ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

NDNoT: Name Based Routing in IoT Networks– A Survey

[I]Deepa R, [II]K Suresh Joseph
[I,II]Pondicherry University, Pondicherry, India

Abstract
Over years of pragmatic research Named Data Networking (NDN) has emerged as the future of Internet Architecture to overcome disadvantages faced in the present IP Architecture. Internet of Things (IoT) poses many stringent requirements with respect to heterogeneity, mobility, bandwidth, power, storage and computing. In the present networking scenario a wide gamut of interconnected devices need to communicate seamlessly without human intervention and poses various scalability and security issues. This paper surveys remediation of NDN Architecture design to meet challenges of IoT with respect to routing. NDN also promises efficient data retrieval solutions in both wired and wireless networks.

Keywords
Named Data Networking (NDN), Internet of Things (IoT), Wireless Sensor Networks (WSN)

I. Introduction

In recent past, nature of internet applications and changes in user's requirements have become more content centric. For Example social networking sites like Facebook, Twitter, Ecommerce applications such as Amazon, Flipkart and video archives like YouTube allows users to share texts, images, audio and video. Today most of the applications are concerned with the data irrespective of their location. However the present IP Architecture retrieves data based on its location (IP Address). NDN is completely a new Architecture which retrieves data based on content regardless to their location. Design of NDN architecture requires understanding the strength and limitations of the present IP Architecture.

II. Internet Of Things (IOT)

Internet of Things (IoT) is a term used to describe a wide range of Objects (Physical and Virtual) connected to the internet, that communicates with each other as well as with different users using various communication methods. This amalgamation of physical and virtual objects opens access to anything from any place. Physical Objects are those which exist in real and are able to sense, operate and connect to other objects. Whereas Virtual Objects are those which can be stored, accessed and processed as and when required [1].

ITU's Telecommunication Standardization Sector defines IoT as *"A global infrastructure for information society enabling advanced services for interconnecting Objects (Physical and Virtual) based on existing and evolving interoperable information and communication technologies"*.

III. Backbone of Internet of Things

Communication is the backbone for achieving IoT, which enables different objects connected to the internet to communicate between each other. Communication between objects can be realized in various ways and how this communication is achieved is insignificant. Different possible methods of communication are shown in Fig 1.

(i). Direct Communication

Objects in close proximity communicate directly by using simple radio protocols like Bluetooth or ZigBee which enable direct communication without using any communication network.

(ii). Communication through Gateway

An Object may communicate through a gateway using some protocol and then the gateway will communicate with the internet using a different protocol through a communication network.

(iii). Communication without Gateway

Two Objects located at different places can also communicate directly with each other through a communication network without using any gateway.

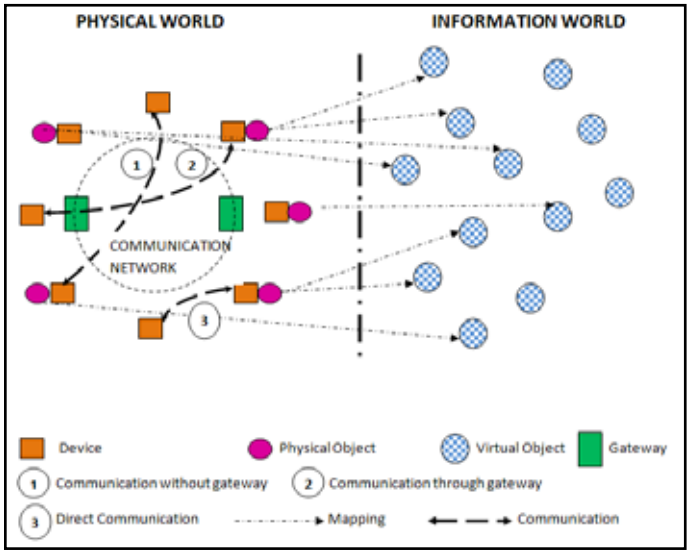

Fig 1: Internet of Things – An Overview

IV. Characteristics of IoT Devices

IoT Objects can easily be differentiated from other Objects from various salient features enumerated as under.

