*Journal of Universal Computer Science, vol. 24, no. 9 (2018), 1282-1305*
*submitted: 30/12/17, accepted: 30/6/18, appeared: 28/9/18 © J.UCS*

# Crumbling Walls Log Quorum System-based Name Resolution Routing for CCN based IoT

**Pir Imran Shah**
(Department of Computing, Iqra University, Islamabad 44000, Pakistan
imran.pir@ciit-attock.edu.pk)

**Peer Azmat Shah, Sadaf Yasmin, Zahoor ur-Rehman**
(Internet, Communication & Networks (ICNet) Research Lab
Department of Computer Science, COMSATS University Islamabad, Attock Campus
43600, Pakistan
hod_cs@ciit-attock.edu.pk, sadaf_yasmin@ciit-attock.edu.pk
xahoor@ciit-attock.edu.pk)

**Akhlaque Ahmad**
(Department of Computer Science, Dhanani School of Science & Engineering
Habib University, Karachi, Pakistan
akhlaque.ahmad@sse.habib.edu.pk)

**Yunyoung Nam**
(Department of Computer Science and Engineering, Soonchunhyang University
Asan 31538, South Korea
Corresponding author
ynam@sch.ac.kr)

**Seungmin Rho**
(Department of Media Software, Sungkyul University, Anyang, South Korea
smrho@sungkyul.ac.kr)

**Abstract:** Content Centric Networking (CCN) is recently gaining attention for its potential to support emerging applications within Internet of Things (IoT). IoT generates huge volumes of data, with millions of nodes frequently requesting or generating different contents. CCN helps in breaking the coupling between a content and its location by addressing data with name rather than its location. This paper supports a CCN based approach in the IoT environment. To address scalability problems associated with CCN-assisted IoTs, we propose a new crumbling walls log quorum system based name resolution routing technique. The proposed system supports scalability, as the intersection property of a quorum system, inevitably minimizes the read/write operations overhead on distributed name resolution servers. Results show that the proposed technique increases the availability of the system along with low lookup overhead, latency, and load on distributed servers.

**Keywords:** IoT, Content centric networking, Routing, Big data, Scalability, Quorum systems
**Categories:** C.2.1, C.2.2, C.2.4

# 1 Introduction

Traditional IP-based Internet architecture is designed based on the idea "where the contents are?". However, advancements in technology are rapidly expanding the connectivity of Internet with millions of new low-cost devices. These devices generate huge amount of data to be shared around the Internet. Inevitably, the research community is showing an increasing interest in improving content distribution [Jmal et al. 2017] rather focusing on host-to-host communication, in recent years. The emerging design paradigm has changed the traditional concept of the Internet to provide host-to-host connectivity only. Now people are interested in what the contents are? However, current Internet communication is still in the form of "where", which leads to problems like availability, security and location dependence. The idea of Content Centric Networking (CCN) is envisioned by Jacobson et al. [Jacobson et al. 2009]. Authors [Jacobson et al. 2009] realize the need to change the current traditional IP-based communication model, where two powerful machines communicate with each other using host based IP addresses. As today, we have billions of devices being part of the Internet, and this may lead to trillions of devices in the near future. According to CISCO, more than 12 billion devices were connected to the Internet in 2011 [Evans 2011]. In such a scenario, Internet of Things (IoT) is considered as a promising direction for a Future Internet architecture, which aims to connect everything to the Internet.

Connecting a large number of devices for communication, challenges the current state of the Internet in terms of connectivity and communication stability [Waltari et al. 2016]. Addressing data or contents through host based IP addresses, bounds the presence of a content to a specific location or geographical area within the Internet. On the contrary, CCN architecture replaces the data delivery model from traditional host-to-host (IP address) communications with content name based retrieval model. The primary objective of CCN is to break the coupling between data and location, by addressing data contents with names rather than the location of source node. Baccelli et al. [Baccelli et al. 2014] suggest, that an IoT environment may take benefit of cache assisted, hop-by-hop replication characteristics of CCN. As, the latter is best suitable for content request/retrieval, scheduled content update, and communication patterns of IoT environments.

IoT nodes are resource constrained, and generate huge amounts of data [Bari et al. 2012]. Therefore, using CCN in an IoT environment poses new challenges such as, content naming, name-based routing, name resolution, in-network caching, on-demand replication, security, privacy, and content dissemination. From these challenges, naming and routing are the core of any CCN architecture. Since the evolution of Information Centric Networking (ICN), which is a superset of CCN, many research studies has been carried to propose solutions for routing in such networks. A comprehensive survey of these schemes is discussed by Bari et al. [Bari et al. 2012]. However, majority of the projects discussed in [Bari et al. 2012] use flooding for content discovery and retrieval, which may result into scalability problems when used in an IoT environment with millions of nodes. The growing size of IoT network cannot afford the use of any routing scheme that floods the network for content delivery. Hence, there is need for a new protocol that can efficiently utilize the benefits of using CCN in IoT, and may not use the broadcast mechanism for content dissemination and retrieval. With this in mind, a new content name resolution based routing scheme for IoT is proposed in this paper. The new protocol overcomes the problems of scalability (while using CCN based routing in an IoT environment) by using content centric routing with a distributed quorum system. Name resolution Servers (NRSs) within the proposed system are arranged in the form of different quorums/sets. Nodes within the same quorum coordinate among members to answer name resolution queries. Moreover, data across different NRSs remain consistent due to the intersection property of a quorum system. Hence, the user is guaranteed to have a consistent view of the system, and it eliminates the need to flood the network for content name resolution; which results in increasing the performance of the network.

Our contributions, in this paper, are summarized as follows:

i. A new name resolution system based on quorums is introduced for CCN-assisted IoT environments.
ii. Data is consistent across the system due to different intersection points between quorums. Thereby, a user receives the most recent information only by requesting the nearest NRS.
iii. A dynamic mechanism is suggested to handle addition & deletion of NRSs in the proposed quorum system.
iv. A through evaluation of a quorum system is presented against different performance matrices.

The rest of the paper is organized as: Literature review is presented in Section 2, followed by motivation and design challenges in Section 3. The proposed design is presented in Section 4, and performance analysis is performed in Section 5. Results & evaluations are discussed in Section 6 followed by conclusion & future work in Section 7 at the end.

## 2 Related Work

The routing in CCN based networks can be of two types: name-based routing and name resolution based routing. In case of name-based routing, a data request based on some identifier (name) is forwarded directly and state information is maintained at each intermediate node so that the contents can be delivered on the backward path to the requester, as used by most of the CCN architectures. In the other case when name resolution based routing is used, the content names are resolved to one or more content locations or addresses using some name resolution server and then the data request is routed to any of the content location using some topology based shortest path routing protocol. Bari et al. [Bari et al. 2012] discussed a qualitative analysis of some of name-based and name resolution based approaches.

