EPiC Series in Computing

Volume 89, 2022, Pages 62–71

Proceedings of 35th International Conference on Computer Applications in Industry and Engineering

Efficient Secured Public-Key based Data Lookup and Multicast Protocols with Anonymity in RC-Based Two-level Hierarchical Structured P2P Network

Indranil Roy[1], Nick Rahimi[2], Reshmi Mitra[1], and Swathi Kaluvakuri[3]

[1] Southeast Missouri State University, Cape Girardeau, Missouri, U.S.A
iroy@semo.edu , rmitra@semo.edu
[2] University of Southern Mississippi, Hattiesburg, Mississippi, U.S.A.
nick.rahimi@usm.edu
[3] Southern Illinois University, Carbondale, Carbondale,Illinois, U.S.A
swathi.kaluvakuri@siu.edu

Abstract

Because peer-to-peer networks are inherently insecure, they provide a special challenge in terms of network security. In this study, we have considered a recently described non-DHT-based 2-level structured P2P network. It is an architecture built on interests. Utilizing RC, a modular arithmetic-based residue class, the overlay topology has been achieved. This design was chosen because it allows for minimal latency in both intra and inter-group communications. In the present study, we provide efficient schemes for public-key cryptographic security of existing communication protocols. We have also extended these approaches to include anonymity.

1 Introduction

Due to their capacity to offer computational and data resource sharing in a scalable, self-organizing, distributed manner, peer-to-peer (P2P) overlay networks are widely used in distributed systems. P2P networks are divided into two categories: unstructured networks and structured networks. Peers in unstructured systems [2] are arranged in any random topology. For data lookup, flooding is necessary. In unstructured systems, problems brought on by frequent peer joining and leaving the system, or "churn," are effectively handled. However, this compromises the effectiveness of data querying and the crucial flexibility. Lookups are not guaranteed in unstructured networks. On the other hand, structured overlay networks offer deterministic limits on data discovery. They create scalable network overlays based on a distributed data structure that truly allows deterministic data lookup behavior. The usage of distributed hash tables (DHTs) is a recent trend in the design of structured overlay systems [6, 10, 19]. Overlay designs of this type can provide efficient, flexible, and resilient service [6, 10, 12, 19, 20]. However, maintaining DHTs is a complicated operation that requires significant effort to address the churn issue. As a result, the main difficulty for such designs is reducing this amount

of labor while yet offering an effective data query service. There are numerous notable publications in this area that have examined creating hybrid systems [5, 15, 17, 21]. These works make an attempt to incorporate the benefits of both structured and unstructured structures. These works, however, have their own set of advantages and disadvantages [1].

The study and application of encrypted communication protocols is known as cryptography. It is concerned with the development and examination of protocols that prohibit harmful third parties from gaining access to information transferred between two companies, hence complying to many principles of information security. Secure communication refers to a scenario in which a message or data transmitted between two parties cannot be accessed by an adversary. An adversary in cryptography is a malevolent actor who seeks to get usable information or data by violating information security rules. Cryptographic techniques are used to ensure authentication and confidentiality stability in peer-to-peer networks. The two most common forms of cryptographic algorithms are secret key cryptographic algorithms and public key cryptographic algorithms. Secret key cryptographic algorithms are also known as symmetric key algorithms since the same key is used for encryption and decryption and is shared by all parties involved. Public key cryptography algorithms, on the other hand, are also known as asymmetric key algorithms. This version employs a pair of keys, one for encryption and the other for decryption [13].

In [9] the authors have used a well defined approach of combining the symmetric key and the public key cryptography methods to ensure security in the architecture. The main issue with symmetric key encryption is that the key must be delivered to the entity with whom you are exchanging data. Key transportation is a difficulty in symmetric cryptosystems. The secret key must be sent to the receiving system before the actual message can be sent. Every kind of electronic communication is unsafe since no one can guarantee that communication lines will not be tapped. Another problem is, if someone obtains the shared symmetric key, they can decode everything encrypted with that key. When symmetric encryption is used for two-way communications, both sides of the discussion are vulnerable. We thus suggested robust public-key cryptography approaches for the security of current communication protocols in [9] with comparably lower costs in order to overcome the aforementioned issues with employing symmetric key. We have added anonymity to these strategies as well. However, asymmetric encryption can be more expensive than symmetric encryption but it does allow us to overcome the downfall's of using symmetric encryption.

