International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Distributed Hashing Based Group Management Scheme for the Peer-to-Peer Trust Model

Prasida Sunanda[1], K.A. Janardhanan[2], Mr. Rajesh Gupta[3], Hendy Tannady[4], Dr. Navin Kumar Shrivastava[5], Dr. Tarun K. Sharma[6]

Submitted: 02/11/2022 **Revised**: 11/01/2023 **Accepted**: 01/02/2023

Abstract: In recent days, computing and communication environments are extensively more difficult and disorganized than classically distributed systems over the internet, lacking any centralized organization or hierarchical control. In such case the emerging technology peer to peer overlay network is the answerable one. The peer to peer networks will provide a good layer for creating a data sharing, content delivery and optimal routing in many applications. Structured peer to peer network has a fixed structure that will be formed as a fixed topology. If any one of the nodes leaves or enters in the network, topology may vary. In such case, it will lead to load failure, link failure and resilience. a new architecture namely Distributed Hashing distributed grouping management (DHDGM) is proposed. The proposed DHDGM model uses the secure group architecture model those are processed vertically for the selection of group header. The resures are shared between the group headers for the detection of the intruders. With the distributed grop management of the data between the network group data is transmitted in the P2P network. The simulation analysis of the proposed DHDGM model exhibist the ~4% - 7% reduced delay and packet drop rate compared with the existing ATAR and RSPP model.

Keywords*: Peer-to-peer Network (P2P), Distributed management, Trust scheme, secure group, Intruders.*

1. Introduction

With the overlay existing network, the underlying features are computed based on the data forwarding and routing. The nodes in the network are connected with the overlay virtual logical links related to the underlying network path [1]. Peer to peer (P2P) features are computed with the overlay network for the internet connection. Peer-to-Peer networks (P2P) are the file swapping networks for supporting the distributed content sharing. The file sharing is considered to be an important goal in P2P networks, which is developed and deployed [2]. The working group gave the definition for P2P systems as “The sharing of resources and services of computers by directly exchanging among the systems”. The P2P networks have two main key characteristics of scalability and reliability.

Peer-to-Peer (P2P) networks are the self-organizing networks, which acts either as the client or the server at any particular time. The main aim of the P2P network is to collect and distribute the resources among several servers and clients [3]. File sharing is considered to be an important issue among the Peer nodes. The trust management approaches and the Data Integrity approaches are used for securing the files by encrypting the files using the AES encryption algorithms. The Peer selection strategies are used for selecting the peers optimal from the set of peers. The files are shared among the peer nodes by efficiently encrypting using the encryption algorithms [4]. The files shared using some other networks are not effective so, the Peer-to-Peer networks are used for sharing the files among the peers.

The malicious node effects are evaluated with the introduced mitigation scheme for the trust overlay. The different processing in P2P are presented as follows [5]:

1. Assignment of the certificates for the authority those are external to drawbacks associated with the centralized elements in the network.
2. Using peers sign reciprocal values the Pretty Good Privacy (PGP) values are estimated based on the

[1] *Research Scholar, Management Studies, NICHE, Noorul Islam Centre for Higher Education, Thucklay.*
prasidasunandas@gmail.com
0000-0001-9243-4284
[2] *Professor, Management Studies, NICHE, Noorul Islam Centre for Higher Education, Thucklay.*
*kajanardhanan@****yahoo****.com*
0000-0001-5188-6903
[3] *Pro Chancellor, Department of Management, Sanskriti University, Mathura, Uttar Pradesh, India.*
prochancellor@sanskriti.edu.in
0000-0002-2118-8474
[4] *Faculty of Business, Department of Management, Universitas Multimedia Nusantara, Banten.*
hendy.tannady@umn.ac.id
0000-0001-6911-7010
[5] *Associate Professor, Birla Institute of Management Technology, Greater Noida, India.*
n.shrivastava@bimtech.ac.in
0000-0003-2845-9115
[6] *Professor & Dean, Department of Computer Science, Shobhit Institute of Engineering & Technology (Deemed to-be University), Meerut, Uttar Pradesh, India.*
tarun.sharma@shobhituniversity.ac.in
0000-0002-9043-8641

features for the trust model in the peer certificates. However, the theoretical features are evaluated with the extreme features those are significant for the trust scheme.