The problem of CCN based routing has been discussed in literature since the evolution of ICN. Many approaches were proposed for name-based as well as for name resolution based routing. Some of the well-known name resolution based approaches are: Publish/Subscribe Internet Routing Paradigm (PSIRP) [Lagutin et al. 2010] and its extension Publish-Subscribe Internet Technologies (PURSUIT) [Fotiou et al. 2010], and a reliable IoT using ICN that was proposed by Polyzos and Fotiou [Polyzos et al. 2015]. All of these approaches are based on publish-subscribe architecture for routing and are centralized in nature. Network of Information (NetInf) [Dannewitz et al. 2010] is also a name resolution based idea and it uses a multi-level DHT-based name resolution service called Multi-level Distributed Hash Table (MDHT) [D'Ambrosio et al. 2011] that provides name-based anycast routing. MDHT [D'Ambrosio et al. 2011], [Dannewitz et al. 2013] divides the network into different topological levels, e.g., the Autonomous System (AS) level and the Point of Presence (POP) level. At each level one DHT exists and a name resolution request is fulfilled by a local hash table or forwarded to the one up in the hierarchy if cannot be resolved locally. In this scheme, in case of failure of local hash table at POP level the requests of end nodes at that level cannot be fulfilled. Majority of name resolution based schemes are centralized and have single point of failure. Garcia et al. [Bee 1999] proposed CCN-RAMP which is basically an extension to the name resolution routing mechanism of ICN. Major short comings of basic ICN model suffers DDOS attacks in PIT domain and broadcast overhead due to Forwarding Information Base (FIB) which are targeted in CCN-RAMP model by Anchor based Loop free forwarding approach. It has a disadvantage in perspective of large scale networks due to its naming Prefix Resolution Table (PRT) unbounded broadcast of updates even to each and every local router not only to relays for recent name prefix entries which will cost in high memory requirements for heterogeneous networks. But if it is maintained at each router it is really an overhead that can affect routing node performance. Separate table is only used for reverse path traversal. Secondly, for proposed technique it is very hard to serve wireless, limited memory and limited energy wireless sensor nodes.

Name-based routing approaches include: Named Data Networking (NDN) [Jacobson et al. 2009], [Zhang et al. 2010], Combined Broadcast and Content Based routing (CBCB) [Carzaniga et al. 2004], Data-Oriented Network Architecture (DONA) [Koponen et al. 2007], Distance-based Content Routing (DCR) [Garcia 2014], CCN [Song et al. 2013] and Reactive Optimistic Name-based Routing (RONR) [Baccelli et al. 2014]. All of these approaches are based on flooding that will cause scalability problems when used in the IoT environment, however the CBCB uses a strategy mix of publish-subscribe and flooding. The RONR is specifically proposed for the IoT networks and it has optimized the flooding using vanilla flooding for the first Interest message and then used the FIB entries for next Interest messages. However, if a FIB entry expires, then it needs to re-flood the network.

Both types of routing schemes, name resolution based and name-based, have advantages as well as some drawbacks. Name resolution approaches guarantee the discovery of any content while name-based approaches do not guarantee rather they attempt to discover the content with high probability of discovery. Name-based approaches flood the network for content discovery, thus creating high overhead as compared to the name resolution based approaches. However, the failure of a name resolution entity may create some contents to be inaccessible even they exist, in the name resolution based approaches. Keeping in view all these pros and cons of routing approaches, there is a need to design and develop a new routing scheme for IoT environment that is scalable with minimum overhead and is distributed in nature to distribute the network load and to eliminate the single point of failure.

# 3 Motivation & Design Challenges

IoT is characterized as a large size network, with millions of devices generating different kinds of traffic. Hence, scalability is one of the major issues, a routing protocol designed for an IoT environment needs to handle. In name resolution based content centric routing for IoT, a content producing node updates content name to content address mappings in a name resolution server. Similarly, a content requesting node requests the name resolution servers to resolve these content names to content address entries. Here, a number of distributed servers are used for increasing the availability of the system. However, high overhead involved in read/write operations against a large number of contents, produced by millions of IoT nodes on each distributed server, may lead to scalability problems in the IoT environment.

Quorum systems, proposed in this paper, provide a uniform and reliable way of coordination among a number of distributed servers with minimum read and write operations overhead. Using these systems, a content producing node may write its content name to content address mappings to a nearest server. This eventually results in updating each server within the write quorum of the latter. Due to the intersection property between quorums, write operation guarantees that each server in a quorum is updated with the most recent information of a content name to content address mappings. Accordingly, when a node requests any given content from its nearest server, the latter resolves the query from its read quorum. This results in minimizing the read and write operation on distributed servers by just reading and writing to only servers in a single quorum, instead of performing the read and write operation on each distributed server in the network.

In following, we discuss some important design challenges [Bari et al. 2012] [Fotiou et al. 2010] [Polyzos et al. 2015], an IoT name resolution based protocol need to address for improving the performance of the network.

## 3.1 Design Challenges for Name Resolution Based Protocols

We envision that a major goal of distributed name resolution routing in CCN is to maximize availability of information with minimum delay, and low coordination overhead [D'Ambrosio et al. 2011] [Dannewitz et al. 2013]. In order to achieve this goal, here, we identify some important design issues need to be considered, while designing a new name resolution protocol, such as: name resolution node selection, scalability of the system, control traffic overhead for content information updates and query, addition and deletion of name resolution node etc.

### 3.1.1 Name Resolution Node Selection

Name resolution node selection is an important design challenge for a distributed name resolution system. As discussed in [Elbreiki et al. 2016] and [Torres et al. 2015], distribution of anchor points may vary within different parts of the network. For example, a name resolution node might be placed within 1) the core network, 2)access network, or 3) at the edge point, as shown in Figure 1. Moreover, an IoT node can also serve as a distributed name resolution server.

Name Resolution Node in the Core Network: A single name resolution server, in the core network, may cause concentration of name resolution traffic, and single point of failure. In this regard, multiple anchor points can be topologically distributed within the core network to cover different geographical areas. In this manner, IoT nodes can be managed in a decentralized way and data traffic can also be made distributed.

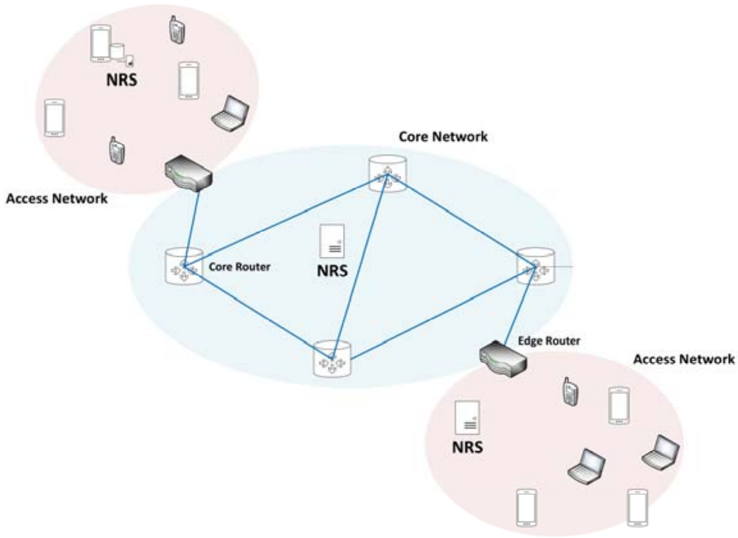


*Figure 1: Name Resolution Server (NRS) located within an IoT Network*

*Name Resolution Node in Access Network:* Wireless access technologies, such as: WiFi, WiMAX, UMTS, HSPA+ are rapidly getting popular among mobile users. Accordingly, a large number of Access Points (AP) or Base Stations (BS) are being installed in residential and public areas. Although, these access nodes (AP and BS) exhibit layer 2 functionality only, however, they can serve as name resolution points by adding layer 2 & 3 capabilities. This kind of distribution can be helpful to reduce the delay in scenarios, where required contents are located closer to access networks.

*Name Resolution at Host Node:* Name resolution at host level is like peerto-peer communication, where one IoT node interacts directly with another IoT node for name resolution. This type of distribution is helpful in scenarios, where both nodes are located closer to one another in the Internet, e.g. inside a single access network. However, if the two nodes are located far away from each other within the Internet, then, this distribution may result in higher delays and packet loss.

### 3.1.2 Scalability of the System

Fast growth of IoT traffic within the Internet during the last decade give rise to new challenges faced by the network operators. Currently, network operators provide services to their users using the hierarchical core network [Shah et al. 2014]. Therefore, traffic and content name resolution requests generated by a large number of mobile or IoT nodes go through the core network in order to avail these services when needed. However, a majority of CCN based IoT nodes require data located on nearby nodes. Hence, generating traffic to core network, against every content name resolution request, puts unnecessary burden over the network. Additionally, large size of an IoT network poses additional challenges with respect to scalability when name resolution is managed by the core Internet.