1.1 Our Contribution

In this research, interest-based P2P systems have been taken into consideration [21, 22]. We have thought about creating secure protocols for both intra and inter lookup algorithm . Public keys for asymmetric key cryptography have been utilized. Additionally, we have thought about how to make the capacity-constrained multicast algorithms more secure both inside groups and for the two-level design. We have also taken anonymity into account. The rest of the paper is organized as follows. We give the preliminaries and the overview of the RC-based 2-level non-DHT-based structured P2P network proposed in [9] in section 2. The secured data lookup algorithms for both the inter and the intra cluster are explained in section 3. In section section 4 we present the multicast algorithms with anonymity and security. In section 5 we discuss different security attacks and its effect on our proposed network. Finally, we conclude in section 6.

2 Preliminaries

Here, we have taken into consideration some of the first results of an RC-based low diameter two level hierarchical structured P2P network [7, 8, 14]. We provide a structured design for an interest-based peer-to-peer system in this section. We will use the following notations and their meanings to define the architecture.

Definition 1. We define a resource as a tuple $<Res_i$, V $>$, where Res_i denotes the type of a resource and V is the value of the resource. Note that a resource can have many values.

Definition 2. Let S be the set of all peers in a peer-to-peer system. Then $S = \{P^{Ri}\}$, $0 \leq i \leq n-1$, where P^{Ri} denotes the subset consisting of all peers with the same resource type Res_i. and the number of distinct resource types present in the system is n. Also, for each subset P^{Ri}, we assume that H_i is the first peer among the peers in P^{Ri} to join the system. We call H_i as the group-head of group G_i formed by the peers in the subset P^{Ri}.

We now describe our proposed architecture suitable for interest-based peer-to-peer system. Generalization of the architecture is considered in [8]. We use the following notations along with their interpretations while we define the architecture.

2.1 Two Level Hierarchy

It is a two-level overlay architecture and at each level structured networks of peers exist. It is explained in detail below.

1. At level-1, we have a ring network consisting of the peers H_i $(0 \leq i \leq n-1)$. The number of peers on the ring is n which is also the number of distinct resource types. This ring network is used for efficient data lookup and so we name it as transit ring network.

2. At level-2, there are n numbers of completely connected networks (groups) of peers. Each such group, say G_i is formed by the peers of the subset P^{Ri}, $(0 \leq i \leq n-1)$, such that all peers $(\in P^{Ri})$ are directly connected (logically) to each other, resulting in the network diameter of 1. Each G_i is connected to the transit ring network via its group-head H_i.

3. Each peer in the network maintains a Information Resource Table (IRT) that consists of n number of tuples.

   - The group heads will have a tuple of the form <Resource Type, Resource Code, Group Head Logical Address, Group Head public Key>for other group heads and <Resource Type, Resource Code, Peer Logical Address, Peer public Key>for the other peers present in the network. The Group Head Logical Address are assigned according to the proposed logical address assignment algorithm proposed in section 2.3 and the public key of the group heads or the peers are exchanged when they are joining the network and the IRT is updated and broadcasted in the network. Also, Resource Code is the same as the group head logical address.
   - The peers P_i, who are not group heads but belongs to a group G_i ($P_i \in G_i$) will have the tuple of the form <Resource Type, Resource Code, Group Head Logical Address, Group Head public Key>for group head of G_i and <Resource Type, Resource Code, Peer Logical Address, Peer public Key>for the other peers present in G_i.

4. Any communication between a peer $G_{x,i} \in$ group G_x and $G_{y,j} \in$ group G_y takes place only through the corresponding group heads H_x and H_y.

The proposed architecture is shown in Figure 1.