The P2P network trust model classifies the different models such as identity and behaviour trust model. The identity trust model uses the identity authentication scheme for the charges in the encryption of the user rights, digital signature and authentication [6]. The network security features are evaluated with the authentication mechanism such as certificate for electronic process and biometry. The cryptography scheme is evaluated based on the electronic authentication scheme for archieving the electronic data. The behaviour trust model uses the malicious peers for the different research concern. The trust behaviour considers the trust problem associated with the significance of the P2P network features [7]. To improve the peer-to-peer communication between the groups Distributed Hashing distributed grouping management (DHDGM) is propsoed. The developed model involved in reduced delay and packet drop rate.

2. Related Works

In [8] discussed about topology mismatch problem in structured and unstructured P2P overlay networks. To reduce the cost of traversing a path in the network, one has to adopt a perfect topology which became a best fit for underlying network. Finally, the author concluded that the criteria used for comparison are efficiency, overhead and scalability in which none of the proposed solutions is superior to the others on all three aspects.

In [9] proposed a new trust model to avoid the issues which are occurring in the rough and simplistic trust models. A service is requested by the requester as a broadcasting message in the network and it will wait to receive the responses. After the requester receiving the responses from several responders, the receiver has to select a trusted one. In such case, the receiver has to calculate its expectation vector and each responders trust vector in order to choose a trusted one. After the service, the requester updates the recommenders recommending reliability, which will be used for the future transactions.

In [10] proposed the microblogging network architecture with three different networks. The first network is used to authenticate the users, second network is used to storing and assigning key for the users and the third network is used to disjoint the affected nodes using the bit tolerant protocol.

In [11] suggested fuzzy type 2 logic framework for P2P networks. A trust value is computed based on the previous transaction of the individual peers with their counterpart. Also, the trust value received from other peers in the network will be used to compute the reputation of the individual peers. The proposed system achieves a high level of accuracy in detecting the malicious nodes in the network.

In [12] suggested the artificial neural network which is used to predict the location of the mobile peers in the P2P network. The Geographic routing protocols are typically light weighted and require only local network knowledge to make the routing decisions. But it is not providing more resistant to the vulnerability effect of the mobile nodes. In such cases, the proposed system uses an artificial neural network to perform the location prediction in the network.

In [13] explained about the Distributed Spatial Data Structure (DSDS) for P2P network. The DSDS is implemented using non redundant Rainbow Skip graph. This graph can be used by DSDS in order to coordinate the transmission of information between the nodes. The distributed model aims to provide the increased reliability, flexibility and robustness to data structure. A failure method has also been introduced in order to serve the queries even when a node in the network fails. The proposed method requires only fewer messages to answer the queries compared to its existing system.

3. Overlaying Strategy with the Distributed Hashing distributed grouping management (DHDGM)

With the proposed DHDGM comprised of the Internet-Autonomous System (AS), the peers in the network are divided into many groups. The single administrative authority in AS topologies decides the border between the peers. The Distributed Hash Table (DHT) maintenance and the similar ID mechanism are applied to generate the overlay models. The two-level mapping mechanism is such that the participated peers are overlaid into groups in one level and teams in another level. The variations of the nodes within the team govern the physical clustering activity and hence the stabilization improvement. Each team comprises a Ꜧ◌̇Ꜧ number of nodes and the node with the high bandwidth and availability is selected as the leader. The proposed DHDGM model uses the unique ID-generation through MAC depends on the length of bits. The first 16-bit represents the group ID and the next 16-bit denotes the team ID. The object generated during the communication process is stored in the team. In general, the team includes two copies of objects as follows:

Condition I: The header file uses the response obtained through the queries from the peers

Condition II: The group members comprises of the peer copy II those are splitted based on the coding techniques.

