PUSH-BASED CRITICAL DATA FORWARDING FOR IoT IN HEALTHCARE USING NAMED NODE NETWORKING

A THESIS SUBMITTED TO THE

DEPARTMENT OF COMPUTER SCIENCE AND COMMUNICATION ENGINEERING,

THE GRADUATE SCHOOL OF FUNDAMENTAL SCIENCE AND ENGINEERING

OF WASEDA UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIRMENTS

FOR THE DEGREE OF MASTER OF ENGINEERIING

JANUARY 30th, 2018

BY

OMID JAN HUMRAZ

(5116FG06-0)

OF

SATO LAB

ADVISOR: PROF. SATO TAKURO

Acknowledgments

IN THE NAME OF ALLAH THE MOST GRACIOUS AND THE MOST MERCIFUL

First and foremost, I would like to thank almighty ALLAH for all the countless gifts given to me and making me capable of learning and completing this work. Secondly, I would like to express my immeasurable appreciation and deepest gratitude to the following persons who continuously helped me to accomplish this task:

- My Supervisor, **Prof. Sato Takuro**, your unconditional support throughout the program given me the opportunity to explore new knowledge and learn lots of valuable experiences. Without your advice, guidance and valuable comments this wouldn't be possible.
- The **PEACE** team, I would like to express my gratitude for providing the scholarship opportunity, to your support, dedication and cooperation in different situations.
- **Mom and Dad**, many thanks for your love, affection, care, trust and always support. You have devoted a lot and were aegis for me in all the tough times. You are the two precious gift of Allah and your unconditional love makes me stronger. Lucky to have you both and wish you long life.
- My beloved **spouse and lovely children**, being far from you all within this long period was really tough but your immeasurable support, messages and calls always make me stronger. I am very lucky for having you all in my life.
- Last but not the least I would like to express my gratitude to my **sister** and all **those** for being by my side and encouraging me during my studies.

Abstract

Recently Internet of Things (IoT)-based healthcare systems have facilitated remote healthcare monitoring services which offer enormous benefits over the customary healthcare monitoring systems. Healthcare IoT can provide access to services anytime and everywhere. This is particularly beneficial for those who suffer from chronic diseases and thus require regular monitoring. However, forwarding critical information regarding a patient's body, such as blood pressure, heart rate, body temperature etc., in a prompt manner to the healthcare server and caregiver units without waiting for someone to fetch the data is still the main problem. Along with this, exchange of IoT data over host-centric networks, which are different in many aspects compared to IoT networks, has many drawbacks and vulnerabilities which represent yet more problems.

To solve these problems, this paper proposes an efficient push-based critical data forwarding approach for IoT in healthcare, considering a content-centric communication infrastructure. We use named node networking, which is an Information Centric Network (ICN)-based architecture, with two new completely independent namespaces for proof of our concept. We compare our proposal with Name Data Networking (NDN). The simulation results and performance evaluation showed the feasibility and efficiency of our proposed architecture.

Keywords: Healthcare; Internet of Things; Named Node Networking; Information Centrinc Networking

Table of Contents

List of Figures

List of Abbreviations

ICT: Information and Communication Technologies

IoT: Internet of Things

IoE: Internet of Everything

RoI: Return on Investment

3N: Node Name Namespaces

ICN: Information Centric Networking

PDU: Protocol Data Units

NDN: Named Data Networking

PIT: Pending Interest Table

FIB: Forwarding Information Base

CS: Content Store

DO: Destination Only

NDNoT: Named Data Network of Things

PSIRP: Publish Subscribe Internet Routing Paradigm

CCN: Content Centric Networking

LPU: Local Processing Unit

NNST: Named Node Signature Table

NNPT: Named Node Pair Table

PoA: Point of Attachment

TCP/IP: Transmission Control Protocol/Internet Protocol

DHCP: Dynamic Host Configuration Protocol

EN: Enroll Node

IEEE: Institute of Electrical and Electronic Engineers

OEN: Offer to Enrolling Node

URL: Universal Resource Locator

AEN: Acknowledges the Enrollment of Node

NNN: Named Node Network

CHAPTER 1

INTRODUCTION

Chapter 1

Introduction

1.1 Background

The efficiency of the customary healthcare system remains a major challenge in most countries. Since services are limited to hospital facilities, people need to spend a considerable amount of their time making appointments and visiting healthcare centers. It is also inconvenient for people who suffer from chronic diseases (e.g., mental health disorder, respiratory diseases, stroke diabetes etc.,) and disabilities to regularly visit hospitals since they need regular health monitoring.

In many cases a home assistant is employed to care the patients who requires regular healthcare, but due to increasing cost it is tough for everyone to afford [13]. This further degrades the coverage of healthcare services for needy people and introduces risks to patients' welfare. Although the healthcare industry invests enough in resources and information technology, still has however failed to realize any actual advancement in patients' healthcare and easement [1]. Heterogeneous nature of hospital centric healthcare system and luck of tools for communication among specialists and patients further worsened the health services. To ensure quality, efficiency and maximum coverage of healthcare services, Information and Communication Technology (ICT) is considered to be a necessity rather than supporting tool, and it is vital to integrate information and communication technologies into the healthcare system in order to build a smart healthcare infrastructure [2]. Smart health tends to relate to the Internet of Things (IoT) using different sensors connected to smart devices.

Fig. 1 IoT Application Verticals [21]

The IoT or Internet of Everything (IoE) could have multiple application verticals e.g., shown in Fig. 1, and its integration to the healthcare, by embedding sensors into the patient's body in different manners will help in automation of various data collection related to the patient's health. IoT will improve the quality of healthcare services by avoiding human errors and collecting reliable information with minimal error rate. It will also reform healthcare in terms of reliability, privacy, security, investment and return-on-investment (ROI). This new paradigm provides us with a broad window of advancement in patient healthcare from monitoring in one vertical to diagnosing, managing and preventing chronic diseases in another.

The IoT, which is a networked connection of people, process and things at anytime, anywhere ideally using any services, can be used to monitor patients everywhere, either on the move or in their home environment while considering their privacy and liberty. The IoT can collect a vast amount of various real-time data from different sources. This can make IoT even more efficient for monitoring large number of patients connected to smart devices and healthcare sensors.

Although the smart health can reduce cost and guarantees improved healthcare services, they still have however some loopholes.

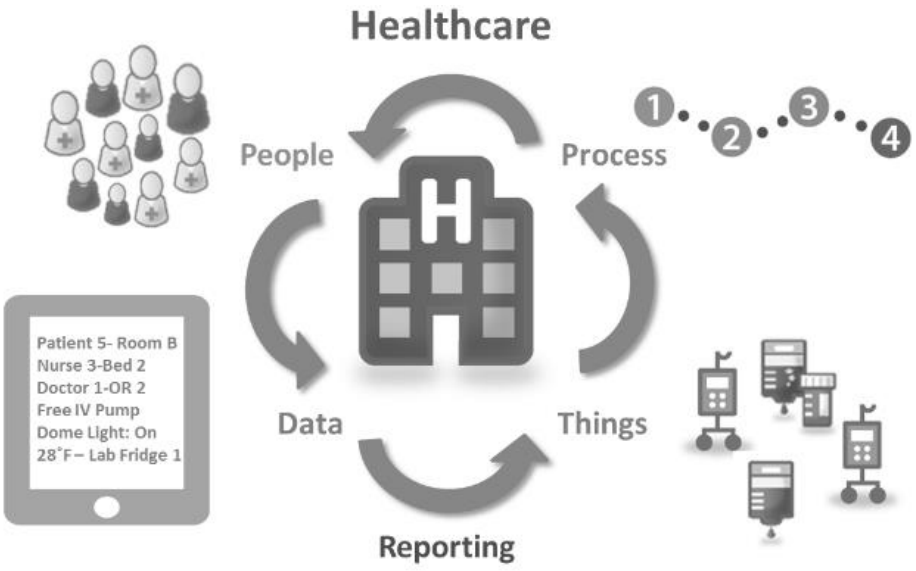

Fig. 2 Internet of Things (IoT) and Healthcare [22]

Among several issues few are prompt health data transmission to healthcare centers, reliable data transmission, scalability, security and mobility which comprise our work here. However, we especially focus on push-based data transmission to promptly forward the data to healthcare centers, considering next generation of internet as a communication infrastructure.

1.2 Motivation

The emergence of IoT has had its influence in the healthcare infrastructure by providing a wide window for advancement in the areas of communications, patient care, reducing inaccuracies and decision making. A primary perspective in the healthcare system is to regularly monitor vital signs related to patient's health (e.g., body temperature, blood pressure, heart rate)

[14]. In this context, IoT-assisted patients can be monitored regularly by doctors and caregivers, and there are many devices commonly present in the hospitals and critical care units to monitor and display the patient's health signs but the main problem is that, crucial health issues can occur at any moment, 24/7 and there could be situations where the doctor or care givers couldn't retrieve the critical health data in-time and may not be informed promptly when there is an emergency. To cope with this issue, a reliable data transmission mechanism is required to transfer critical health signs and data promptly to healthcare centers without waiting for solicitation.

Moreover, the exchange of IoT data and it's reliance on traditional IP-based internet is yet another problem. By emergence of IoT, it is estimated that more than 50 billion devices will be connected to the internet by 2020 [15] and there will be almost the shortage of available IP addresses. Along with that, the IoT is different than the traditional internet in many ways, including constraint resources such as using battery for sensors operation, memory, computational power, support for mobility, exchange of small size data (e.g., switch on or off a heating system), scalability, security and management. IP-based internet has the host-centric architecture and supports these features as add-ons which cause extra overheads for mobile users in IoT networks.

Considering the peculiarities of IoT and limitation of traditional IP-based internet, we are focusing on an approach to support the aforementioned features efficiently and could benefit healthcare services in terms of network connectivity and data communication. We used Information Centric Networking (ICN), which is a new paradigm for future internet and has the potential to benefit IoT by its simplest communication model and native support for mobility, security, information centric communication, scalability, and management as a communication

infrastructure in our study. In ICN data is the first class entity, and it is directly addressable regardless of location and what host distributes it [16]. All the data in ICN networks are exchanged through an interest packet for solicitation and data packet to deliver the actual data.

