IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Survey on Approaches of Information Centric Networks

Mohamed Koroma[1] (PHD Candidate)

Lecturer: Njala University

Department of Computer Science & Information Technology, School of Technology

Michael Komba Tommy[2]

Lecturer: Njala University

Department of Computer Science & Information Technology, School of Technology

John Mambu Koroma[3]

Lecturer: Njala University

Department of Physics & Basic Science, School of Technology

Mohamed Sheriff Hull[4]

Lecturer: Freetown Polytechnic

Electrical & Electronics Department

King David Kamara[5]

Lecturer: Freetown Polytechnic

Computer Science Department

Abstract: Information-Centric Networking (ICN) proposes a future Internet architecture that revolves about the contents being exchanged rather than the communication of hosts and network devices. This paradigm shift is caused by the tremendous growth of information on the Internet and the increased demands for data access. The ICN approach is being explored by several research projects. We described design choices and features of proposed ICN architectures, focusing on the following main components: named data objects, naming and security, routing and transport, and caching. The main objective of this survey is to help readers to become familiar with the transformation of these architectures.

Keywords: Information centric networking, approaches, architecture, comet, convergence

I. INTRODUCTION

Information-centric networking (ICN) is an approach to evolve the Internet infrastructure away from a host-centric 4 paradigm based on perpetual connectivity and the end-to-end principle, to a network architecture in which the focal point is named information (or content or data). In this paradigm, connectivity may well be intermittent, end-host and in-network storage can be capitalized

upon transparently as bits in the network and on data storage devices have the same value, mobility and multi access are the norm and any cast, multicast and broadcast are natively supported. Data becomes independent from location, application, storage, and means of transportation, enabling in-network caching and replication. The expected benefits are improved efficiency, better scalability with respect to information/bandwidth demand and better robustness in challenging communication scenarios. In Information-centric networking the cache is a network level solution, and it has rapidly changing cache states, higher request arrival rates and smaller cache sizes. Information-centric networking caching policies should be fast and lightweight.

ICN proposes a future Internet architecture that revolves about the contents being exchanged rather than the communication of hosts and network devices. This paradigm shift is caused by the tremendous growth of information on the Internet and the increased demands for data access. Many research projects have proposed different ICN approaches over the past few years. Therefore, this paper gives an overview of the ICN concept, and will provide a detailed summary of the recent

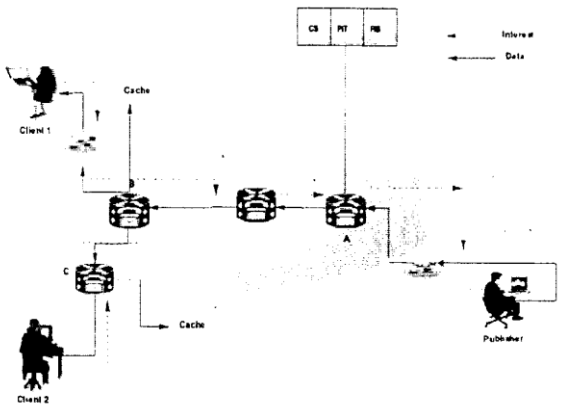


Fig. L ICN Architecture.

proposed ICN architectures, which include Data-Oriented Network Architecture (DONA), Network of Information (Netlnf), Content-Centric Networking (CCN), Named Data Networking (NDN), Publish-Subscribe Internet Technology (PURSUIT), COMET, and CONVERGENCE.

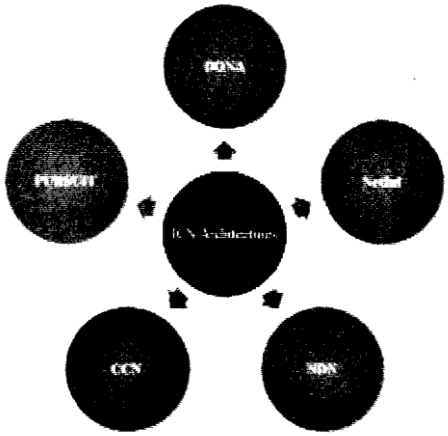


Fig. 2. Different ICN Approaches.

This paper is organized as follows. Section II describes the components that needs to be considered during ICN design.

Section 111 describes different ICN architecture schemes. Section IV describes the current 1CN approaches in which research is being on going. Finally, Section V concludes the paper.