In the figure 1 the simulated P2P network topology for the network are presented.

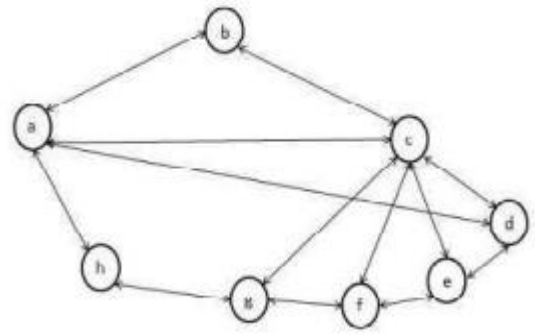

Fig. 1: General Topology

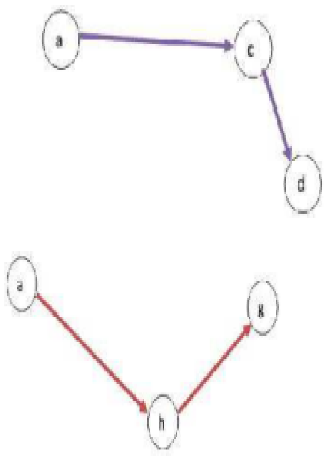

Fig. 2: Data transmission between nodes a to d and a to r

The proposed DHDGM uses the data transmission path between the path those are estimated based on the feature vector. The proposed scheme uses the trust model for the estimation of the features.

3.1 Trust Metrics for DHDGM

The trust management unit is responsible for the peer networks to perform the secured data transfer. The trust ratings depend on the past transactions and the neighbor recommendations. The detailed description of trust metrics and their influence on secured P2P network creation are described as follows:

3.1.1 Service trust metrics

The computation of competence and integrity belief functions is the initial stage of the service trust metric computation. The acquaintance satisfaction level and the average value of past interactions govern the competence belief estimation. The peer t_i calculates the competence belief function by using the equation (1)

$$st_{ij} = \frac{1}{\beta_{cb}} \sum_{k=1}^{ct_{ij}} \left(a_{ij}^{k}.b_{ij}^{k}.c_{ij}^{k}\right) \qquad (1)$$

In the above eqution (1), the Normalized coefficient is defiend as β_{cb}; a_{ij}^{k} -satisfaction level; b_{ij}^{k} – weights in the relay and c_{ij}^{k} – fading values

The integrity belief defines the deviation from the average behavior. The standard deviation formulation of the integrity belief function is mathematically expressed as in equation (2)

$$at_{ij} = \sqrt{\frac{1}{st_{ij}} \sum_{k=1}^{ct_{ij}} \left(a_{ij}^{k}.b_{ij}^{k}.c_{ij}^{k} - m_{ij}\right)^{2}}$$

(2)

The fading effect and the weight parameters are independent and they are eliminated for service trust metric computation since it depends on the transaction size as follows:

3.1.2 Lower Transactions

The lower estimate value of peer t_i assures more confidence level$t_i$about . The service trust metric for lower transactions is mathematically expressed as follows in equation (3)

$$bt_{ij} = st_{ij} - at_{ij}/2$$

(3)

Large Transactions

The more transaction size increases the importance level of the integrity belief gain value is given in equation (4)

$$ct_{ij} = \frac{nt_{ij}}{gt_{max}}\left(st_{ij} - \frac{at_{ij}}{2}\right) + (1 - \frac{nt_{ij}}{gt_{max}})g_{ij}$$

(4)

In the above equation (4) the reputation trust metrics are stated as g_{ij}. If the peer is a stranger, then the value of $nt_{ij}$is zero and hence the service trust metric depends on the reputation trust metric. Alternatively, if the peer has more transactions, then the $\frac{nt_{ij}}{gt_{max}}$ equation defines that the reputation metric has no effect on service trust metric.