All these challenges suggest conventional schemes to be re-visited and redesigned. As explained in Section 2, the existing name resolution routing solutions are designed to provide support using centralized or distributed network entities in the core network. This creates scalability problems, especially for CCN based IoTs.

### 3.1.3 Control Traffic Overhead

Signalling exchange against content's information updates, and queries greatly affects the performance of a routing protocol in CCN. The number of update and query messages exchanged during name resolution determines the overhead. Distributed name resolution routing mechanisms require consistency of data at each distributed node [Elbreiki et al. 2016]. Inevitably, a significant amount of signalling messages is required to be exchanged in order to periodically refresh data located at different distributed servers, as explained in Section 2. This signalling results in an increased overhead over the network, which may affect its performance. Hence, the major design challenge for a newly designed protocol is to reduce these exchanges.

### 3.1.4 Addition and Deletion of Name Resolution Node

Name resolution based routing protocols for CCN should be able to manage the addition of new or failure of existing name resolution servers. Implicit addition of new servers or deletion of existing servers due to failure is a design challenge for new protocols.

## 4 Crumbling Walls based Name Resolution Routing For IoT Networks

To address the problem of scalability in IoT environments, a new quorum system based routing approach is discussed in this section. By using the quorum system based name resolution routing, content names can be resolved without pushing the entire traffic to core network. Thereby, the solution is scalable to use in an IoT environment with millions of nodes. The Crumbling Walls log (CWlog) [Peleq et al. 1997] is a quorum system with high availability for small architectures, and an improved availability for larger systems (O(n/logn)), as compared to other quorum based solutions [Peleg and Wool 1997]. Due to this promising feature, the CWlog quorum system is best suitable for IoT environments, where the size of the network can vary from a few nodes to millions of users. For example, an IoT network can be as small as a home networking solution, or as large as the global Internet-based IoTs.
In CCN based IoTs, an IoT node requires location of a content to make requests, hence, some name resolution servers are required that can translate content names to location addresses. As an IoT network is known to contain millions of nodes, thereby, a large number of name resolution servers are required for high availability and low

query response time. Moreover, with the increase in the size of IoT by continuous addition of new nodes, additional servers are required to be added for distribution of the growing load. With the increase in the size of networks, continuous addition of new servers is also needed to maintain an efficient response time against content queries. In this regard, addition of new servers in the CWlog quorum system is very simple, and a new server can be added with minimal overhead as compared to the other quorum based systems [Peleq et al. 1997].

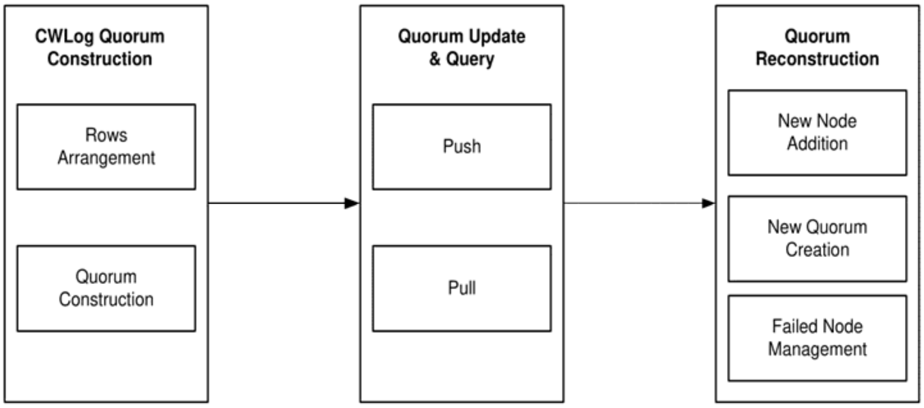


*Figure 2: Component diagram for the proposed system*

In this section, a new routing mechanism is proposed for content centric based IoT networks using the CWlog quorum system. The proposed solution contains following three components: (i) CWLog quorum construction, (ii) Quorum database update and query, and (iii) Quorum reconstruction and rearrangement. Fig. 2 shows the component diagram of the proposed system with these components. The working of each of these components is explained next in detail.

### 4.1 Network Model

A Name Resolution Server (NRS), in a CWlog quorum based content centric IoT network, contains content based location databases. It serves as the name resolution entity for resolving content name to content address queries. These NRSs are equipped with large memory, high computational power, and low processing time for efficient performance of the network. The CWlog quorum system is constructed using a number of such NRSs. Figure 3 shows our proposed model for an IoT network containing different domains and selected NRS nodes (circle nodes with numbers). A cloud between two or more NRSs represents a network consisting of many IoT nodes. Additionally, a dotted line between two NRSs shows that they are connected with each other through many IoT nodes between them. The nodes mentioned as x, y and z are IoT nodes, which may have contents to share with other nodes, or they may generate requests for content name resolution. We refer to these end nodes, and selected NRSs (labelled with numbers) throughout the text for a clear explanation of our proposed system.

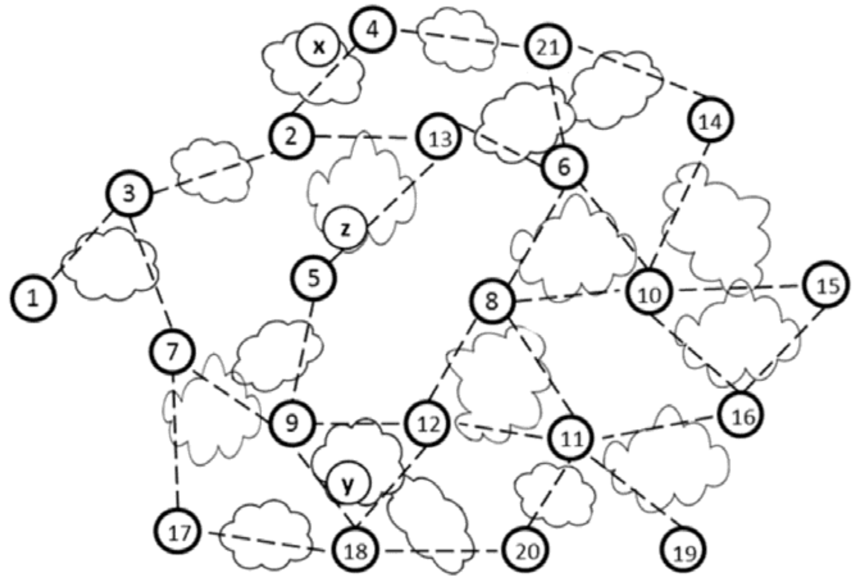


*Figure 3: Network model of a CWlog Quorum based IoT Network*

### 4.2 CWlog Quorum Construction

CWlog quorum system is constructed by arranging selected NRSs (e.g. circular nodes with integer labels in Figure 3) in the form of rows, where each row *i* can have maximum $\lfloor \log_2 2i \rfloor$ CWlog quorum system is constructed by arranging selected NRSs (e.g. circular nodes with integer labels in Figure 3) in form of rows, where each row *i* can have maximum $Q_i$ is defined as the union of complete $i^{th}$ row, and one node from every row below the $i^{th}$ row as shown in Figure 4(b). In this way, for a quorum system with *r* rows and $m_k$ elements in each $k^{th}$ row constructed for a NRS universe of size $n = \sum_{k=1}^{r} m_k$ , first quorum (e.g. $Q_1$) is the largest quorum of size ≈ $n/\log_2 n$, consisting of the complete top row and one element from each row below this row. Similarly, bottom row will create the smallest quorum of size ≈ $\log_2 n - \log_2(\log_2 n)$ consisting of all the elements of bottom row only. Moreover, a quorum based on row *i* will be of size $\lfloor \log_2 2i \rfloor + r - i$. Figure 4 shows a possible arrangement of NRSs in a CWlog quorum system in the form of rows (shown in Figure 4(a)), and the respective quorums against each row (shown in Figure 4(b)). The maximum quorum size is for $Q_1$ and $Q_2$ and the minimum quorum size is for $Q_8$. A quorum based on row 5 is highlighted in Figure 4(a), and the algorithm for quorum construction is shown in Table 1. Input of the algorithm is IoT nodes that can serve as NRSs, and it produces

| | | | |
|---|---|---|---|
| 1 | | | |
| 2 | 3 | | |
| 4 | 5 | | |
| 6 | 7 | 8 | |
| 9 | 10 | 11 | |
| 12 | 13 | 14 | |
| 15 | 16 | 17 | |
| 18 | 19 | 20 | 21 |

