ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

A Survey on Information Centric Networks

Jitha P B , Saranya R

P.G Scholar, Dept. of Computer Science and Engineering, Cochin College of Engineering, Kerala, India

P.G Scholar, Dept. of Computer Science and Engineering, Cochin College of Engineering, Kerala, India

ABSTRACT: Information-centric network architectures are an increasingly important approach for future Internet architectures. Several approaches are based on a non-hierarchical identifier (ID) name space that requires some kind of global Name Resolution Service (NRS) to translate the object IDs into network addresses. This paper focuses on the current progress of the ICN. It investigates various key aspects such as naming and routing schemes, in-network caching policies, etc., we propose an NRS called Multi-level Distributed Hash Table (MDHT). It provides name-based any cast routing, can support constant hop resolution, and fulfills the afore mentioned requirements.We also discuss the different issues of ICN and its existing solutions.

KEYWORDS: Information centric networking, multi-level distributed hash table.

I. INTRODUCTION

Information-Centric Networking (ICN) is an important networking paradigm that has the potential to solve several problems of today's Internet architecture, including inefficient resource utilization, problems caused by flash crowds, Distributed Denial of Service (DDoS) attacks, and inadequate security. Several ICN approaches have been proposed for the Future Internet, e.g., the Data-Oriented Network Architecture (DONA) , Content-Centric Networking (CCN) , and the Network of Information (NetInf) . ICN approaches put the information at the center of the architecture and shift the communication model from the node-centric paradigm that focuses on conversations to the information-centric paradigm that focuses on information dissemination.

Efficient information dissemination should make use of any available data source. To do so, most ICN architectures are in some way based on an identifier/locator split. Information is identified with a location- independent identifier (ID) that cannot be used for forwarding/routing purposes with current schemes like IP. As a result, ICN architectures have to solve the problem how to retrieve data based on these location-independent IDs. In general, there are two major solutions to this problem. First, performing *name based routing* on these IDs. Second, performing a *name resolution* step first that resolves the information ID into a Locator , which can be used by some other forwarding scheme (e.g. IP) to retrieve the information. In this paper, we focus on a Name Resolution Service (NRS) for ICN architectures, also in-network caching policies ,security issues and existing solutions for them.

We propose a distributed NRS with integrated name-based routing functionality called Multi-level Distributed Hash Table (MDHT). The MDHT system provides a nested, hierarchical DHT architecture for scalable distributed name resolution and efficient any cast routing of flat IDs. If the Ids include some additional structure like owner/publisher information, the MDHT system can use this structure to perform name aggregation on the global level to simplify global deployment and further improve scalability. The hierarchical architecture can reflect the existing network topology, topologically embedding the NRS for efficient data dissemination.

II. RELATED WORK

Several ICN architectures like NetInf use a non-hierarchical name space to achieve, among others, name persistence. The need for persistent names is also emphasized by the spreading of persistent naming schemes like the Digital Object Identifier (DOI). However, with a non-hierarchical namespace, we cannot use approaches that require hierarchical names for aggregation, like CCN in routing tables or DNS for name resolution. Like DNS, our system uses a hierarchical architecture. However, we do not use hierarchy to perform aggregation based on hierarchical names as

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

done in DNS. Instead, MDHT uses the hierarchy to minimize inter domain traffic (request and data traffic), to reduce latency, and to benefit from locality in request patterns.

Structured DHT systems like CHORD and Kademlia represent a scalable solution for handling flat namespaces. Approaches like CoDoNS use a DHT to build an NRS. However, those flat DHT systems do not support efficient data dissemination. They are not topologically embedded, making the locality requirements hard to fulfill. Constant hop DHTs like Structured Super peers have the same problem but could be used as subsystems in MDHT to reduce latency.

Hierarchical DHTs can fulfill those requirements. Approaches like Cyclone , the Generic Hierarchical DHT Framework , Hierarchical Rings , as well as Canon provide topological embedding. However, none of the hierarchical DHT systems that we are aware of fulfills the combination of our requirements, especially when considering deployability.

