enhancing security and data balancing control in the P2P network. The BCI index computation and ERR processing also presented in the section 3. The implementation results of the proposed method are described in the section 4. Finally, section 5 concludes the document.

2. REVIEW OF RELATED WORKS

In recent years, load balancing control and security enhancement methods in P2P networks were developed by the researcher. Some of the methods are reviewed here,

Moufida Rahmani et al. [11] have developed a multichip proximity aware clustering scheme to mobile peer-to-peer systems (PCSM). The PCSM method was working based on the physical proximity of peers and reduction of mismatch among the P2P overlay and network layer. The PCSM has integrated three factors for allowing the new peer to select the cluster to join such as availability of the cluster head, cluster size and number of physical hops. The PCSM method was compared with the existing cluster based P2P overlay regarding routing overhead and load balancing.

Abhinav Jain et al. [12] have developed friendShare to overcome the problems of collusion attack, Sybil attack and selfish nodes in P2P networks. FriendShare was mainly operating the concept of a friend to friend in the social network. In friendShare, each node has in keeping list of friends and transactions can be attained by friends. FriendShare consists of a weighted graph system and reputation system. Additionally, it included a proxy server empowerment complete anonymity in the network which improves the freedom of speech. The developed method has enhanced the operation and reducing the delivery time.

Jianwei Zhang et al. [13] have introduced water filling (WF) algorithm for enhancing the steaming efficiency of multiple streams in P2P networks. Here, they developed the optimal non-Forwarding (ONF) and Optimal Forwarding (OF) into linear programs (LPs) to getting the dc facto upper bounds. After that, to facilitate the collaboration among servers while maintaining as even load distribution occurred. The WF algorithm was proved that low time complexity and near optimal efficiency. In the method, theoretical bounds, methods, and algorithm with key parameters were evaluated in the terms of bandwidth of the server in the P2P network and size of P2P network. The flow-based method was used for analysing the

intrinsic features of the problems associated with multiple streams. The developed method was used for P2P networks and content distribution in datacentre networks (DCNs).

R. Thiyagarajan et al. [14] have developed EAACK (Enhanced Adaptive Acknowledgment) with Enhanced Interior Gateway Routing Protocol (EIGRP) for detecting misbehaviour of nodes during packet deliver with acknowledgment to protect of P2P networks. Here, EIGRP was a hybrid method that consists of P2P ACK (peer to peer Acknowledgement) and RSA (named after Ron Rivest, Adi Shamir, and Len Adleman) algorithm. EIGRP was introduced to reduce the network overhead occurred by digital signature in EAACK. RSA can encrypt the session key which encourages the key more secure to enhance the security level and P2P ACK. To verify and sign the acknowledgment packets, the RSA is utilized by generating keys in P2P ACK. The developed method was improvising security level and reduce the routing overhead by the secured acknowledgment in P2P network.

Amna Qureshi et al. [15] have developed a P2P content distribution system for improving efficiency, security, and privacy of merchants and buyers. The developed method was able to solve the difficulties of dispute resolution, buyer anonymity, collusion resistance, buyer frame proofness, and piracy tracing. The performance of the developed method was analysed with the terms of content delivery cost, throughput, robustness, and imperceptibility. The developed method was provided a better solution to different issues in P2P network such as infringement issues, reducing multimedia file sizes as much as five times on average, privacy and anonymity.

Generally, the P2P systems are attractive because they no need any additional administrative arrangements, fault tolerant, bandwidth efficient, decentralized, distributed nature make them scalable and unlike centralized facilities. This network also has problems related to load balancing during data sharing operation and data security. To enable the load balancing and security in P2P network, the researchers are developed various method. Some of the methods are reviewed here, such as PCSM, friendShare, WF algorithm, EAACKP2P and content distribution system. In [11] author developed PCSM to reduce mismatch among the P2P overlay and network layer. However, it was not clearly addressing for a super/cluster based unstructured MP2P system for the reason that they did not consider an overlay distinct from an underlay. In [12] the author developed friendShare to overcome the problems of collusion attack, Sybil attack and selfish nodes in P2P networks. However, the method of detection non-cooperative behaviour, i.e., sending dishonest feedback was required to detect such cases.

In [13] the author developed WF algorithm for enhancing the steaming efficiency of multiple streams in P2P networks. However, they can focus on the server capacity provisioning and P2P node collaboration. In [14] the author developed EAACK protocol for detecting misbehaviour of nodes during packet deliver with acknowledgment to protect of P2P networks. Moreover, these results can operate only if the packets were dropped. In [15] the author developed P2P content distribution system for improving efficiency, security, and privacy of merchants and buyers. However, this illegal re-distribution act is not only onerous to content providers but also to the end users. To overcome the above drawbacks, the proposed method will be developed and implemented in this paper.

3. PROPOSED MODEL OF PEER TO PEER NETWORK

Generally, the P2P systems deliver an efficient infrastructure for large-scale distributed applications like as data sharing. The popularity of the P2P network, it has many advantages compare to the conventional client server model such as cost effectiveness, robustness, scalability, diversity of available data etc. The P2P network initial setup of the cost is very less compare to the conventional client- server model because it not needs costly central servers. Thus, lack of central control introduces the problem of inefficient data sharing in these networks. In the meantime, the P2P systems essentially depend on the need of peers with each other, so the security implications raise from harming the trust among peers. From the conventional client-server model, the internal data not be showing to the client, but in the P2P, some internals should be showed to parallel peers in the name of distributing the workload. So attackers can influence this in compromising P2P network [16]. However, these networks are affected by the security and load balancing problems in the data sharing process. In recent years many methods are developed by the researchers to main the efficient data sharing and secure data securing in the P2P network and some of the methods are reviewed in the section 2. At same, many researchers only focus either load balancing or security of data sharing in the P2P network [17]. In this paper, BCIRR technique is developed to balancing the data sharing and enhancing the security in the P2P network.

Figure 1 shows the architecture of the proposed method in P2P networks. Each peer has the capability of share data and the data should be balanced with secure operation for enhancing the reliability of the P2P networks. The data sharing resources are balanced with the help of the BCI index values. In the P2P

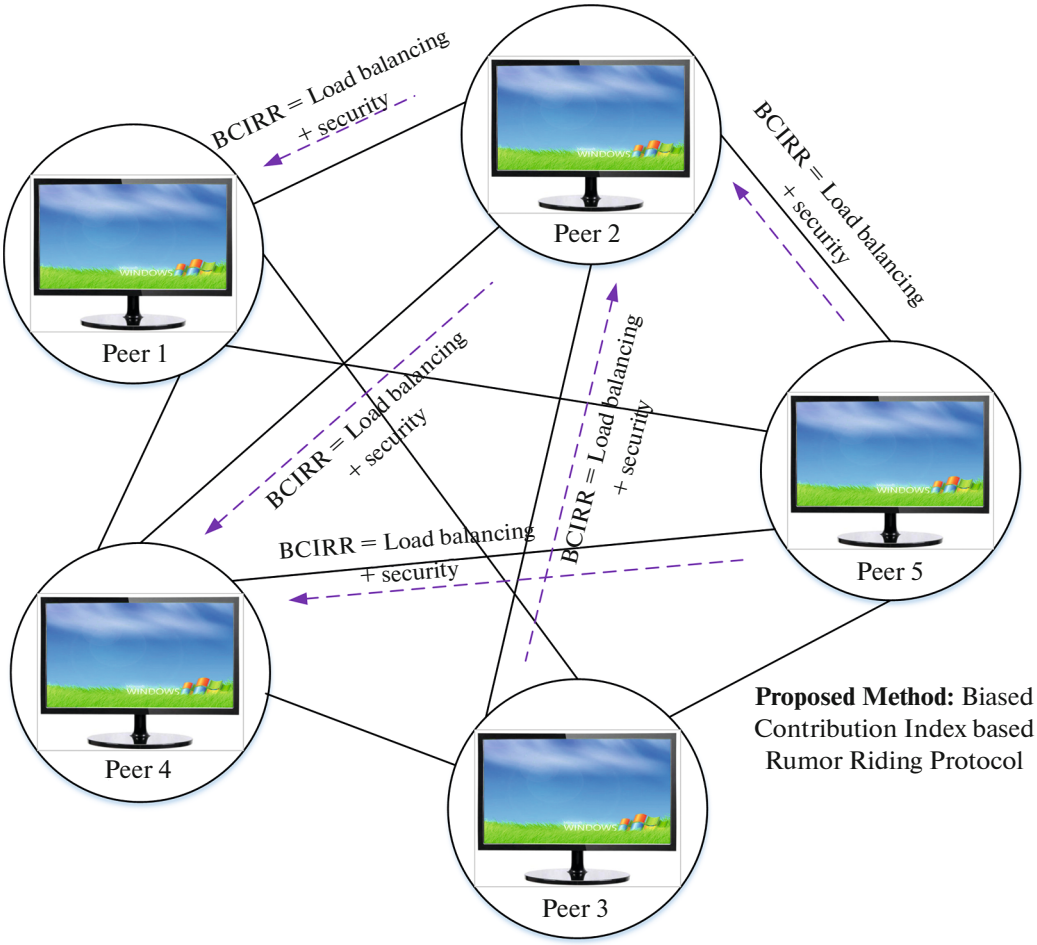

Fig. 1. Architecture of the proposed model in P2P network.

