Scholars Journal of Engineering and Technology
OPEN ACCESS
Abbreviated Key Title: Sch J Eng Tech
ISSN 2347-9523 (Print) | ISSN 2321-435X (Online)
Journal homepage: https://saspublishers.com/journal/sjet/home

A Survey: Routing Schemes in Information-Centric Networks (ICN)

Ghassan Jaber[1*], Patsei Natallia Vladimirovna[2] and Fatima Rahal

[1]PhD Student, Belarusian State Technological University, улица Свердлова 13А Минск BY, 220006, Belarus
[2]PhD Engineering, Associate Professor, Assistant Professor, Department of Information systems and technologies, Belarusian State Technological University, улица Свердлова 13А Минск BY, 220006, Belarus

DOI: 10.36347/sjet.2019.v07i08.004 | **Received:** 18.08.2019 | **Accepted:** 26.08.2019 | **Published:** 30.08.2019

***Corresponding author:** Ghassan Jaber

Abstract **Review Article**

Information-Centric Networking (ICN) proposes a new future communication model, which is set to replace the current host-centric internet architecture. From the ICN perspective, the goal is to shift towards a content centric model in order to better suit today is needs as effective content distribution and mobility. Content-based routing and caching are core challenges in the research community. This paper describes data routing mechanisms in major architectures proposals.
Keywords: Information-Centric Networking, Routing, Naming Scheme.

INTRODUCTION

Information-centric networking (ICN) is a new research topic in recent years. The current Internet architecture, which is built and designed for of a host-to-host communications model, has many shortcomings and adds some complexity, as it is experiencing a vast growth in network traffic [1]. By time, the demand of the network end-users on accessing and delivering high volume of digital contents like movies from YouTube, high definition Video on Demand (VoD), time-shift televisions and photos etc. is increasing in a tremendous manner. ICN is a future architecture that aims to cache content objects in the network nodes or routers and allow the access to these contents from any location by ensuring in-network storage for caching contents, decoupling the content from the host address. The decoupling between publisher and subscriber removes the role of IP address, which works only as an identifier and locator enabling multiparty communication through replication [2].

Various projects like DONA, NDN, PURSUIT, SAIL, COMET, CONVERGENCE, MobilityFirst, PSIRP, CBCB, NetInf, KBN presented proposals in the ICN field in order to suit the new requirements including the effective distributions of contents.

ICN Projects

In this paper we survey the routing schemes in these ICN architectures mentioned above and proposes a new schema in this field - semantic routing scheme (SICN).

DONA

The name resolution is established by the route-by-name paradigm spread above the IP layer, and it is provided by at least one logical specialized interconnected servers or name resolution entities called Resolution Handlers (RHs) at each (Autonomous System) AS which are organized hierarchically. The name resolution is hierarchical based on top of the routing relations resulting from the interconnection between RHs. name resolution and data routing ensures obeying routing policies between AS’s. In order to make an information object available, the publisher (principal) sends a REGISTER message with the object’s name to its local RH, who stores a pointer to the principal. The RH then propagates this registration to the RHs in its parent and peering domains, following the established routing policies, causing each intermediate RH to store a mapping between the object’s name and the address of the RH that forwarded the registration. As a result, registrations are replicated in RHs all the way up to the tier-1 providers and, since all tier-1 providers are peers with each other, RHs located at tier-1 providers are aware of all registrations in the entire network. Publishers can also issue wildcard REGISTER messages to notify the RH hierarchy that they can provide all possible data items for a specific principal.

The interface only two operations: *FIND* (*P*: *L*) and *REGISTER* (*P*:*L*) where P is the ciphered hash of the public key of the content owner, and L identifies uniquely one of the contents respecting the same owner. *FIND* (*P*: *L*) operation is used to locate the object named *P*: *L*, whereas *REGISTER* (*P*:*L*) establish needed states in the RHs to route following *FIND* messages effectively. Routing between the RHs occurs directly on the name. When a *FIND* message is forwarded, the hop-by-hop domain- level address can follow it. As the *FIND* message is resolved, content will be sent to the client over the inverse of the followed path or forwarded directly to the client. Alternatively, IP routing could be used by DONA to return found content to the client [3].

This occurs as follows: the subscriber sends a FIND message to its local RH to find an item location. RH in its turn also propagates this message to its parent respecting its routing policies, till finding a matching registration entry.