(a) Arrangement of nodes in crumbling walls

| |
|---|
| $Q_1$={1,2,5,6,9,12,16,19} |
| $Q_2$={2,3,5,8,10,12,15,19} |
| $Q_3$={4,5,7,9,13,15,18} |
| $Q_4$={6,7,8,10,14,16,20} |
| $Q_5$={9,10,11,14,17,19} |
| $Q_6$={12,13,14,15,21} |
| $Q_7$={15,16,17,20} |
| $Q_8$={18,19,20,21} |

(b) Nodes in each CWlog quorum

*Figure 4: Crumbling wall CWlog quorum systems construction*

---

**Algorithm 1: CWlog Quorum Construction**

---

**Input:** IoT nodes that can serve as NRS

**Output:** CWLog quorums ($Q_{1\text{-}r}$)

**Process:**

**1.** *NRS-SET* = { *NRS* nodes ($1 - n$) | arranged in decreasing number of outdegree } [Faloutsos et al. 1999]

**2.** Create Rows $R_1$.. $R_r$ **until** *NRS-SET* $\neq \emptyset$ | $SizeOf(R_i) \leq \lfloor log2i \rfloor$

**3.** $R_i = \emptyset$

**4.** $R_i = R_i \cup$ {first $\lfloor \log_2 2i \rfloor$ *nodes* $\epsilon$ *NRS-SET* }

**5.** *NRS-SET* = *NRS-SET* - $R_i$

**6.** Construct Quorums $Q_1$.. $Q_{r-1}$

**7.** $Q_i = \emptyset$

8. $Q_i = Q_i \cup R_i \cup$ one node from each Row $R_{i+1}$ to $R_r$

9. $Q_r = \emptyset \cup R_r$

---

*Table 1: Algorithm for CWLog Quorum Construction*

CWlog quorums as the output. In step-1 of Algorithm 1 nodes are first arranged in rows in decreasing number of outdegree. Inevitably, our largest quorum consists of topologically important nodes according to power-laws of the Internet defined in

[Faloutsos et al. 1999]. This ultimately results in high availability of information to nodes across different regions.

**Algorithm 2: CWlog Quorum Update and Query**

**Input:** CWlog Quorums(1 .. n), Content requester, Content provider
**Output:** Database updation/ Data retrieval
**Process:**
**Node y (as shown in Figure 3) has content (c)**
*PUSH(c)*
1. $NRSi \leftarrow$ content update request from node $y$
2. IF $NRSi \in Q_k$ AND $NRSi \notin Q_k \cap Q_j$ where $j \neq k$, $j,k \in [1 ..n]$
3. $WQ = Q_k$ // WQ is write quorum of NRSi
4. IF $NRSi \in Q_k$ AND $NRSi \in Q_k \cap Q_j$ where $j \neq k$, $j,k \in [1 ..n]$
5. $WQ = Q_k \cup \forall Q_j$
6. Update mapping $c \leftrightarrow y$ in $\forall$ *NRS nodes* $\in WQ$

**Node x (as shown in Figure 3) needs content (c) information** *PULL(c)*
1. $NRSi \leftarrow$ *content (c)* query request from node $x$
2. *IF LookUp(c)* is **true**
3. **send** mapping $c \leftrightarrow y$ to node $x$
4. ELSE
5. IF $NRSi \in Q_k$ AND $NRSi \notin Q_k \cap Q_j$ where $j \neq k$, $j,k \in [1 ..n]$
6. $RQ = Q_k$ // $RQ$ is read quorum of $NRSi$
7. IF $NRSi \in Q_k$ AND $NRSi \in Q_k \cap Q_j$ where $j \neq k$, $j,k \in [1 ..n]$
8. $RQ = Q_k \cup \forall Q_j$ // $RQ$ is read quorum
9. IF $\{\exists$ nodes $j \in RQ \mid c \leftrightarrow y$ exists in database of $j\} \neq \emptyset$
10. **send** mapping $c \leftrightarrow y$ to node $x$
11. **update** mapping $c \leftrightarrow y$ in $NRSi$

*Table 2: Algorithm for CWlog Quorum Update and Query*

### 4.3 Quorum Database Update and Query

Let an IoT node y have some contents to publish. It sends content name to location mappings to a nearest NRS using Push mechanism (defined in Table 2). Push is the process, in which content names are updated/added in write quorum of an NRS for content name to content address resolutions. Assume an IoT node has data for room temperature, it sends its content information to a nearest NRS by sending an update/add request. NRS updates its database, and share signalling messages with its write quorum Qi for data consistency. It results in the update of databases of all NRSs present in Qi. Thus, all the NRSs in the specified write quorum Qi have the same copy of content information for resolving future requests. In reference with Figure 3, node y updates its content information to the nearest quorum node i.e. NRS 18. The quorum node NRS 18 is part of quorums Q3 and Q8, as can be seen in Figure 4(b). In this case, both Q3 and Q8 form the write quorum; thereby, new information is pushed to all the members of both quorums.

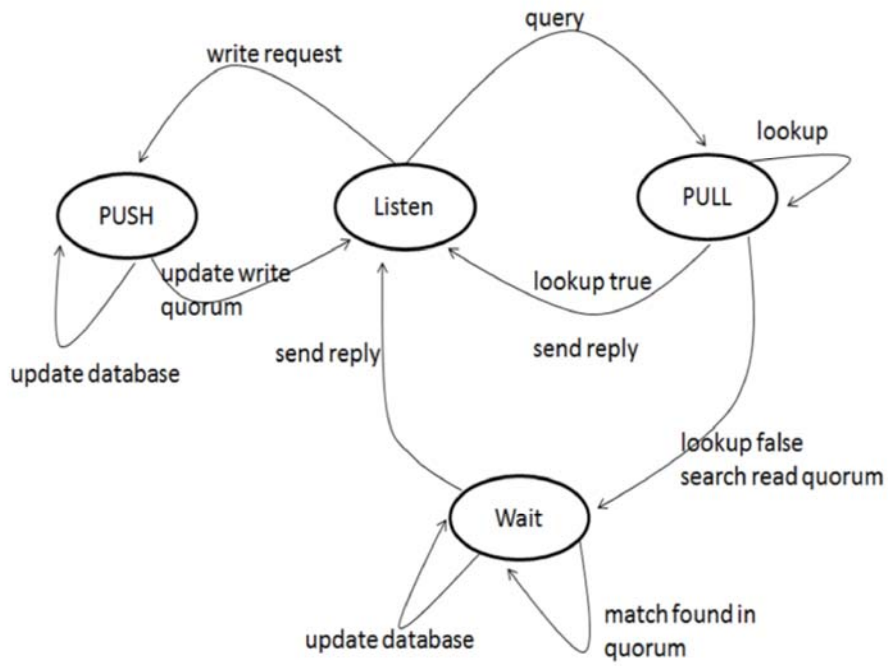


*Figure 5: Network model of a CWlog Quorum based IoT Network*

On the other hand, when a node in an IoT network needs some contents, it requests the content using Pull mechanism (defined in Table 2). In this process, a node query read quorum of a nearest NRS database with content name to get the location information of content source. Any of the nodes from read quorum having content information will respond to the content query. For example, in Figure 3, let node *x* sends query to its closest NRS (i.e. 4) about the room temperature content which was published by node *y*.