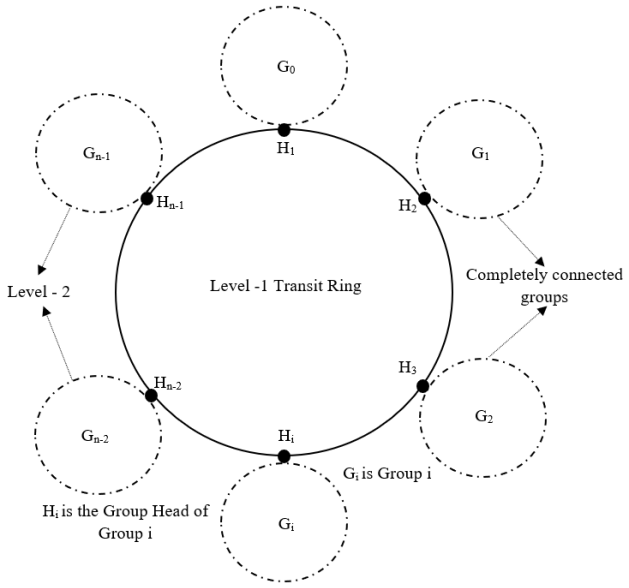

Figure 1: A two-level RC based structured P2P architecture with n distinct resource types

2.2 Assignments of Overlay Addresses

Assume that in an interest-based P2P system there are n distinct resource types. Note that n can be set to an extremely large value a priori to accommodate a large number of distinct resource types. Consider the set of all peers in the system given as S = $\{P^{Ri}\}$,$(0 \leq i \leq n-1)$. Also, as mentioned earlier, for each subset P^{Ri} (i.e. group G_i) peer H_i is the first peer with resource type R_i to join the system. The assignment of logical addresses to the peers at the two levels and the resources happen as explained in [7-8, 12].

Remark 1. IRT remains sorted with respect to the logical addresses of the group-heads.

Definition 3. Two peers H_i and H_j on the ring network are logically linked together if (i + 1) mod n = j.

Remark 2. The last group-head $H_n - 1$ and the first group-head P_0 are neighbors based on Definition 3. It justifies that the transit network is a ring.

Definition 2. Two peers of a group G_r are logically linked together if their assigned logical addresses are mutually congruent.

Lemma 2. Diameter of the transit ring network is $n/2$.

Lemma 3. Each group G_r forms a complete graph.

2.3 Salient Features of Overlay Architecture

We summarize the salient features of this architecture.

1. It is a hierarchical overlay network architecture consisting of two levels; at each level the network is a structured one.

2. Use of modular arithmetic allows a group-head address to be identical to the resource type owned by the group. We will show in the following section the benefit of this idea from the viewpoint of achieving reasonably very low search latency.

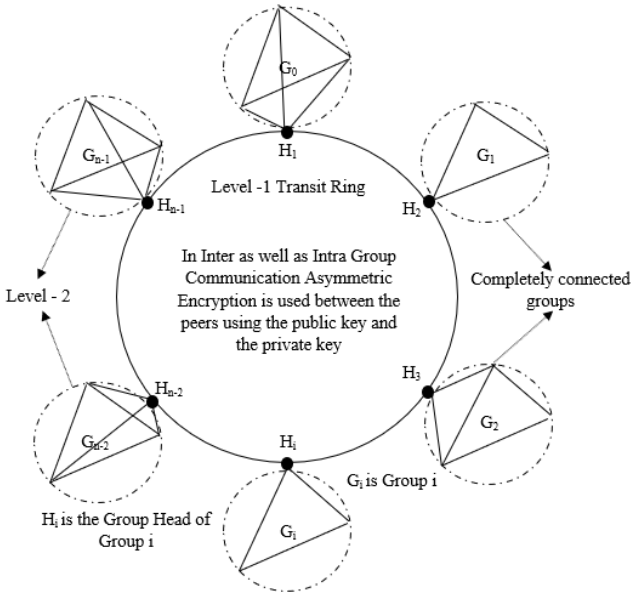

Figure 2: Inter and Intra Group Communication using Asymmetric Encryption

3. Number of peers on the ring is equal to the number of distinct resource types, unlike in existing distributed hash table-based works some of which use a ring network at the heart of their proposed architecture [12].