NDN

In NDN there are two key messages exchanged: INTEREST and DATA. Subscribers issue INTEREST messages to request information objects. INREREST message will broadcast over all available connections and they return in the form of DATA messages. Both types of message carry the name of the requested/transferred information object and both identify the content being exchanged by name so are routed using a *route-by-name* paradigm. When the subscriber issues Interest for a content, any NDN node having or caching the main or copy of that content, will respond with the corresponding Data to satisfy the interest identified by name. In NDN there are a strict flow balance between Interest and Data due to using of a one-to-one mapping which means that Data is sent only in response to an Interest and that Interest is consumed by the Data [4]. An NDN node holds the tables: The *Forwarding Information Base* (FIB), the *Pending Interest Table* (PIT). It forms the NDN forwarding engine.

The FIB maps information names to the output interface(s) that will be used to forward INTEREST messages to the suitable data sources.

The PIT supports the incoming interface(s) from which INTEREST messages have arrived.

Content store (CS) which is used for caching data passes through the Content Router (CR) [5].

NDN ensures efficient routing depending on the component structure of names. It carries out prefix grouping, loop free forwarding for routing table compression, and reduced messaging overhead.

When an INTEREST arrives, the CR excerpt the data name and search for data in its CS. If a data name that matches the requested prefix is found, it is directly sent back through the incoming interface in a DATA message and the INTEREST is discarded. Else, the router executes a longest prefix match on its FIB to know where to forward the interest. If an entry is discovered in the FIB, the router records the INTEREST's arriving interface in the PIT and forwards the INTEREST to the CR pointed by the FIB [6].

PURSUIT

Name resolution in PURSUIT occurs by the rendezvous function, which is a collection of *Rendezvous Nodes* (RNs). The *Rendezvous Network* (RENE) implemented as a hierarchical Distributed Hash Table (DHT) [7, 8]. When a publisher wants to publish an information object, it issues a PUBLISH message to its local RN which is routed by the DHT to the RN assigned with the corresponding scope ID. When a subscriber releases a SUBSCRIBE message for the same information object to its local RN, it is routed by the DHT to the same RN. The RN then instructs a *Topology Manager* (TM) node to create a route connecting the publisher with the subscriber for data delivery. The TM sends a route to the publisher in a START PUBLISH message, which finally uses this route to send the information object via a set of *Forwarding Nodes* (FNs). The TM nodes in PURSUIT jointly implement the topology management function by executing a distributed routing protocol to discover the network topology. The NDN project is developing an open shortest path first (OSPF) like routing protocal for named data, called OSPF for populating and updating the routing table. The actual delivery paths are calculated upon request by the rendezvous function as a series of links between FNs and encoded into source routes using a technique based on Bloom filters [9]. Specifically, each network node assigns a tag as a long bit string produced by a set of hash functions, to each of its outgoing links, and advertises these tags via the routing protocol. A path through the network is then encoded by ORing the tags of its constituent links and the resulting Bloom filter is included in each data packet. When a data packet arrives at a FN, the FN simply ANDs the tags of its outgoing links with the Bloom filter in the packet; if any tag matches, then the packet is forwarded over the corresponding link [10]. In this manner, the only state maintained at the FNs is the link tags. Multicast transmission can be achieved by simply.

Encoding the entire multicast tree into a single Bloom filter. Subsequent packets belonging to the same information object can be individually requested by the subscriber using the notion of *Algorithmic IDs*, i.e., packet names generated by an algorithm agreed by the communicating entities. These requests are forwarded similarly to data packets, using reverse Bloom filters calculated by the TM to bypass the

RENE. This allows the realization of transport layer protocols, e.g., via a sliding window of pending requests.

Name resolution and data routing are decoupled in PURSUIT, since the RENE performs name resolution, while data routing is organized by the TMs and executed by the FNs. While name resolution can be time consuming, especially since DHT routing does not follow the shortest paths between the communicating nodes, data forwarding can take place at line speeds, without placing any state at the FNs. Furthermore, the separation of routing and forwarding allows the TMs to calculate paths using complex criteria (e.g., load balancing), without requiring signaling to the (stateless) FNs. On the other hand, the topology management and forwarding functions as described are only adequate for the intra-domain case and need to be extended (e.g., with label switching) for the inter-domain level.