networks, each peer BCI values are computed based on the data sharing concerns. Based on the index values, the peers are motivated to share the resources for balancing the data in the P2P networks. The security also important concern in the P2P networks during data sharing operation. Because, in the P2P network, any peer can be able to add the network for download and upload of data. So easily malicious peer can be connected in the network. With the utilization of the ERR protocol, the attacker peer is identified in the P2P network. Finally, the load balancing and security of the P2P network is achieved with the consumption of the BCIRR techniques. The detail description of the proposed method is explained in the below section

3.1. Biased Contribution Index Based Rumour Riding Protocol (BCIRR)

The P2P networks may increase to a significant amount of traffic on internet because of its inherent advantages over conventional client-server networks such as diversity of data, scalability and robustness. The P2P network is an open and anonymous environment which gives permission an opportunity to interact with others it also brings the security threats and unbalanced data sharing conditions. To enhance the load balancing control and security in the P2P network, BCIRR is developed in this paper. The BCIRR method is working based on the two mode of operation such as load balancing control and security control. In the first mode of operation, develop the incentive mechanism based on the BCI of peers to attain the load balancing in data sharing. The mechanism can balance the upload and download amount of resources in each peer. It is used to balance the data sharing from the user to receiver in P2P networks without packet data loss, jitter etc. In the second mode of operation, ERR protocol for enhance the security in P2P networks. The conventional RR protocol can be an anonymous method which is used to hide the information from source to destination without authentication. However, it is not effective method.

Here, the ERR is used for enhancing security in the P2P network by cryptographic puzzle attributed to the challenge question method. The descriptions of the process of the BCI and ERR is presented in the below section.

3.1.1. Biased contribution index (BCI). P2P systems are utilized in the internet to share resources such as consuming power, data storage, data sharing and band width among the computers [18]. The resources are distributed in the P2P network. In the P2P network load balancing under the data sharing is difficult concern. To balance the resources in the P2P network, BCI index is developed in this paper. In the BCI index computation have some assumption of rules are developed for ensuring the design of P2P network which are presented below,

—The BCI should be zero; If any peer only downloads the resources from the network

—The BCI should be one; If any peer only uploads to the network

—The BCI value should not increase under the condition of uploading to the free-riders

—The BCI value is increased at the condition of uploading resources to any other peer

—The BCI values is decreases at the condition of download resources

—The upload scenario of peer is motivated to attain high contributing peers

For example, N number of peers are taken in a P2P network. Additionally, the discrete instances are considered as time evolution. The T_N can be considered as the time instants and it is happened in the time interval i.e. (T_N, T_{N-1}). At the time instant T_N the entire network share matrix in denoted as the $SM(T_N)$. In the share matrix, ab element is the amount of resources shared through the peer a to peer b at the time interval T_N i.e. (T_N, T_{N-1}). The bias ratio of the peer a at the time instant T_N is represented as the $B_a(T_N)$ which can be formulated by below equation,

$$B_a(T_N) = \frac{E_a SM(T_N) Y(T_N)}{E_a SM^{\mathrm{Tr}}(T_N) Y(T_N)}. \tag{1}$$

Where, E_a is referred as the row vector and its a^{th} entry taken as 1 and remaining part as zero, $Y(T_N)$ can be represented as BCI vectors of peers at time T_N. With the consumption of the bias ratio computation, the BCI index of the P2P networks calculated based on the below equation,

$$X_a(T_N) = \frac{B_a(T_{N-1})}{1 + B_a(T_{N-1})}, \tag{2}$$

$$= \frac{E_a SM(T_{N-1}) Y(T_{N-1})}{E_a SM^{\mathrm{Tr}}(T_{N-1}) Y(T_{N-1}) + E_a SM^{\mathrm{Tr}}(T_{N-1}) Y(T_{N-1})}. \tag{3}$$

From the equation (3), the BCI index can be calculated and peer a as on monotonically increasing function of the bias ratio at time T_{N-1} and $Y(T_{N-1})$ can be referred as BCI vectors of peers at T_{N-1}. Based on the BCI index computation rules, if peer a does not upload anything in the P2P network in the time duration T_{N-1}, the $E_a SM(T_{N-1}) Y(T_{N-1}) = 0$. Additionally, the peer a did not download somewhat from the network which time $E_a SM^{\mathrm{Tr}}(T_{N-1}) Y(T_{N-1}) \neq 0$ and $Y(T_{N-1}) \neq 0$. Based on the conditions, the denominator values should be changed to zero. To avoid the zero values and maintain the nonzero values for nonzero downloading, zero uploading, from the equation (3) terms of $E_a SM^{\mathrm{Tr}}(T_{N-1}) Y(T_{N-1})$ is changed to $\alpha E_a SM^{\mathrm{Tr}}(T_{N-1}) Y(T_{N-1}) + (1-\alpha) E_a SM^{\mathrm{Tr}}(T_{N-1}) E$. Where, E can be represented as the column vector with each element as 1 and α can be taken as the constant value it is have the limit as $\alpha \in (0,1)$. By replacing the terms in the equation 2 and it was changed as below,

$$X_a(T_N) = \frac{E_a SM(T_{N-1}) Y(T_{N-1})}{\left[\alpha E_a SM^{\mathrm{Tr}}(T_{N-1}) Y(T_{N-1}) + (1-\alpha) E_a SM^{\mathrm{Tr}}(T_{N-1}) E\right]}. \tag{4}$$

At the time duration T_{N-1}, the BCI values of peers are calculated from the equation (4). The past transactions BCI index can be calculated based on the below equation,

$$X_a(T_N) = (1-\beta_a(T_{N-1})) X_a(T_{N-1}) + \beta_a(T_{N-1}) \frac{E_a SM(T_{N-1}) Y(T_{N-1})}{\left[\alpha E_a SM^{\mathrm{Tr}}(T_{N-1}) Y(T_{N-1}) + (1-\alpha) E_a SM^{\mathrm{Tr}}(T_{N-1}) E\right]}. \tag{5}$$

From the equation (5), peer a does not do any transactions under the time T_{N-1} at $X_a(T_N)$ should be considered as the $X_a(T_{N-1})$. Based on the fraction of transaction, the factor $\beta_a(T_{N-1})$ can be decided which are presented in the time instant (T_{N-1}) at node a. The factor can be represented by the below equation,

$$\beta_a(T_{N-1}) = \begin{cases} 0 & \text{if } C_a = 0 \\ \dfrac{E_a\left[SM(T_{N-1}) + SM^{\mathrm{Tr}}(T_{N-1})\right]E}{E_a\left[SM_{\mathrm{comp}}(T_{N-1}) + SM^{\mathrm{Tr}}_{\mathrm{comp}(T_{N-1})}\right]E} & \text{otherwise} \end{cases}. \quad (6)$$

Where, SM_{comp} can be referred as the complete share matrix based on shared resources by peer a to peer b under the time instant T_{N-1} and C_a is considered as the terms of $E_a[SM(T_{N-1})Y(T_{N-1}) + E_aSM^{\mathrm{Tr}}(T_{N-1})]E$. To compute the BCI value for each peer by initialization process. In the initialize process can be taken as $X(0) = \dfrac{\alpha}{1-\alpha}e$ after that calculated the upload and download amounts of the P2P network. Based on the above calculations, the BCI values are computed in the peers to balance uploads and download resources in the P2P network. The initial rules of the BCI value computation are justified in the below section.