In case, NRS 4 does not have the required mapping in its database, due to the intersection property between quorums Q3 and Q8, the query is ultimately resolved by the read quorum of the former. We can see in Figure 4(b), NRS 18 is intersecting both the quorums $Q_3$ and $Q_8$, and its database has the information about the room temperature contents which were published by node y, as explained earlier. NRS 18 responds to the query, and sends the complete content information, which is eventually delivered to node x. Now, node *x* can directly send data requests to node *y* using location address. The process of receiving (read & write) requests at any given NRS node is shown with the help of a state transition diagram in Figure 5, and the corresponding algorithm is presented in Table 2.

### 4.4 Quorum Reconstruction and Rearrangement

An existing CWlog quorum system for a content centric IoT network is dynamically rearranged/reconstructed, if new NRSs are required to be added or existing NRS fails.

**Algorithm 3: CWlog Quorum Reconstruction and Rearrangement**

**Input:** CWlog Quorums, New NRS addition or existing NRS failure
**Output:** CWLog Quorums
**Process:**
*New_NRS$_i$_addition( )*
1. $NRS\text{-}SET = NRS\text{-}SET \; U \; NRS_i$ *//NRS-SET defined in Table 1*
2. $R_j \leftarrow$ *Row with node* $NRS_{i-1}$
3. $R_m \leftarrow$ *Row with node* $NRS_{i+1}$
4. *IF* $SizeOf(R_i) < \lfloor \log_2 2j \rfloor$
5. $\quad R_j = R_j \; U \; NRS_i$
6. *ELSE IF* $SizeOf(R_m) < \lfloor \log_2 2m \rfloor$
7. $\quad R_m = R_m \; U \; NRS_i$
8. *ELSE*
9. $\quad$ *Update system with new Row* $R_{j+1}$ *and new Quorum* $Q_{j+1}$ *from* $NRS_i$
10. $\quad \forall Quorums(1 .. j)$
11. $\quad\quad Q_k = Q_k \; U \; NRS_i$

*Existing_NRS$_i$_deletion( )*
1. $Q_i \leftarrow$ *Quorum of node* $NRS_i$
2. $NRS_j \leftarrow$ *any working node from* $Q_i$
3. $\forall$ *Quorums* $Q(1 .. i-1)$ *where* $NRS_i \in Q_k$
4. $\quad Q_k = Q_k \; U \, NRS_j$

*Table 3: Algorithm for CWlog Quorum Reconstruction and Rearrangement*

The size of IoT network is growing day by day. Thousands of new nodes are being added in the network and only a few leaves the network. Due to the addition of large number of nodes in some new parts of the world, new NRSs are required to be configured for load distribution and to minimize name resolution response time. For this purpose, the quorum system which is already constructed needs to be modified and rearranged. In such scenarios, the proposed system allows the addition of new servers in the existing quorums as well as the creation of new quorums. The addition of new NRS in the existing quorum or the creation of new quorum depends upon the size (width) $w_i$ of the corresponding crumbling wall, as defined in Algorithm 3 in Table 3.

Addition of new NRS in an existing quorum set or the creation of new quorum depends upon the size (width) $w_j$ of the corresponding crumbling wall (row), as defined in Table 3. If the width $w_j < \lfloor \log_2 2j \rfloor$, then the new NRS can be added to any of the two connective rows (steps 4-7 in Algorithm 3). In the other case, a new quorum will be created, and the existing quorums need to be updated, as defined in step 10 of Algorithm 3. The addition of new quorum, in this case, requires an addition of a new crumbling wall (row) at position j + 1 in the quorum system. All the quorums from 1 to j are then updated by including a working member of new row(quorum).

In case of any failure of one or many NRSs, the proposed CWlog based system can adjust the size of quorum by removing the failed NRS. In case, all NRSs of a quorum fail, then the complete quorum is removed. For a failed server in row *i* of quorum $Q_i$ , the system attempts to ensure that each row (quorum) from $Q_1$ to $Q_{i-1}$ have a live representation of $Q_i$. In this way, if the failed NRS is part of any quorum from $Q_1$ to $Q_{i-1}$, then a new live $NRS_j$ from $Q_i$ is included there. This process reduced the size of quorum $Q_i$ and all other quorums remains of the same size. Table 3 shows the algorithm for this whole process.

## 5 Performance Analysis

We analyse the performance of our name resolution based routing protocol for IoT in terms of scalability and availability.

### 5.1 The Model

A quorum system for name resolution routing is constructed from n number of NRSs arranged in r rows and each row i have $m_i$ number of servers in it. A quorum which is based on row *i* has $N_Q$ number of quorum nodes in it with $N_Q \geq m_i$.

The number of content name resolution requests to the NRS determines the load on the system. However, the proposed system uniformly distributes the load among many quorum nodes, thus reducing the load on an individual server. The load L on any quorum element e in a row *i* can be modelled as a function of probability that the row *i* is critical row. A critical row is one that has high load for name resolution requests.

$$L_e = \Pr(i)\left(1 + \frac{i-1}{m_i}\right)$$

where *Pr(i)* is the probability that row i is selected from a set of r rows in the quorum system and is critical row with maximum load.

$$\Pr(i) = \frac{1}{r}$$

Thus, the load on *e* becomes [Friedman et al. 2010]:

$$L_e = \frac{1}{r}\left(1 + \frac{i-1}{m_i}\right) \qquad (1)$$

This load can be decreased by increasing the value of *r*, i.e. adding more rows to the quorum system. However, this expressional value is maximal when $i = r$ i.e. maximum load will be observed on the nodes in the last row (last quorum) because the quorum based on the last row is the smallest one of size $\approx log_2 n - log_2(log_2 n)$.

The overhead of the proposed system can be measured for lookup overhead and the update overhead. To request contents from the network, an IoT node performs the lookup operation in the quorum so that content name can be resolved to content address. Any available copy of the content name in the quorum can be used to answer the lookup query. For performance reasons, it is generally desirable that closest copy is accessed and responds. Assuming that quorum node having closest copy with minimum response time responds first to the query, then the expected lookup overhead ($O_{Lookup}$) to find the desired content name in a quorum with $N_Q$ number of nodes can be modelled as [Peleg et al. 1995], [Bee 1999]:

$$E\left[O_{Lookup}\right] = C + \sum_{i=1}^{N_Q} Prob(i) D_i \tag{2}$$

where *Prob(i)* is the probability of retrieving the desired content name from NRS *i*, *D* is the search cost to find the content name in the database and *C* is the name resolution cost to resolve the content name to content address.

If there are *R* number of replicated content name copies in a single quorum which is being accessed for name resolution, then using combinations the probability to retrieve the content name from NRS *i* from a set of $N_Q$ servers is [Malkhi et al. 2001]:

$$Prob(i) = \frac{\binom{N_Q - i}{R - 1}}{\binom{N_Q}{R}}$$

Thus, equation 2 becomes:

$$E\left[O_{Lookup}\right] = C + \sum_{i=1}^{N_Q} \left( \frac{\binom{N_Q - i}{R-1}}{\binom{N_Q}{R}} D_i \right) \tag{3}$$

The overhead for lookup query can also be calculated using the probability that whether an IoT node has requested the same content previously or not. Let an IoT node generates *a* requests per unit time for contents and *p* is the probability that this node has requested the same content previously and already has the information of content name to content address, then the overhead generated is [Malkhi et al. 2001]:

$$O_{Lookup_Q} = a . \sum_{i=1}^{N_Q} (1 - p_i) \tag{4}$$

As the lookup request is sent to all the nodes in a quorum using a single quorum read operation, hence the overhead of lookup includes the sum of overhead for each lookup operation in the quorum.