3.1.3 Reputation trust metric

After all the recommendations are collected by the peer t_i , The estimation of reputation of peer is defined by equation (5)

$$rt_{ij} = \frac{1}{\beta_{cb}} \sum_{tk \in r} ij_{ik}, jk_{ik}, rj_{jk}$$

(5)

In the above equation (5) the variables considered are jk_{ik} stated as the Reputation trust metric and rj_{jk} stated as the recommendation count.

3.2 Secure Group Management with the DHDGM

Based on the requirements, number of peers in P2P overlay network will vary. Further, number of nodes will be divided in to sub groups and are indicated as identifiers. Moreover, each sub group will create its own group head and all the group heads are interconnected. The groups separated into equal column consist of some limited nodes and that nodes will further create a group. Group node is elected as Group Head (GH), if the distance between group node and its neighbouring group node will be nearer and common to both sides of the group. DHDGM structure.

3.2.1 Group Selection

DHDGM is portioned into vertical columns in such a way that each column contains some nodes as its member. The overall network is considered as a connected graph $G = (V, E)$, and the columns denoted as group1, group2 and group3 are considered to be the subgroups as presented in equation (6) and (7)

$$G(V') = G(V, E) - \sum_{i=E}^{N}\{v_i\} \quad (6)$$

$$G(V'') = G(V, E) - \sum_{i=A}^{N}\{v_i\} - \sum_{ii=j}^{N}\{v_i\} \quad (7)$$

In other words, subgroup will be formed by removing some vertices (nodes) from overall group . Subgroup will be formed by removing the vertices from as well as from . Similarly, subgroup will be formed by removing some vertices in and so on. Groups in the overlay can be constructed as stated in the above equations. The algorithm for the proposed DHDGM model is presented as follwos:

Algorithm 1: DHDGM for the computation of the network assignment

```
Select the group features
    Assign the group members $GM = GM1, GM2 \dots\dots$
Assign the group member features as Gm
Group member transmit request as { Gmi} // i=1,2..n
 Acknowledge the group members in the network
Check entity for the GM
if
      entity <=1
Eliminates the intruders
else
Affects the intruders
Discard GM
```

With the group head selection scheme the groups are identified with the group members. The transmission is evaluated based on the group head based on the message request for the members. The members in the group are requested based on the entity features. The value of the entity is higher in intruders are not affected for the data. The intruders higher than one are affected for the data group head based on the members.

4. Results and Discussion

Distributed Hashing distributed grouping management (DHDGM) features are evaluated based on the consideration of the simulation settings. Simulation results are examined with the proposed DHDGM model for the varying different size of data. The performance of the proposed DHDGM model the features are estimated for the Gs= 5, 10, and 20. In table 1 the group members for the every group are increased with the node number as with the size in group. With the increase in group size the each members in the network are reduced.

Table 1: Group Members in the P2P

Number of nodes	**Gs=5**	**Gs=10**	**Gs=20**
100	30 to 40	5 to 10	3 to 5
200	50 to 60	15 to 20	8 to 11
300	70 to 80	25 to 30	12 to 15
400	90 to 100	35 to 40	16 to 19
500	100 to 110	45 to 50	20 to 25

In table 2 the overhead ration for the P2P network with the trust model is presented based the distributed group assignment. The performance of the propsoed DHDGM model is evaluated for the increases in size of nodes. In figure 2 the comparative analysis of the overhead values is presented for the ration of number of control packets to th total received data packets.

Table 2: Comparative analysis of Overhead Ratio

Number of nodes	**ATAR**	**RSPP**	**DHDGM Gs=5**	**DHDGM Gs=10**	**DHDGM Gs=20**
50	0.703	0.607	0.335	0.349	0.2
150	0.826	0.801932	0.407	0.316	0.392
250	0.726	0.703	0.495	0.302	0.301
350	0.875	0.804	0.309	0.395	0.392
450	0.892	0.857	0.484	0.302	0.229

In figure 2 the overhead ratio of the proposed DHDGM model for the varying number of nodes are presented.