4. The transit ring network has the diameter of n/2. Note that in general in any P2P network, the total number of peers N >>n.

5. Each overlay network at level 2 is completely connected. That is, in graph theoretic term it is a complete graph consisting of the peers in the group. So, its diameter is just 1. Because of this smallest possible diameter (in terms of number of overlay hops) the architecture offers minimum search latency inside a group.

3 Data Lookup Algorithms with Public Key Cryptography

This part introduces data lookup techniques [7, 14], both intra and inter, with the idea of security using public key cryptography. Figure 2 explains how cryptographic operations are used in a two-level RC-based design.

3.1 Intra Group Lookup Algorithm in RC Based Architecture with Public Key Security

The resource lookup occurs within the group in this scenario, which means that the resource type is the same for both parties but the value is different. The algorithm for intra group data lookup is explained as follows.

Let us assume that in a group G_y, a peer $G_{y,i}$ with the resource $<Res_y, V_i>$is querying for a resource $<Res_y, V_j>$. The requesting peer will broadcast the request message in the group G_i using the IRT table as explained in Algorithm 1.

Algorithm 1 Intra Group Lookup Algorithm in RC Based Architecture with Public Key Security

$G_{y,i}$ broadcast the request message $<Res_y, V_j>$in G_i using the IRT table
if $\ni G_{y,j} \in G_y$ with $<Res_y, V_j>$ **then**
    $G_{y,j}$ encrypts$<Res_y, V_j>$with $Pbl_{G_{y,i}}$ ▷ $G_{y,j}$ gets the $Pbl_{G_{y,i}}$ from IRT
    Unicast the encrypted message to $G_{y,i}$
else
    Search for $<Res_y, V_j>$fails
end if

3.2 Inter Group Lookup Algorithm in RC Based Architecture with Public Key Security

Inter group communication takes place between nodes from two separate interest-based groups.Any communication between the peers $G_{x,i} \in$ group G_x and $G_{y,j} \in$ group G_y in our public-key based secure RC-based architecture occurs solely through the appropriate group heads H_x and H_y.

Let us assume that a peer $G_{x,i} \in$ group G_x with the resource $<Res_x, V_i>$is querying for a resource $<Res_y, V_j>$.Both the peer $G_{x,i}$ and the group head H_x are aware about the fact that $Res_y \notin G_x$. The algorithm for the secured public-key based data lookup search for the inter group data lookup in RC Based Architecture is explained in Algorithm 2.

Algorithm 2 Inter Group Lookup Algorithm in RC Based Architecture with Public Key Security

$G_{x,i}$ encrypts the request message $<Res_y, V_j>$with Pbl_{H_x} using the IRT table
H_x decrypts the request message $<Res_y, V_j>$with Pvt_{H_x}
H_x looks at its IRT and find $H_y : Res_y \in H_y$
H_x encrypts the request message $<Res_y, V_j>$with Pbl_{H_y} using the IRT table
H_y decrypts the request message $<Res_y, V_j>$with Pvt_{H_y}
if H_y itself have $<Res_y, V_j>$ **then**
    H_y encrypts the message with Pbl_{H_x} and unicast it to H_x
    H_x decrypts the message with Pvt_{H_x} and encrypts with $Pbl_{G_{x,i}}$ and unicast it to $G_{x,i}$
    $G_{x,i}$ decrypts the message with $Pvt_{G_{x,i}}$
else if $\ni G_{y,j} \in G_y$ with $<Res_y, V_j>$ **then**
    $G_{y,j}$ encrypts$<Res_y, V_j>$with Pbl_{H_y} and unicast to H_y
    H_y decrypts with Pvt_{H_y} and encrypts the message with Pbl_{H_x} and unicast it to H_x
    H_x decrypts the message with Pvt_{H_x} and encrypts with $Pbl_{G_{x,i}}$ and unicast it to $G_{x,i}$
    $G_{x,i}$ decrypts the message with $Pvt_{G_{x,i}}$
else
    Search for $<Res_y, V_j>$fails
end if