Design Rule Justification Process

To compute the BCI value of P2P network, some assumption rules are developed for ensuring the design of P2P network. The design rules are justified by the theorems which are presented below,

Rule no. 1: The BCI should be zero; if any peer only downloads the resources from the network

If any peer a only do downloads and does not upload the resources in P2P network under the time instance T_{N-1}. At the condition, the term $E_a.SM(T_{N-1}).Y(T_{N-1}) = 0$ should be equal to zero, and the term $E_aSM^{\mathrm{Tr}}(T_{N-1}) \neq 0$. The conditions are applied in the equation (5) and get the equation (7),

$$X_a(T_N) = (1-\beta_a(T_{N-1}))X_a(T_{N-1}). \quad (7)$$

The peer a does not upload resources in the P2P network under the time T_N, and only do downloading resources in the network [19] and first time at T_M. In this conditions are applied to the equation (6) and $\beta_a(T_M) = 1$, from this time,

$$X_a(T_N) = (1-\beta_a(T_{N-1}))(1-\beta_a(T_{N-2})\ldots(1-\beta_a(T_M))X_a(T_M) = 0 \quad (8)$$

Rule no. 2: The BCI value should not increase under the condition of uploading to the free-riders

If any peer a upload resources to the free-riders, which means peers who only downloads does not upload anything in the network then the below condition are analysed as follows, $E_aSM(T_{N-1})Y(T_{N-1}) = 0$ and at the time T_{N-1} does not download anything in the peer which is presented as $E_aSM^{\mathrm{Tr}}(T_{N-1})E = 0$. Hence, $C_a = 0$ computed from the equation (6) and $\beta_a(T_{N-1}) = 0$ is analysed from the equation (5), which is presented below,

$$X_a(T_N) = X_a(T_{N-1}). \quad (9)$$

Rule no. 3: The BCI should be one; if any peer only uploads to the network

At the time condition of T_{M-1}, if any peer a only do uploads in the P2P network and does not concentrate on down load anything from it have two conditions such as $E_aSM(T_{M-1})Y(T_{M-1}) \neq 0$, $\alpha E_aSM^{\mathrm{Tr}}(T_{M-1})Y(T_{M-1}) + (1-\alpha)E_aSM^{\mathrm{Tr}}(T_{M-1})E = 0$. Therefore, justify the rules from the equation (5), the justification solution of the results presented in the below equation,

$$X_a(T_M) = (1-\beta_a(T_M - 1)X_a(T_{M-1}) + \beta_a(T_{M-1})). \quad (10)$$

For assumption, if peer a do any transactions at first time in the P2P network, the conditions are applied to equation (6), we get the solution is $\beta_a(T_{M-1}) = 1$. Therefore, the condition is presented in the below equation,

$$X_a(T_M) = 0,\ X_a(T_{M-1}) + \beta_a(T_{M-1}) = \beta_a(T_{M-1}) = 1. \quad (11)$$

At the time of T_M, if a does not do any transactions of upload and download resources, it is presented as below,

$$X_a(T_{M+1}) = X_a(T_M) = 1. \tag{12}$$

If peer a does not download resources in P2P network and upload resources to the free riders which is presented below,

$$X_a(T_{M+1}) = X_a(T_M) = 1. \tag{13}$$

If peer a does not download resource in P2P network and uploads to at least one of the peer in the network which can be presented below,

$$X_a(T_{M+1}) = (1-\beta_a(T_M))X_a(T_M) + \beta_a(T_M) = (1-\beta_a(T_M))1 + \beta_a(T_M) = 1. \tag{14}$$

Based on the above discussion, we can say the rule is true for any P2P networks, hence, $X_a(T_M) = 1$

Rule no. 4: The BCI value is increased at the condition of uploading resources to any other peer

At the time of T_{N-1}, the peer a did not download resources in the network and upload resources to non-free rider peer which are introduced two conditions such as $E_aSM(T_{N-1})Y(T_{N-1}) \neq 0$, $\alpha E_aSM^{\mathrm{Tr}}(T_{N-1})Y(T_{N-1}) + (1-\alpha)E_aSM^{\mathrm{Tr}}(T_{N-1})E = o$. Hence, these conditions are applied to equation (5),

$$X_a(T_N) = (1-\beta_a(T_{N-1}))X_a(T_N) + \beta_a(T_{N-1}). \tag{15}$$

Basically, 1 and $X_a(T_{N-1})$ is a convex combination. Therefore the below conditions are generated in this justification of rules,

$$\begin{gathered} X_a(T_{N-1}) < X_a(T_N) < 1, \\ \forall \beta_a(T_{N-1}) \in (0,1). \end{gathered} \tag{16}$$

Rule no. 5: The BCI values is decreases at the condition of download resources

At the time of T_{N-1}, the peer a did not download resources in the network and download resource [20] from the network is belongs to conditions such as $E_aSM^{\mathrm{Tr}}(T_{N-1})E \neq 0$ with $C_a = 0$ and $E_aSM(T_{N-1})Y(T_{N-1}) = 0$ with $\beta_a(T_{N-1}) > 0$. The conditions are applied to the equations 5 and 6, we get,

$$X_a(T_N) = (1-\beta_a(T_{N-1}))X_a(T_N) + \beta_a(T_{N-1})0 = (1-\beta_a(T_{N-1}))X_a(T_N), \tag{17}$$

$$X_a(T_{N-1}) < X_a(T_{N-1}). \tag{18}$$

Rule no. 6: The upload scenario of peer is motivated to attain high contributing peers

From the above discussions, the rule can be concluded as high BCI index is motivated to upload the resources in the P2P network. Based on the discussions and computation of the BCI index values, in the P2P network load balancing control is attained. Simultaneously, the security of the P2P network is concentrated in the proposed method. To enhance the security of the P2P network, the ERR protocol is developed in this paper. The index value is used to balance the resources which means equalize the upload and download resources of the peers. To analysis the BCI index computation, some of the rules are developed which are justified in the section. The proposed method is computed the BCI index value and ERR protocol in the P2P network for enhancing security and load balancing control. The ERR protocol description is presented in the below section clearly.

3.1.2. Enhanced Rumour riding protocol (ERR). In this paper, ERR is developed to enable the security in the P2P networks. This protocol is used to identify the attacker peer in the P2P networks. Generally, In the P2P networks any peer can be come in or leave the networks at random condition, there is a chance for entering malicious peer can be enter the P2P system. If any malicious peer enters in the P2P networks, it will be act as an attacker and affect the system additionally spread the viruses. When malicious peer enter in the system, the security can be questionable one during upload and download resources [21]. The P2P networks, resources are forwarded through the three important nodes such as initiator node, intermediate node and responder node. From the three nodes, any one node act as an attacker, the whole process can be affected and reduce the performance of the system [22, 23]. Correspondingly, the responder node is ready to send the file to the initiator node, if responder node is a malicious node attack may introduce and send the fake response to the initiator. Hence, it sends virus all over the networks and performance of the P2P network is reduced. The initiator, intermediate and responder node attacks are illustrated in the

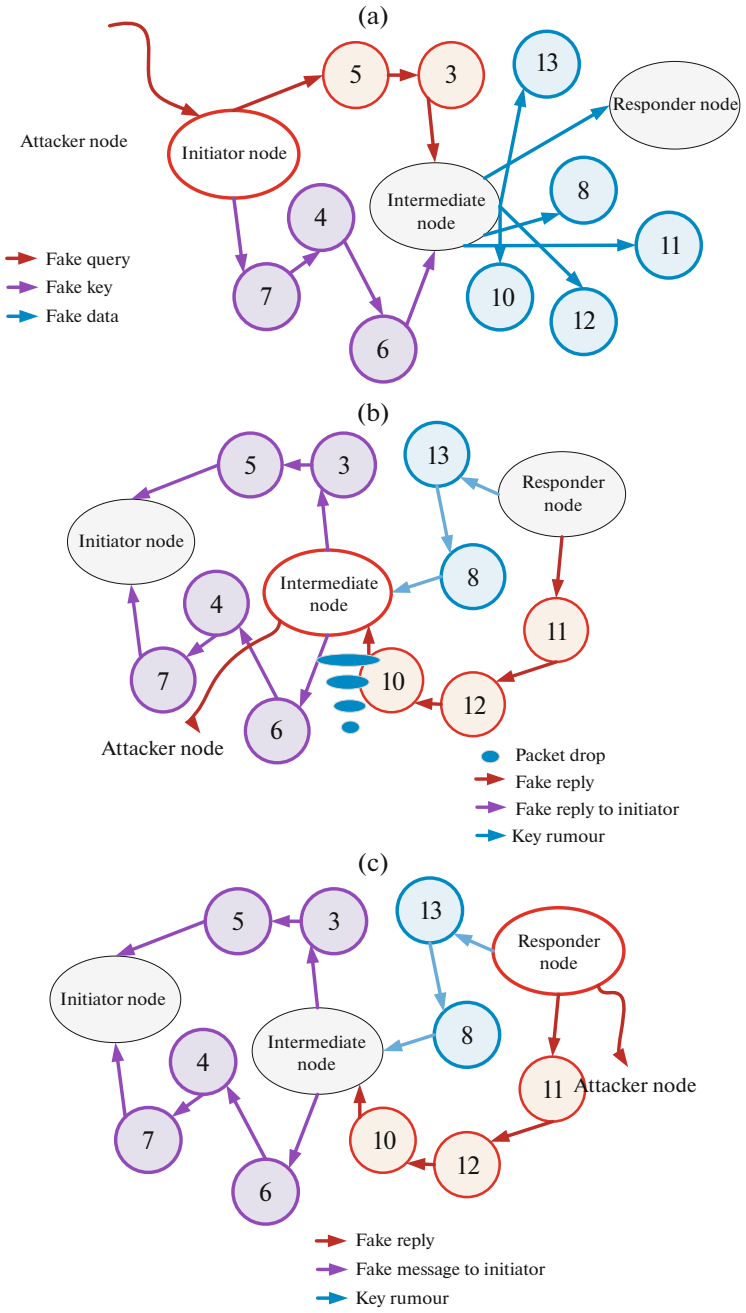

Fig. 2. Analysis of (a) initiator node attack, (b) intermediate node attack and (c) responder node attack.