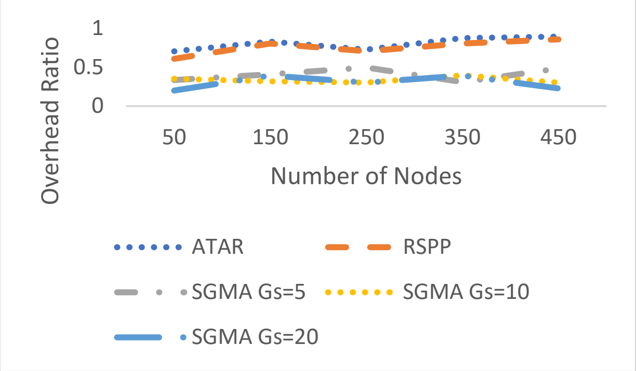

Fig. 2: Comparison of Overhead Ratio

The performance of the proposed DHDGM model is comparatively examined with the existing Adaptive Trusted Authorization and Request (ATAR) and Resource Sharing in P2P network (RSPP) is examined. The comparative analysis expressed that proposed DHDGM model exhibist the higher performance than the existing ATAR and RSSP model. The proposed DHDGM model exhibits the reduced overhead value. In table 3 the delay of the proposed DHDGM model and conventional techniques are examined.

Table 3: Comparison of Delay

Number of nodes	ATAR	RSPP	DHDGM Gs=5	DHDGM Gs=10	DHDGM Gs=20
50	0.5	0.40	0.2	0.17	0.11
150	0.63	0.47	0.25	0.20	0.14
250	0.64	0.59	0.23	0.35	0.23
350	0.79	0.71	0.35	0.34	0.25
450	0.87	0.79	0.48	0.39	0.26

In figure 3 the proposed DHDGM model characteristics for the varying number of nodes are presented. The proposed model exhibits the existing ATAR and RSPP model achieves the higher delay and the proposed DHDGm model achieves the minimal delay .

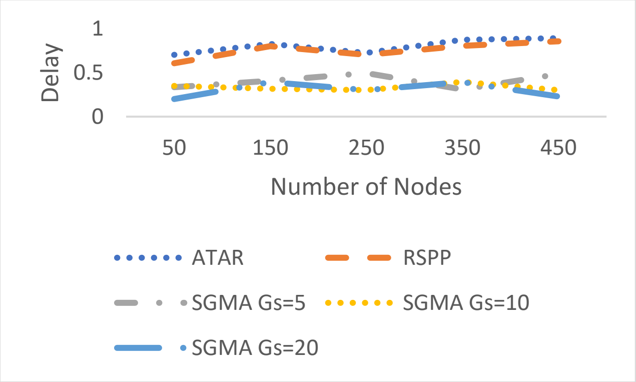

Fig. 3: Comparison of Delay

The packet drop rate measured for the varying number of nodes from 50 to 450 is estimated based on the table 4.

Table 4: Comparison of Packet Drop

Number of nodes	ATAR	RSPP	DHDGM Gs=5	DHDGM Gs=10	DHDGM Gs=20
50	0.48	0.44	0.29	0.22	0.26
150	0.44	0.47	0.32	0.23	0.25
250	0.51	0.48	0.35	0.31	0.28
350	0.60	0.55	0.38	0.36	0.38
450	0.8	0.77	0.44	0.47	0.34

THe figreu 4 provides the comparative analysis of the proposed DHDGM model with the existing model is presented.

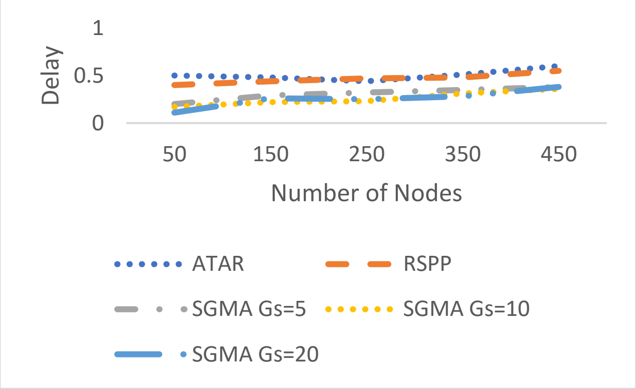

Fig. 4: Comparison of Packet Drop

The performance of the proposed DHDGM model for the varying number of nodes for the different nodes are considered. The performance of the proposed model exhibited that proposed DHDGM model achieves the minimal packet drop rate compared with the conventional ATAR and RSPP model.