1.3 Objective

However, the ICN as a candidate for future internet has many benefits than traditional IP-based internet and can bring various improvements to IoT system but the naïve receive-driven architecture of the ICN can have some limitations that cannot be applicable in several cases especially in the healthcare. IoT has multiple application areas and in contrast to wired internet, it also has heterogeneous and very challenging environment.

There could be some instances where data generated by a producer requires immediate transmission to the specified destination without having to wait for a solicitation or interest. This creates a motive to think and create a reliable data transmission method in healthcare considering the next generation of internet as a communication architecture so, our objective in this study is to create an architecture where the data generated by sensors embedded in the patient's body is promptly forwarded to healthcare canters without waiting for interest. In this context we proposes a push-based critical data forwarding mechanism for IoT in healthcare using a named node networking [3] architecture.

Named node networking is an ICN based content-centric architecture that uses an extra namespace to identify the nodes participating in the network while, keeping the ICN native content naming namespace without any modification. The extra namespace is introduced to insure seamless producer mobility in information centric networking architecture however, it is also useful when we are intended to forward or push data to a predefined specific destination.

Although pushing is a one way data transmission which is not naively supported in ICN but, applying an additional logic and mechanisms makes it possible. Named node networking also supports scalability, built-in security, in-network cache and has the ability to retrieve data by its name independent of its location.

1.4 Contributions

To realize prompt critical data transmission in healthcare and push data to a predefined destination, in addition to naming the content in ICN, we use separate namespaces to assign names to the nodes and their physical interfaces. This is to identify each node participating in the network and to insure its reachability throughout the network regardless of it physical location. Furthermore, we have used some special transmission and mechanism Protocol Data Units (PDUs) in order to encapsulate the ICN packets into new naming architecture, handle the naming process, carry information between nodes and also realize pushing data to a predefined destination.

Our scheme improves the network performance by minimizing the network congestion through sending only critical data to healthcare centers and keeping the normal data local as well as the means of data forwarding which could enable healthcare issues to be addressed promptly and more efficiently. For performance evaluation, we simulate our proposal in nnnSIM [4] with a scenario in which a patient carrying a smart device regularly retrieves data from sensors embedded in the patient body and pushes only the critical data towards the healthcare server. We compare our proposed method with the Named Data Networking (NDN) [5] architecture with a scenario in which the healthcare server requests (pull) data from sensors embedded in patient's

body. The result shows both the feasibility and better performance of our push-based critical data forwarding architecture for IoT in the healthcare sector.

1.5 Organization of thesis

The thesis is organized as follows:

In order to have a look to some related works, in chapter II we describe literature review and similar works. To know the benefits and limitations of using ICN in IoT healthcare, in chapter III we explain the ICN framework and IoT. The chapter IV briefs about the push-based critical data forwarding approach for IoT in healthcare using named node networking architecture. Likewise, the simulation scenario, parameters and the results are also included in chapter IV. Finally the chapter V concludes the thesis.

CHAPTER 2

LITERATURE REVIEW

Chapter 2

Literature Review

2.1 Introduction

Healthcare is one of the essential needs to everyone's life. However, the luck of services and medical facilities are among the main obstacles in most countries for effective treatment. To make it more efficient and optimize the healthcare system, various IoT solutions have been proposed in the literature to facilitate healthcare services outside of a hospital environment. Many of these solutions aim at helping patients with special needs to stay at home and to be cared remotely by caregivers, rather than being confined to hospital facilities [17] Fig. 3 shows the main concept of remote healthcare service.

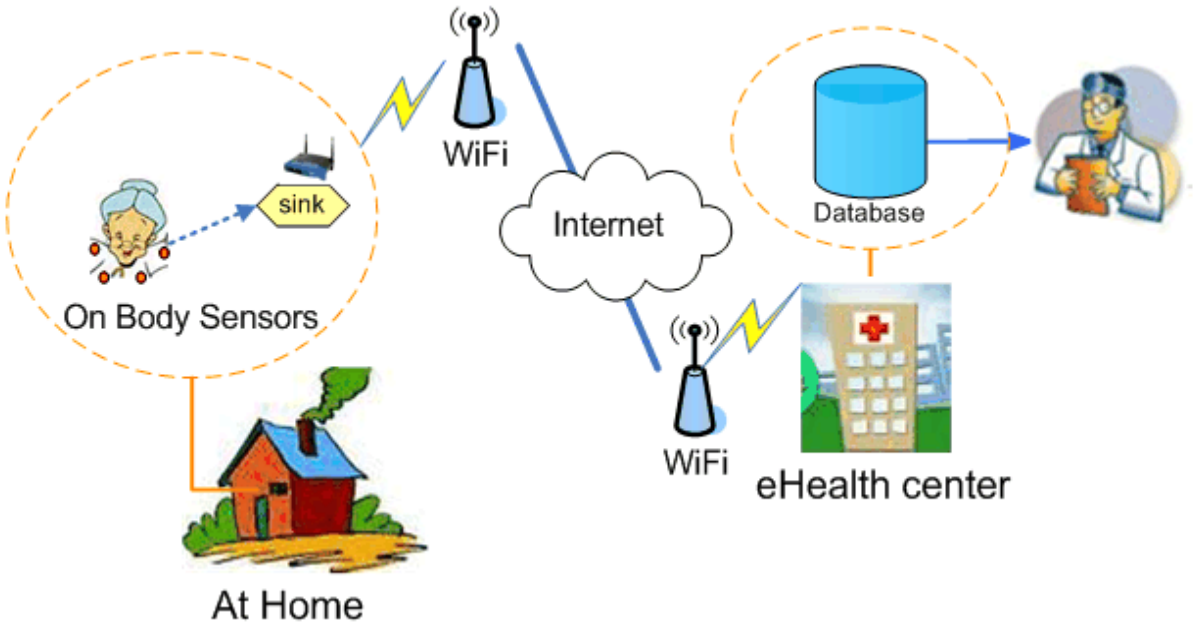

Fig. 3 IoT Assisted Healthcare Service [23]

Most of the remote healthcare services exploit mobile technologies and intelligent environment to assist and address the need of patients with chronic diseases and elderly people living in their home environment. However, most of these solutions are aiming at supporting entities rather than patients in their home environment and caregivers in the hospitals. Moreover, most of the proposed solutions are relying on traditional IP-based internet, and as of our knowledge there are few based on ICN. Some researchers have proposed push-based content forwarding using ICN as the network infrastructure, but not for healthcare.

2.2 Related Works

As mentioned, some related works are as follow: Push-based data dissemination for vehicular NDN is proposed in [6]. These authors use broadcast beacon messages in the producer to push the content into the nearest roadside unit. Each content router receiving the beacon generates synthetic interest to trigger the creation of Pending Interest Table (PIT) entries and prevent the dropping of unsolicited data. In [7] a push-pull traffic model is proposed in order to cope with the NDN's customary support of pull traffic for diverse classes in IoT. The authors classified the traffic into three types: periodical update, event-based and query-based. They also evaluated an IPv6 over NDN communication infrastructure in an IoT scenario.

A push-based distributed caching system, called P-TAC, is proposed in [8]. In this system, each content router has the option of caching and pushing when data arrive at the router. The caching stores the data in the content store while during pushing, the router asks its neighbor to store the data on its behalf. In [9] the authors divide traffic into four different categories and propose three schemes to support reliable pushing of data using IoT-NDN. Using a naming convention instead of an IP address to locate healthcare services is proposed in [2]. They used

the open mHealth architecture to build NDNoT for clinical care, remote patient monitoring and diagnosis. Finally, the authors in [3] proposed a named node networking architecture to support seamless mobility in ICN. This mechanism is orthogonal to ours. The authors added two independent namespaces in the ICN network layer while maintaining standard ICN content naming without modification.

2.3 Summary

In order to provide high availability, efficiency, quality, network connectivity, interoperability and unified remote health services, a couple of IoT based healthcare services have been proposed in literature. However, most of the proposed solutions rely on traditional internet, which suffers from different issues. To cope with it, the researchers are exploring a clean-slate and cutting edge Information Centric Networking (ICN) approach for next generation of internet where, content retrieval is based on name independent of physical location.

Many approaches using ICN as communication architecture have been proposed for different verticals but, healthcare has not yet received sufficient attention. Few papers have proposed the IoT based healthcare services using ICN as infrastructure however; the data retrieval in ICN is pull-based and may not be applicable in different situations of IoT especially for transferring critical data related to patient's health promptly to caregiver centers without waiting for interest. Moreover, since the ICN packets do not consider a specific node but instead the content, even most of the push-based ICN solutions proposed so far, forward the data to one-hope nearest device and does, not support pushing data to predefined multi-hope destination. This further creates the need and makes a space for having a reliable push-based data forwarding mechanism.

CHAPTER 3

INFORMATION CENTRIC NETWORKING AND INTERNET OF THINGS (IoT)

Chapter 3

Information Centric Networking and IoT

3.1 ICN Architecture

Information Centric Networking (ICN), which is a new paradigm for next generation of internet, attempts to consider the contents in the network as the first class entity rather being bounded to a peripheral device or location. It means that unlike the traditional host-centric based internet which uses IP address to make connections between the endpoints that are involved in data communication, ICN shifts the focus from endpoint to the information or data. All the data and packets in ICN architecture, are assigned a persistent, unique and location-independent name, and are handled by the network nodes as a self –authenticating and self-employing data unit. The consumers can directly retrieve content by its name, without considering the producers IP address and location. ICN shift the host-centric model to information-centric which implies various benefits to IoT due to its simple communication model, native support for mobility, easier data exchange, in-network caching, security and scalability. Many projects with various designs are exploring the ICN theme such as Content Centric Networking (CCN) [18] in which the network layer deals with content rather than providing communication channels between endpoints, PSIRP [19] which has the publish-subscribe architecture and define the identifiers in an information-centric manner and etc.,.