SAIL

In SAIL name resolution and data routing could be decoupled, coupled, or hybrid. In the decoupled case, a *Name Resolution System* (NRS) maps object names to locators which will arrive the corresponding information object, such as IP addresses. The NRS is some form of DHT, either a multilevel DHT [13]. In the multilevel DHT solution, a global NRS treats the resolution of the A part and concerning, the handling of resolution of the L part, each authority keeps its own local NRS to achieve this. A publisher sends a PUBLISH message with its locator to the local NRS to provide an information. NRS will then store the L to locator mapping. After that, all the L parts for the same authority A will be grouped into a Bloom filter, and sends a PUBLISH message to the global NRS. The authority A, the Bloom filter and the local NRS will be stored by global NRS, replacing any previous such mapping. Whenever there is a subscriber interest in an information, global NRS forwards a GET message to its local NRS which refers to the global NRS to return a locator for the object. At last, returned locator is used to send a GET message from the subscriber sends to the publisher, and the publisher sends a DATA message in response to the information object.

In the coupled case, similar to NDN, a routing protocol is used to advertise object names and populate the routing tables of *Content Routers* (CRs). A subscriber sends a GET message to its local CR, which propagates it hop-by-hop towards the publisher or a cache. When the information object is found, it is returned by a DATA message, reversing the path taken by the GET message. The difference between NDN and SAIL in this case is that in NDN pointers left in CRs are used for the return path, while in SAIL the GET messages collect routing directions during their path and are reversed at the publisher or cache to arrive the subscriber.

Concerning the hybrid mode, routing in SAIL could mix between hop-by-hop and partial paths. The NRS returns partial locators (*routing hints)* to direct a GET message in one or multiple directions where more information of the asked information object may exist. Thus, in this case, a GET message with some routing hints will go first from the NRS to reach the nearness of the requested information object, and then uses name-based routing information saved in the CRs to arrive. Otherwise, a GET message can begin with the name-based routing information stored in the CRs and consults the NRS for more routing hints if a CR does not possess enough information to forward it.

COMET

The approaches used in COMET may be coupled or decoupled. In the coupled one, the publisher sends a REGISTER message to its local CRS node to publish information. Local CRS node will then produce a name for the information and saves the original location of the information as the IP address of the publisher. PUBLISH messages will then spread the information in the AS hierarchy, and thus each parent CRS ends up with a pointer to its child CRS that sent the PUBLISH message. The publisher could put boundaries to the spread of this information to a specific area, for example to an IP prefix, and thus PUBLISH messages may not arrive to the Tier-1 provider. An interested subscriber in some information releases a CONSUME message to its local CRS, which also spreads in the CRS hierarchy to arrive a CRS that has information about that name. Here also, the subscriber may put boundaries to the spread of the information to a specific area or even could eliminate specific areas from this spread. If there is matching [8], the CONSUME message follows the pointers in the CRSs to arrive the original publisher. As the CONSUME message propagates from the subscriber to the publisher, each CRS installs forwarding state at the *Content- aware Routers* (CaRs) of each intermediate AS, pointing back towards the subscriber. Thus, the publisher can send the data to the subscriber by using these pointers.

In coupled approach, COMET is similar to DONA in name resolution and to NDN in data routing, but also differs from them in some important aspects. concerning name resolution, in COMET the PUBLISH messages are only propagated to parents and not to peering AS's to reduce the state kept at CRSs. This leads to these issues:

- if a CONSUME message arrives a tier-1 provider and no matching occurs, then it must be disseminated to all other Tier-1 providers to find a match exists as all tier-1 providers are peers
- Name resolution and data routing (which are coupled) do not employ peering links, thus there is need for more signaling to switch to

peering paths if available [14].

Concerning the difference between data routing in NDN and in COMET is that in NDN both name resolution and data routing use the same CRs, whereas in COMET name resolution uses the CRSs while data routing uses the CaRs, which ensures that CRSs in each AS have more flexibility in finding the most preferable paths between the available CaRs of that AS. In the decoupled approach in COMET, the CRS system shares DNS with that the CRSs divide the object namespace among themselves hierarchically in a fixed manner. So if a publisher wants to publish certain information, only a REGISTER message to its local CRS is sent, and it is not spread further because it must belong to the namespace assigned to that CRS. When an interested subscriber in a certain information releases a CONSUME message, this is determined by the root CRS to a pointer towards the publisher's CRS. The subscriber's CRS gets the location of the publisher by contacting the publisher's CRS to get the as its IP address. Then the subscriber's *Path Configurator* (PC) consults the publisher's PC (shown co-located with the CRS nodes for simplicity) to ask for a source route from the subscriber to the publisher. This source route is returned to the subscriber, which uses it to request information; the publisher to return the information uses its reverse. There are also some boundaries in COMET's decoupled approach has some as in DNS as the location-dependence of names because of the fixed assignment of namespace areas to network areas.