III. PROPOSED SYSTEM

The MDHT system uses a two-step process to retrieve data objects based on IDs. In the first phase (resolution phase), the ID is resolved into a list of locators that point to copies of the desired data object. In the second phase (data forwarding phase), a set of locators is selected from the list based on configurable parameters (e.g. network conditions).Subsequently, the data object is delivered from the source(s) to the requester.The MDHT system is independent of the underlying transport and forwarding/routing layer.

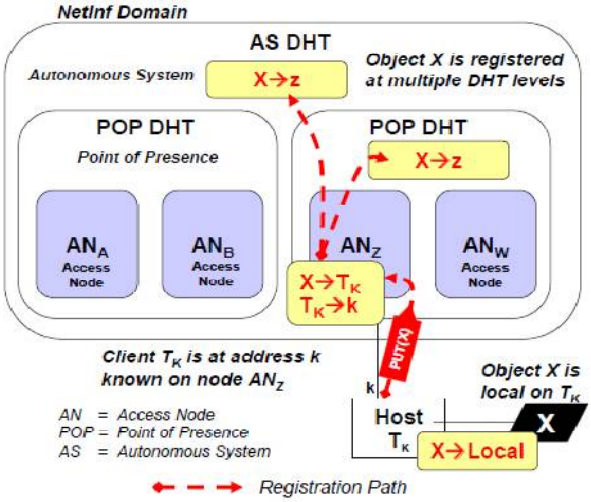

Figure. 1 Register object X into an intra-domain MDHT system with areas on three levels: AN, POP, AS.

For the resolution phase, the list of object locators is stored in so called Dictionary Record (D-REC) entries, containing the ID–locator bindings as well as potentially related metadata. The MDHT dictionary storing the D-REC entries consists of multiple interconnected DHT systems, called DHT areas. The DHT areas are arranged in a nested, hierarchical structure as shown in Figure 1, building a DHT tree structure. Multiple connected DHT areas of the same provider are called NetInf domain. The nested arrangement reflects the underlying network topology. Thereby, it minimizes the routing stretch inefficiencies of common DHT systems resulting from missing topological embedding. Each DHT area represents a network on a different topological level.On the lowest level are the Access Nodes (ANs) where client/host nodes are attached to the MDHT system, from the clients' point of view somewhat similar to a local DNS server. These ANs use a local Hash Table (HT). Each DHT area can use its own DHT mechanism. Each MDHT node participates in its own DHT area and, typically, in some or all higher DHT areas. This means that higher DHT areas are built by aggregating the MDHT nodes of the DHT areas below into a single, larger DHT area, leading to the name "nested hierarchical". Each MDHT node can freely choose the number of DHT areas that it participates in. This hierarchical, area-based approach makes deployment of the MDHT system easy as it can grow "from the edges" of the Internet, i.e., the MDHT system can be deployed in small networks first, which can subsequently be interconnected to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

build a larger system. Routing and forwarding requests in the MDHT system happens in two separate ways: Intra-area routing/forwarding, i.e., within an DHT area, is performed via the respective routing/forwarding mechanism chosen by the MDHT-area provider, e.g. via Chord. Inter-area routing/forwarding, i.e., between MDHT areas, is performed via the MDHT nodes that are part of both respective levels. This is done by handing the request to the forwarding process of the next higher level within the same physical node. If a node is not part of the next higher level, the request is forwarded to the next node that participates in both levels.

A. *DATA REGISTRATION AND RETRIEVAL*

The MDHT interface offers two main primitives :

(1)PUT(ID, metadata) is used to register bindings in the network dictionary, i.e., the ID is made public and bound to a set of locators or metadata.

(2)GET(ID) may return a (list of) locator(s) where the data object can be retrieved or the object itself. In addition, related metadata bound to the specified ID can be returned.