However, most of these share the same structure such as; retrieving data by name instead of IP address, defining two types packets shown in the Fig. 4 to exchange solicitation and actual data, maintain few data structures to preform content store and forwarding packets between source and

destination etc.,. We will next briefly discuss some of the general structures found in ICN architecture with special focus on Named Data Networking NDN [20].

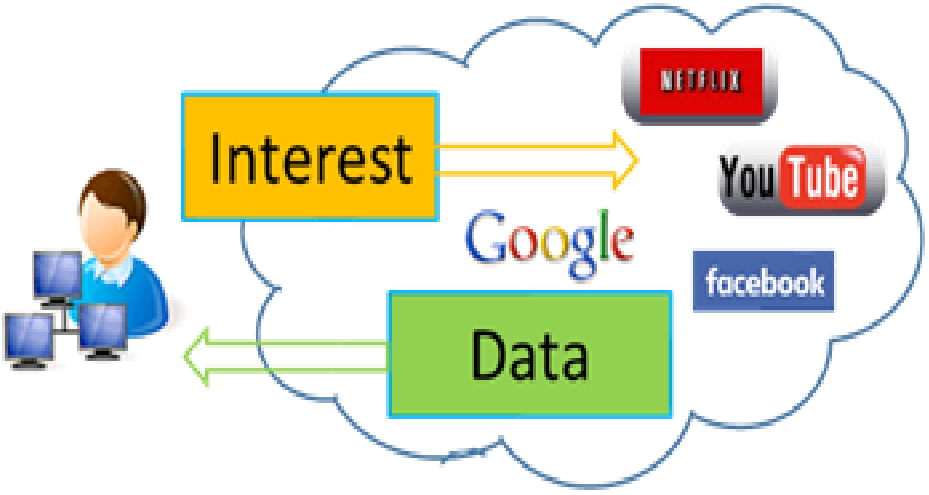

Fig. 4 Interest and Data Flow in ICN [24]

3.1.1 Packets

The ICN uses two types of packet to fetch and forward the data, consumers are required to send a packet called an interest in order to retrieve the data. The interest packet structure shown in the Fig. 5 is defined by various fields. The content name field which we will further describe it in section 3.1.2 is used to identify the desired content requested by the user and the selector field is used to deploy filters if needed by the consumer. The last field called nonce is used to introduce a randomly generated number for forwarding ICN entities to identify a specific partition for a named content and to notice if re-transmission is occurring. It means that each time an ICN node forwards an interest packet; it creates and includes a nonce in the packet till a corresponding data packet is received back. Likewise the data packet shown in fig. 6 is sent to the consumer in respond to the interest.

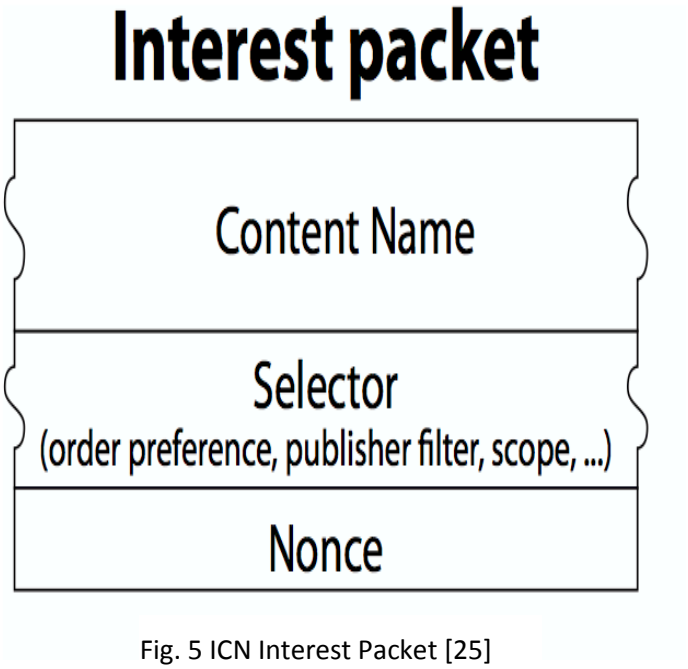

Fig. 5 ICN Interest Packet [25]

The content name field in the data packet contains the name of desired data requested by consumer through an interest and the signature field is basically used to insure the data integrity.

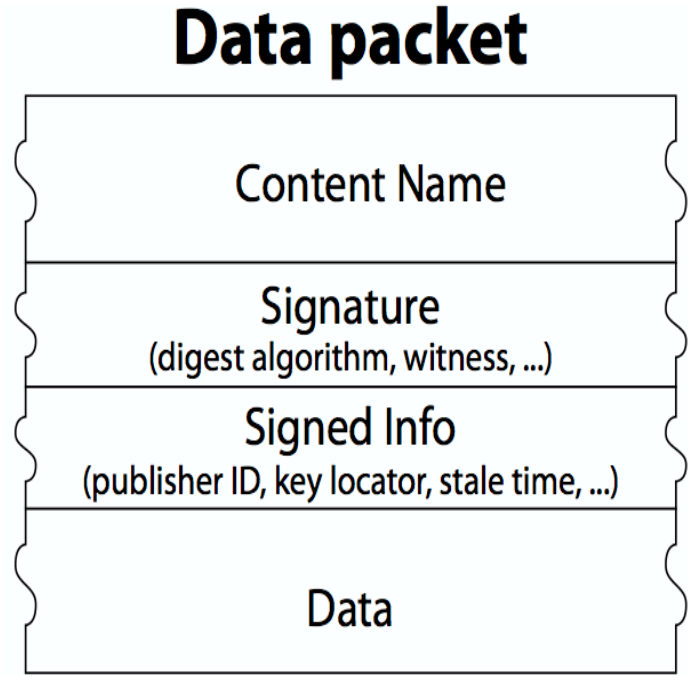

Fig. 6 ICN Data Packet [25]

To verify the integrity, the field is using a digest algorithm, which can be used to compare the recalculated digest by the receiver. Publisher of the data uses the signed info field to sign their data and ensure non-repudiation of the source and the last field contains the actual requested data.

3.1.2 Content Naming

Although many ICN naming structures have been proposed by researchers, but names in NDN are hierarchical and similar to the URL. The names are independent of particular location and even for the first part, it doesn't have to be human readable. It means that name space will be unbounded where the applications and the users must know what they require. In NDN all the content must have name and will only be reachable by its name. The user can use prefix searching and the data that fits the desired name will be returned by the network.

3.1.3 Content Store

Network devices in ICN that handles the interest and data packets generally have three main components and the Content Store (CS) is one among those. The CS is a big temporary storage similar to web cache servers in current web for named content.

In ICN when a node or router receives and interest, its first lookup is its content store; if a match is found, then the interest will be satisfied. It means that each node in ICN network that handle the data packets will store a copy of that data in the cache or CS (In-network caching) to satisfy any future interest for the same content in order to minimize the load and response time. Using this mechanism, the popular contents in the network will be spread among other nodes

which can positively affect network performance. To improve data transmission, ICN uses some strategies and replacement policies for cached named content.

3.1.4 Pending Interest Table

Pending Interest Table (PIT) stores or keeps the record of content names and incoming face of all the interest packets that has been forwarded by the node or router and not yet satisfied. As mentioned previously that when a node receive the interest packet, it will first look its CS to satisfy with data; if the data was not in the content store the node or router will create and entry in the PIT containing the content name in the interest and identifier of the face from which the interest is received and the interest is forwarded to the forwarding information based for further processing. The entry will be later used to transmit the data packet using the face identifier and content name stored in the PIT. It means that the data packet follows the reverse path in order to be delivered to the appropriate node and the PIT entry will be canceled. Data packet with no prior entry in the PIT will be assumed as unsolicited and therefor dropped.

3.1.4 Forwarding Information Base

The Forwarding Information Base (FIB) is a table which keeps information about the next-hops and uses the name-prefix match to forward the interest packet. It means that FIB maps the output faces to the information names in order to forward the interest packet to appropriate data sources. To ensure that accurate information about where the requested data is located and which hope to take to reach there, the FIB can be updated Using name-prefix base routing protocols.

3.2 ICN limitations for IoT in Healthcare

The ICN architecture and its data structures are briefly described. Although this new paradigm could benefit IoT in different perspectives but, it also has some limitations which we will describe in section 3.2.1 and 3.2.2 briefly.

3.2.1 In-network Catching

In ICN, in-network caching is considered to be an important aspect. For performance efficiency, all the routers in ICN cache the content which passes through them and stores the content in the CS. These CSs will be used to satisfy any future interest for the same content. This is not useful in some cases of the IoT, in particular in healthcare where we would like to monitor patients in real time and receive original data from the main source rather than a copy of the data from the CS of another device.

3.2.2 Receiver-driven Architecture

Likewise, receiver-driven data flow in ICN networks is also not efficient for the IoT in some instances (e.g., healthcare). This means that there is always an interest packet required in order to fetch the data but the IoT could have multiple application scopes and may generate various types of traffic. We classify the IoT traffic flow into two types:

- Pull-based traffic: this is the on-demand data generated by a query from the consumer. This may also include the data which perform a specific action and send feedback.
- Push-based traffic: this includes all the periodic and event-based data generated by a device and is required to be forwarded promptly without a solicitation.

Receiver-driven communication introduces suboptimal data forwarding delay and congestion in large-scale networks, while critical data related to the patients' health are sensitive and need to be pushed promptly to the healthcare centers. Push-based data transmission is considered to be one-way traffic and cannot be naively forwarded in ICN networks. Additional logic and mechanisms need to be applied in transport and forwarding services.