(i). Interconnectivity

IoT Objects can be connected to global information and communication infrastructure.

(ii). Heterogeneity

IoT Objects can communicate with other Objects through different network using different protocols or hardware.

(iii). Object Related Services

IoT Objects can provide Object Related Services like privacy and semantic consistency between physical and virtual Objects.

(iv). Dynamic Changes

The state of an IoT Object is dynamic like connected, disconnected,

sleeping etc.

(v). Enormous Scale
The number of devices connected in the network is very high compared to the Internet.

V. Named Data Networking: Design
The basic design of NDN Architecture illustrated in Fig 2 is derived [2] from the **Hour Glass Architecture** of present IP Architecture with addition of two modified layers. Firstly, **Security Layer** in NDN is inbuilt in the architecture to meet the requirements of present day's highly hostile environment. This is achieved by signing all the named data unlike IP Architecture wherein only the communication channel is secured. Secondly, **Strategy Layer** in NDN enables dynamic selection of multiple Forwarding Information Base (FIB) interfaces to forward each Interest Packet and thus enabling rich connectivity utilization and protection against route hijacking.

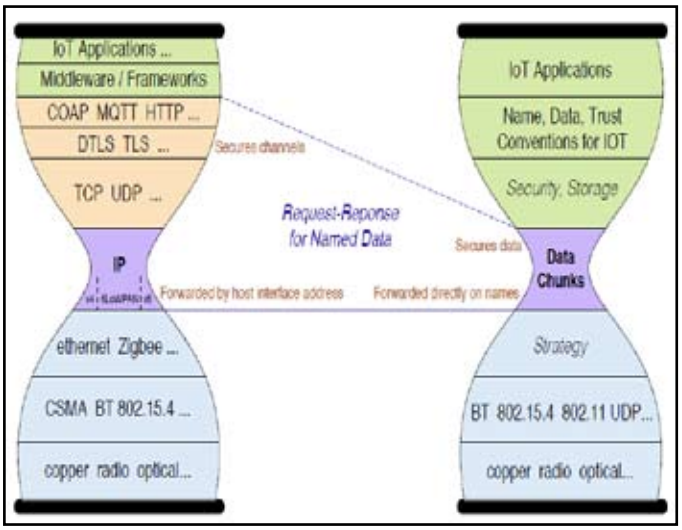

Fig 2: Hour Glass Architecture

Basic principles considered for design on NDN are enumerated as under.

(i). Universality
NDN should be a common network protocol and packet format should be flexible and extensible with all applications and wide variety of network environments ranging from constrained IoT environment to Big Data scientific application. They should support evolution of protocol without flag days i.e. should not contain any fixed parts or fixed length fields in header. The core network protocol operations should not be dependent on clock synchronization.

(ii). Data Centricity and Data Immutability
NDN should be able to fetch uniquely named immutable "Data Packets" using "Interest Packets". The Protocol and Packet format should include only elements directly related to the data i.e. universally needed and meaningful in all communication environments. Other elements needed in specific environment should go to the Network Adaptation Layer. Data immutability allows disambiguation of coordination in distributed systems that may not be always connected. Applications can make changes to communicated content by creating new version of immutable data packets.

(iii). Securing Data Directly
Data Packets should possess high security and should stay the same whether in motion or if at rest. Directly secured and uniquely named data, removes the requirement of direct channels for communication. It also enables asynchronous production and consumption of named and secured data.

(iv). Hierarchical Naming
Data Packets should have hierarchical names to enable de-multiplexing and provide structured context. Name hierarchy provides the context to implement and enforce various security models. It also allows "Flat" naming models as and when desired.

(v). In-Network Name Discovery
Interest Packets should be able to retrieve Data Packets even when incomplete names are presented. It should support dynamic production of data and should also have less emphasis on service infrastructure to achieve multiple party communications.