To make a new object known and accessible for other users, it has to be registered (via *PUT*) in the MDHT system (Figure 1). Two types of bindings can be registered in D-RECs: location bindings, which map object/node IDs to network locations, and indirection bindings, which map Ids to other IDs. First, the user's device ID T_K is registered in the MDHT system. On the user's AN, T_K is mapped to its local address k, which can be private. Thereafter, the data object can be registered in the user's AN to make it accessible for local users connected to the same AN. Registering a new object creates a new D-REC storing an indirection binding which maps the object ID X into the user device ID T_K. Second, the registration request is propagated up the MDHT tree so that a new binding for object X is recorded in the upper DHT areas along the path from leaf (AN) to root (AS DHT). On all levels (except the top level REX), the hash(ID) is used as DHT key to store the binding. The used hash function depends on the implemented DHT system.

Note that, in the upper DHT areas, the object ID is mapped to the address z of Access Node AN_Z, where X can be reached via the address k of host T_K. This binding scheme allows to keep host addresses private and reduces firewall issues as responses are received from the initially Queried Access Node. In addition, this indirection scheme has good mobility support for mobile users and objects as the Access Node can perform a role similar to a mobile IP "home agent", redirecting requests to the new location of node T_K.

To provide control of ID registrations, the publisher can specify the scope of the registration for each ID, i.e., up to which level registration takes place. The scope limits the propagation of the respective D-REC entries within the tree. Figure 2 shows a user (host T_0) requesting a data object by ID X. The request is first processed in the Access Node AN_A. When resolution in the AN fails because the ID is unknown (i.e., no data copy is registered in this area yet), the request is propagated to the next higher DHT level until a hit is found or the resolution fails on the highest level. By starting the resolution process in the AN and propagating the request higher only if required, the routing stretch is minimized because nodes in lower DHT areas are generally closer (in terms of no. hops and hop latency) to each other than nodes in higher areas. At the same time, traffic is kept local as this approach always selects a copy from the "closest" area and prevents inter-area traffic whenever possible/desired.

This approach also ensures that the MDHT system fulfills the Content Locality property: if a local copy is available close to a source, resolution and routing can happen locally. This enables any cast strategies and locality-aware content distribution policies. Given that content is likely to have local access patterns, we also profit from smaller DHT structures.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

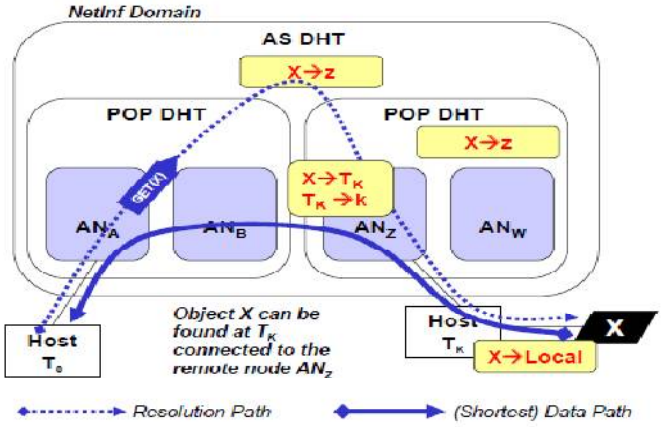

Figure. 2 Resolving and retrieving object X

B. ***COPIES AND CASHING***

When a user resolves and downloads a published data object, a new copy is stored on his local machine. In addition, new copies can be created by caching popular data objects in the MDHT nodes (in-network caching). In both cases, the new copy can be made available for other users by simply registering new bindings to the new copies' locators in the MDHT system. Again, the scope of each published copy can be limited, e.g., to limit the load on the user's node or on a caching server.

C. ***BINDING SCHEME***

MDHT supports multiple binding schemes, i.e., different ways how object IDs are (directly or indirectly) bound to their locations. Object IDs can be bound, e.g., to the (public) address of the server which holds a copy of the object or to the ID of that server. The binding scheme shown in Figure 1 keeps host addresses private at the edge and facilitates mobility of users and objects by means of indirection of objects to user devices and Access Nodes. In general, this kind of indirection is very powerful. It can be used to provide useful capabilities, like private address masking, support of mobility and multi homing, and redirecting traffic towards application servers, e.g., firewalls and accounting servers.