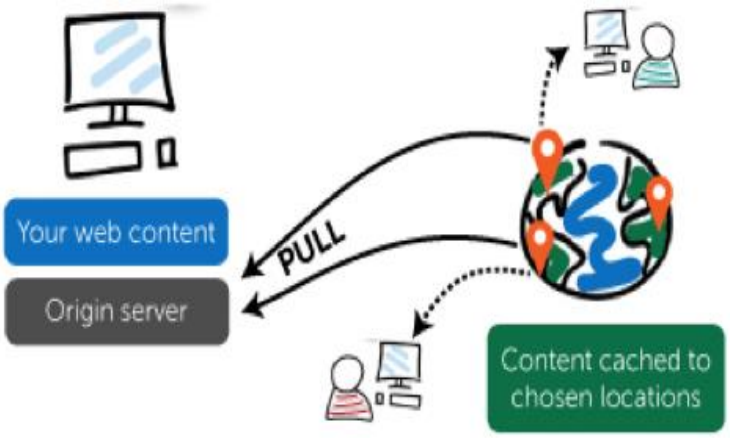

Fig. 7 Data Pull [26]

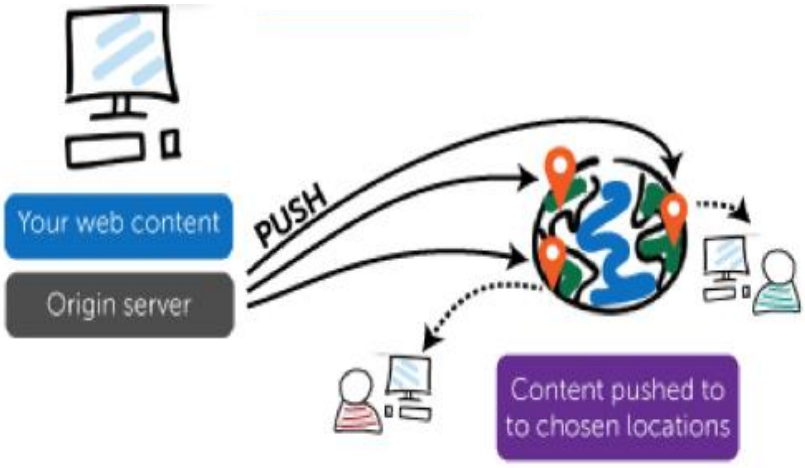

Fig. 8 Data Push [26]

CHAPTER 4

PUSH-BASED CRITICAL DATA FORWARDING ARCHITECTURE FOR IoT IN HEALTHCAR USING NAMED NODE NETWORKING

Chapter 4

Push-Based Critical Data Forwarding Architecture for IoT in Healthcare Using Named Node Networking

4.1 Architecture Framework

Considering named node networking [3], we classify the taxonomy of our architecture into four layers, as shown in Fig. 9. They are the healthcare sensors layer, Local Processing Unit (LPU) layer, Central layer and Operational layer.

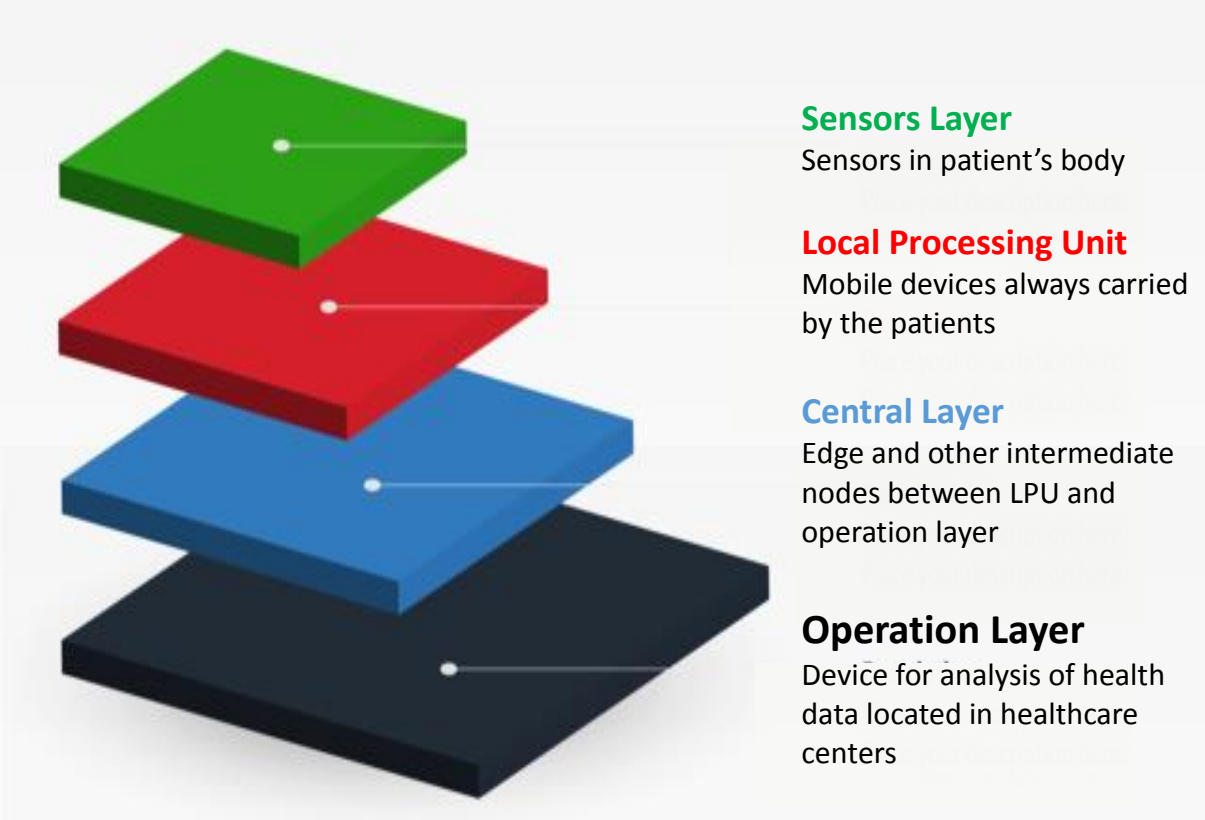

Fig. 9 Taxonomy of Push-based Critical Data Forwarding architecture for IoT in Healthcare Using Named Node Networking

Fig. 10 illustrates the classification of push-based named node network architecture for IoT in healthcare in a use case scenario.

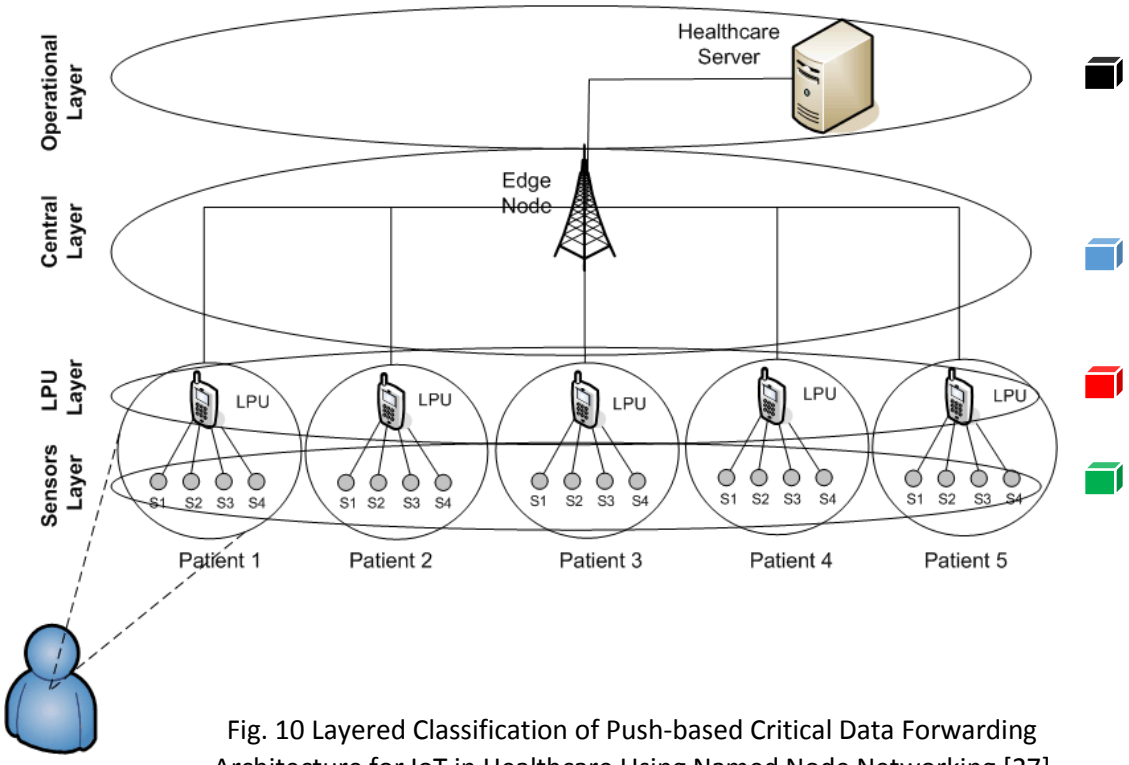

Fig. 10 Layered Classification of Push-based Critical Data Forwarding Architecture for IoT in Healthcare Using Named Node Networking [27]

We further divide the network traffic into two categories: Local area traffic and wide area traffic shown in Fig.11. Local area traffic includes all the data exchanged in a single hop between sensors and the LPU and wide area traffic encompasses all of the data exchanged in multiple hops from the LPU to operational layer. The sensors layer includes all of the healthcare sensors embedded in the patient body and always has a connection to the LPU. Sensors can be applied in different ways to a patients' body, either as a stand-alone device or may be built into clothes, jewelry or worn as a tiny patch on the skin. The sensors are responsible for replying to interests from the LPU with matching data. The LPU layer contains all of the mobile devices always

carried by the patient. These devices will act as both the gateway for the sensors and decision maker for the determination of critical data.