(vi). Hop-by-Hop Flow Balance
Each node should be able to control the load over its links using Hop by Hop Flow Balancing. Router commits bandwidth for restricted data and client node controls how much data it will receive. This ensures maximum utilization of all the links and avoids congestion on any of the links.

VI. Named Data Network: OPERATION
Communication in NDN is driven by the Consumer of Data. The Data Consumer sends out an **Interest Packet** which carries the name and identifies the required data. When the Interest Packet reaches a node containing the desired data, the **Data Packet** is issued to the Interest Packet. This activity of routing the Interest Packet and Data Packet from and to the Consumer is done by the NDN Router. The router carries out this activity using three main data structures viz. Content Store (CS), Pending Interest Table (PIT) and Forwarding Information Base (FIB) as illustrated in Figure 3.

(i). Content Store (CS)
Content Store acts as the router's buffer memory with a finite cache size in which the data is cached based on caching policy until replacement by a new content. Each data cashed can be accessed by multiple Data Consumers. Character by Character matching is carried out to search any content in Content Store.

(ii). Pending Interest Table (PIT)
Pending Interest Table contains the name of Interest Packet and the details of Interfaces from which matching Interest Packets are received. When an arrived Data Packet matches the Interest Packet, it is sent to the Data Consumer as well as to all the interfaces listed in PIT entry. The router removes the relevant PIT entry and stores it in CS. If no Data Packet arrives then the PIT entry will be removed after entry life time expires.

(iii). Forwarding Information Base (FIB)
Forwarding Information Base contains name prefixes and corresponding interfaces. The FIB is populated by name based routing protocol and is used for forwarding the Interest Packet upstream. The router remembers the interface from which the request came, and then forwards the interest packet by looking

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

up the name in FIB. This process comes to an end when the Interest Packet reaches the node which has the requested Data Packet. Now, the Data Packet is sent back to the Data Consumer by tracing the reverse path created by the Interest Packet. The Data Packet contains the name and the content of the data along with the signature (using Producer's key).
It is to be noted that the Interest Packet and Data Packet do not carry any interface addresses. Interest Packets are forwarded based on the names carried in their packet and Data Packets are returned based on the state information created by the Interest Packet at each router hop (FIB maintains the next hop).

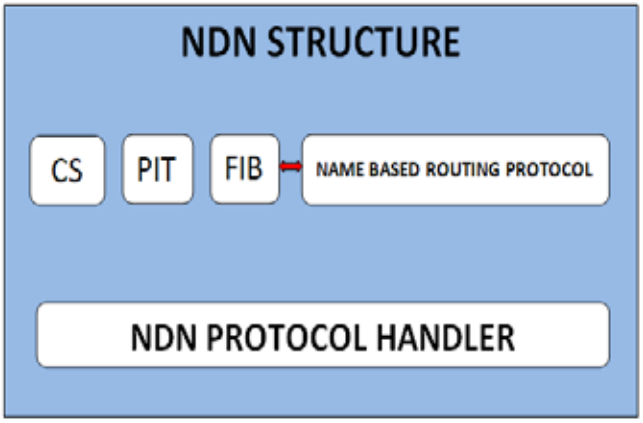

Fig 3: NDN Structure

VII. NDN For IOT

IoT being a huge set of resource constrained Objects, agile network management, scalability, security, reliability and robustness are a few critical requirements that the networking architecture should meet.
The main components of NDN viz. PIT and FIB has the capability to manage several functions like security, naming, data aggregation etc. by using name based routing at the network layer which help it meet several requirements of IoT. PIT performs interest aggregation to identify multiple requests for the same Object and process a single Interest specifically to deal with multiple data in IoT. Packet signatures in NDN ensure securing of Objects in IoT environment. Multipath routing and in-network caching and interest retransmission in NDN ensures reliable retrieval of Data. Various NDN features which help in meeting IoT requirements are listed as under.

- Hierarchical application specific names, in-network caching and interest retransmission enusres eneregy efficiency, scalability and robustness of the acrchitecture.
- Per Packet signature, origin authentication and optional data encription ensures data security.
- Location independent naming, consumer driven connection communication and multy source retrieval assists mobility of comsumers.
- Interest retransmission from consumers, retries from intermediate routers, in-network caching and multipath routing ensures high reliability of the network.