4 Multicast Algorithms with Anonymity and Security using Public Key Cryptography

In this part, public-key based security and anonymity principles have been added to the multicast algorithms of the RC-based architecture that were first introduced in [14]. We discussed creating a very effective overlay multicast protocol with capacity constraints in [14]. Our structure consists of two levels. There are just as many unique resource categories as there are nodes (group-heads) on the level-1 ring, and every group (cluster) at level 2 may contain any number of nodes. The number of different resources n, as shown in [3], is significantly less than the total number of nodes N on the ring. It has motivated us to use some of the concepts from [3], particularly changing the multicast problem into a broadcast one and appropriately enhancing it with ours to design a highly efficient any source capacity-constrained multicast protocol suitable for the RC-based architecture with significantly fewer hops and communication complexities than the work in [3].

4.1 Multicast Algorithm [14] with PublicKey based Security and Anonymity where capacity of group head $\geq$ #groupheads

The multicast algorithm where $c_x^s \geq n_r$ considering the concepts of anonymity and security using public-key is explained in Algorithm 3, where c_x^s denotes the degree/capacity of the multicast source group-head and n_r denotes the number of receiver group-heads.

Let $G_{x,i}$ represents the source peer of the multicast message($mcast\_msg$) and H_x represent the source group-head.

Algorithm 3 Multicast Algorithm with Public-Key based Security and Anonymity where $c_x^s \geq n_r$

1: $G_{x,i}$ encrypts $mcast\_msg$ with the Pbl_{H_x} from IRT and unicast it to H_x
2: H_x decrypts $mcast\_msg$ with the Pvt_{H_x} and then replaces the ip_address of $G_{x,i}$ with its own
3: H_x then gather the ip_addresses and the public key of the participating group-heads from the IRT.
4: H_x then encrypts $mcast\_msg$ with the respective public keys of the group-heads and unicast it to them
5: On receiving the encrypted $mcast\_msg$, every group-head will decrypt it with their own private key
6: **if** receiver group-head $\in$ multicast group **then**
7: It copies the $mcast\_msg$ and stores it
8: Replaces the ip_address of H_x with its own and encrypts it with the public-key of each receiver in the group and unicast it to them
9: **else**
10: Replaces the ip_address of H_x with its own and encrypts it with the public-key of each receiver in the group and unicast it to them
11: **end if**

4.2 Multicast Algorithm [14] with Public-Key based Security and Anonymity where capacity of group head < #groupheads

Let $G_{x,i}$ represents the source peer of the multicast message($mcast\_msg$) and H_x represent the source group-head. The algorithm is explained in Algorithm 4.

Algorithm 4 Multicast Algorithm with Public-Key based Security and Anonymity where $c_x^s < n_r$

$G_{x,i}$ encrypts $mcast\_msg$ with the Pbl_{H_x} from IRT and unicast it to H_x
H_x decrypts $mcast\_msg$ with the Pvt_{H_x} and then replaces the ip_address of $G_{x,i}$ with its own
H_x then gather the ip_addresses and the public key of the participating group-heads from the IRT.
According to its capacity/degree, H_x randomly chooses as many group heads as there are
Additionally, H_x will retrieve its successor's public key and IP address from the IRT table.
H_x then encrypts $mcast\_msg$ with the respective public keys of the group-heads and unicast it to them
H_x also encrypts $mcast\_msg$ with the public key of its successor and unicast it
if $mcast\_msg$ is received by receiver group-head for first time(no duplicates) **then**
    Each receiver group-head decrypts the $mcast\_msg$ with their private key
    if receiver group-head ∈ multicast group **then**
        It copies the $mcast\_msg$ and stores it
        Replaces the ip_address of H_x with its own and encrypts it with the public-key of each receiver in the group and unicast it to them
    else
        Replaces the ip_address of H_x with its own and encrypts it with the public-key of each receiver in the group and unicast it to them
    end if
    Replaces the ip_address of H_x with its own and find the ip_address and the public key of its successor group-head encrypts it with the public-key of Pbl_s, the successor and forwards it
    Until the message reaches all of the group heads on level 1 transit ring, message propagation in the first level ring continues in a similar manner
else
    Head of the receiver group discards the duplicate message
end if