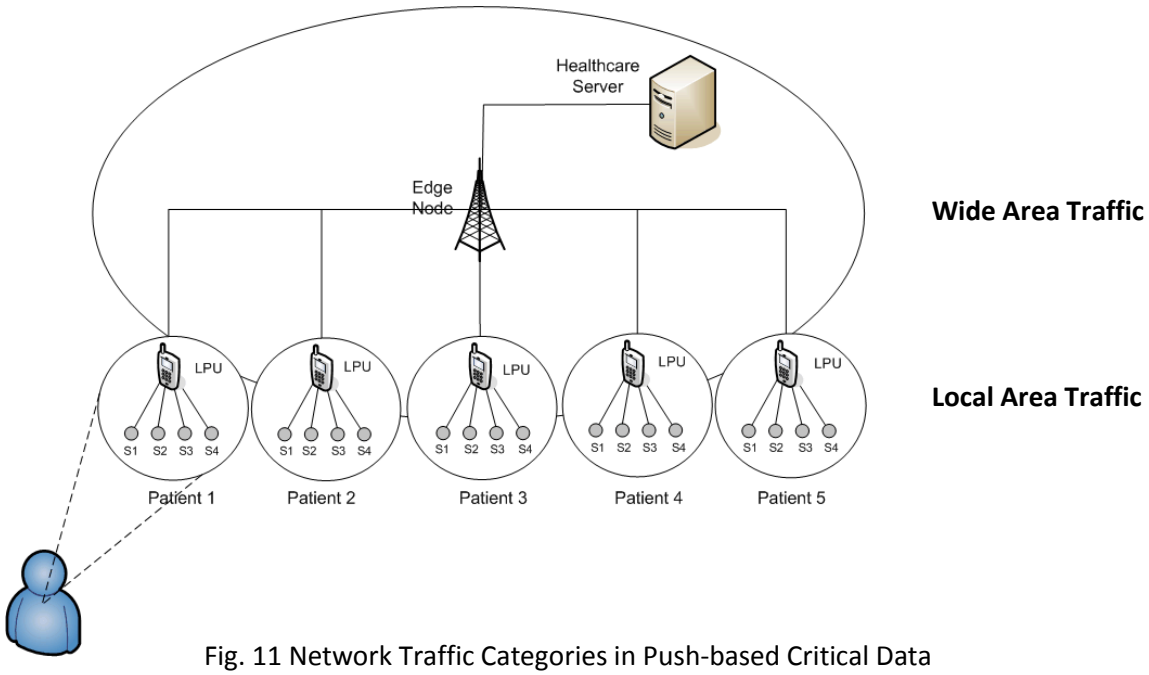

Fig. 11 Network Traffic Categories in Push-based Critical Data Forwarding Architecture for IoT in Healthcare

The LPU sends regular interest packets to the sensors and pushes the data to the wide area after the process shown in Fig. 12. To ensure the efficiency and to minimize the congestion of the network we attempted to keep the normal traffic in the local area. This means that, once the LPU has made a determination regarding the data, only the critical data will be pushed to the wide area while the normal data are stored in the content store. The central layer encompasses the edge and other intermediate nodes between the LPU and the operation layers. Finally the operation layer includes the entire device located in healthcare senders which analyze the data received from sensors and take reaction.

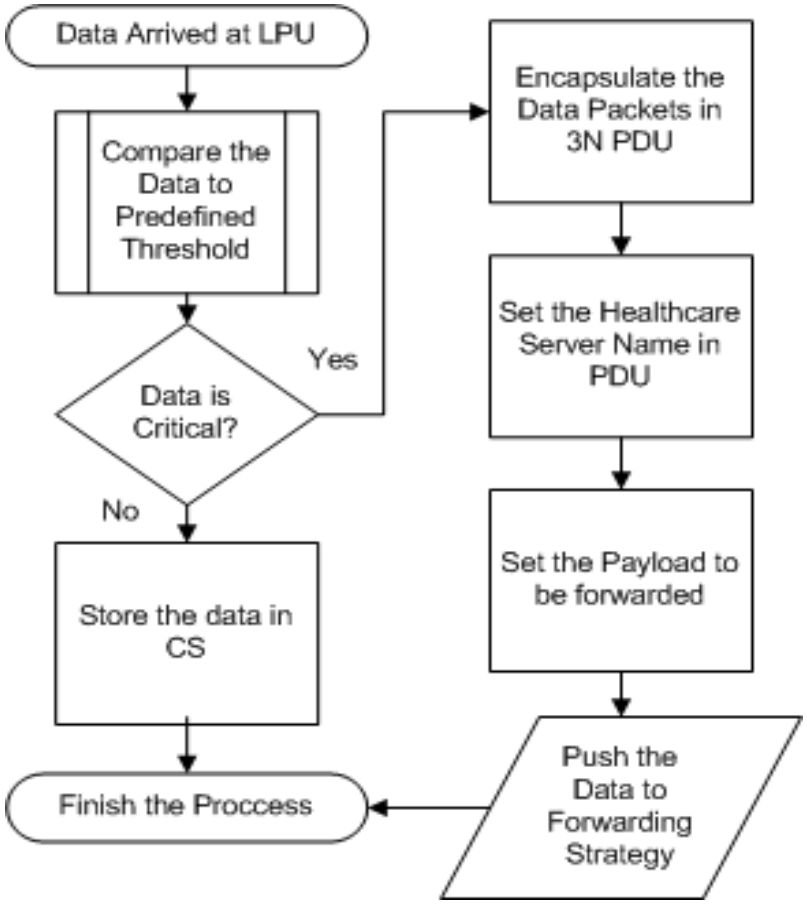

Fig. 12 Data Processing on Arrival from Sensors in Push-based Critical Data Forwarding Architecture for IoT in Healthcare Using Named Node Networking [27]

4.2 Node Naming

Since the native ICN does not care about destination or location but only the content itself therefor, to push the data to a multi-hop predefined destination, such as a healthcare server or caregiver unit we are convinced that, in addition to naming the content, a node name is also required to identify the nodes participating in the network. In this context, we use two completely independent namespaces, called Node name namespace and Point of Attachment (PoA) namespace, in ICN, while maintaining the standard ICN content naming namespace without any modification. Names in the Node name namespace will be called 3N names. The

node name namespace consist of a complex, single, multi-level hierarchal structure that is organized starting from single root to subsectors. The sectors can have either individual 3N name or additional specific sub-sector. The 3N namespace is used to assign names to every node participating in the network and also acts as the indirection level for the content namespace and PoA namespace. The PoA namespace is basically used to identify the physical interfaces between the devices or nodes in the network.

A node could be assigned a static or a dynamic 3N name by its edge node, to which it has physical connectivity. In the named node network architecture every node uses two table called Node Name Pair Table (NNPT) and Node Name Signature Table (NNST). NNPT is basically used to keep the records of the old name given by and edge node and new name given by a different edge node. The aim here is to support seamless mobility and have the update record of the node name while it is roaming from one location to another. The NNST is used to record the PoA names, the lease time of the 3N name that is dynamically assigned to the neighbor by the edge node and to maintain the mapping of the name to the PoA. Since we are considering a static use case, thus we have only used the NNST in our proposed architecture however, in real scenario it will be more likely a mobile environment. All nodes in the network, except the healthcare sensors, are capable of generating new names and have access to the NNST table. Every node participating in the LPU and operation layers will go through a naming process by using some mechanism Protocol Data Units which we will describe in section 4.3.

4.3 Protocol Data Units (PDUs)

To assign names for the node, each node participating in the network should go for an enrollment process and should ask for a fixed 3N name by issuing a mechanism PDU, called an

Enroll Node (EN). The EN is used to obtain a single 3N name for a node participating in the network, regardless of the number of interfaces. This is to ensure that the device assigning the names receives all of the possible PoAs the new device can use. Basically, any node can be delegated in the named node architecture to assign the 3N names for new nodes by issuing another mechanism PDU, called an Offer to Enroll Node (OEN). The OEN is used to offer a name to a node enrolling into a sector or edge device. This naming procedure is different from TCP/IP's DHCP in a sense that, for enrollment, timer-based protocol is used and any node enrolling to a sector will obtain only a single 3N name. Once the new node or device received the OEN or name, the process will ends through the generation of an acknowledgment PDU, called an Acknowledge the Enroll Node (AEN). In our architecture, the central layer is responsible for assigning the fixed names dynamically to all devices in the LPU and operation layers. However, we have assigned to the central layer device itself a static name.

With this new structure, every node in the architecture will have a 3N name and would be reachable, regardless of its location. However, to realize push-based critical data forwarding, a special mechanism to encapsulate ICN packets into the 3N architecture and to carry information between nodes is also required.

4.4 Push-based Data Transmissions

In order to encapsulating the ICN packets to 3N architecture and handling the new naming process, for pushing the data to a predefined destination, override of the PIT decisions is also required, since pushing is a form of one-way data transmission with no prior PIT entry, it would be assumed to be unsolicited data in ICN. To overcome this, and make data pushing to a specific destination feasible, we used another special data transmission PDU, called a DO. Regardless of

the source name, the DO uses only the destination node's name for data transmission. This means that, by using the new naming structure, we can forward data to a predefined destination. In our scenario shown in Fig. 13, we have used the name of the healthcare server located in the operational layer as a constant destination in the DO and we push the data towards the forwarding strategy for further processing. Unlike the normal ICN, here we use the DO to override the PIT decisions and use the NNST as the final arbiter to check which route should be taken. Moreover, the DO is also used to encapsulate the ICN packets into the 3N architecture.

Contrary to other NDN push-based architectures which only push the data to one hop, our proposed architecture ensures efficient data pushing to a multi-hop predefined destination with better performance and mobility. Our approach could have multiple application aspects, however; we have only analyzed its efficiency in the healthcare.