D. ***LOCATOR SELECTION***

The MDHT system can support three different ways to select appropriate locators from the list of locators for a certain ID. In the Requester-controlled mode the MDHT system returns the list of (public) locators to the requester, the requester locally selects a suitable one, and the requester triggers the download of the data. The requester has full control over the process, which is similar to today's DNS System . In the MDHT-controlled mode, the MDHT system performs the locator selection and also triggers and handles the data transfer from the source(s) to the requester, i.e., the resolution is transparent to the requester. This is the case shown in Figure 2. Because the MDHT system is embedded in the underlying network infrastructure, it can use its knowledge about the network topology and current network status to select the best locator(s). This integration of resolution and data routing phase also reduces the overall routing stretch. In the Hybrid mode, MDHT returns a ranked locator list, based on its network knowledge. The requester can choose the desired locator(s) based on the ranking and other factors, and downloads the data. This mode combines best locator selection based on network knowledge with full requester control.

E. ***GLOBAL RESOLUTION NAME(REX)***

Global Name resolution on the highest MDHT level must be highly scalable because of the large number oglobally available data objects. If the namespace is flat without any structure, the top level can use a global DHT composed of all/most of the MDHT nodes from the lower levels.Most requests will already be answered in lower levels. Hence, load on the top level will be limited. Our preliminary simulation results support this expectation .

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Using a global DHT at the top level is unfeasible, due to the *key placement* issue: for security and reliability, bindings generated by users of a given network domain should be managed on systems under the control of that domain's provider or on independent systems.If the namespace is structured, e.g., names contain information about the publisher, global name resolution can be further improved by combining the MDHT system with our Resolution Exchange (REX) system. The REX system is based on independent REX points which offer global resolution services to client ISPs. The REX system, just as the DNS top level domains, can be managed by an independent third party.This trusted third party guarantees its clients the correct management of their resolution bindings .

REX is based on the idea that each owner/publisher has a primary resolution system where his IDs are stored. In addition, the REX system performs aggregation based on the ID structure. Let us assume an ID structure *A:L*, where *A* is a prefix with some semantic (object owner in the NetInf case), and *L* is a label which unambiguously identifies the object in the scope of *A*. This structure can be used to aggregate all data objects of an owner into a single binding, i.e., the system only has to scale with the number of owners and not with the much larger number of data objects. The REX system only stores redirects to the primary resolution system. The *A* part of each ID can be mapped and redirected to the primary resolution system which is responsible for managing bindings for all IDs with that prefix. Although the REX system can be designed to handle and redirect the resolution traffic itself, we think of it more as an administrative entity. Instead of performing resolution itself, the REX system only manages registrations, updates, and aggregation of bindings on the global level. These aggregated bindings are then cached within intra-domain MDHT systems. By using these cached bindings, requests for IDs registered in other NetInf domains can (already on the levels below REX) be redirected to the appropriate primary resolution system in the remote domain via a topological inter-domain routing protocol. Hence, they do not have to be forwarded to the REX system.

IV. OTHER ISSUES AND EXISTING SOLUTIONS

In this paper,we also intend to give a general presentation of different ICN features with the goal of raising an in-depth discussion of this novel Internet paradigm. Our study is arranged according to the common components in various ICN designs such as naming and routing schemes, in-network caching technique and security issues.They are as follows:

A. *NAMING AND ROUTING*

The fundamental concept of the ICN is to switch the address based Internet architecture to a named-content based one.The content retrieving in ICN can be mainly divided into two parts: the content discovery and the content delivery. The content discovery is related to how a content is named, how it is published and how an ICN node addresses it. The content delivery defines the ICN routing protocol which is about how a content provider propagate its contents into the network ,how an ICN router routes the end-users' interests to the best content sources and how an ICN router deliver the contents to the end-users.. The content name is the only identifier of each content object, which permits either the end-user or the intermediate networking unit locates the best content holder. The content name usually is a globally unique identifier, but the unique named content can sojourn in different containers, for example the origin content servers, the CDN repositories or the on-path caches. In the following we will try to summarize the different naming issues of the ICN domain.