CONVERGENCE

The CONVERGENCE architecture, shares many similarities with NDN; as it was an adjustment to the prototype of NDN [15]. When Subscribers want to request an information, they issue INTEREST messages, which are sent hop-by-hop by *Border Nodes* (BNs) to publishers or *Internal Nodes* (INs) where it will be cached. Publishers respond with DATA messages, which reverse the path. To minimize the state requirements at the BNs, CONET differs from NDN in three issues:

- BNs keep name- based routing information for a small number of advertised name prefix, which operates their routing table like a route cache. If an INTEREST message cannot be forwarded because there is no routing information for the corresponding name, the BN contacts an external *Name Resolution System* (NRS) as DNS, to know how to forward the INTEREST.
- There is no need to keep the pointers at BNs because while INTEREST messages are spread they collect the network addresses of the BNs they pass, so the publisher to route the DATA message that crosses the reverse path of the reversing information.
- The path between two BNs could include multiple hops, e.g., via IP routers, so there is need for BNs to be directly connected, thus their designation as *border* nodes. Hence, BNs map names to network as IP addresses, rather than to interfaces. Which is CRs in NDN.

In CONVERGENCE, name resolution and data routing are coupled, as the path of DATA message is the reverse of the path of the corresponding INTEREST message. However, each step of this path may not be a one hop but an entire IP path, thus the path segments between BNs, which an INTEREST message and its corresponding DATA message are not necessarily symmetric. If a suitable path is not found at some BN, NRS is used. The details of the NRS used have not been defined by the CONVERGENCE project. The name-based routing tables at BNs may also be partially filled without consulting the NRS, by using a routing protocol for name prefixes as OSPF, similar to the used in NDN.

MobilityFirst

All communication in MobilityFirst starts with GUIDs, which are translated to network addresses in one or more steps, by a Global *Name Resolution Service* (GNRS). If a publisher wants to publish some information to the network, it registers the GUID with its network address in the GNRS. A GUID is mapped via hashing to a set of GNRS server addresses, which are contacted using regular routing [16]. When a subscriber requires certain information, it sends a GET message involving the GUID of the requested object, along with its own GUID for the response, to its local *Content Router* (CR). The CR can only route based on actual network addresses, as IP addresses, thus, it asks the GNRS for a mapping between the destination GUID and one or more network addresses. The GNRS replies with many network addresses and may send a source route, a partial source route and/or intermediate network addresses. The CR chooses one of these network addresses adds it to the GET message, which it then forwards using the regular routing tables in the CRs. The GET message includes both the destination GUID and the destination network address, and any CR along the path can consult the GNRS to receive an updated list of network addresses for the destination GUID if, for example, due to mobility the GET message cannot be delivered to the publisher. The publisher sends its response to the subscriber's GUID, using the same procedure.

The resulting name resolution and data routing process is a hybrid between IP routing and name-based routing. The actual routing is performed based on network addresses, with the GNRS only used to map GUIDs to network addresses. For less dynamic services, MobilityFirst can translate each GUID to a network address once, as with DNS, and operate based on network addresses only, ignoring the GUID. For more dynamic services, the GUID may be translated multiple times; the first router (optionally, others too) asks the GNRS for the network addresses bound to a given GUID and makes forwarding decisions based on the reply from the GNRS. Forwarding can thus be “fast path”, when the GNRS is bypassed, or “slow path”, when routers (re-)consult the GNRS in order to obtain an updated list of network addresses. This late binding or re-binding is especially useful for mobile destinations. Note that each message is delivered separately, i.e., the GET message and the information object sent in response to it are individually routed based on their destination GUIDs, therefore name resolution and data routing are decoupled in MobilityFirst.