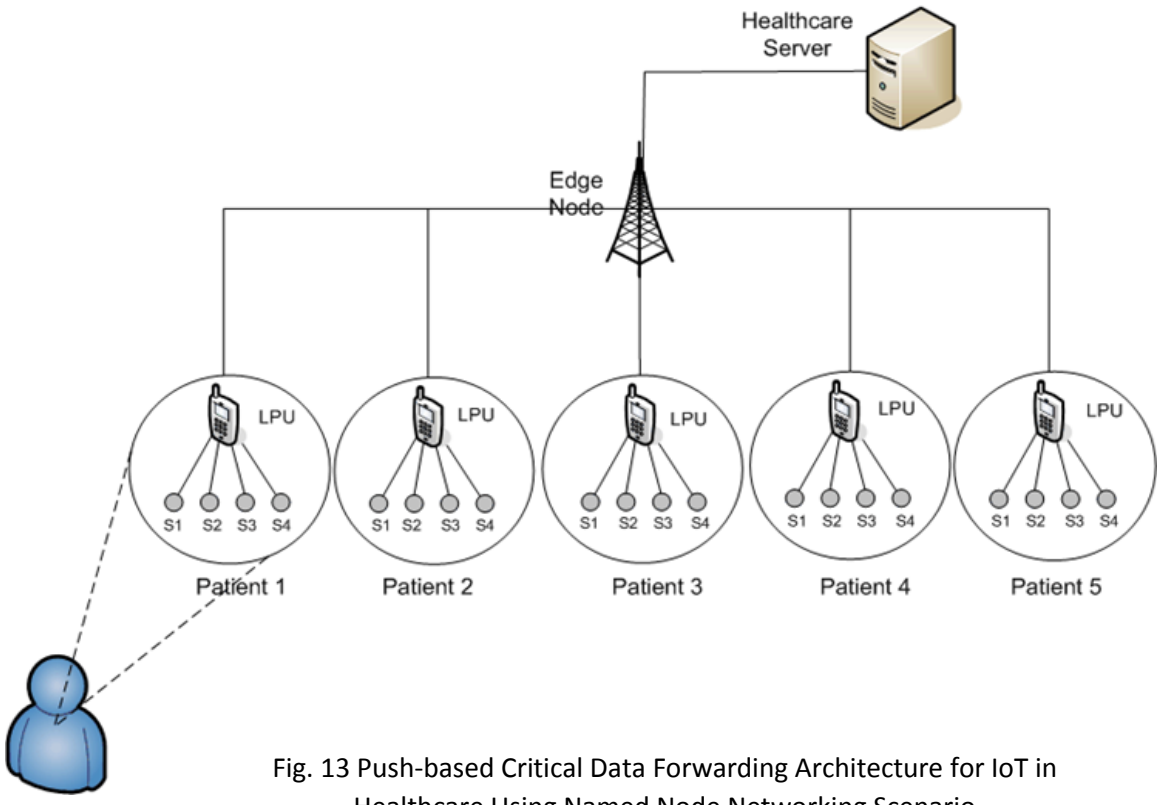

Fig. 13 Push-based Critical Data Forwarding Architecture for IoT in Healthcare Using Named Node Networking Scenario

The patient can roam anywhere and at any time without needing to be concerned about health monitoring and reporting any critical issues to the healthcare center. The patients only need to carry a mobile device (LPU). As soon as the mobile device detects any abnormal sign in the patient's body, it will promptly push this to the healthcare center for a further decision. Next we will be discussing the simulation and the results.

4.5 Simulation Scenario

To evaluate the performance of our proposed architecture, we simulate our architecture shown in Fig. 4.5 with nnnSIM [4] which is an ns-3 [10] module that executes our topology. We have considered a tree topology with a scenario in which five patients have four different healthcare sensors (e.g., blood pressure, heart beat, body temperature and movement) embedded in their bodies. The patients carry a smart mobile device (LPU) which regularly retrieves data from the sensors and only pushes it to the healthcare server when it is deemed to be critical. The simulation parameters are listed in Table 1.

All nodes are connected via point-to-point links. Considering the IEEE 802.15.6 [12] standard, which supports medical and nonmedical applications by using multi-level security, low energy consumption, higher data transmission and different frequency band usage, we have set the data transmission rate of the sensors to 10 Mbps, we set the link capacity between the sensors and the LPU to be lower than other devices with higher channel delay. Although the healthcare sensors exchange small size data in real cases (e.g., sending data about patient's heart beat to healthcare unit), to ensure good performance, the payload size is set to 1024 Bytes with a frequency of 10 interests per second.

Table 1 [27]

Simulation Parameters	Value
Number of Sensor Nodes	20
Number of Gateway (LPU)	5
Number of Edge Nodes	1
Number of Healthcare Server	1
Link Capacity (Sensors to LPU)	10 Mbps
Link Capacity (Other Nodes)	100 Mbps
Link Delay (Sensors to LPU)	10 ms
Link Delay (Other Nodes)	3 ms
Payload Size	1024 Byte
Content Store Size	1000 Object
Forwarding Strategy	Smart Flooding
Interest Packet Generation	10/s
Simulation Time	100 s

All nodes in the topology have the standard ICN CS, Forwarding Information Base (FIB) and PIT data structures. The PIT has a capability equivalent to the 3N and NNST functions. The CS is set to one thousand objects with freshness and the least recently used replacement policy. We chose smart flooding as the forwarding strategy for all nodes in the topology and set a 50 milliseconds delay in order to perform data determination before pushing the data to the forwarding strategy. To compare the results we also run the same scenario with the same parameters in ndnSIM [11] without any modification to NDN default functionalities. Unlike the

previous architecture, in this scenario the healthcare server pulls the data from the sensors attached to the patient's body by sending regular interests.

4.6 Results and Discussion

In the simulation the following performance metrics are analyzed:

Network Delay: the network delay is considered to be an important metric in patient monitoring, especially for sensitive data, including the handling of emergency data for medical applications where long delays cannot be tolerated. Fig. 14 shows the network delay for push-based critical data forwarding using the named node network architecture. Likewise, Fig. 15 shows the network delay for a pull-based network architecture using NDN.

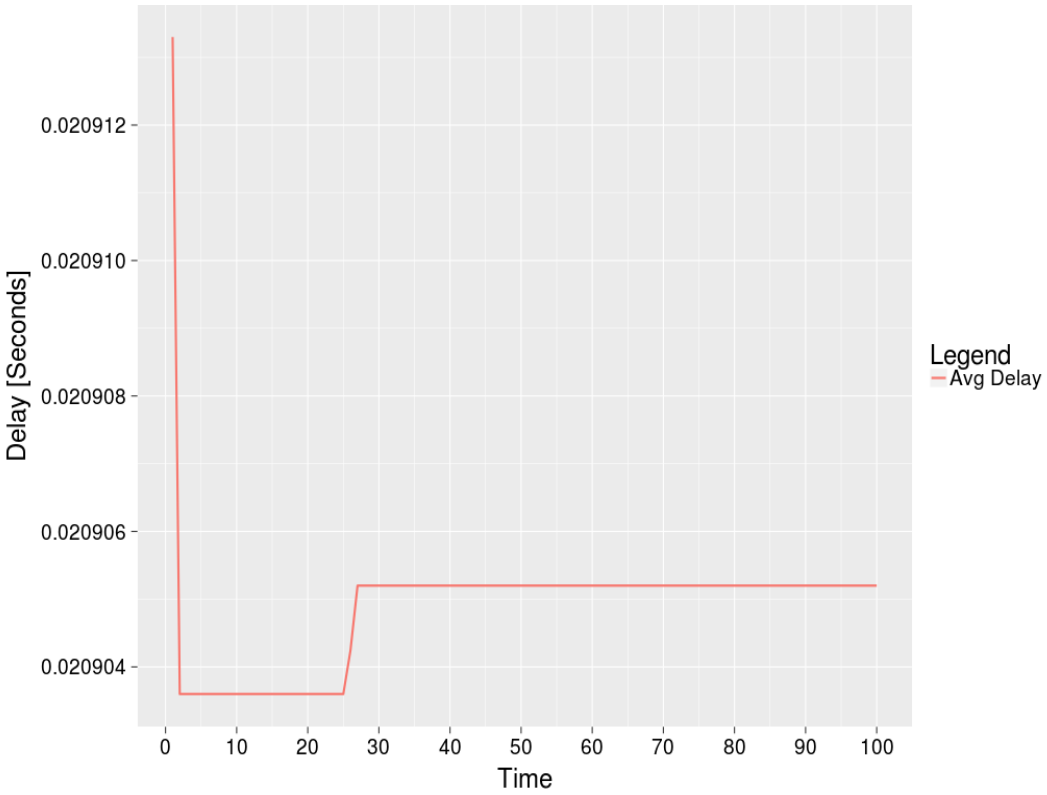

Fig. 14 Average Network Delay in Push-based Critical Data Forwarding Architecture for IoT in Healthcare Using Named Node Networking [27]

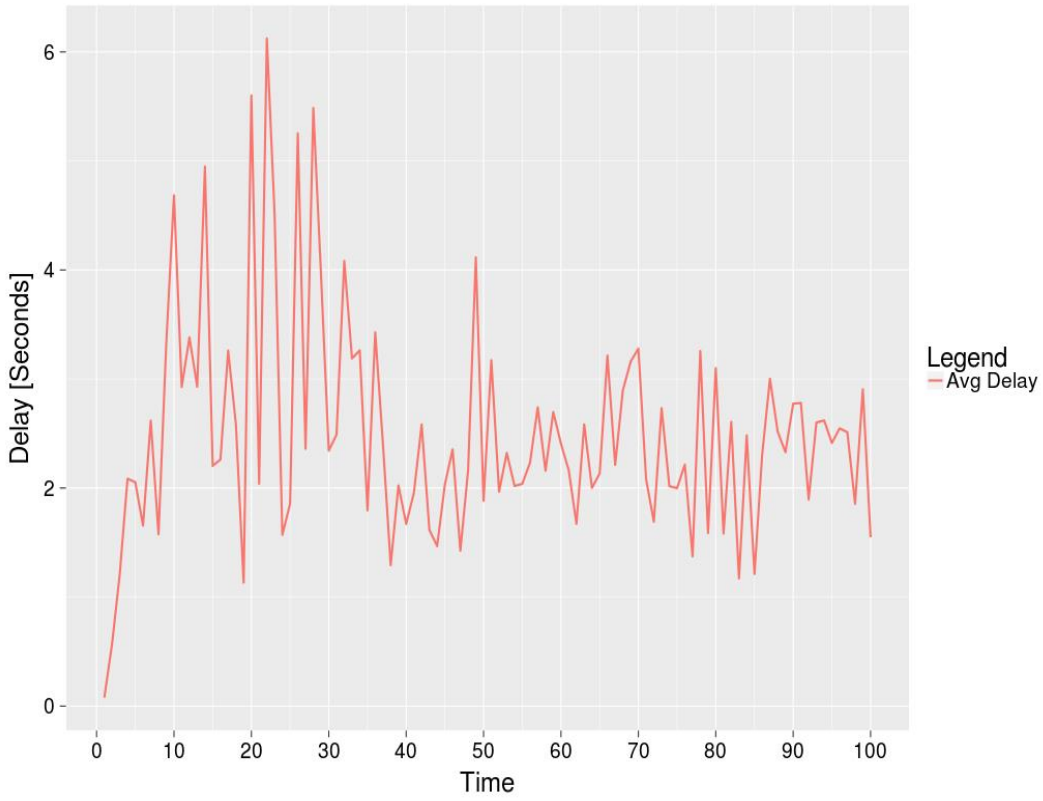

Fig. 15 Average Network Delay in Pull-Based Architecture Using Named Data Networking [27]