The latency to resolve the content name to content address at an IoT node can be modelled as the sum of latencies to find the content name ($E[L_1]$) in a quorum server and to return the answer ($E[L_2]$) to the IoT content requesting node [Friedman et al. 2010], i.e.

$$E[L] = E[L_1] + E[L_2] \tag{5}$$

The latency to find the content name in a quorum server depends upon the probability of its existence in quorum and its expected lookup time if it is present there i.e.

$$E[L_1] = \prod_{i=1}^{N_Q} (P(Y_i).E[L|Y_i])$$

where, L is latency to reach a copy of content name, P(Y ) is the probability that an event Y occurs successfully and Y is the event that a required content name is found in the quorum.

The expected latency when the event $Y_i$ occurs is:

$$E[L|Y_i] = \prod_{i=1}^{N_Q} l_i$$

where $l$ is the average hops latency from requesting IoT node to the quorum node and vice versa.

$$E[L_1] = \prod_{i=1}^{N_Q} \left(P(Y_i).\prod_{i=1}^{N_Q} l_i\right)$$

latency to return the answer ($E[L_2]$) to the IoT content requesting node is:

$$E[L_2] = P(Y).l$$

Putting the values of $E[L1]$ and $E[L_2]$ in equation (5)

$$E[L] = \prod_{i=1}^{N_Q} \left(P(Y_i).\prod_{i=1}^{N_Q} l_i\right) + P(Y).l$$

For simplicity, we use $P(Y)=P$ then

$$E[L] = \prod_{i=1}^{N_Q} \left(P_i.\prod_{i=1}^{N_Q} l_i\right) + P.l \tag{6}$$

The first term on the right-hand side of equation 6 is the expected latency for all the requests sent in parallel to all the quorum nodes, while the second term is the expected latency that a content name is found in a quorum node and response is sent back to the requesting node.

The availability of the proposed system can be calculated using the failure probability of CWlog quorum systems. The failure probability ($F$) is the probability that the complete quorum system fails, and no content name resolution request can be fulfilled in the network. The availability of system will be:

$$A = 1 - F$$

Let the failure probability of a single quorum node in the quorum system is $p$ and the probability that it is working is $q$ with $p = 1 - q$, then the failure probability of crumbling walls log quorum system as discussed by [Peleg and Wool 1997] is:

$$F = \left(\frac{1}{r+1}\right)^q \sum_{i=1}^{r} (i+1)^q p^{m_i} \tag{7}$$

Assuming that the failure probability of a single quorum node $p<1/2$ then $log_2(1/p)>1$. As the number of nodes in a row $mi \geq log_2 i$ and $p^{m_i} \leq \left(\frac{1}{i}\right)^{log_2\left(\frac{1}{p}\right)}$ so equation (7) becomes [Peleg and Wool 1997], [Peleq et al. 1997]:

$$F \leq \left(\frac{1}{r+1}\right)^q \sum_{i=1}^{r} (2i)^q \left(\frac{1}{i}\right)^{log_2\left(\frac{1}{p}\right)}$$

$$F = \left(\frac{2}{r+1}\right)^q \sum_{i=1}^{r} \left(\frac{1}{i}\right)^{log_2\left(\frac{1}{p}\right)-q}$$

Putting this failure probability value in the equation for availability [Peleq et al. 1997], [Peleg and Wool 1997]:

$$A = 1 - \left(\frac{2}{r+1}\right)^q \sum_{i=1}^{r} \left(\frac{1}{i}\right)^{log_2\left(\frac{1}{p}\right)-q} \quad (8)$$

## 6 Evaluation & Results

In this section, the performance of the proposed protocol is analysed in comparison to MDHT [D'Ambrosio et al. 2011]. Simulations are carried out in NDNSim version 2.3. For simulations, we considered a scenario where the content provider was located in the core wired Internet and the CCN nodes were also wired nodes. Simulation parameters are defined in Table 4.

| Attribute | Value |
|---|---|
| Area Size | 1600 x 1600 meters |
| Number of contents | 100 |
| Total number of nodes | 600 |
| Number of content requesting nodes | 100 to 500 |
| Cache size (number of contents) | 10 |
| Maximum residence time | 8 sec |
| Simulation time | 500 sec |
| Start-up time | 15 sec |
| Simulation runs | 5 |
| Number of NRSs | 5 to 50 |

*Table 4: Simulation Parameters*

The number of content requesting nodes is kept changing from 100 to 500 and created two chains towards the content provider in the core network. Almost half of the content requesting nodes were connected to each chain towards the content provider. Some content requesting nodes were wired connected in the network through Ethernet link of data rate 100 Mbps. Some content requesting nodes were wirelessly connected in the network. The MAC layer protocol configured for wireless was IEEE 802.11b with channel data rate of 10 Mbps. The transmission range of each node in the wireless is set to 150 meters. The simulation topology is configured in a square area of 1600 × 1600 meter$^2$.

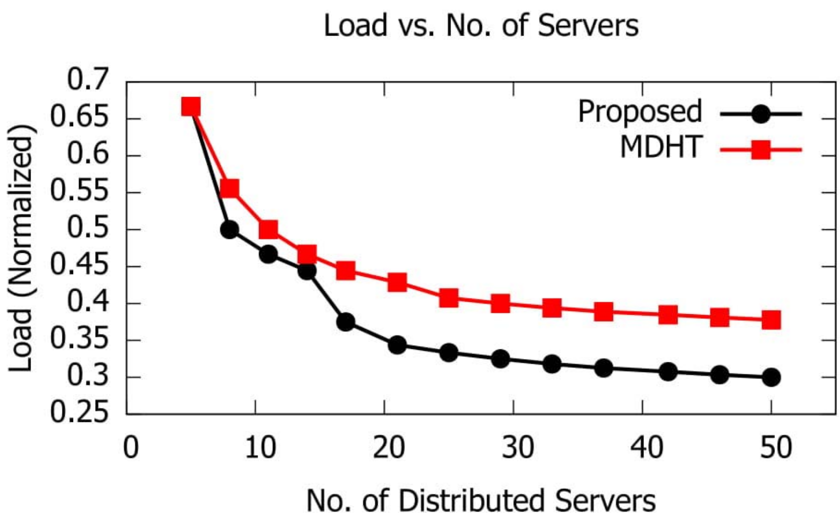


*Figure 6: Average System's load comparison*

We use following performance metrics to evaluate our proposed technique.

1. **System Load:** The number of content name resolution requests to the name resolution server determines the load on the system.
2. **Lookup Overhead:** In case the mapping is not available on a given server, amount of signalling exchange between NRSs for resolving the query is termed as Lookup Overhead.
3. **Latency or Delay**: Time required to resolve content name to content address.
4. **Availability:** Probability that the system will be available at a given time determines the availability of system.

The load on distributed name servers is shown in Figure 6. With an increase in the number of distributed servers the load for content name resolution on an individual server is decreasing. It is because, the load got distributed with an addition of every new distributed server in the proposed quorum-based routing or MDHT. However, this decrease in load is better (20% improvement for n=33) for the proposed routing as compared to the MDHT because the proposed protocol divides the NRSs into many quorums and only single quorums is accessed for any read or write operation instead of trying to find or update the content name in all the distributed servers up in the hierarchy.