Fig. 2. The different types of the attack can be identified with the help of the ERR protocol. By utilization of the ERR, the P2P networks security can be enhanced. For example, in the P2P networks, the peer 1 needs to send data to the peer 3.

Initially, finding the shortest path of the system [24]. By the way, peer 1 taken as the initiator node, peer 2 taken as the intermediate node and peer 3 taken as the responder node. For security reasons, the data should be encrypted with the utilization of the encryption algorithm which is named as the SXOR (Split XOR) encryption algorithm. The send data is divided in to two parts and randomly generate the key in the initial step [25]. After that, the separated data do the XOR operation and the send resources can be encrypted. The decryption process is a reverse process of the encryption procedure. The SXOR operation is explained in the below example,

Input data $(\mathbf{x})$: 0100 1010 0101 1110
Input data split into two parts: A : 0001 0110 0001 0010
B : 0001 0110 0100 1100
Random key generation : 0000 0000 0000 0100
XOR key : A : 0001 0110 0001 0110
B : 0011 0100 0100 1000
– Encryption process

Merge two components : 0100 1010 0101 1010
Key : 0100 1010 0101 1010
Output data $(\mathbf{y})$: 0100 1010 0101 1110
– Decryption process

For an example of the proposed method have some assumptions which are mentioned below,

—Assume input data divided as A and B

—Input data X is 0100 1010 0101 1110.

Already discussed, the proposed method has more number of peer are connected and communication process also take place. The data can be split into two components such as A and B which is represented as $X \rightarrow \{A, B\}$. For example, randomly generate component A as 0001 0110 0001 0010 so that the other component B can be computed by $X - A =$ 0011 1100 0100 1100. Finally, the original input data referred as the $X = A + B$. After that, randomly generate the key value as 0100 and this key is used for doing XOR operators with both A and S. The XOR operations are mathematically derived as, $S1 = AXOR$ key and $S2 = SXOR$ key. The values of $S1 =$ 0011010001001000 and $S2 =$ 0001011000010110. After this encryption, these data are sent to the A and B with encrypted format. So unauthorized users cannot retrieve the data without key. The method enhances the security of P2P networks. The user retrieves the data from the sending peer with the use of a key. The retrieved data is attained by following some steps. Initially, the gain data from both A and B utilize the secret key to do the XOR operations in the data. To get data from this step, which are 0001 0110 0001 0010 and 0011010001001100. After that, the two data are summed up for getting single string data. Then do an XOR operation in the summed up single string data, finally getting the original data 0100 1010 0101 1110. Based on the method, user data can be protected efficiently. In the scheme, key-value is randomly generated and additionally data split didn't carry any content information without permission. The unauthorized user cannot get sensitive information even though they touch the data from the peers. The process of the ERR protocol is presented in the Fig. 3.

The encrypted data is added with the challenge question method $(M = y + CQ)$. The challenge question method is identifying the attackers in the P2P networks. M is send to the intermediate node of peer 2 and peer 1 question the peer 2 these questions are what is the IP address, index value and location of the peer 2. The BCI index values are low, the download and upload resources are balanced in the P2P networks. The peer 2 answers the challenge question to the peer 1, based on the peer 2 answers, the true value of the peer 2 can be computed. Based on the analysis, we can found out, the peer 2 is an attacker or not. The peer 2 answers are identify the attacker status. The peer 2 not an attacker, the message is send to the intermediate node. Similarly, the challenge question with encrypted message send to the responder node, the status of the peer 3 can be identified by the peer 2. Finally, the attacker node can be found out and send the message to the receiver side. The key of the decryption process send to the key path and data are send to the data path. With the utilization of the ERR protocol, the security of the resources and attacker node can be omitted for enhancing security concerns in the P2P networks. In the proposed methodology, BCI index value computation is balance the P2P networks in data sharing and ERR protocol is enhance the security of the P2P networks. The example of the proposed method is presented in the below section.

3.2. Numerical Explanation of BCIRR in P2P Networks

In the proposed methodology, the BCIRR is used to enhance the data sharing and security of the P2P network. The BCI is developed for balancing the upload and download resources of the peers and ERR is developed for enhancing the security of the peers. The BCI index values of the each peer can be calculated based on the formulation which is presented in the section 3.1.1. The ERR protocol is used for finding attacker node and enhancing information security with the help of SXOR operation. In this section provides the numerical explanation of the BCIRR in the P2P networks. Here, five peer nodes are taken for the analysis purpose, each peer can do download and upload resources to each other. The operation of

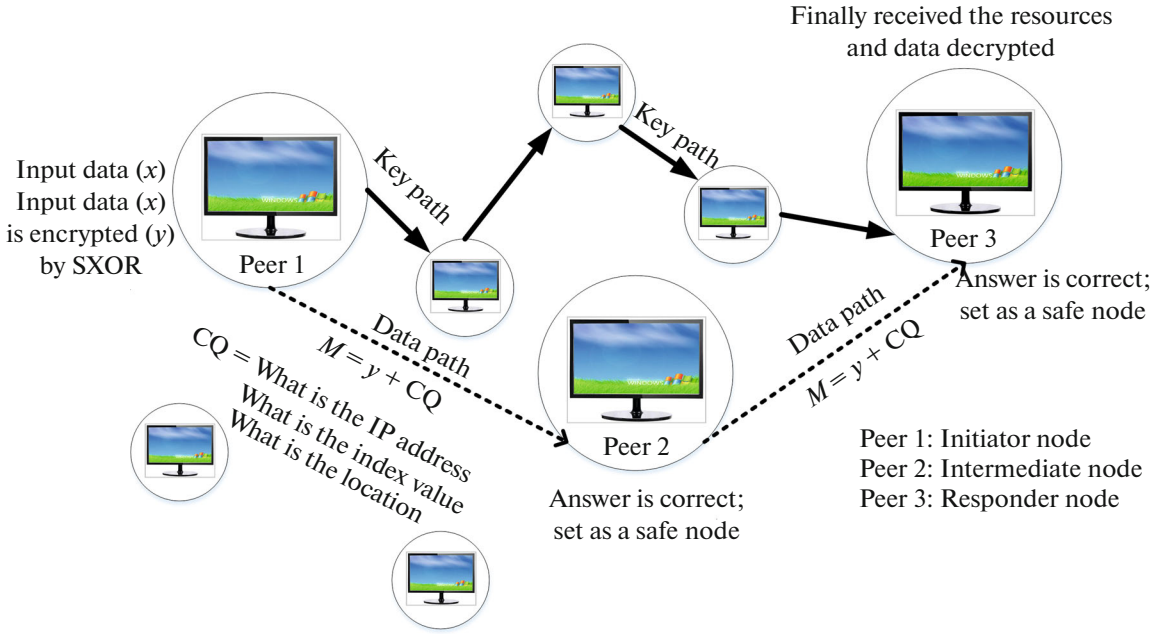

Fig. 3. Process of ERR protocol for P1-P3 transaction.

upload and download resources in the P2P network can be enhanced with the help of the proposed method. The upload and download resources with five peer nodes are illustrated in the Fig. 4.

Step 1: Initialize the five peers in the P2P network and allocate the upload and download resources of each peers at the time T_M.

Step 2: Based on the allocated resources, the share matrix is formed in the P2P network. In the proposed methodology, the share matrix is generated based on the upload and download amount of peers.

Step 3: The share matrix is applied to the equation (5), in the equation E and E_a are taken as the $E = [1\ 0\ 0\ 0\ 0]^T$, $E_a = [1\ 1\ 1\ 1\ 1]$ and $\alpha = 0.9$. At initial BCI of all peers can be taken as $X_a(T_N) = \frac{\alpha}{1-\alpha}$ and $\beta_a(T_N) = 1$. With the computation of the BCI index using the equation (5), we can get the first iteration values of BCI index.