Though NDN meets most of the expectations of IoT, its architecture should be able to meet the future requirements viz large data transfers between low power and low memory Objects through wireless medium. A probable architecture of NDN that would be able to meet future requirements of IoT is shown in Fig 4.

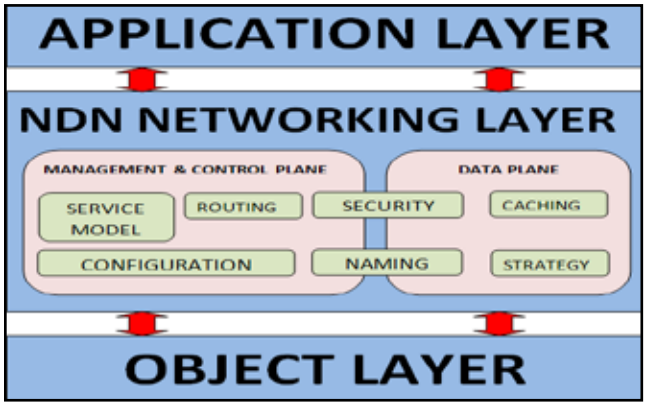

Fig 4: NDN IoT Architecture

All the heterogeneous Devices / Objects exhibiting different characteristics in terms of mobility, size, processing and storage are connected to the Object Layer. The Objects communicate with various applications through the NDN Networking Layer which masks the complexity and diversity of the devices to the Applications [3].
Data Plane of Networking Layer handles the Data, Interest Packets and operations performed on them like naming, caching, security and strategy. Designing naming structures is very crucial so that requests and information are easily understood by different entities and data sharing is possible to reduce traffic load.[4] User friendly names in NDN make it more vulnerable to security issues and spoofing. The Security module handles design of models, access control policies and authorizations methods to ensure security of Data and Interest Packets. Caching module decided the level of caching like short term or long term to meet the requirements of applications and devices. In-network caching eliminates the requirement to query the device repeatedly. Strategy module performs forwarding and transporting routines to facilitate interaction between Networking and Objects Layer.
The Management and Control Plane perform device configuration and management operations. Service model component provides wide range control and monitoring capabilities like Content Pull based on Interest and periodic of event triggered Content Push. The network setup and signalling operation for management purposes is done by the Configuration module. After configuration is completed connectivity can be established globally through routing operations. Unique and persistent content names in Name Based Routing make it very ideal for IoT applications. There is no need to resolve network addresses and constrained devices can communicate directly.

VIII. IOT routing

As shown in Fig 5 IoT architecture has three layers to fulfill its functionality, The Device Layer, The Gate Way layer and the Server or Data Center Layer.

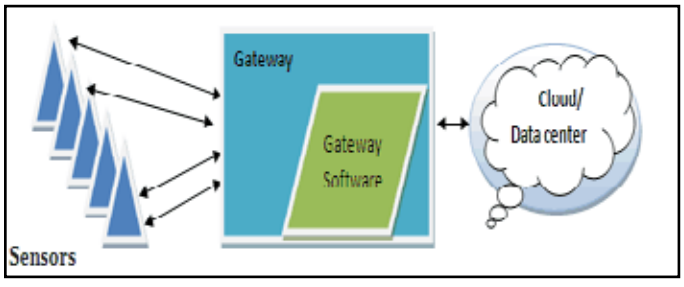

Fig 5: Internet of Things

Various routing protocol as enumerated under are designed to route the requests and data between these layers and achieve seamless networking capability in IoT.

(i). Naive Routing

In Naive Routing [5] the source nodes flood route request packets until it reaches the destination. The destination nodes reply back to the source with a route reply message. On receipt of route reply message, the source unicast data packets to the destination along the constructed route. Many of the popular adhoc routing protocols such as DSR, AODV and DSDV fall under this category.