II. COMPONENTS OF ICN DESIGN

Named Data Object: Information/content unit in ICN is generally called Named Data Object (NDO). NDO can be any kind of digital content such as a video, an image, a document, a webpage, etc, or it can represent a real-world object it consists of a location-independent identifier (name), data, and possibly a metadata, which describes an NDO. The same NDO can be identified by multiple names. The NDO is independent of location, storage method, application program, and transportation method.

Naming and Security: ICN categorizes the naming scheme into 2 different types. First, Hierarchical Naming consisting of multiple components separated by “I”. For example:

compl/comp2/obj. It enhances scalability since name prefix can be aggregated in the same way as the URL. The name is user-friendly and conveys meaning to users. Therefore, it is easy to remember. However, it imposes security vulnerability since the name is visible and does not bind to a hash. Second, Flat Naming offers uniqueness and persistency. There are no structure binds to the name. The hash of the content or the hash of the source’s key is put as part of the name, which adds self- certifying property. Therefore, the name is not human-friendly. Flat

naming has a scalability problem since it does not support routing aggregation.

Application Programming Interfaces: API is responsible for requesting and delivering of NDOs. The source/producer makes an NDO available to others by publishing it to the network (called publish or register by the different approaches). A client l consumer asks for an NDO by name (called get, interest, request, find, or subscribe). The latter operation is in most 1CN designs a synchronous one-time operation.

Routing and Forwarding: ICN handles NDO packets routing and forwarding using two methods. First, Name Resolution approach provides means for client to search NDO by name. it does name to NDO storage mapping and forwarding of request message to source with help of Name Resolution System translation. Drawback of this approach is, NRS is main point of failure, and more storage is necessary for name to NDO storage mapping. Second, Name-Based Routing does NDO request forwarding by content routers (CR), where CR locally decides next hop of NDO request based on NDO name. It has two models, unstructured routing which is like traditional routing and structured routing which uses distributed hash table to provide lookup and routing services.

Caching: ICN offers caching service to improve the performance of NDO access of the subsequent requests. Multiple copies of NDOs can be distributed across the networks. It can be stored locally on a node's cache or can be a shared on a network cache. Caching can also be classified into in-network caching where the caching is done within the networks, i.e., on the content routers, and the edge caching in which the end nodes store the cache. Furthermore, caching can also be divided into 3 levels based on granularity: object level (complete NDO), chunk level (part of NDO) and packet level (bytes of NDO). Caching helps reducing the request traffic towards the source. It also enhances the response time of NDO requests.

III. ICN ARCHITECTURE APPROACHES

A. Data-Oriented Network Architecture (DONA)

Introduction: Data Oriented Network Architecture (DONA) is a popular ICN architecture uses the flat names. It's like current Internet naming, i.e, DNS names are replaced with flat, self-certifying names, and DNS name resolution is replaced with name resolution system (NRS). In DONA, the source/content provider is responsible for publishing the content in the network. To serve data, the nodes authorize with the resolution infrastructure. A route-by-name paradigm is used for name resolution. DONA relies on the network entities called resolution handlers (RHs). The request packets are forwarded through multiple RHs toward the node with a copy of the content. The content l data can be acquired through two methods: (I) it is sent back through the same path the interest packet came in on with caching enabled on each encountered RH or (2) it can be sent back directly toward the consumer. The source also has the option to register their principals with the RH so that the request packets can be sent to them directly. Registrations are renewed periodically. RH routes requests using a hierarchical approach to find the closest content provider. The architecture provides improved data retrieval as well as improved service by providing persistence, authentication, and availability.

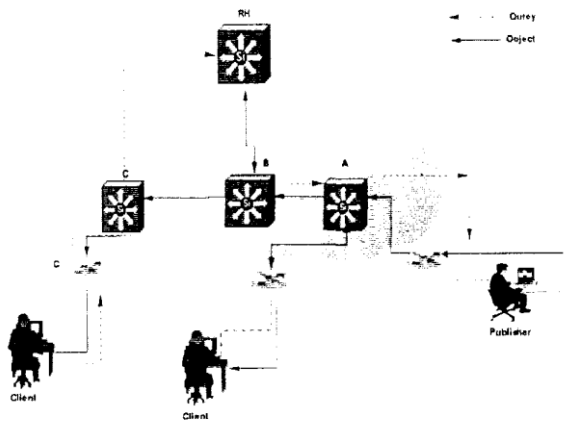


Fig. 3. DONA Architecture.