Step 4: The BCI least value is selected to share the resources in the peers. Similarly, the send data's are encrypted for security enhancement. The SXOR operation is used to encrypt the data from the share matrix. For example, only one value encryption and decryption examples are presented in this step. From the share matrix, the $SM_{11} = 10$, the resource 10 is encrypted with the help of the SXOR operation. The process of encryption and decryption is presented in follows,

Input: $SM_{11} = 10$
//* divided in to two parts A and B*//
A= [1010 0000] and B= [1010 0000]
//*Key generation*//
Key= [0000 1110]
//*divided data merged and encrypted data*/
10

Step 5: The encrypted data (y) is added with the challenge question method for identify the attacker peer in the P2P networks which is mentioned as $M = y + CQ$, where C is described as the challenge question. Here three types of questions are framed to identify the attacker in the P2P networks. The questions are presented below,

—What is the IP address?
—What is the success rate?
—What is the location?

In the P2P network, each peer has the different IP address, location and index value. The values of the each peer can be presented in the Table 1.

Step 6: If the peer answer the challenge questions we can take as the safe node. Additionally, the BCI value is checked and low value is motivated to upload the resources. The pseudo code of the proposed method is presented in the below,

Algorithm 1: Pseudo code for BCIRR process

Input: Amount of upload and download of peers
Output: BCI value and attacker node identification
//***Initialization***//
Initiator node
Responder node
Intermediate
Random key
Data path
Key path
Upload data
Download data
Encrypt= SXOR
CQ=Challenge question
//* **BCI- data balancing control***//
for each peer a **do**
for all peer b, who is carefully chosen as source peer do
Download the resource
send the value of resource
end for all
do
upload the resource
send the value of resource
end **for all**

if $t = 0$ then, initial condition start with $X(0) = \frac{\alpha}{1-\alpha} e$
after that, BCI index value is calculated using equation (5)
Low value is selected for uploading resources (data balancing control achieved).
//*** ERR-security enhancement***//
Check the selected peer (attacker or not)
The data is encrypted with SXOR (y)
Added the query message with encrypted data

With the utilization of the BCIRR method, the security and load balancing is achieved in the P2P network. The process of the proposed methods is presented in the above steps. The upload and download resources of P2P network can be transferred without loss, delay and secure manner. The BCI index and ERR is used to enhance the performance of the P2P network which reduce the security problems and balance data sharing problems.

4. EVALUATION OF PROPOSED METHOD

In this evaluation section, the performance of the proposed method is assessed and verify the load balancing control and security enhancement in P2P networks data sharing. The proposed method is implemented in the CPU speed of 2.20 GHz with 8GB of RAM using Matlab platform. To investigation the efficiency of the developed method, comparison analysis is performed in this segment. The projected technique is contrasted by the existing technique of CA algorithm. The performance of the projected scheme is measured with multiple criteria such as delivery ratio, packet loss, Average end to end delay, throughput, encryption time and decryption time. The above mentioned criteria's are contrasted with the

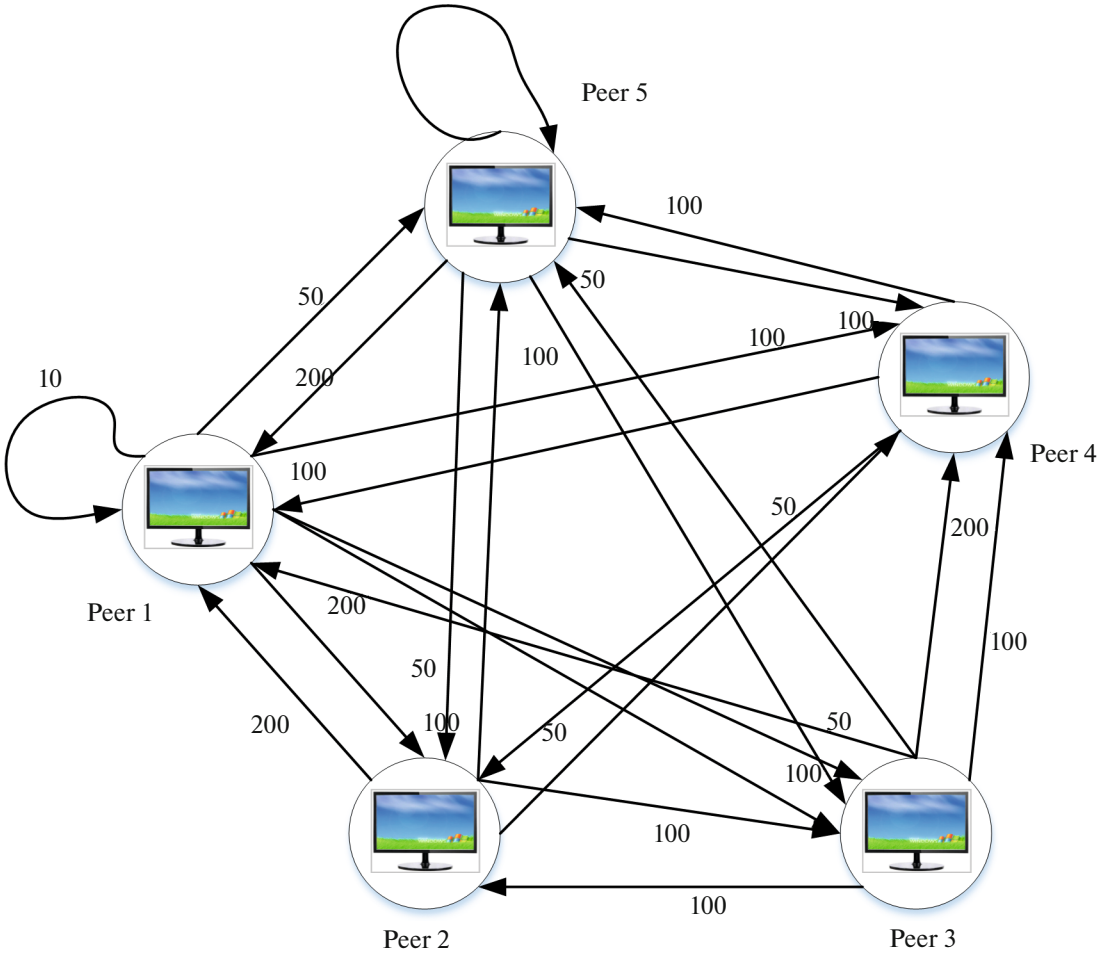

Fig. 4. Upload and download of P2P network.

previous method. The implementation parameters of the projected technique are presented in the Table 2. The initialization of the nodes is illustrated in the Fig. 5.

Here simulated a typical P2P network with parameters and distribution of resources taken as random. In this network load balancing control and security enhancement are considered as the objective function which attained with the help of proposed BCIRR method.

4.1. Performance Analysis

The load balancing control and security enhancement of P2P networks are attained with the help of the proposed BCIRR method. Initially, the nodes are initialized after that, for analysis purpose, one transaction is taken in the account. In the transaction, the security and load balancing control is attained. The load balancing control is attained based on the BCI index value. Based on the previous transactions,

Table 1. Parameters of authentication

S.No/Peer No	IP address	Success rate	Location
1	149.01.13.13	13	497/203
2	180.01.6.10	10	110/225
3	187.08.6.17	17	53/183
4	37.08.6.19	19	55/282
5	27.01.40.14	14	32/314

Table 2. Matlab implementation parameters for BCIRR method

S.No	Description	Value
1	Simulator	Matlab
2	Number of nodes	10
3	Simulation area	500 × 500m
4	Packet size	100–500
5	Node type	Static
6	Time of simulation	100 sec

each node have the different BCI index value. The low BCI index value of peers are motivated to download the resources. So, which peer have the low value of BCI that is chosen for transaction. To enable the secure transaction of resources in the P2P network, the ERR is utilized in the proposed method. The ERR is used for identify the malicious peer in the P2P network. The attacker node can be finding by generate the challenge question to each peer and get answer from that peer which was identified with the help of the reputation table. The challenge question and success rate are important factors for identify the attacker node in the P2P network. To secure the transfer information, the SXOR are initialized. The SXOR operation is used to encrypt the data for avoiding the unauthorized person access the data. And, to ensure the operation the data and keys are transferred with different paths. The decryption and encryption process of the projected technique is presented in Table 3.