(ii). Hierarchical Routing

In hierarchical routing [6], nodes form clusters and a cluster head is chosen in each cluster to forward data to the sink on-behalf of the cluster nodes. Cluster-heads are rotated among the nodes in the network to balance the load. This type of routing is most suitable for nodes distributed across groups.

(iii). Query Based Routing

In Query-based Routing [7] nodes disseminate data among themselves such that the querying node retrieves the data from any node in the network. Few popular query based routing protocols are SPIN and Directed Diffusion.

IX. NDN routing

In NDN routing techniques [8] decide the topologies, policies and handling of changes in routing policies and also update the forwarding table. Routing techniques decide the routes available and forwarding selects the preferred routes based on their availability status and performance. The routing techniques followed for IP based networking is required to be slightly modified in NDN networks. While IP searches the destination address in FIB, NDN searches the name prefix in FIB and fetches the required data. Link State Routing (LSR), Open Shortest Path First (OSPF) and Two Layer Routing are various routing techniques proposed future architectures for NDN.

Main parameters that indicate the performance of NDN routing are

- CPU Utilization
- CPU Time
- PIT Count
- Memory Consumption
- Network Consumption
- Interest Re Transmission Rate
- Time To Completion

(i). OSPF Routing

In NDN modified IP OSPF protocol is used for distributing name prefixes and finalizing routes making it dynamic. This protocol runs the following three modules simultaneously at every node.

- Content Centric Networking Daemon (CCND)
- OSPF Daemon (OSPFD)
- OSPF for Named data (OSPFN)

OSPF Routing in NDN works in seven main steps as listed below.

- Prepares OLSA for each name prefix, when a node boots up.
- OLSA is provided to its local OSPFD and floods the entire network.
- On receipt of OLSA, the OSPFD provides the received updated OLSA to OSPFN.
- OSPFN extracts the name prefix, router ID and created name prefix table
- OSPFN send query to OSPFD for finding next hop.
- On receipt of query OSPFD checks routing table to find next hop list, path costs and sends it back to OSPFN.
- OSPFN prepares FIB entries and updates to CCND.
- OSPF also supports multipath routing by ranking the list of next hops in CCND's FIB.

(ii). Two Layer Routing

Two Layer Routing is a combined routing protocol by merging Topology Maintaining Layer (TM) and Prefix Announcing Layer (PA) together. TM provides shortest path to upper PA and the content is published to all nodes using shortest path available to the router. Active publishing of content increases FIB entries and passive service of contents increases traffic in the network. Hence the protocol is further modified for popularity based publishing i.e. actively publish only popular contents based on their access frequency. In this protocol Name Aggression can also be applied for reduction of FIB size.

(iii). Link State Routing

Link State Routing in NDN runs on top of NDN where each packet are authenticated by originating router with signature. LSR protocol carries out the following actions to achieve effective routing.

- Names the routers, links processes and data
- Distributes the keys and trusts
- Pulls routing updates instead of pushing them
- Ranks the interfaces for facilitating multipath forwarding
- The salient difference between LSR, NLSR and Two Layer Routing is tabulated below.

Table 1: Differences - IP LSR, Two Layer & NLSR

Properties	IP LSR	Two Layer	NLSR
Sync Support	No	No	No
Push / Pull Updates	Push	Pull	Pull
Multipath forwarding	Limited	Limited	Full
Authenticity of update packets	No	No	Yes
Scalability	Poor due to fast routing convergence	Best due to slow routing convergence	Best due to slow routing convergence

X. NDNoT applications

NDN architecture and functionalities like multipath forwarding, enhanced security, named data routing, scalability, caching and mobility makes it very advantageous over current IP based internet for various future applications. NDN facilitates hassle free networking options in various domains as enumerated below.

(i). Building Automation System

There are many critical areas where automation solutions can be

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

built using NDNoT such as building home automation gateway, Building energy management system, Water management, environment control like pollution management and HVAC (Heating, ventilation and air conditioning systems) building asset management systems, and Safety Systems such as Fire/Smoke Detection and Alarm.