Naming: DONA names NDOs with a flat namespace in the form P: L, where P is the globally unique principal field, which contains the cryptographic hash of the publisher's public key, and L is the unique object label. As P identifies the publisher (and not the owner), republishing the same content by a different publisher (e.g., by an in-network cache) generally results in a different name for the same content. While this can be circumvented with specific means in DONA (e.g., via wildcard queries or principal delegation), it might complicate benefiting from all available content copies.

Security. The self-certifying narne space used in DONA attributes to name-data integrity removing the necessity for PKIs. It is achieved by adding the cryptographic hash function of the content in the object label L. The signature of the contents hash is added in the metadata of the content; furthermore, the

public key corresponding to the hash in the lBs authenticator field is used to sign the metadata. This allows the object label to be securely bound with the data. This leads to trade-off between the human readability of the content names and name-data integrity.

Routing and Name Resolution. DONA uses name-based routing to route the query via the RHs to a copy of the requested NDO. Nodes that are authorized to serve data use the REGISTER (P: L) primitive to register a datum with an RH. Each domain/publisher has an RH. To resolve a name, the FIND (P: L) primitive is used. Both primitives allow for wildcards being used in place of P or L. RHs are organized in a hierarchical structure. Every request that an RH cannot handle is forwarded to its parent RH. The RH tries to find a copy of the content closest to the client. Once a copy is found, the data is returned to the client, potentially via the RH request path when the RH performs caching. Otherwise, the data can also be returned directly to the client. Originally, DONA used longest-prefix matching for name matching, currently the more scalable deepest-match approach is being proposed.

Caching: In DONA, caching is inherent in the architecture. Any RH can also serve as a cache. To populate its cache, the RH modifies the FIND request so that the NDO is returned to the RH before it is returned to the original requester. Any cache can respond to a FIND request by returning a cached copy of the NDO.

B. Network of Information (Netlnf)

Introduction: Network of information (Netinf) is one of the proposed designs for the future Internet architecture. It was initiated by the European FP7 4WARD project [4WARD] and has been further developed by the SAIL project [SAIL). In this section, we will focus on the Netlnf architecture of the SAIL project. Two classes of objects are defined in Netlnf. I.) Information Object (10) which represents the real-world object 2.) Data Object (DO) represents a digital object. In Netlnf information model, each information object can be decomposed into multiple information objects, which mapped to one or more data object. The data object then mapped to one or more locators. This model allows users to access information by specifying a semantic object rather than a host.

Naming: Netlnf generally employs a fiat namespace with some structure like the DONA narne space. To accommodate different ICN deployment requirements, Netlnf distinguishes between a common naming format (that all nodes must understand) and name semantics and name-object-binding validation mechanisms. The common Netlnf naming

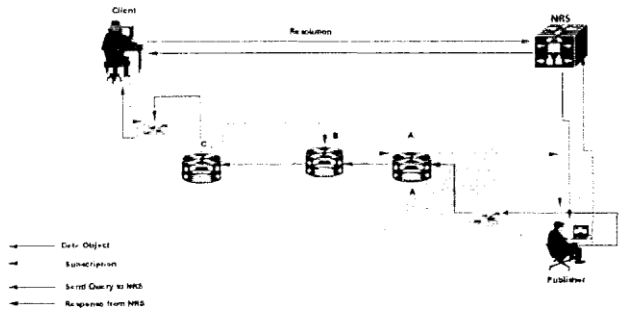


Fig. 4. Netlnf Architecture.

format is based on containing hash digests in the name, and different hashing schemes (e.g., SHA2-based object content digests) are supported. The hash digest of the owner's public key (PK) can also be contained in the name to support dynamic data. Netlnf names can be transformed to different representations, including a URI representation and a binary representation.

Security: Netinf uses the self-certifying namespace, which provides object security service for static as well as dynamic objects. The naming format and the object model enable data-integrity validation by the nodes. Netlnf validation of the named data can be achieved without the PKI infrastructure. Object security is provided through public key cryptography, the pseudonym of the owner, and identification.