5. Conclusion

With the P2P overlay network the proposed Distributed Hashing distributed grouping management (DHDGM) scheme shares the resources between the peer groups. The proposed DHDGM model classifies the network vertically to form a group. Every node in the group comprises of the head for the group members those are assigned internally for the assigned group. The proposed distributed group manages the intruders for the entity level for the examination of the different groups for the size. The simulation resulst expressed that proposed DHDGM model achieves the ~4% - 7% reduced dealy and packet drop rate.

References:

Wippold, G. M., Frary, S. G., Abshire, D., & Wilson, D. K.

(2021). Peer-to-peer health promotion interventions among African American men: a scoping review protocol. *Systematic reviews*, *10*(1), 1-6.

Al-Rakhami, M. S., & Al-Mashari, M. (2021). A blockchain-based trust model for the internet of things supply chain management. *Sensors*, *21*(5), 1759.

Gupta, R., Singh, Y. N., & Goswami, A. (2021). Trust estimation in peer-to-peer network using BLUE. *Peer-to-Peer Networking and Applications*, *14*(2), 888-897.

Esmat, A., de Vos, M., Ghiassi-Farrokhfal, Y., Palensky, P., & Epema, D. (2021). A novel decentralized platform for peer-to-peer energy trading market with blockchain technology. *Applied Energy*, *282*, 116123.

Khan, P. W., & Byun, Y. C. (2021). Blockchain-based peer-to-peer energy trading and charging payment system for electric vehicles. *Sustainability*, *13*(14), 7962.

Munoz, P., Pérez-Vereda, A., Moreno, N., Troya, J., & Vallecillo, A. (2021, October). Incorporating Trust into Collaborative Social Computing Applications. In *2021 IEEE 25th International Enterprise Distributed Object Computing Conference (EDOC)* (pp. 21-30). IEEE.

Tennakoon, P., Karunathilaka, S., Lavakumar, R., & Alawatugoda, J. (2021). Anonymous and Distributed Authentication for Peer-to-Peer Networks. *Cryptology ePrint Archive*.

Hasan, I., He, Q., & Lu, H. (2022). Social capital, trusting, and trustworthiness: Evidence from peer-to-peer lending. *Journal of Financial and Quantitative Analysis*, *57*(4), 1409-1453.

Verma, R., & Chandra, S. (2021). A systematic survey on fog steered IoT: Architecture, prevalent threats and trust models. *International Journal of Wireless Information Networks*, *28*(1), 116-133.

Verma, M. (2021). Smart contract model for trust based agriculture using blockchain technology. *International journal of research and analytical reviews*, *8*(2), 354-355.

Vatankhah Barenji, R. (2022). A blockchain technology based trust system for cloud manufacturing. *Journal of Intelligent Manufacturing*, *33*(5), 1451-1465.

Jiao, R., Przepiorka, W., & Buskens, V. (2021). Reputation effects in peer-to-peer online markets: A meta-analysis∗. *Social Science Research*, *95*, 102522.

Mohamed, M. A., Hajjiah, A., Alnowibet, K. A., Alrasheedi, A. F., Awwad, E. M., & Muyeen, S. M. (2021). A secured advanced management architecture in peer-to-peer energy trading for multi-microgrid in the stochastic environment. *IEEE access*, *9*, 92083-92100.

Soto, E. A., Bosman, L. B., Wollega, E., & Leon-Salas, W. D. (2021). Peer-to-peer energy trading: A review of the literature. *Applied Energy*, *283*, 116268.