(1)The properties of the ICN naming: Of course the fundamental role of the unique name is to identify the different content, but it also include other properties:

(a) Globally unique: In ICN, each networking unit is identified by a content name. Thus the content name should be globally unique inorder to arrive at a global level routing.

(b) Location independent: The IP address is highly related to the geography location. When the location is changed ,the IP address is changed. The ICN name is independent from the physical location. A content is named when it is created, no matter where or from who. A named content can be re-published ,replicated everywhere, but the name doesnot changed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

(c) Security intergraded: The security was not designed in the first version of IP network. As long as the Internet evolution, the security service is added into the IP prototype, e.g. IP sec. In ICN, the security is directly guaranteed into the content name. The information objects are self-certificated by their names, which means each content name is signed by its legal publisher and it is binded with the related content. Only the authorized receivers can decrypt the content name and the content data

(d)Self-defined: Unlike the IP addresses which are attributed by a centralized organization , the ICN name can be created by the content providers themselves, only follows the defined naming rules. However, the self-defined names will introduce a huge number of content identifiers in the network

(2) Hierarchical or flat name structure: There exists mainly two categories of ICN naming structures: the hierarchical names and the flat names. Each naming structure has the advantages. The hierarchical structure is similar as the IP CIDR. The IP addresses can be aggregated into the prefixes and perform the longest match or shortest match. The hierarchical names, for example the CCN naming are structured for aggregation and extending. The names are uniqueness for routing but are human-readable for the end-users. The flat structure is not suitable for aggregation but it is easy to perform the DHT-like lookup methods.

(3)Metadatas: Besides the unique names for identifying the content objects, ICN includes also the additional metadata in the names for describing the contents. For example a photo which is offered by Flickr can be named in a hierarchical structure as ccnx:/flickr.com/group_xxx/photo1/. It can also con- tain the tags as the metadata for example the author, the subject, the camera model or the place where the photo was taken. The metadata is important in ICN.First of all, the additional metadata can better describe the content. The content name is unique but sometimes the user may not know the exact name of each content. Thus the metadata is here for helping the user find out the right content for example by using the search engine with some keywords. The metadata scan also establish the association between similar content objects. For example a user who requests this photo may be also interested in the other photos that are token by the same camera model.

(4) Named based routing or DNS-like resolution: The ICN routing can be realized in two manners: the undirected naming resolution service and the direct name based routing. The naming resolution requires one or several centralized servers (e.g.Ren- dezVous points, register servers, trigger points,etc.) in the networking topology. The content publications are collected in these servers, which have a global view of all the published content objects and the networking topology. When an ICN router wants to forward a request message, the routing path is calculated in the centralized server by implementing the IS-IS or OSPF like Shortest Path protocol. Contrarily, the name based routing is directly performed in the ICN routers. Each router has a local forwarding information base which is filled by the content publication messages. The request forwarding paths are thus calculated in the local routers followed their own forwarding strategies.In the following subsection we will give a brief view of some advanced ICN research project and their naming and routing solutions.