CCN

In CCN, NDOs are published at nodes, and routing protocols are used to propagate information about NDO location. Routing in CCN can leverage aggregation through a hierarchical naming scheme. NDO security is achieved through public key cryptography [17]. Trust in keys could be ensured by many ways a PKI-like certificate chain based on the naming hierarchy, or information provided by a friend. The interested requests for an NDO are sent to a publisher location. A CCN router keeps an outstanding interest table (PIT) for outstanding forwarded requests, which enables request aggregation; that is, a CCN router would normally not forward a second request for a specific NDO when it has recently sent a request for that particular NDO. The PIT maintains state for all interests and maps them to network interface where corresponding requests have been received from. Data is then routed back on the reverse request path using this state. CCN supports *on-path caching*: NDOs a CCN router receives (in responses to requests) can be cached so that subsequent received requests for the same object can be answered from that cache. From a CCN node’s perspective, there is balance of requests and responses; that is, every single sent request is answered by one response (or no response). CCN nodes can employ different *strategies* for requests (re-) transmission pace and interface selection depending on local configuration, observed network performance, and other factors. The NDN project advances the CCN approach. It provides a topology-independent naming scheme and is exploring greedy routing for better router routing scalability.

CBCB

CBCB has a publish/subscribe architecture. It ensures routing of “publish” messages by content names that is on attribute-value pairs. A CBCB router have two protocols: Broadcast routing protocol and Content-based routing protocol

The broadcast routing protocol uses the network topology information to ensure loop-free routing paths. Publishers publish their content using messages and broadcast the messages over the broadcast tree rooted at them. The content- based routing protocol prunes branches in the broadcast tree according to the predicates (interest) declared by the nodes, to ensure delivery of a published message to only those hosts that have expressed interest in that message. A router maintains a content-based forwarding table, where each interface i_k is mapped with a predicate p_k. A router forwards a message to interface i_k if the message’s set of attribute-value pairs satisfy predicate p_k. The predicates in the routing table are constructed and updated using two mechanisms: receiver advertisements (RAs) and sender requests (SRs)/update replies (URs).

The routers in the network periodically issue predicates as RAs to push their interest into all potential senders in the network using the broad- cast tree rooted at the issuer [18].

The routers to pull content-based addresses from the other routers and update their routing tables use sRs/URs. A router broadcasts an SR and each router on the broadcast tree that receives the SR sends a UR back to the issuing router. The leaf routers of the broadcast tree include their content-based address in the UR. Other non-leaf routers accumulate all the URs they receive, add their content-based address to the set, perform logical OR operation on them to construct their UR, and send it to the interface where the SR originally arrived. The original issuer of the SR updates its routing table entries using the URs it receives through its interfaces.

NetInF

NetInf uses a multilevel DHT-based name resolution service called MDHT [12] that provides name-based any cast routing. MDHT is a topologically embedded multilevel, nested, hierarchical DHT that utilizes locality in request patterns to minimize intra-AS routing latency. For instance if three DHTs are nested in the access node (AN), point of presence (POP), and autonomous system (AS) levels, respectively. Each of these DHTs (DHT areas) can run its own DHT algorithm, and any node can take part in multiple DHTs. Intra-area routing and forwarding is done according to the rules of the local DHT algorithms. Inter-area routing is done by finding a node in the local DHT that also takes part in the next higher level DHT.

Concerning The registration process for content X, Host T_k registers content X at three different levels: AN, POP, and AS. The AN stores two mappings: the first one says that content X belongs to host T_k, and the second one says that host T_k can be found at address k, which can be an IP address or a private address to access node C. POP and AS level DHTs map the content X to the access node C. Concerning the name resolution and data transmission path for content X. Host T_o looking for content X, first looks it up at its local AN, if it is not found then at its local POP, and after that at the AS level DHT. If the lookup is unsuccessful at the AS level, T_o looks up the name in the Resolution Exchange (REX) system, which is an independent entity responsible for managing registration, updates, and aggregation of names on a global level. Aggregated bindings generated by the REX system are cached by the AS level DHTs to reduce load on the REX system.

These ICN projects have tried to design innovative information-centric networking (ICN) trying to shift from host-centric end-to-end communication to requester-driven content retrieval. Despite the potential advantages of ICN proposals, several significant research challenges remain to be addressed before, including consistent routing, local cached content, privacy, security and trust.

CONCLUSION

The study has demonstrated a focused survey in ICN as it relates to routing. There is a real need to provide a new internet architecture to meet the increasing demand of Internet. In this regard, ICN became a promising future architecture that meet the future requirements of the high growing numbers of users who are interested in the contents regardless of their location on the network However, ICN is still in its developmental stages. Thus, several proposals were presented, and analyzed.