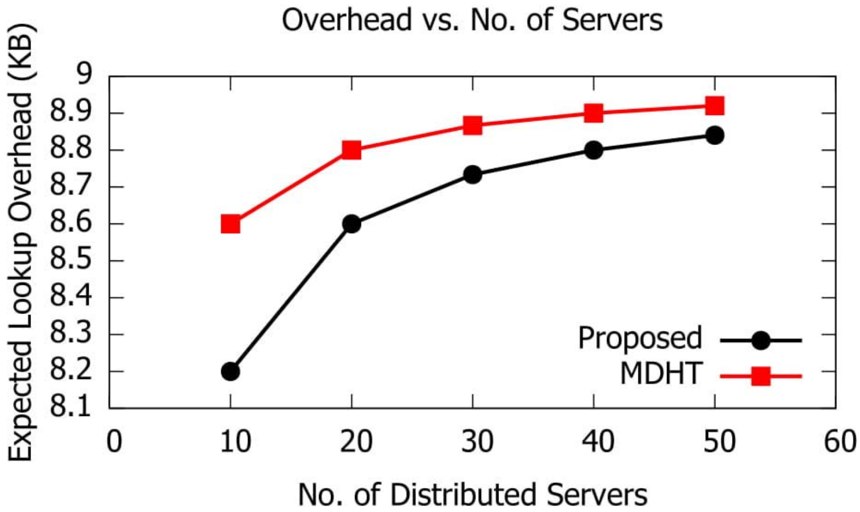


*Figure 7: Expected Lookup overhead*

The expected lookup overhead to find and resolve the content name to content address is shown in Figure 7. The overhead is calculated with varying number of distributed servers and assuming a single copy of content name is present in the quorum. Results show that the lookup overhead increases with an increase in the number of distributed servers, because with an addition of each new node in the quorum causes additional lookup operation in the quorum node. In case of the proposed routing protocol, this lookup operation is still restricted to the same quorum causing minimum increase in the overhead. On the other hand, the increase in the overhead for MDHT is high because the addition of new servers causes the lookup operation to be performed at the next higher level.

Figure 8 shows the lookup query overhead comparison for the proposed routing protocol and the MDHT. The probability p varie from 0.1 to 0.5 for 10 to 50 number of distributed servers and n/log2n number of servers in each quorum. The result shows that the increase in the lookup query overhead for the proposed routing protocol is low. It is because, an increase in the number of distributed servers causes the addition of a new quorum in the proposed system and the size of existing quorums is increased by one. As, the content name lookup query is sent only to single quorum instead of sending to all the servers, thus decreasing the lookup query overhead as compared to the MDHT.

The expected latency to resolve a content name to content address is shown in Figure 9. The probability P(Yi), used for this simulation result, is set to 0.3. It can be observed from the figure that the expected latency for the proposed protocol almost remains constant as compared to the MDHT for which it is increasing with an increase in the number of distributed servers.

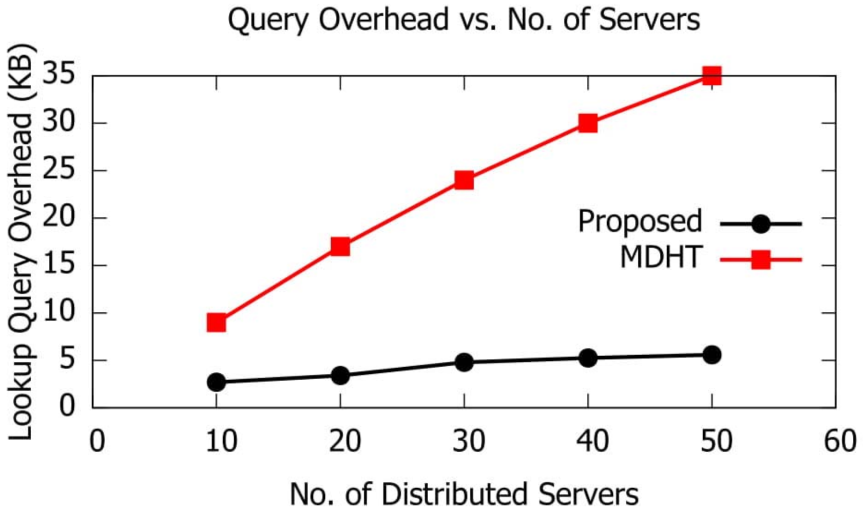


*Figure 8: Comparison of Lookup query overhead against no. of servers*

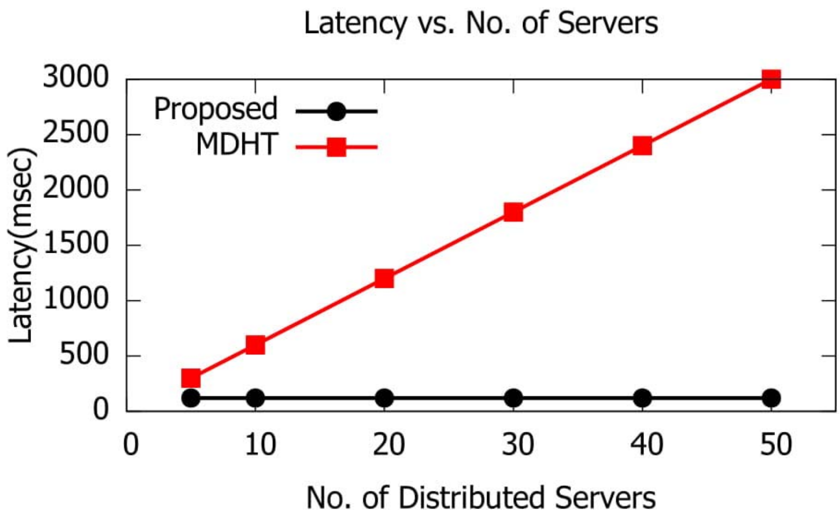


*Figure 9: Comparison of expected latency against no. of servers*

The reason for constant expected latency is the read operation that is performed by the IoT node on the same quorum instead of looking it up in the new servers. While the expected latency for MDHT increases due to lookup operation to be performed at the next higher level to find the content name.

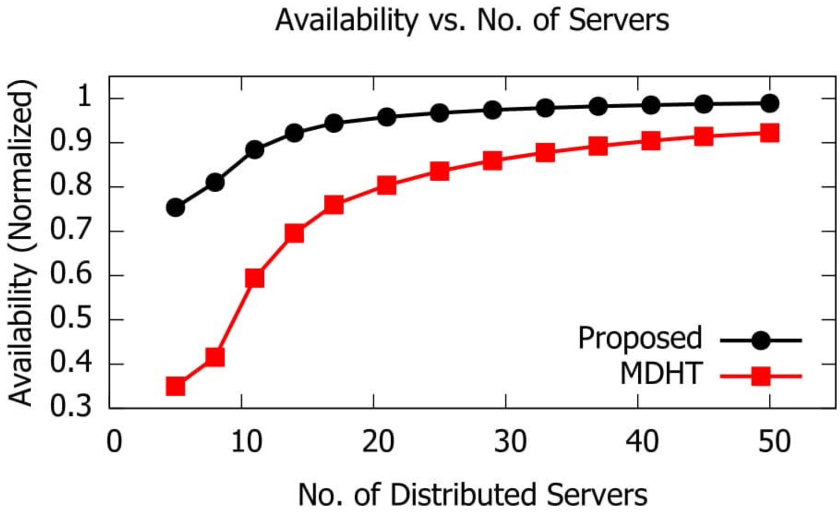


*Figure 10: Normalized Availability of system*

Figure 10 shows the system's availability comparison. The availability of both systems increases with the addition of new distributed name servers. The availability of the proposed protocol is high (11% improvement for n=33) as compared to the MDHT, because the CWlog quorum systems have very low failure probability. The failure of any distributed server does not affect the system as the replicated content name information is also present in the other nodes of the same quorum. In case of failure of all the servers in a complete row the proposed system again reconstructs the quorums without the loss of any content name information. Thus the proposed system has high availability as compared to the MDHT.