Based on the load balancing control and security control of BCIRR method, the key path and data path are illustrated in the Fig. 6. The presentation of the projected technique is analysed through different performance metric like as delivery ratio, packet loss, Average end to end delay, throughput, encryption time and decryption time. The performance metric of the delivery ratio, packet loss, average end to end delay and throughput is used for analysing the proposed method. It can be defined as the time engaged aimed at a packet to be communicated diagonally the network from one pee to another destination peer. The packet loss is derived as the disappointment of solitary or additional communicated packets to send the destination peer from sender. The failure packet data can be considered as the packet loss. Delivery ratio can be derived as the percentage of packets gathered to the over-all sending packet amount. Throughput is a measurement of how many units of packets can be processed in a given amount of time. The computation of performance metrics is presented in the given formula.

$$\mathrm{AED} = \frac{\mathrm{TD}}{\mathrm{PR}} = \frac{\text{Total delivery time}}{\text{Packets received}}, \tag{19}$$

$$\text{packet loss} = \text{Packet received}\,(\mathrm{PR}) - \text{packet send}\,(\mathrm{PS}), \tag{20}$$

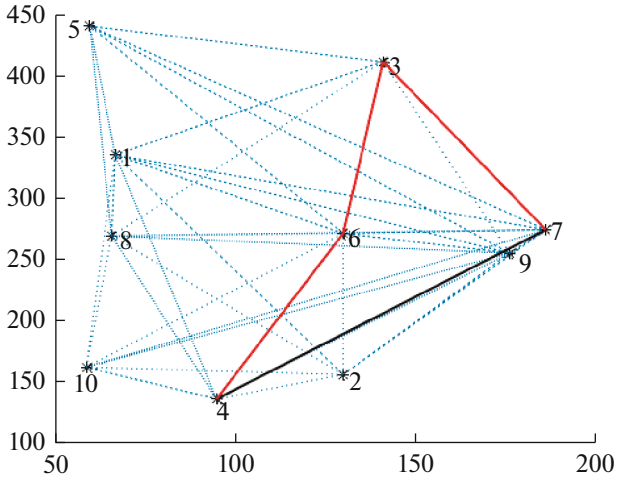

Fig. 5. Initialization of P2P nodes.

Table 3. Process of encryption and decryption in BCIRR

//*Input data of the proposed method in one transaction*//
Input data= [239]
//* input data divided in to two parts such as A and B*//
A = [0 0 0 1 0 0 0 0]
B = [1 1 1 0 0 0 0 0]
//*Key value of the proposed method*//
Key = [0 0 0 0 1 1 1 0]
//* decryption of the proposed method by added two parts*//
Decryption= [239]

$$\text{Delivery ratio}DR = \frac{PR}{PS} \times 100\% = \frac{\text{Packet ratio}}{\text{packet send}} \times 100\%, \tag{21}$$

$$\text{Throughput} = \frac{PR}{SE} \times SZ = \frac{\text{Packet received}}{\text{Simulation end time}} \times \text{packet size}. \tag{22}$$

Based on the performance metric calculation, the proposed method of BCIRR is analysed which illustrated in the Fig. 7. The encryption and decryption time of the projected technique is illustrated in the Fig. 8.

The proposed method is analysed with the performance metric of average end to end delay and it have the minimum and maximum limits. The minimum delay of the projected technique is 1.5; similarly, the maximum delay of the projected technique is 5.8; with the utilization of the BCIRR method, the delay of the projected technique is reduced and load balancing and security enhancement is attained in the P2P networks. The packet loss of the projected technique is computed established on the mentioned formula. The minimum packet loss of the projected technique is 0.35 at 6ms and maximum packet loss of the projected technique is 7 at 5 milliseconds. The throughput of the proposed method minimum and maximum value is 0.13 at 6 ms and 4.6 at 28 ms. The delivery ratio of the proposed method minimum and maximum value is 94 at 5 ms and 100 at 2 ms. The proposed method encryption and decryption time is presented in Fig. 8, which consume less amount of time for securing data for transaction. The proposed method performance metrics are analysed in the section. The proposed method efficiency is analysed by the comparison method which presented in the below section.

4.2. Comparison Analysis

The proposed technique is contrasted with the previous methods of CA for analysis the performance. The performance of proposed method obtained by different parameters is shown in the terms of delivery ratio, packet loss, average end to end delay and throughput. The variance among the minimum in addition maximum values of performance parameters in proposed and existing methods are decided the perfor-

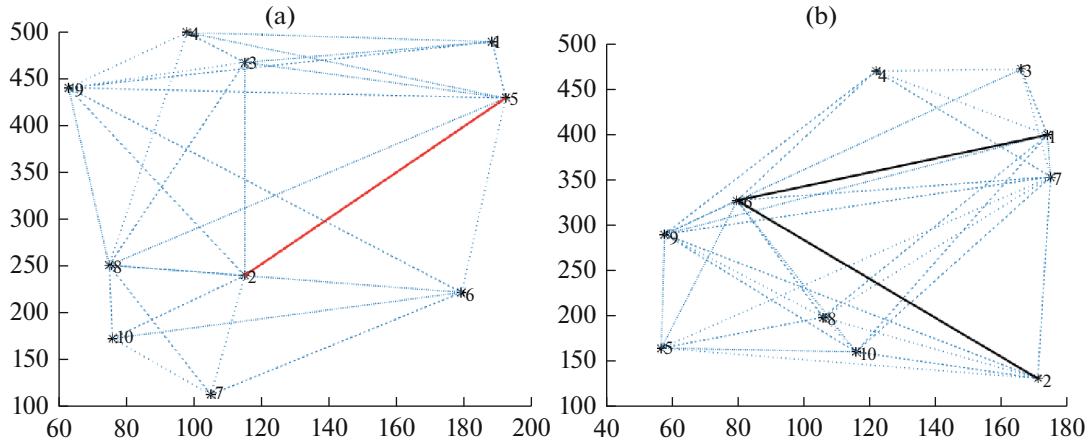

Fig. 6. Analysis of (a) data path and (b) key path.

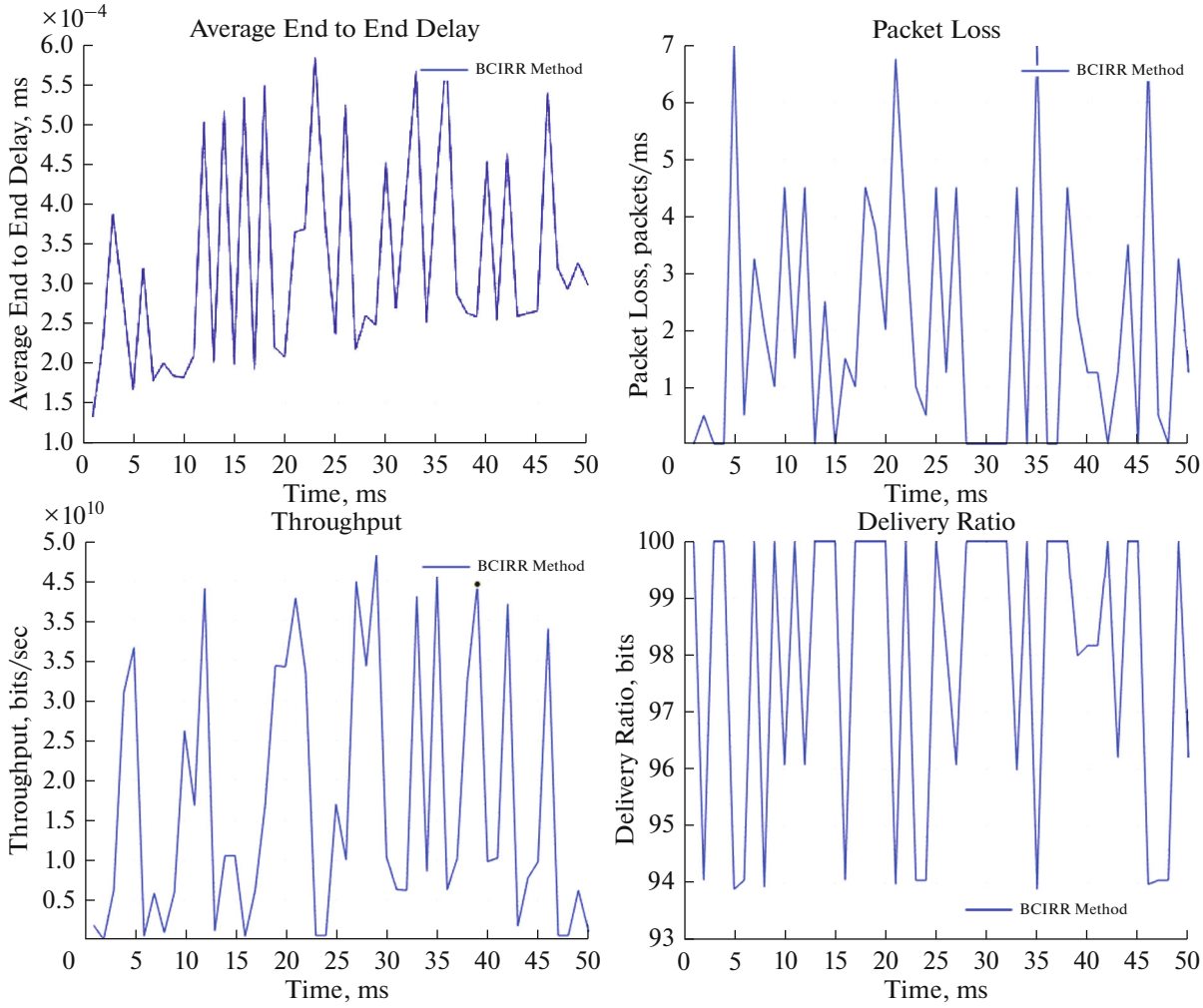

Fig. 7. Analysis of proposed method (a) Average end to end delay (b) packet loss (c) throughput and (d) Delivery ratio.