Routing and Name Resolution: Netlnf represents a hybrid architecture that supports name resolution as well as name- based routing to retrieve data objects. Netlnf supports a wide variety of name resolution services to have flexibility and scalability. Netlnf defines an interdomain interface for name resolution and routing that allows using different mechanisms in different parts of the network. Two explicit name resolution mechanisms are used. First, Multilevel Distributed Hash Table (MDHT) which uses a topologically embedded hierarchy of resolvers, potentially distributed hash tables (DHTs), for enabling scalable and location-aware resolution of flat names- paces. Second, Late Locator Construction (LLC) that focuses on handling highly dynamic network topologies. It resolves object

names into traditional URL, which can be retrieved using the existing HTfP protocol.

Caching: Netlnf supports three caching options: on-path caching, off-path caching, and peer caching. On-path cache caches objects while routing objects in response to the GET request. Off-path cache is connected to NRS and reduces the traffic and latency. It is responsible for broadcasting objects and informing NRS to cache a data. In peer caching, nodes functions as on/off cache i.e, peers can broadcast cached data in network.

C. Named Data Networking (NDN)

Introduction: Named Data Networking (NDN) proposed an architecture that is shifted from the current IP model to the data-oriented communication. NDN was developed from the proposed Content-Centric Networking (CCN). In NDN, there are two types of packets. An INTEREST packet that client sends out to request for a Named Data Object (NDO). It includes the name specifying the NDO. A DATA packet is a response from the data source. It contains the name, as well as the signature, and the data content. NDN device provides 3 modules for forwarding, routing packet and caching data: Forwarding Information Base (FIB), Pending Interest Table (PIT) and Content Store (CS).

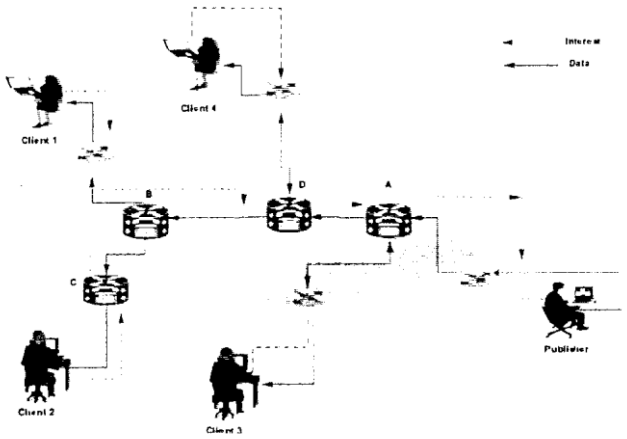


Fig. 5. NDN Architecture.

Naming: The NON namespace is hierarchical to achieve better routing scalability through name-prefix aggregation. The names are rooted in a prefix unique to each publisher. The publisher prefix makes it possible for clients to construct valid names for data that does not yet exist, and publishers can respond with dynamically generated data. NDN names are used for both naming information and routing purposes. The granularity of the names is very fine: single chunks (packets) are named.

Security: In NON, the content publisher provides security by cryptographically signing each data packet. To achieve data integrity, every content is signed with the publisher's secret key, but the trust in the signing key must be established through some external means. The naming in CCNINDN typically does not contain the publishers key (PK). Although this helps with the human readability of the names, self-certification is not possible. Multiple methods are used to verify the key, such as information through a friend, direct information, information through a trusted third party, or information through a global

PM.

Routing and Name Resolution: CCN uses name-based routing. Clients ask for a data object by sending interest packets, which are routed toward the publisher of the name prefix using longest-prefix matching in the forwarding information base (FIB) of each node. The CCN nodes keep state for each outstanding request in the pending interest table. This makes request aggregation possible, i.e., when the same node receives multiple requests for the same NDO, only the first is forwarded towards the source. When a copy of the data object is encountered on the path, a data packet containing the requested object is sent on the reverse path back to the client (all nodes along the path cache a copy of the object). The reverse path is found using the state that the interest packet has left in the nodes.

Caching: CCN can cache both requests (through its request aggregation) and objects. CCN routes a request for data toward the publisher and makes use of any cached copies along that path. A CCN node can keep received interest packets in a pending interest table and thus suppress forwarding of subsequently received requests for the same object if it has already sent a request. Object copies can also be found by local search. As single packets are the atomic objects in CCN, it is possible that only a part of a bigger object is cached.

D. Publish-Subscribe Internet Technology (PURSUIT)

Introduction: The Publish-Subscribe Internet Technology (PURSUIT) project was previously known as the Publish- Subscribe Internet Routing Paradigm (PSIRP). Both PSIRP and PURSUIT are part of the European FP 7 project. In PURSUIT, NDO sources publish the NDO contents into the network. The receivers can subscribe to the

published contents through the rendezvous systems. A rendezvous system helps in locating the scope and publications in the network. Each piece of the published content belongs to a specific named scope. The subscription requests contain the scope identifier (SI) and the rendezvous identifier (RI), which together identify/name the desired content.