## 7 Conclusion & Future Work

Huge amount of data generated by IoT nodes may lead to problems regarding scalability and availability of information, due to read/write operations overhead, in name resolution protocols. To address these issues, in this paper, we propose a new name resolution routing protocol for the content centric Internet of Things, using crumbling walls log quorum system. In write quorum of an NRS, content name to content address mappings are published using Push mechanism, Similarly, queries regarding these mapping are resolved by the read quorum of an NRS using Pull mechanism. We evaluate the proposed mechanism against MDHT, and find that the former efficiently distribute the load on servers, with small latency, and lookup overhead. The inherent advantage of uniformly distributing the content name information across multiple quorums has also resulted in increasing the availability of the system by 11% as compared to MDHT.

In future, we intend to extend the system to handle hybrid name resolution based and name-based routing protocol in CCN-assisted IoT environments. Managing mobility of quorum nodes is another important research direction for improving performance of the proposed quorum system in mobile environments.

**Acknowledgements**

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A3B03028309) and also supported by the Soonchunhyang University Research Fund.

## References

[Baccelli et al. 2014] Baccelli, E., Mehlis, C., Hahm, O., Schmidt, T. C., & Wahlisch, M.: "Information centric networking in the IoT: experiments with NDN in the wild"; Proceedings of the 1st ACM Conference on Information-Centric Networking, (pp. 77-86), ACM, (Sep 2014).

[Bari et al. 2012] Bari, M. F., Chowdhury, S. R., Ahmed, R., Boutaba, R., & Mathieu, B.: "A survey of naming and routing in information-centric networks"; IEEE Communications Magazine, 50(12), (Dec 2012).

[Bee 1999] Bae, I. H.: "A quorum-based dynamic location management method for mobile computings"; Sixth International Conference on Real-Time Computing Systems and Applications, RTCSA'99 (pp. 398-401). IEEE (1999).

[Carzaniga et al. 2004] Carzaniga, A., Rutherford, M. J., & Wolf, A. L.: "A routing scheme for content-based networking"; INFOCOM 2004, Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies (Vol. 2, pp. 918928), IEEE, (March 2004).

[D'Ambrosio et al. 2011] D'Ambrosio, M., Dannewitz, C., Karl, H., & Vercellone, V.: "MDHT: a hierarchical name resolution service for information-centric networks"; Proceedings of the ACM SIGCOMM workshop on Information-centric networking (pp. 7-12), ACM, (Aug 2011).

[Dannewitz et al. 2010] Dannewitz, C., Golic, J., Ohlman, B., & Ahlgren, B.: "Secure naming for a network of information"; In INFOCOM IEEE Conference on Computer Communications Workshops, (pp. 1-6), IEEE, (March 2010).

[Dannewitz et al. 2013] Dannewitz, C., D'Ambrosio, M., & Vercellone, V.: "Hierarchical DHT-based name resolution for information-centric networks"; Computer Communications, 36(7), (pp. 736-749), (Apr 2013).

[Elbreiki et al. 2016] Elbreiki, W., Arlimatti, S., Hassan, S., Habbal, A., & Elshaikh, M.: "A distributed name resolution system in information centric networks"; AIP Conference Proceedings (Vol. 1761, No. 1, p. 020038), AIP Publishing, (August 2016).

[Evans 2011] Evans, D.: "The internet of things: How the next evolution of the internet is changing everything"; CISCO white paper, (pp. 1-11), (Apr 2011).

[Faloutsos et al. 1999] Faloutsos, M., Faloutsos, P., & Faloutsos, C.: "On power-law relationships of the Internet topology"; In ACM SIGCOMM computer communication review (Vol. 29, No. 4, pp. 251-262), ACM, (Aug 1999).

[Fotiou et al. 2010] Fotiou, N., Nikander, P., Trossen, D., & Polyzos, G. C.: "Developing information networking further: From PSIRP to PURSUIT"; International Conference on Broadband Communications, Networks and Systems (pp. 1-13) Springer, Berlin, (Oct 2010).

[Friedman et al. 2010] Friedman, R., Kliot, G., & Avin, C.: "Probabilistic quorum systems in wireless ad hoc networks"; ACM Transactions on Computer Systems (TOCS), 28(3), 7, ACM, (Sep 2010).

[Garcia 2014] Garcia-Luna-Aceves, J. J.: "Name-based content routing in information centric networks using distance information"; Proceedings of the 1st ACM Conference on Information-Centric Networking (pp. 7-16), ACM, (Sep 2014).

[Jacobson et al. 2009] Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., & Braynard, R. L.: "Networking named content"; Proceedings of the 5th international conference on Emerging networking experiments and technologies, (pp. 1-12), ACM, (Dec 2009).

[Jmal et al. 2017] Jmal, R., & Fourati, L. C.: "An OpenFlow architecture for managing content-centric-network (OFAM-CCN) based on popularity caching strategy"; Computer Standards & Interfaces, 51, (pp. 22-29), (Mar 2017).

[Koponen et al. 2007] Koponen, T., Chawla, M., Chun, B. G., Ermolinskiy, A., Kim, K. H., Shenker, S., & Stoica, I.: "A data-oriented (and beyond) network architecture"; ACM SIGCOMM Computer Communication Review (Vol. 37, No. 4, pp. 181-192), ACM, (Aug 2007).

[Lagutin et al. 2010] Lagutin, D., Visala, K., & Tarkoma, S.: "Publish/Subscribe for Internet: PSIRP Perspective"; Future internet assembly, 84, (Apr 2010).

[Malkhi et al. 2001] Malkhi, D., Reiter, M. K., Wool A., & Wright, R. N.: "Probabilistic quorum systems"; Information and Computation, Vol. 170, (pp 184-206), (2001).

[Peleq et al. 1997] Peleg, D., & Wool, A.: "Crumbling walls: A class of practical and efficient quorum systems"; Distributed Computing, 10(2), (pp. 87-97), Springer, (Feb 1997).

[Peleg and Wool 1997] Peleg, D., & Wool, A.: "The availability of crumbling wall quorum systems"; Discrete applied mathematics, 74(1), (pp. 69-83), Elsevier, (Apr 1997).

[Peleg et al. 1995] Peleg, D., & Wool, A.: "The availability of quorum systems"; Information and Computation, 123(2), (pp. 210-223), (Dec 1995).

[Polyzos et al. 2015] Polyzos, G. C., & Fotiou, N.: "Building a reliable internet of things using information-centric networking"; Journal of Reliable Intelligent Environments, 1(1), (pp. 47-58), Springer, (Jul 2015).

[Shah et al. 2014] Shah, P. A., Hasbullah, H. B., Lawal, I. A., Aminu Mu'azu, A., & Tang Jung, L.: "A TOTP-based enhanced route optimization procedure for mobile IPv6 to reduce handover delay and signalling overhead"; The Scientific World Journal, 2014.

[Song et al. 2013] Song, Y., Ma, H., & Liu, L.: "Content-centric internetworking for resource-constrained devices in the Internet of Things"; IEEE International Conference on Communications (ICC), (pp. 1742-1747), IEEE, (June 2013).

[Torres et al. 2015] Torres, J., & Duarte, O. C. M.:"CRoS-NDN: Controller-based routing strategy for named data networking", 2015, https://www.gta.ufrj.br/ftp/gta/TechReports/ToDu14a.pdf.

[Waltari et al. 2016] Waltari, O., & Kangasharju, J.: “Content-centric networking in the internet of things”; 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), (pp. 73-78), IEEE, (Jan 2016).

[Zhang et al. 2010] Zhang, L., Estrin, D., Burke, J., Jacobson, V., Thornton, J. D., Smetters, D. K., & Papadopoulos, C.: “Named data networking (ndn) project”; Relato´rio T´ecnico NDN-0001, Xerox Palo Alto Research Center-PARC, (Oct 2010).