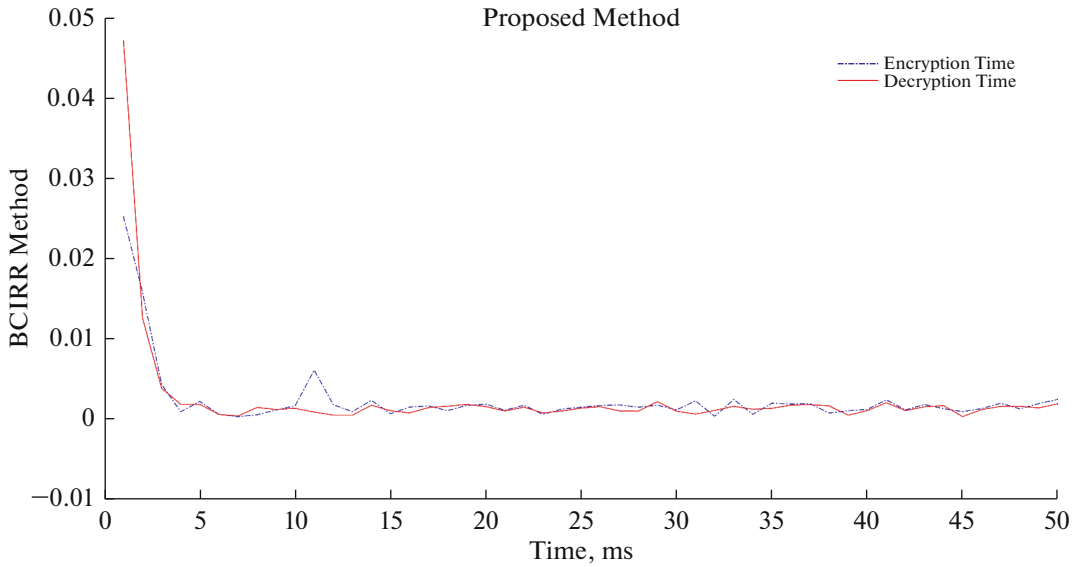

Fig. 8. Analysis of proposed method decryption time and Encryption time.

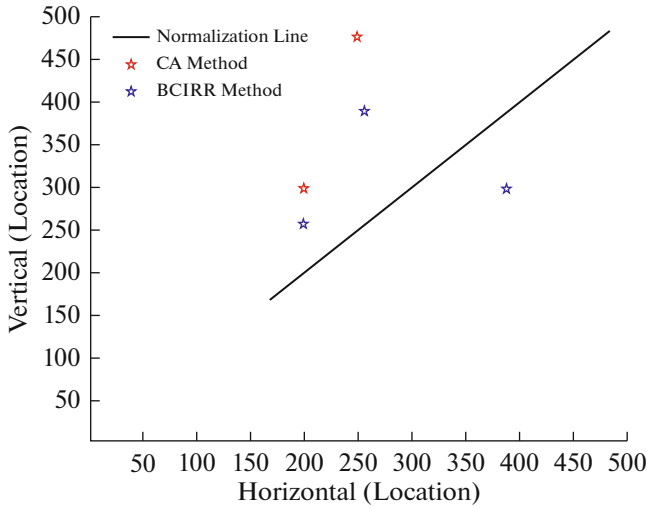

Fig. 9. Comparison analysis of Location of the peers.

mance of the proposed system. In the computation process, the one method has the maximum value, another method has the lower value. Then the performance is computed based on the minimum value. In terms of delivery ratio, packet loss, average end to end delay, and throughput, the proposed technique should have the minimum value under the different method. Based on the computation which one have the lowest values of performance parameters, which is taken as the efficient method. The delivery ratio, packet loss, average end to end delay, and throughput comparison analysis is presented in the Fig. 10. Additionally, the location of the peers of the projected and previous technique is demonstrated in the Fig. 9.

Figure 9 describes the location of the peers (nodes) in the proposed method and existing method of CA. In the figure, the location of the node is analysed with the normalization line. The proposed method peer location is denoted as the blue colour and CA method is denoted as the red colour. Figure 10, end to end delay, packet loss, delivery ratio and throughput comparison analysis is illustrated. In Fig. 10a describes the packet loss values of proposed and existing methods. From the figure, the proposed method have the packet loss values is 2.00; the CA have the packet loss values are 9.2231. From the analysis, the proposed method has the low packet loss value compared with the CA methods. In Fig. 10b describes the end to end delay standards of proposed in addition existing methods. From the figure, the proposed technique has delay values is 1.0735; the CA have the delay standards are 2.512. From the analysis, the proposed technique has the low value of end to end delay compared with the CA methods. In Fig. 10c describes the delivery ratio values of proposed and existing methods.

From the figure, the proposed method has the delivery ratio values is 100 percentages; the CA have the delivery ratio values are 90 percentages. From the analysis, the proposed method has the high delivery ratio value compared with the CA methods. In Fig. 10d describes the throughput values of proposed and existing methods. From the figure, the proposed method has the throughput values is 2.578; the CA have the throughput values are 2.180. From the analysis, the proposed method has the throughput value compared with the CA methods. Similarly, the decryption time in addition encryption time, the proposed technique have the low values contrasted with the existing techniques such CA. Based on the comparison analysis, we can concluded, the proposed technique is delivers the optimal solutions with efficiently.

5. CONCLUSIONS

The proposed method is developed a BCIRR protocol toward make P2P network fair and efficient by load balancing control and security enhancement. The proposed method, BCI was used to balance the load in between the P2P networks and ERR was used to enhance the security control by SXOR and challenge question. The BCI was vary from 0 to 1. The computation of BCI was based on two factors such as resources contributed by the peer and BCI of peer with whom it is transacting. To achieve the load balancing control in P2P networks, some design rules were make and justified. The ERR method consists of SXOR operation and challenge question for enhancing the security. The method was used to find the attacker node in P2P networks. With the utilization of the mathematical justification, the proposed method can fulfil the load balancing control and security enhancement of the P2P networks. The pro-