In Content Centric networking(CCN), the ultimate objective is to replace the IP based Internet with a named content based model. In CCN,the information exchange is realized with two types of packet: the Interest and Data. The Interests are used to express which content the end-users want to retrieve and the Datas are the response packets which contain the real binary contents.The Interest routing is based on the Content Name .Each CCN node has an element so-called Forwarding Information Base(FIB).It contains the Interest routing information. When a content provider has some contents to publish into the network,it spreads the advertisements into the network. These advertisements will fill the CCN FIB together with the incoming faces as the Interest outgoing faces. Each CCN node can aggregate the FIB entries on the prefix as the case might be. When the CCN node wants to route an Interest request, it will look the Interest Content Name up in the FIB table.And the Interest will be sent out through the faces of the longest match FIB entry.The CCN routing supports the multicast by default,which means that one FIB entry may contain more than one out going face.This is because one content can be provided by different providers. In CCN,the Datapackets are not routed.Each CCNnode contains another component which is called Pending-interest. When a CCN node receives an Interest, if it locally does not have the right content, it should forward the Interest out according to its FIB. Meanwhile,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

it appends also the Interest name (the ContentName) in its PIT together with the incoming face identifier of the Interest. After several forwarding hops,the Interest arrives at one content container which holds the required content.The container will reply the Data packet and the Datapacket will follow the reverse path of the Interest forwarding until it is returned to the origin asker.The reverse path forwarding is realized as everytime the Data is back to a CCN node, the node will check the Data name in its PIT.If it finds a matched PIT entry,which means this node did received the Interest for this content, the Data will then sent out through the face(s) of the matched entry.

The NetInf proposes ICN architecture based on the content register scheme. The NetInf applies the Information Object(IO) and Bit-level Object (BO) to differentiate the content identifiers and the real binary content in a Named DataObject (NDO). The naming of NetInf is included in the IOs.TheNetInf IO contains three parts: the content-identifier,the metadata and the security attributes. The NetInf name uses a flat structure as P:L, which contains and separates the identifier of the content provider and the content self. The P is the content provider identifier that is usually the hash of the public key of the provider.The L is the label of the content chosen by the content provider, it is usually the hash of the content itself.The NetInf routing is a multi-levelDHT(MDHT) based registration method which includes a name resolution service. The MDHT structure is a three level topology: the Access Node level(AN),the Point of Presence level(POP)and the Autonomous System level(AS),from the lower to the upper. Each level applies its own DHT algorithm and any nodes at any levels can join in a cross-level DHT—the MDHT. The routing in NetInf has two processes: the content registration and the content discovery.When a content provider wants to register a content, it will firstly map the content to an access node by the AN level DHT algorithm.The access node has two information bases. One is to tell which content can be found at which host, another one is to memorize the address or any other access information for reaching which host.After the AN level registration, the content will be registered in the MDHT, which means the content name and the attached access node are registered in both the local DHTs of the POP and the AS level.When an client want to retrieve a content,it will first try to get it in DHTs follows the order of AN,POP and then AS.If it cannot find the content even in the AS level,it will look the content name in a naming resolution service which is named REX (ResolutionExchange).The REX is an independent entity that runs at the AS level.The mappings generated by the REX are cached in the DHT of each AS.

B. *IN-NETWORK CASHING*

One of the most remarkable characteristics that differs ICN from the current Internet is the in-network caching mechanism.In-network caching mechanism further reduces the response delay by embedding cache storage deep into the network. Instead of leveraging the storage resource at the edge of network as P2P systems, or stand alone web cache proxies, ICN enriches various network equipments (e.g., routers , gateways) with caching capability. This widespread caching significantly improves the content searching efficiency and alleviates the traffic load on transit links between content provider and ISPs.Their existing solutions are :

The in-network caching in NetInf is achieved by two different models that can coexist in the system: the network-based storage model and the network- managed storage model. The former model supposes that network operators have the total control of the storage resources since they integrate storage resources within network nodes, or deploy dedicated storage servers in the network considering certain criteria as resource dimensioning and performance targets.The latter one leverages the storage space at the user side. A user device contributes a portion of its storage capacity to the network when it is on-line. The network nodes that connect with on-line users manage the portions of donated storage and use them as the storage system under the operator's control. Accordingly, there are two approaches to retrieve those cached contents. Firstly, the required content can be found in the caching node on the path to the content source by cache-aware transport protocol. The content source could be the origin server of the content, or the location hosting a copy of the content. This location is registered in the Storage Engine used by NetInf to handle storage requests from user applications and manage the long term memory of the network. In the second approach, the cached object is retrieved directly by querying the name resolution system since either the location of the object is registered there, or it can be found by local search(e.g., broadcast).