5 Performance Evaluation

P2P networks offer the potential to improve network capabilities through the sharing of music, video, and other services. Nonetheless, P2P networks pose security issues since the nodes are exposed to a variety of security attacks. One of them is the Man-in-the-middle Attack. It is an indirect intrusion attempt in which the attacker places his computing device between two nodes. As a result, the intermediary node can intercept and change communications sent between two valid users without the knowledge of the sender and recipient. Encryption technologies can be used for data transmission as a defense measure.

The algorithms we proposed for data-lookup and multicast in sections 3 and 4 are immune

to such attacks because every message communicated is encrypted with the public key of the immediate destination peer, and the message can be decrypted by only the destination peer with its own private key. This prohibits anybody along the path of the message from interfering with the communication between the source and the destination.

There is no overhead of control messages for maintaining network security since when a peer joins the network, they update the IRT with their ip_address, resource code, and public key information, which is then broadcast across the network. As a result, following the broadcast, everyone in the network will have access to the most up-to-date information..

6 Conclusion

In this work, a 2-level non-DHT-based P2P architecture was considered. The choice to utilize an interest-based architecture was made because

1. We have previously shown [8] that the data lookup strategies outperform many really well-known DHT-based contributions [16, 18, 23] in terms of search latency.

2. Its benefit over several existing interest-based systems [1, 4, 6, 10, 11, 19]. Public-key cryptography has been used to successfully integrate security and anonymity into the intra-group and inter-group communication techniques described in [8] in this work.

To guarantee the security of the architecture, the writers of [9] combined the symmetric key and public key cryptography approaches using a well-defined methodology. The primary drawback of symmetric key encryption is that the recipient of the key, with whom you are transmitting data, must receive it. Both parties to a conversation are exposed when symmetric encryption is utilized. We thus used asymmetric key cryptography to address the aforementioned problems and offered strong public-key cryptography methodologies for the security of contemporary communication protocols in [9] with correspondingly reduced costs.

References

[1] Lyes Badis, Mourad Amad, Djamil Aïssani, Kahina Bedjguelal, and Aldja Benkerrou. Routil: P2p routing protocol based on interest links. In *2016 International Conference on Advanced Aspects of Software Engineering (ICAASE)*, pages 1–5. IEEE, 2016.

[2] Yatin Chawathe, Sylvia Ratnasamy, Lee Breslau, Nick Lanham, and Scott Shenker. Making gnutella-like p2p systems scalable. In *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 407–418, 2003.

[3] Shiping Chen, Baile Shi, Shigang Chen, and Ye Xia. Acom: Any-source capacity-constrained overlay multicast in non-dht p2p networks. *IEEE Transactions on Parallel and Distributed Systems*, 18(9):1188–1201, 2007.

[4] Wen-Tsuen Chen, Chi-Hong Chao, and Jeng-Long Chiang. An interested-based architecture for peer-to-peer network systems. In *20th International Conference on Advanced Information Networking and Applications-Volume 1 (AINA'06)*, volume 1, pages 707–712. IEEE, 2006.

[5] Prasanna Ganesan, Qixiang Sun, and Hector Garcia-Molina. Yappers: A peer-to-peer lookup service over arbitrary topology. In *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428)*, volume 2, pages 1250–1260. IEEE, 2003.

[6] Mo Hai and Yan Tu. A p2p e-commerce model based on interest community. In *2010 International Conference on Management of e-Commerce and e-Government*, pages 362–365. IEEE, 2010.

[7] Swathi Kaluvakuri, Bidyut Gupta, Banafsheh Rekabdar, Koushik Maddali, and Narayan Debnath. Design of rc-based low diameter two-level hierarchical structured p2p network architecture. In Mohammed Serrhini, Carla Silva, and Sultan Aljahdali, editors, *Innovation in Information Systems and Technologies to Support Learning Research*, pages 312–320, Cham, 2020. Springer International Publishing.