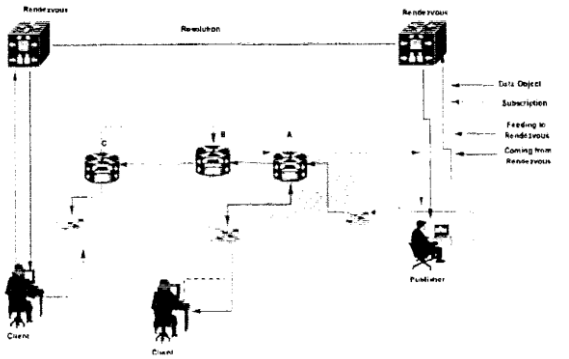


Fig. 6. PURSUIT Architecture.

Naming: PURSUIT makes use of two types of names:

rendezvous identifiers and scope identifiers; they both belong to a flat namespace. Rendezvous identifiers (together with scope identifiers) name NDOs. The NDOs are mapped to rendezvous points, which are used to establish contact between publishers and subscribers. PURSUIT also uses forwarding identifiers, which are used by the forwarding fabric to transport data after contact is established at a rendezvous point. The forwarding identifiers (Bloom filters in LLPSIN) are not names for NDOs; they are transient and identify a path from the publisher to the subscriber.

Security: PURSUIT uses self-certifying names, which alleviate the need for a PK1. The other security aims are to avoid unwanted traffic on both the rendezvous and forwarding layers. PURSUIT makes use of elliptic-curve cryptography (ECC) for signature verification and packet-level authentication (PLA) to provide network layer confidentiality, authenticity, and accountability of the data.

Routing and Name Resolution: Pursuit uses a resolution model where the resolver is called the rendezvous point. The data return path to the client can, potentially, take a different path than the name resolution/rendezvous path. Data is forwarded using a source routing approach called z-Filters:

a Bloom filter describing the route is built by the rendezvous point and used to forward packets from the selected source to the destination. The Bloom filter is attached to the packet itself, and it contains all names of the links that must be followed. The Bloom filter approach allows packet length to be traded off against wasting network resources. A large Bloom filter gives fewer false positives, thus resulting in less packets being forwarded on links without any receiver.

Caching: Caching in Pursuit is mainly provided as a dedicated solution to a problem for which caching might offer some benefit. Multiple caches of an object can be maintained based on the scope of the rendezvous point for the identifier associated with the object.

A. COMET

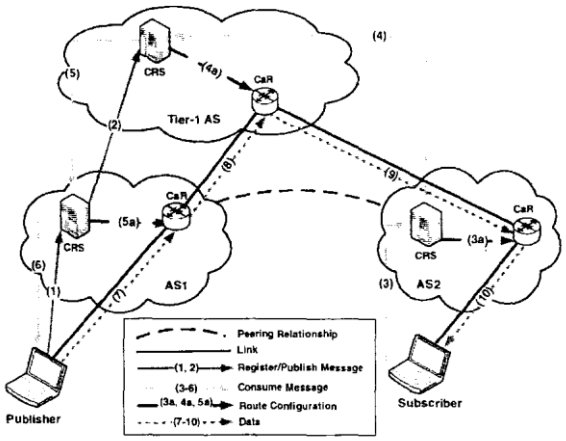
IV. CURRENT RESEARCH

Introduction. The Content Mediator architecture for content-aware networks (COMET) project, funded by the EU Framework 7 Programme, is designing mechanisms for optimizing information source selection and distribution by mapping information to appropriate hosts or servers based on transmission requirements, user preferences and network state. The core component of the COMET architecture is a Content Mediation Plane (CMP) which mediates between the network providers and the information servers, being aware of both information and infrastructure. Unlike other ICN approaches which strive for location independence, COMET allows both subscribers and publishers to explicitly include location preferences for information, following established business practices.

Naming: In COMET the information names are provided by a Content Resolution System (CRS) when the information is registered by the publishers, thus allowing names for related information to be explicitly aggregatable. This allows the naming system to scale by exploiting existing relationships between information objects. Thus, we can say, precise naming scheme has not been defined for COMET.