CCN protocol takes advantages of its URL alike hierarchical content name and an multi-cast routing mechanism to forward user's request to multiple sources of the content. The source could be the original provider of the content, or the users who are willing to share their local copies of it. Any network nodes along the path from the requester to the source holding the corresponding content can directly satisfy the end-user and consume the request. At the mean time

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

,the node that does not cache it can decide to store the content passing through according to a certain policy. Since the copyright check and the authentication of the content are accomplished at the application level ,network opera- tor does not need to implement specific function to manage the storage space at user side and authorize the publication of the content from them. Because of the same reason, CCN protocol deals with the cache storage offered by operator and con- tributed by user in the same manner. The CCN name-based routing is simple and efficient enough to retrieve the cached content.

C.*SECURITY ISSUES:*

ICN requires location independent security mechanism to enable ubiquitous in-network caching system.To this end, the next generation security model should provide an information oriented data integrity and authen ticity check mechanism. Moreover, the model should get rid of the trusted third party(e.g., software vendor)that compiles the trusted authorities in the current data integrity checking process. While ICN is intrinsically immune to the host-oriented attack because of the content based communication, solutions for denial-of- service(DoF) attack is worth to be addressed.The existing solutions are:

In order to realize the content centric security model ,ICN protocol usually integrates its proper security design as an in separable part from its architecture.

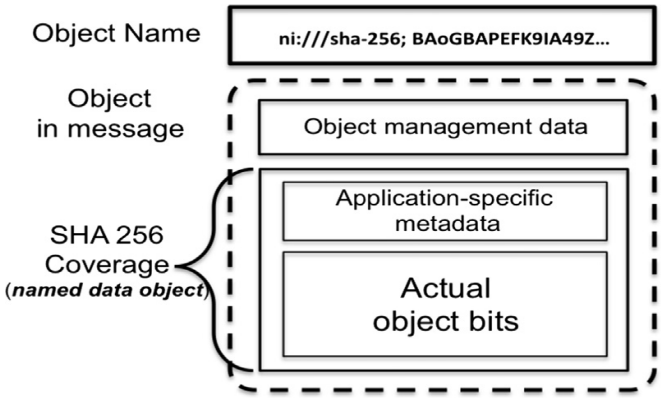

Figure 3:Common format of NetInf message

The common data format in NetInf is illustrated in Figure. 3. The NetInf name of a named data object (NDO) contains a hash algorithm and the corresponding hash value of the object's content body. The named information (ni) is registered in a URI architecture to foster application development and simplify migration. The functionality of this NetInf name is first to explicitly identify NDOs, then to enable name-data integrity and other advanced security features, and finally to perform as a key for name resolution and routing mechanisms. The integrity is ensured by verifying that the received data corresponds to the requested name, assuming that the correct name is obtained before hand. Various accessories(e.g., authority field, query string) can be added into the name with the aim of accessing the NDO for routing requests or assisting scalable name resolution service (NRS). Further more, the ni URL scheme can also provide the integrity check for dynamically changing data by means of including a hash of a public key in the ni URL rather than the hash of the NDO.

The CCN content-based security is achieved by authenticating all content with digital signatures, and encrypting private content. Each CCN data packet is validated by a self contained signature covering the name, the content ,and a small amount of supporting data used to signature verification. Leveraging this per-packet signature scheme, CCN data becomes publicly authenticatable, which means not only the end points of the communication but also the nodes in the data forwarding path can verify that a name-content binding is signed by a particular key. The key can be obtained at a certain place indicated by a key locator included in the message. In terms of network security, the DoF attack is again the only focus of a malicious user .Two different ways to carry out the action are either hiding the legitimate content or preventing the delivery of the content by overwhelming it with massive spurious packets. To effectively defend the first case, users can put constraints on the publishers whose content can satisfy their requests. The second predicament is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

easily resolved by the interest driven communication scheme.No matter how many unsolicited data packets are produced, they will be eliminated immediately in the forwarding process.