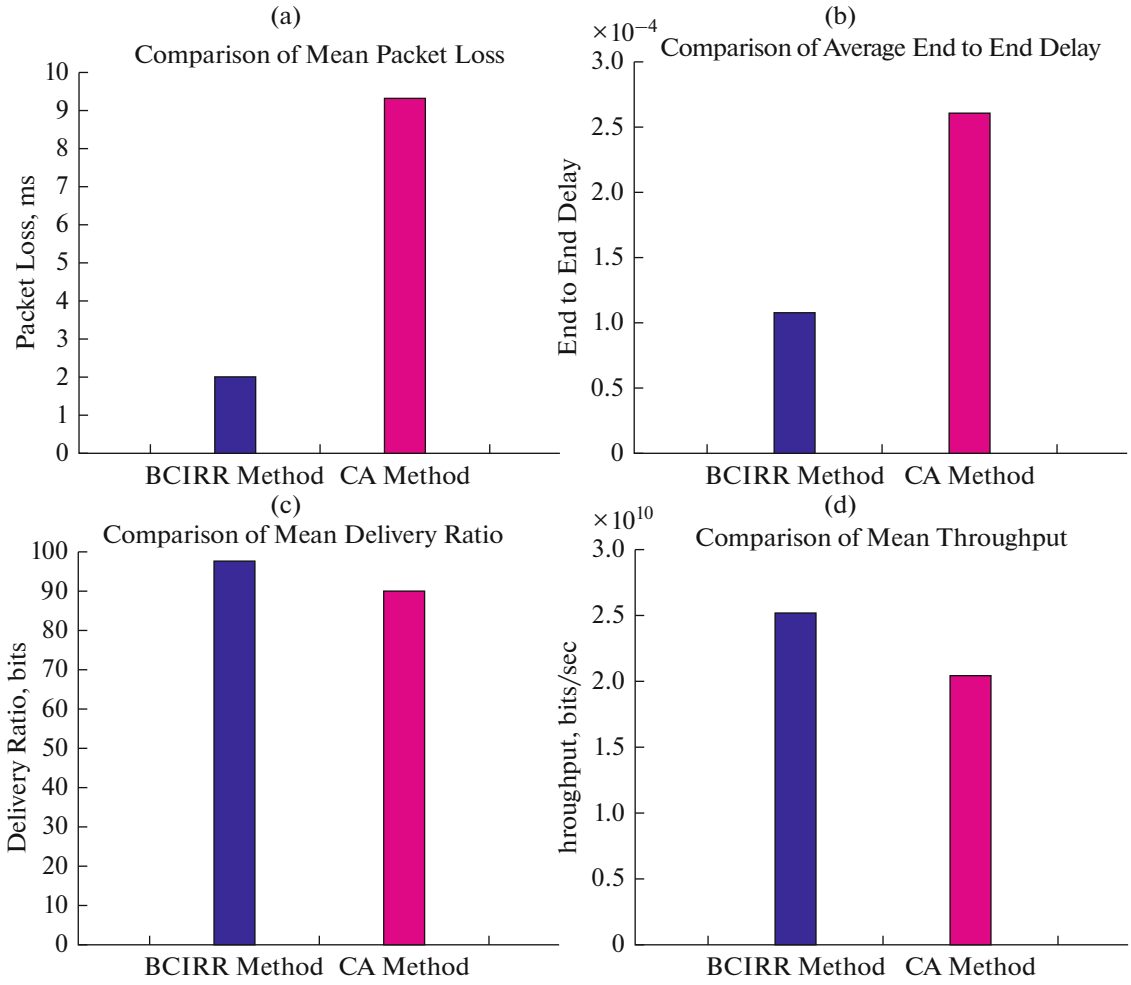

Fig. 10. Comparison analysis of proposed method (a) packet loss (b) end to end delay, (c) delivery ratio and (d) throughput.

posed method was implemented and analysis with different performance metric such as packet loss, throughput, average end to end delay in addition delivery ratio. The proposed technique provides the best solution for solving load balancing and security in the P2P networks which was proved by performance analysis and comparison analysis.

COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of potential conflicts of interest: There is no potential of conflict of Interest between the authors regarding the manuscript preparation and submission.

Research involving human participants and/or animals: There is no involvement of human participants or animals used in this manuscript.

Informed consent: There is nothing to report.

REFERENCES

1. Mocanu, B., Pop, F., Mihaita, A., Dobre, C., and Castiglione, A., Data fusion technique in spider peer-to-peer networks in smart cities for security enhancements, *Int. J. Inf. Sci.*, 2019, vol. 479, pp. 607–621.
2. Dorfleitner, G., Priberny, C., Schuster, Stoiber, J., Weber, M., Castro, I.D., and Kammler, J., Description-text related soft information in peer-to-peer lending–Evidence from two leading European platforms, *Int. J. Banking Finance*, 2016, vol. 64, pp. 169–187.

3. Zhi, Li, Barenji, A.V., and Huang, G.Q., Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform, *Int. J. Rob. Comput.-Integr. Manuf.*, 2018, vol. 54, pp. 133–144.

4. Yaodong, Huang, Song, X., Ye, F., Yang, Y., and Li, X., Fair and efficient caching algorithms and strategies for peer data sharing in pervasive edge computing environments, *IEEE Trans. Mobile Comput.,* 2020, vol. 19, no. 4.

5. Ravichandran, C.G. and Xavier, J.L., Highly available hypercube tokenized sequential matrix partitioned data sharing in Large P2P Networks, *Int. J. Circuits Syst.*, 2016, vol. 7, no. 09.

6. Horacio, Paggi, Soriano, J., and Lara, J.A., A multi-agent system for minimizing information indeterminacy within information fusion scenarios in peer-to-peer networks with limited resources, *Int. J. Inf. Sci.*, 2018, vol. 451, pp. 271–294.

7. Horacio, Paggi, Lara, J.A., and Soriano, J., Structures generated in a multiagent system performing information fusion in peer-to-peer resource-constrained networks, *Int. J. Neural Comput. Appl.*, 2018, pp. 1–19.

8. Ramkumar, V., Secure Data Sharing in Peer to Peer Network Using Replication and DHT Algorithm, *Int. J. Innovative Res. Comput. Commun. Eng.*, 2016, vol. 4, no. 3.

9. Poenaru, A., Istrate, R., and Pop, F., AFT: Adaptive and fault tolerant peer-to-peer overlay—A user-centric solution for data sharing, *Int. J. Future Gener. Comput. Syst.*, 2018, vol. 80, pp. 583–595.

10. Balu Deokate, Lal, C., Trcek, D., and Conti, M., Mobility-aware cross-layer routing for peer-to-peer networks, *Int. J. Comput. Electr. Eng.*, 2019, vol. 73, pp. 209–226.

11. Moufida, Rahmani and Benchaïba, M., PCSM: an efficient multihop proximity aware clustering scheme for mobile peer-to-peer systems, *Int. J. Ambient Intell. Humanized Comput.*, 2018, pp. 1–18.

12. Abhinav, Jain and Kumar, S., Friend Share: A secure and reliable framework for file sharing on network, *Int. J. Network Comput. Appl.*, 2018, vol. 120, pp. 1–16.

13. Jianwei, Zhang, Zhang, X., Sun, M., and Yang, C., Maximizing streaming efficiency of multiple streams in peer-to-peer networks, *Int. J. Network Comput. Appl.*, 2018, vol. 124, pp. 108–120.

14. Thiyagarajan R. and Priya, B.M., An enhancement of EAACK using P2P ACK and RSA public key cryptography, *Int. J. Measurement*, 2019, vol. 136, pp. 116–121.

15. Amna, Qureshi, Megias, D., and Rifa-Pous, H., Framework for preserving security and privacy in peer-to-peer content distribution systems, *Int. J. Expert Syst. Appl.*, 2015, vol. 42, no. 3, pp. 1391–1408.

16. Imran, Memon, I., Hussain, Akhtar, R., and Chen, G., Enhanced privacy and authentication: An efficient and secure anonymous communication for location-based service using asymmetric cryptography scheme, *Int. J. Wireless Pers. Commun.*, 2015, vol. 84, no. 2, pp. 1487–1508.

17. Farash, M.S., Security analysis and enhancements of an improved authentication for session initiation protocol with provable security, *Int. J. Peer-to-Peer Networking Appl.*, 2016, vol. 9, no. 1, pp. 82–91.

18. Awasthi, K.S. and Singh, Y.N., Biased Contribution Index: A Simpler Mechanism to Maintain Fairness in *Peer to Peer Network,* arXiv:1606.00717, 2016.

19. Kumar, S.A. and Singh, Y.N., Simplified Biased Contribution Index (SBCI): A mechanism to make P2P network fair and efficient for resource sharing, *Int. J. Parallel Distrib. Comput.*, 2019, vol. 124, pp. 106–118.

20. Awasthi, S.K. and Singh, Y.N., Biased contribution index: a new faster convergent index to maintain the fairness in peer-to-peer networks, *Electron. Lett.*, 2018, vol. 54, no. 20, pp. 1174–1176.

21. Christo, M.S. and Meenakshi, S., Enhancing Rumour Riding protocol in P2P network with Cryptographic puzzle through challenge question method, *Int. J. Comput. Electr. Eng.,* 2018, no. 65, pp. 122–138.

22. Ruchir, Gupta and Singh, Y.N., Reputation aggregation in peer-to-peer network using differential gossip algorithm, *IEEE Trans. Knowledge Data Eng.*, 2015, vol. 27, no. 10, pp. 2812–2823.

23. Karthiga, R.R. and Aravindhan, K., Enhancing performance of user authentication protocol with resist to password reuse attacks, *Int. J. Comput. Eng. Res.*, 2012, vol. 2, no. 8, pp. 106–115.

24. Yibin, Li, K., Gai, Qiu, L., Qiu, M., and Zhao, H., Intelligent cryptography approach for secure distributed big data storage in cloud computing, *Int. J. Inf. Sci.*, 2017, vol. 387, pp. 103–115.

25. Wen, M., Lu, R., Lei, J., Li, H., Liang, X., and Shen, X., SESA: An efficient searchable encryption scheme for auction in emerging smart grid marketing, *Int. J. Secur. Commun. Networks*, 2014, vol. 7, no. 1, pp. 234–244.