Security: COMET simplifies the security provisioning using AS paths rather than global addresses in both the CRSs and the CaRs, preventing attackers from using arbitrary network paths to launch undetected attacks

Routing and Name Resolution: Routing and name resolution in COMET is carried out by five functional blocks; Content Resolution Function (CRF), Path Management Function



(PMF), Server and Network Monitoring Function (SNMF), Content Mediation Function (CMF) and Content Aware Forwarding Function (CAFF). CRF resolves content name to one or more content sources. The list of candidate content sources is considered based on the server awareness information supplied by SNMF. PMF connects to the physical networks and gathers information regarding network quality of service and route quality. SNMF collects the network information and server information and delivers to CMF and CRF respectively. CMF acts as a main controller. It receives the client request and triggers CRF for name resolution. It then uses network awareness information from SNMF and routing awareness information from PMF to choose the most suitable content source and the best delivery path for the client. CAFF is responsible for forwarding the content based on the path specified by the CMF.

Caching: COMET supports on-path and off-path caching. On-path caching is a by-product of name resolution, while off- path caching requires registering cached copies with the CRS. On-path caching has 2 schemes. First, Probe Cache scheme approximates how many times an information packet should be cached on a path by assuming other Cars have the same caching capacity as itself and estimating the total traffic on the path by the requests it receives per unit time. Second, Centrality scheme helps to approximate where information object should only be cached by the CaR with the highest centrality in its path.

B. CONVERGENCE

Introduction: CONVERGENCE is also a European FP7 project, based on the publish-subscribe model. It introduces VDI (Versatile Digital Item) as its unit of content distribution. VDI acts as a container that holds name, metadata, and resource (data). Metadata in VDI links to a license, which specifies the action that can be performed to the resource. VDI is represented in an XML format. CONVERGENCE introduces a 3-level architecture. First, the Application Level is part of the semantic overlay. It forms and ingests VDI, which

Fig. 7. COMET Architecture.

sent and received through the application-middleware interface. The second is the Middleware Level (CoMid). CoMid provides a VDI processing capability, which allows a node to publish or search for a VDI. Lastly, the Computing Platform offers node's communication infrastructure, which is based on the Content Network (CoNet) architecture. In addition, a content security mechanism (CoSec) is also included in this level.

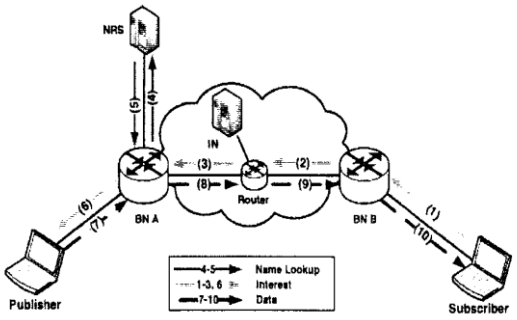


Fig. 8. CONVERGENCE Architecture.

Naming: In CONVERGENCE object names consist of a namespace ID and a name part, whose format is determined by the namespace ID which is like fiat P: L pair. In name part, hierarchical names, uris can be used. The exact properties of the names depend therefore on the specific namespace used.

Security: CONVERGENCE adopts the per DATA message security approach of NDN, i.e., each DATA message contains a digital signature. Due to the large overhead of the meta-data required for signature verification, DATA messages are expected to be much larger than carrier packets. For this reason, CONVERGENCE proposes performing security checks - on information only at the DATA message level at the subscriber.

Routing and Name Resolution: The Lookup and Cache Concept allows nodes to forward carrier-packets to the right destination. Forwarding Information Base (FIB) contains an active forwarding information. When an Interest ICU arrives, a name prefix matching is performed. If there is no matching entry in FIE, FTB will send a name lookup request to a Routing Information Base (RIB)

located on the NRS. RIB holds a complete set of routing information and responds to FIB query. In the case that FIB cannot find a matching entry, and its table is already full, FIB uses a routing replacement algorithm to determine its action. It can either do nothing and drop the Interest packet or query a new entry from RIB and replace the old entry with the new one. FIB uses algorithm such as Inactive Timeout Estimation to replace the least recently used entry. After the Interest CR1 reaches the source or the caching devices, the Data CIU is routed back through the reverse path using the forwarding information collected by the Interest CR1 as it travelled upstream. This is another point that varies CONVERGENCE from NDN since NON uses PIT entry to route Data packet back to the requester.