The outcome shows that our proposed model has lowest delay compared to Named Data Networking. In the NDN the interest propagation using smart flooding forwarding strategy for various data in the pull-based NDN architecture is not proportional. This disproportional propagation of interests in NDN network causes network delay and decreases the overall network performance. It can cause even more network delay as the variety of data and the number of sensors increases while the push-based named node network architecture performs better with lowest network delay.

Network Data Rate: the network data rate is considered to be the other important metric in networks. Fig. 16 shows the network data rate for push-based critical data forwarding using named node network architecture while Fig. 17 shows the same for the pull-based network architecture using NDN. Simulation results show that our proposed architecture outperforms NDN. In the pull-based NDN structure, the variety of data and the smart flooding forwarding strategy negatively affects the network data rate and performance. We also simulate the NDN pull-based scenario with flooding forwarding strategy and the results shows that flooding forwarding strategy for various data shown in Fig. 18 and Fig. 19 has better performance in NDN compared to smart flooding forwarding strategy.

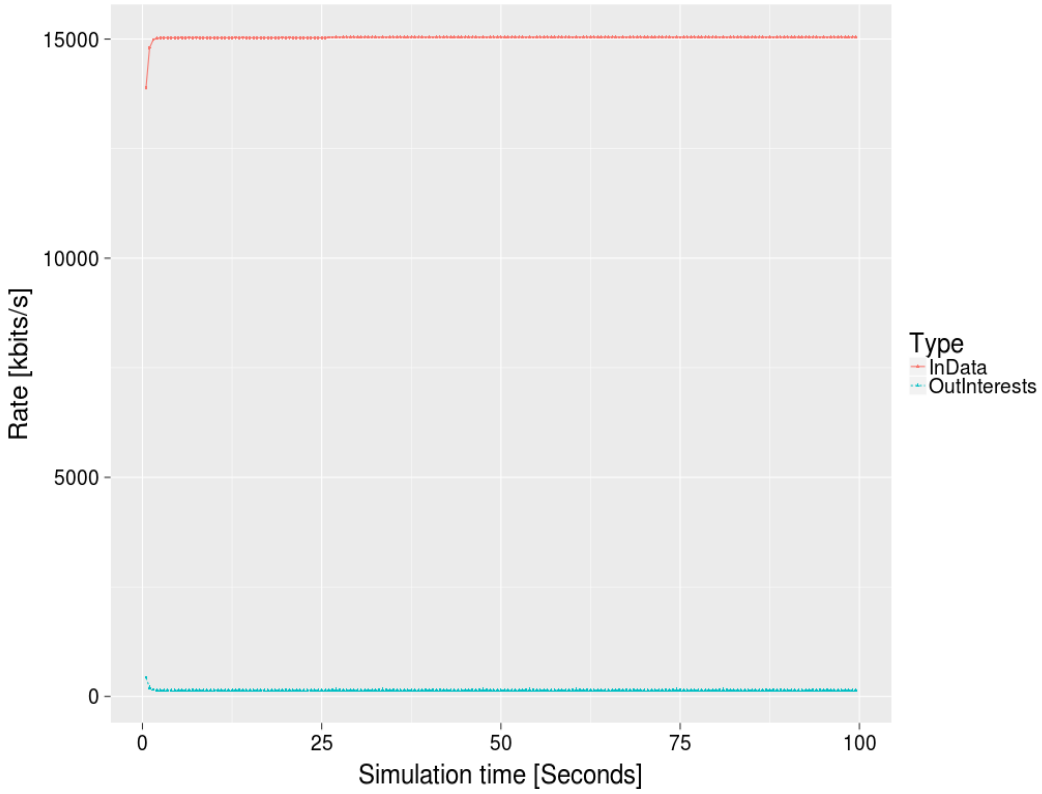

Fig. 16 Average Network Data Rate in Push-based Critical Data Forwarding Architecture for IoT in Healthcare Using Named Node Networking [27]

Since in pull-based architecture there is always an interest required to fetch the data thus, the flooding forwarding strategy introduces network congestion in the large-scale networks and may cause many packet drops if the network bandwidth is congested. Even if we compare the result of push-based critical data forwarding using named node networking with named node networking using flooding forwarding strategy, the result again shows that our proposed architecture performs better.

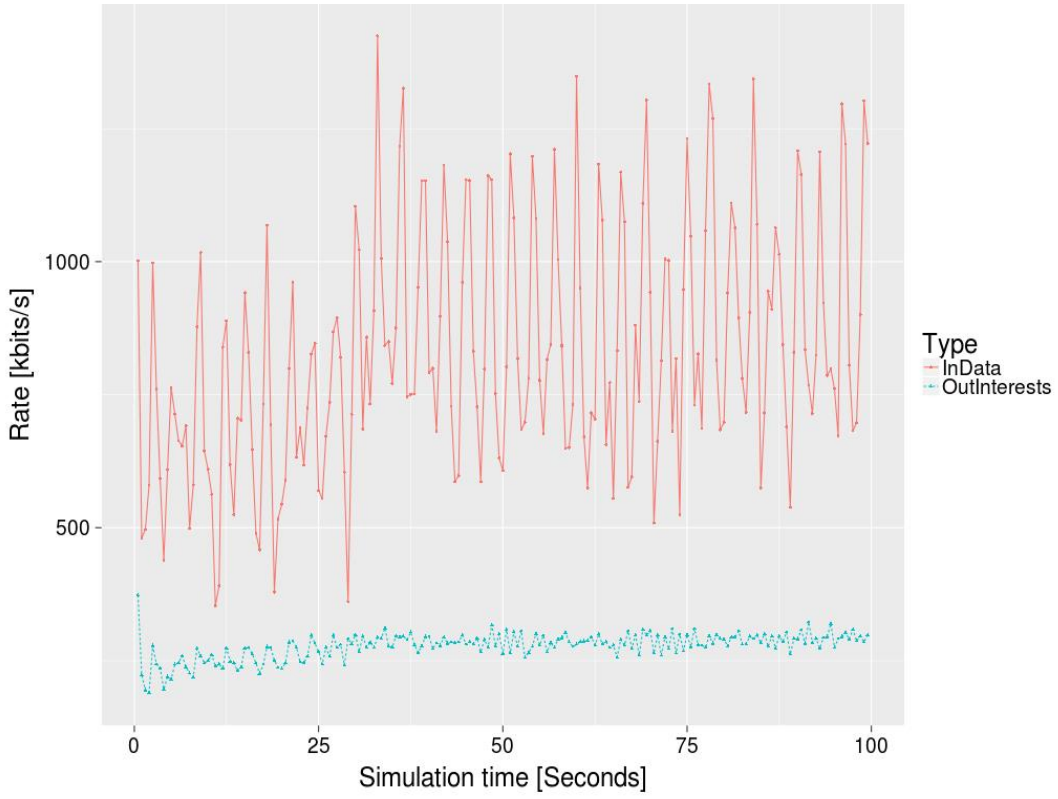

Fig. 17 Average Network Data Rate in Pull-Based Architecture Using Named Data Networking NDN [27]

As the result shows in our proposed model, few kilobits of bandwidth are consumed for sending the interest while in pull-based NDN architecture, we see that considerable amount of bandwidth is used for sending interest. Likewise in pull-based architecture, when an interest is forwarded to fetch the data, that interest is going through some lookup process like CS and PIT which may cause to introduce more delay compare to push-based architecture in the large scale networks.