(ii). Vehicular Control Network

Vehicular control and communication network has gained importance with the development of smart environment or smart cities. NDN has provided mobility solution for infrastructure-less vehicular communication networks for gathering traffic information. A vehicle may also communicate with other vehicles or servers as per their requirement.

(iii). Medical Systems

NDN based health care systems are used for remote diagnosis and monitoring of patients health conditions, hygiene monitoring systems that would detect the degree of cleanliness in healthcare centres, providing better IT infrastructure to patients such as room lighting, personal control and communication with family and friends and other facility such as automatic dispensing of medicine and many other research areas.

(iv). Educational Systems

NDN has facilitated setup of ad hoc communication networks for secure conduct of meetings and lectures. Robust tele-teaching, presentations, musical rehearsals and video streaming for multiple users without client starvation has been possible by NDN.

(v). Wireless Sensor Networks

NDN benefits WSNs through fast data retrieval by using hierarchical naming, caching and flexible applications. Any object can sense communicate and share data in the network locally or remotely in various applications like home automation, health care, smart environment etc. NDN has capability to deal with heterogeneous devices easily with unbounded name spaces and reduced complexity of auto configuration. Power consumption is also on the lower side by performing in-network caching. It provides reliable network which can balance lead variations and has good fault tolerance. It also ensures unhindered communication of high mobility users providing authenticity and integrity of data.

(vi). Military Applications

NDN also presents covert ephemeral communication network to military and they provide robust, reliable and secure network suited for their tightly controlled environment. It enables transmission of messages between two nodes which become disabled after preset time limit.

XI. Conclusion

In this paper we have discussed about the IoT and NDN Design architectures, operation and routing techniques. This survey also discusses about how NDN meets IoT Requirements and NDNoT applications.

References

[1] *ITU Telecommunication Standardization Sector," ITU-T Recommendation Database", 2012 [Online]. Available:http://handle.itu.int/11.1002/1000/11559en?locatt=format:pdf&auth [Accessed 13April 2015]*

[2] *L. Zhang, D. Estrin, J. Burke, V. Jacobson, J.D. Thornton, D.K.Smetters, B. Zhang, G. Tsudik, K.C. Claffy, D. Krioukov, D.Massey, C. Papadopoulos, T. Abdelzaher, L.Wang, P. Crowley,E. Yeh, Named Data Networking (NDN) Project, 2011.[Online]. Available:http://nameddata.net/project/annualprogress-summaries/.*

[3] *Z. Ren et al., "CCN-WSN a lightweight, flexible Content-Centric Networking Protocol for Wireless Sensor Networks," in IEEE ISSNIP'13.*

[4] *R. Ravindran et al., "Information-Centric Networking based Homenet,"in IFIP/IEEE ManFI Workshop, 2013.*

[5] *T. Zahn, G. O'Shea, and A. Rowstron, "An empirical study of flooding in mesh networks," SIGMETRICS Perform. Eval. Rev., vol. 37, no. 2,pp. 57–58, Oct. 2009.*
W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energyefficient communication protocol for wireless microsensor networks," in Proceedings of the 33rd Hawaii International Conference on System Sciences-Volume 8 - Volume 8, ser. HICSS '00. Washington, DC, USA: IEEE Computer Society, 2000, pp. 8020–.

[6] *W. R. Heinemann, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," in Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking. ACM, 1999, pp. 174–185.*

[7] *Divya Saxena, Vaskar Raychoudhurya, Neeraj Surib, Christian Beckerc,Jiannong Caod et al.," Named Data Networking: A survey"in Computer Science Review 2016*

Author's Profile

Deepa R received the B.E degree from Vishweshwariah Technological University and currently pursuing my M.Tech [Network and Internet Engineering] from Pondicherry University. My area of Interest in Research is IoT, Future Internet Architectures, Sensor Networks and Cryptography.

Dr. K Suresh Joseph received the M.E. degree from University of Madras and Ph.D. degree in Information and Communication Engineering from Anna University, Chennai. Area of Specialization is Operating Systems, Analysis of Algorithms and SPM.