Caching: CONVERGENCE supports on-path caching in a manner like NDN. Off-path caching, and replication are supported by registering additional copies of an information object stored at INs to the NRS.

V. CONCLUSION

In this survey, I have surveyed different ICN approaches. Different ICN approaches uses different design choices and features, focusing on the following main components; named data objects, naming and security, routing and transport, and caching. We discussed the ICN approaches based on these components. We aim to aid readers to get concept on Data-Oriented Network Architecture (DONA), Network of Information (Netlnf), Content-Centric Networking (CCN), Named Data Networking (NON), Publish-Subscribe Internet Technology (PURSUIT) COMET, and CONVERGENCE architectures.

REFERENCES

[I] Sripriya S Adhatarao, Jiachen Chen, Mayutan Ammaithurai, Xiaoming

Fu, and KK Ramakrishnan. Comparison of naming schema in icn.

In Local and Metropolitan Area Networks (LANMAN), 2016 IEEE

International Symposium on, pages 1—6. IEEE, 2016.

[2] Bengt Ahigren, Christian Dannewitz, Claudio Imbrenda, Dirk Kotscher, and Borje Ohlman. A survey of information-centric networking. IEEE Communications Magazine, 50(7), 2012.

[3] Sobia Arshad, Babar Shahzaad, Muhammad Awais Azam, Jonathan Lao, Syed Hassan Ahmed, and Saleem Aslam. Hierarchical and fiat-based hybrid naming scheme in content-centric networks of things. IEEE Internet of Things Journal. 5(2):1070—1080, 2018.

[4] Md Faizul Bad, Shihabur Rahmari Chowdhury, Reaz Abased, Raouf Boutaba, and Bertrand Mathieu. A survey of naming and routing in infonnation-centric networks. IEEE Communications Magazine, 50(12), 2012.

[5] Giovanna Carofiglio. Giacomo Morabito. Luca Muscariello, lgnacio Solis, and Matteo Varvello. From content delivery today to information centric networking. Computer Networks. 57(16):3116—3 127, 2013.

[6) Christian Dannewitz, Dirk Kutscher, BdRje Ohlman, Stephen Farrell, Bengt Ahlgren, and Holger Karl. Network of information (netinf)— an information-centric networking architecture. Computer Communications, 36(7):721—735, 2013.

[7] All Ghodsi, Teemu Koponen, Jarno Rajahalme, Pasi Sarolahti, and Scott

Shenker. Naming in content-oriented architectures. In Proceedings of the

ACM SIGCOMM workshop on Information-centric networking, pages

1-6. ACM, 2011.

[8] Dolvara Gunatilaka, Recent information-centric networking approaches. Recent Information-Centric Netw Approaches, pages 1—16. 2013.

[9] Van Jacobson, Diana K Smetters, James D Thornton, Michael F Plass, Nicholas H Bnggs, and Rebecca L Braynard. Networking named content. In Proceedings of the 5th international conference on Emerging networking experiments and technologies, pages 1—12. ACM, 2009.

[JO] Teemu Koponen, Mohit Chawla, Byung-Gon Chun, Andrey Ermolinskiy,

Kye Hyun Kim. Scott Shenker, and lon Stoica. A data-oriented

(and beyond) network architecture. In ACM SIGCOMM Computer

Communication Review, volume 37, pages 181—192. ACM, 2007.

[11] Bing Li, Dijiang Huang, Thijie Wang, and Yan Zhu. Attribute- based access control for icn naming scheme. IEEE Transactions on Dependable and Secure Computing, 15(2):194—206, 2018.

[12) Stefano Salsano, Andrea Detti, Matteo Canceffieri, Matteo Pomposini, and Nicola Blefari-Melazzi. Transpoct-layer issues in information centric networks. In Proceedings of the second edition of the ICN workshop on Infonnation-centric networking. pages 19—24. ACM. 2012.

[13] George Xylomenos, Christopher N Ververidis, Vasilios A Sins, Nikos Fot.iou, Christos Tsiopoulos, Xenofon Vasilakos, Konstantinos V Katsaros, George C Polyzos, et al, A survey of information-centric networking research. IEEE Communications Surreys and Tutorials, 16(2):1024—1049, 2014.

[14) Guoqiang Zhang, Yang Li, and Tao Lin. Caching in information centric networking: A survey. Computer Networks. 57(l6):3128—3141, 2013.