REFERENCES

1. Carofiglio G, Morabito G, Muscariello L, Solis I, Varvello M. From content delivery today to information centric networking. Computer Networks. 2013 Nov 13;57(16):3116-27.
2. Ahlgren B, Dannewitz C, Imbrenda C, Kutscher D, Ohlman B. A survey of information-centric networking. IEEE Communications Magazine. 2012 Jul 6;50(7):26-36.
3. Koponen T, Chawla M, Chun BG, Ermolinskiy A, Kim KH, Shenker S, Stoica I. A data-oriented (and beyond) network architecture. ACM SIGCOMM Computer Communication Review. 2007 Oct 1;37(4):181-92.
4. Jacobson V, Smetters DK, Briggs NH, Plass MF, Stewart P, Thornton JD, Braynard RL. VoCCN: voice-over content-centric networks. InProceedings of the 2009 workshop on Re-architecting the internet 2009 Dec 1 (pp. 1-6). ACM.
5. Misra S, Tourani R, Majd NE. Secure content delivery in information-centric networks: Design, implementation, and analyses. InProceedings of the 3rd ACM SIGCOMM workshop on Information-centric networking 2013 Aug 12 (pp. 73-78). ACM.
6. Wang L, Hoque AK, Yi C, Alyyan A, Zhang B. OSPFN: An OSPF based routing protocol for named data networking. Technical Report NDN-0003; 2012 Jul 25.
7. Rajahalme J, Särelä M, Visala K, Riihijärvi J. On name-based inter-domain routing. Computer Networks. 2011 Mar 10;55(4):975-86.
8. Xylomenos G, Ververidis CN, Siris VA, Fotiou N, Tsilopoulos C, Vasilakos X, Katsaros KV, Polyzos GC. A survey of information-centric networking research. IEEE Communications Surveys & Tutorials. 2013 Jul 19;16(2):1024-49.
9. Bloom BH. Space/time trade-offs in hash coding with allowable errors. Communications of the ACM. 1970 Jul 1;13(7):422-6.
10. Jokela P, Zahemszky A, Esteve Rothenberg C, Arianfar S, Nikander P. LIPSIN: line speed publish/subscribe inter-networking. ACM SIGCOMM Computer Communication Review. 2009 Aug 16;39(4):195-206.
11. Lagutin D, Visala K, Tarkoma S. Publish/Subscribe for Internet: PSIRP Perspective. Future internet assembly. 2010 Apr;84.
12. Fotiou N, Nikander P, Trossen D, Polyzos GC. Developing information networking further: From PSIRP to PURSUIT. InInternational Conference on Broadband Communications, Networks and Systems 2010 Oct 25 (pp. 1-13). Springer, Berlin, Heidelberg.
13. D'Ambrosio M, Dannewitz C, Karl H, Vercellone V. MDHT: a hierarchical name resolution service for information-centric networks. InProceedings of the ACM SIGCOMM workshop on Information-centric networking 2011 Aug 19 (pp. 7-12). ACM.
14. Chai WK, Wang N, Psaras I, Pavlou G, Wang C, De Blas GG, Ramon-Salguero FJ, Liang L, Spirou S, Beben A, Hadjioannou E. Curling: Content-ubiquitous resolution and delivery infrastructure for next-generation services. IEEE Communications Magazine. 2011 Mar 7;49(3):112-20.
15. Salsano S, Detti A, Cancellieri M, Pomposini M, Blefari-Melazzi N. Transport-layer issues in information centric networks. InProceedings of the second edition of the ICN workshop on Information-centric networking 2012 Aug 17 (pp. 19-24). ACM.
16. Vu T, Baid A, Zhang Y, Nguyen TD, Fukuyama J, Martin RP, Raychaudhuri D. Dmap: A shared hosting scheme for dynamic identifier to locator mappings in the global internet. In2012 IEEE 32nd international conference on distributed computing systems 2012 Jun 18 (pp. 698-707). IEEE.
17. Dannewitz C, Golic J, Ohlman B, Ahlgren B. Secure naming for a network of information. In2010 INFOCOM IEEE conference on computer communications workshops 2010 Mar 15 (pp. 1-6). IEEE.
18. Carzaniga A, Rutherford MJ, Wolf AL. A routing scheme for content-based networking. InIEEE INFOCOM 2004 2004 Mar 7 (Vol. 2, pp. 918-928). IEEE.