V. CONCLUSION

The MDHT system offers an efficient, scalable solution for name resolution in information-centric networks with non-hierarchical namespaces. Preliminary simulation results that we will present in our future work show a low average latency acceptable for real-world deployment. The low latency is a result of the hierarchical, topologically embedded architecture, and locally registered information that leverages locality in the user requests.

For now, MDHT has been considered mainly for global name resolution. However, the MDHT system is suited to play a much larger role as part of an overall ICN architecture, which we will investigate in our future work. For example, MDHT nodes could also perform in-network caching, multicast support, metadata management, security and data integrity checks, data transcoding, and efficient locator selection based on network-internal knowledge. This would allow an ICN network to inherently offer services now only available via P2P overlays (BitTorrent, Skype, etc.) and external Over-The-Top services (e.g., Akamai, Google).Currently the ICN attracts much research attention from the ISP operators, Internet hardware vendors, Internet services providers and academical researchers.

REFERENCES

1 B. Ahlgren, M. D'Ambrosio, C. Dannewitz, M. Marchisio , I. Marsh, B. Ohlman, K. Pentikousis,R. Rembarz, O. Strandberg, and V. Vercellone,"Design considerations for a network of information",Proc.ReArch2008, 2008.
2 M. Artigas, P. Lopez, and A. Skarmeta,"A comparative study of hierarchical DHT systems", IEEE Conference on Local Computer Networks(LCN), pages 325 –333, 2007.
3 M. S. Artigas, P. G. Lopez, J. P. Ahullo, and A. F. G Skarmeta. Cyclone,"A novel design schema for hierarchical DHTs",Proc. IEEE International Conference on Peer-to-Peer Computing, pages 49–56, 2005.
4 M. D ' Ambrosio, P. Fasano, M. Marchisio,V. Vercellone, and M. Ullio,"Providing datadissemination services in the future Internet.",Proc.World Telecommunications Congress (WTC'08), 2008.
5 C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren,"Secure naming for a network of information",Proc.13th IEEE Global Internet Symposium, 2010.
6 P. Ganesan, K. Gummadi, and H. Garcia-Molina.Canon ,"G major: Designing DHTs with hierarchical structure", Proc. Conference on Distributed Computing Systems (ICDCS'04), pages 263–272, 2004.
7 J. F. Gantz, C. Chute, A. Manfrediz, S. Minton,D. Reinsel, W. Schlichting, and A. Toncheva,"The diverse and exploding digital universe: An updated forecast of worldwide information growth through 2011", IDC White Paper, 2008.
8 L. Garces-Erice, E. W. Biersack, P. Felber, K. W. Ross, and G. Urvoy-Keller," Hierarchical peer-to-peer systems", Parallel Processing Letters, pages 643–657,2003.
9 V. Jacobson, D. K. Smetters, J. D. Thornton,M. Plass, N. Briggs, and R. L. Braynard," Networking named content", Proc. 5th ACM International Conference on emerging Networking EXperiments and Technologies (ACM CoNEXT), 2009.
10 T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica," A data-oriented(and beyond) network architecture", Proc. ACM SIGCOMM '07, pages 181–192, 2007.
11 P. Maymounkov and D. Mazi`eres,"Kademlia: A peer-to-peer information system based on the xor metric",Proc. Workshop Peer-to peer Systems, pages 53–65,2002.
12 A. Mislove and P. Druschel." Providing administrative control and autonomy in peer-to-peer overlays", Proc. 3rd Workshop on Peer-to-Peer Systems(IPTPS'04), 2004.
13 A. T. M´yzrak, Y. Cheng, V. Kumar, and S. Savage,"Structured superpeers: Leveraging heterogeneity to provide constant-time lookup",WIAPP '03: Proc.3rd IEEE Workshop on Internet Applications, page 104, 2003.