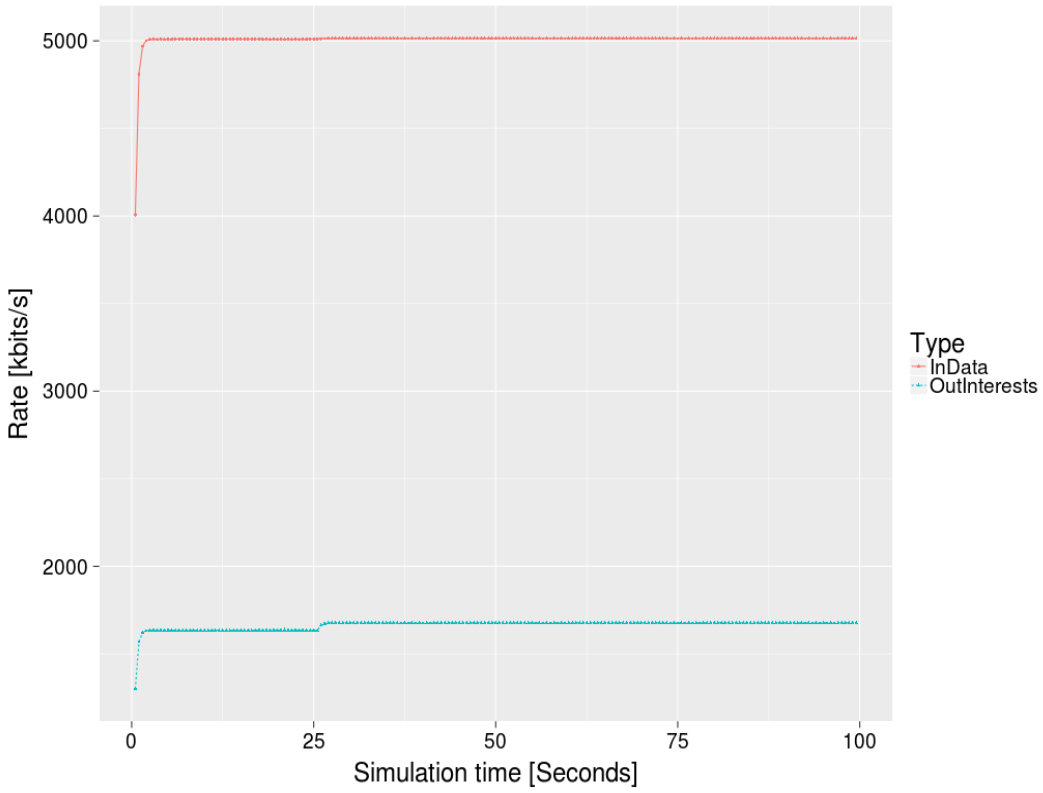

Fig. 18 Average Network Data Rate in Pull-Based Named Data Networking (NDN) Architecture Using Flooding Forwarding Strategy [27]

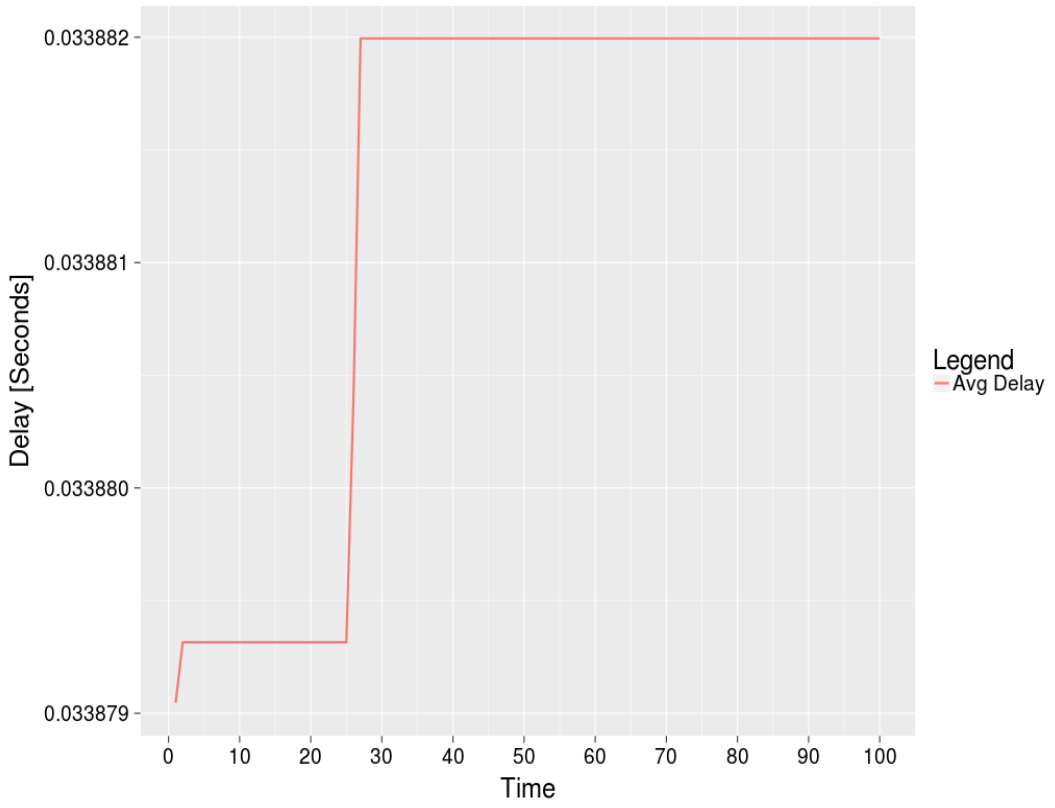

Fig. 19 Average Network Delay in Pull-Based Named Data Networking (NDN) Architecture Using Flooding Forwarding Strategy [27]

CHAPTER 5

CONCLUSION

Chapter 5

Conclusion

Hospital-centric healthcare is not sufficiently efficient since all of the facilities are thus limited to the hospital environment. The IoT, as a new paradigm, creates the possibility for extensive developments in healthcare services. However, IoT networks that rely on IP-based internet have various vulnerabilities including scalability, mobility and security. ICN, as a promising architecture for the future internet and a replacement for IP-based system, brings many benefits to the IoT due to its simple communication model, built-in support for scalability, mobility, in-network caching and security. Conventional ICN, with its receive-driven architecture, is in many cases not effective for monitor the health of patients by, for example, monitoring patients and sending any critical health signs promptly to the caregiver units without waiting for someone to fetch these critical data.

In order to provide reliable healthcare in terms of patient monitoring, we have proposed a push-based critical data forwarding mechanism for the IoT in healthcare considering ICN as a communication infrastructure. In order to identify the nodes participating in the network regardless of their locations, we have used a named node network architecture to assign names to the nodes in addition to naming the content. To handle the new naming approach and to realize the ability to push data to a multi-hop predefined destination we have also considered using the PDUs to process the name assignment and to encapsulate the ICN packets to a new naming structure and forward data between nodes. Simulation result shows the efficiency and feasibility of our proposed approach compared to NDN architecture in terms of network delay and the network data rate.

References

[1] S. Tyagi, A. Agarwal and P. Maheshwari, "A conceptual framework for IoT-based healthcare system using cloud computing," 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), Noida, 2016, pp. 503-507.

[2] Divya saxena, Vaskar Raychoudhury, Nalluri SriMahathi, "SmartHealth-NDNoT: Named Data Network of Things for healthcare services", Proceeding of the 2015 Workshop on Pervasiv Wireless Healthcare, Hangzhou, China, pp. 45-50.

[3] J. E. López, M. Arifuzzaman, L. Zhu, Z. Wen and S. Takuro, "Seamless mobility in data aware networking," 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015), Barcelona, 2015, pp. 1-7.

[4] [4] https://bitbucket.org/nnnsimdev/nnnsim

[5] NDN project team, "Named Data Networking (NDN) project", NDN Technical Report NDN-0001, October 2010.

[6] M. F. Majeed, S. H. Ahmed and M. N. Dailey, "Enabling push-based critical data forwarding in vehicular Named Data Networks," in IEEE Communications Letters, vol. 21, no. 4, pp. 873-876, April 2017.

[7] S. Muralidharan, B. J. R. Sahu, N. Saxena and A. Roy, "PPT: a push pull traffic algorithm to improve QoS provisioning in IoT-NDN environment," in IEEE Communications Letters, vol. 21, no. 6, pp. 1417-1420, June 2017.

[8] K. Mori, T. Kamimoto and H. Shigeno, "Push-based traffic-aware cache management in Named Data Networking," 2015 18th International Conference on Network-Based Information Systems, Taipei, 2015, pp. 309-316.

[9] M. Amadeo, C. Campolo and A. Molinaro, "Internet of Things via Named Data Networking: the support of push traffic," 2014 International Conference and Workshop on the Network of the Future (NOF), Paris, 2014, pp. 1-5.

[10] https://www.nsnam.org/

[11] ndnSIM: https://github.com/named-data-ndnSIM/ndnSIM.git ns-3/src/ndnSIM

[12] Rim Negra, Imen Jemili, Abdelfettah Belghith "Wireless body area networks: applications and technologies" The Second International Workshop on Recent Advances on Machine-to-Machine Communications, Procedia Computer Science, vol. 83, 2016, pp. 1274-1281.*Telecommunications and Information Technology (ECTI-CON),* Nakhon Ratchasima, 2014.

[13] A. Al-Adhab, H. Altmimi, M. Alhawashi, H. Alabduljabbar, F. Harrathi and H. ALmubarek, "IoT

for remote elderly patient care based on Fuzzy logic," 2016 International Symposium on Networks, Computers and Communications (ISNCC), Yasmine Hammamet, 2016, pp. 1-5.

[14] M. S. D. Gupta, V. Patchava and V. Menezes, "Healthcare based on IoT using Raspberry Pi," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015, pp. 796-799.

[15] Cisco white paper, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[16] J. Burke, P. Gasti, N. Nathan and G. Tsudik, "Secure Sensing over Named Data Networking," 2014 IEEE 13th International Symposium on Network Computing and Applications, Cambridge, MA, 2014, pp. 175-180.

[17] F. Corno, L. De Russis and A. M. Roffarello, "A Healthcare Support System for Assisted Living Facilities: An IoT Solution," 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, 2016, pp. 344-352.

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

[19] D. Trossen (ed.), "Architecture definition, component descriptions, and requirements", PSIRP project, 2009.

[20] Nsf named data networking project. http://www.named-data.net, June 2014. Accessed:

2014-06-07.

[21] Cisco Network Academy, IoE webinars, IoE and Healthcare, https://www.netacad.com/careers/webinars/opportunities-in-tech/-/asset_publisher/xUXSnCQaZ4Nt/content/introduction-to-digitization-and-internet-of-everything/, 2016

[22] https://www.linkedin.com/pulse/internet-things-iot-lamp-aladdin-healthcare-industry-raj-shah

[23] http://bbcr.uwaterloo.ca/~x27liang/seehealthbib.htm

[24] https://www.nist.gov/programs-projects/information-centric-networking-program

[25] https://named-data.net/project/archoverview/

[26] https://cdn.net/push-vs-pull-cdn/

[27] http://www.ieice.org/~icn/wp-content/uploads/2017/12/icn_201712_5.pdf