[8] Swathi Kaluvakuri, Koushik Maddali, Nick Rahimi, Bidyut Gupta, and Narayan Debnath. Generalization of rc-based low diameter hierarchical structured p2p network architecture. *INTERNATIONAL JOURNAL OF COMPUTERS AND THEIR APPLICATIONS*, page 74, 2020.

[9] Swathi Kaluvakuri, Indranil Roy, Koushik Maddali, Bidyut Gupta, and Narayan Debnath. Efficient secured data lookup and multicast protocols with anonymity in rc-based two-level hierarchical structured p2p network. *International Journal for Computers & Their Applications*, 28(3), 2021.

[10] Mujtaba Khambatti, Kyung Dong Ryu, and Partha Dasgupta. Structuring peer-to-peer networks using interest-based communities. In *International Workshop On Databases, Information Systems, and Peer-to-Peer Computing*, pages 48–63. Springer, 2003.

[11] Sardar Kashif Ashraf Khan and Laurissa N Tokarchuk. Interest-based self organization in group-structured p2p networks. In *2009 6th IEEE Consumer Communications and Networking Conference*, pages 1–5. IEEE, 2009.

[12] Dmitry Korzun and Andrei Gurtov. Hierarchical architectures in structured peer-to-peer overlay networks. *Peer-to-Peer Networking and Applications*, 7(4):359–395, 2014.

[13] Koushik Maddali, Swathi Kaluvakuri, Nick Rahimi, Bidyut Gupta, and Narayan Debnath. On designing secured communication protocols along with anonymity for crt based structured p2p network architecture. *EPiC Series in Computing*, 75:59–68, 2021.

[14] Koushik Maddali, Banafsheh Rekabdar, Swathi Kaluvakuri, and Bidyut Gupta. Efficient capacity-constrained multicast in rc-based p2p networks. In *Proceedings of 32nd International Conference on*, volume 63, pages 121–129, 2019.

[15] Zhuo Peng, Zhenhua Duan, Jian-Jun Qi, Yang Cao, and Ertao Lv. Hp2p: A hybrid hierarchical p2p network. In *First International Conference on the Digital Society (ICDS'07)*, pages 18–18. IEEE, 2007.

[16] Antony Rowstron and Peter Druschel. Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems. *Distributed Systems Platforms (Middleware),In IFIP/ACM International Conference*, pages 329–350, 2001.

[17] Kai Shuang, Peng Zhang, and Sen Su. Comb: a resilient and efficient two-hop lookup service for distributed communication system. *Security and Communication Networks*, 8(10):1890–1903, 2015.

[18] Ion Stoica, Robert Morris, David Liben-Nowell, David R Karger, M Frans Kaashoek, Frank Dabek, and Hari Balakrishnan. Chord: a scalable peer-to-peer lookup protocol for internet applications. *IEEE/ACM Transactions on networking*, 11(1):17–32, 2003.

[19] Zhiyong Tu, Wei Jiang, and Jinyuan Jia. Hierarchical hybrid dve-p2p networking based on interests clustering. In *2017 International Conference on Virtual Reality and Visualization (ICVRV)*, pages 378–381. IEEE, 2017.

[20] Ming Xu, Shuigeng Zhou, and Jihong Guan. A new and effective hierarchical overlay structure for peer-to-peer networks. *Computer Communications*, 34(7):862–874, 2011.

[21] Min Yang and Yuanyuan Yang. An efficient hybrid peer-to-peer system for distributed data sharing. *IEEE Transactions on computers*, 59(9):1158–1171, 2009.

[22] Rongmei Zhang and Y Charlie Hu. Assisted peer-to-peer search with partial indexing. *IEEE Transactions on Parallel and Distributed Systems*, 18(8):1146–1158, 2007.

[23] Ben Y Zhao, Ling Huang, Jeremy Stribling, Sean C Rhea, Anthony D Joseph, and John D Kubiatowicz. Tapestry: A resilient global-scale overlay for service deployment. *IEEE Journal on selected areas in communications*, 22(1):41–53, 2004.