Push-Based Critical Data Forwarding Mechanism for IoT in Healthcare Using Named Node Network

Omid HUMRAZ Ahmad Shahpoor SERAJ Sato TAKURO

Graduate School of Fundamental Science and Engineering, Waseda University, Tokyo, Japan

E-mail: Omidhumraz@fuji.waseda.jp, Serajsa@akane.waseda.jp t-sato@waseda.jp

Abstract 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 Centric Networking

1. Introduction

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 and disabilities to regularly visit hospitals since they need regular health monitoring. Although the healthcare industry invests enough in information technology, still has however failed to realize any actual advancement in patients' healthcare and easement [1].

To ensure quality, efficiency and maximum coverage of healthcare services, it is vital to integrate Information and Communication Technologies (ICT) 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. The IoT will 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. Although IoT-assisted patients can be monitored regularly by doctors and caregivers, the main problem is that, crucial health issues can occur at any moment, 24/7, and 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. The IoT is different than the traditional internet in many ways, including constraint resources, support for mobility, exchange of small size data (e.g., switch on or off a heating system), scalability, security and management. IP-based internet supports these features as add-ons which cause extra overheads for mobile users in IoT networks.

In order to address the aforementioned problems, this paper proposes a push-based critical data forwarding mechanism for IoT in healthcare using a named node networking [3] architecture which has the ability to support Information Centric Networking (ICN), scalability, security and mobility. To realize this push of 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. Furthermore, some

special Protocol Data Units (PDUs) are used to encapsulate the ICN packets, handle the new naming process and also carry information between nodes. Our scheme improves the network performance 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 and the result shows both the feasibility and better performance of our push-based critical data forwarding architecture for IoT in the healthcare sector. The remainder of this paper is organized as follows. In section 2 we describe related works and in section 3 we explain the push-based critical data forwarding approach for IoT in healthcare. Simulation results are described in section 4 and section 5 concludes the paper.

2. Related Work

Various IoT solutions have been proposed in the literature to facilitate healthcare services outside of a hospital environment. However, most of these solutions are IP-based and few are based on ICN. Some researchers have proposed push-based content forwarding using ICN as the network infrastructure, but not for healthcare. For example, 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. However, in this method, content can be only pushed to the one-hop neighbor and not to a multi-hop specific destination. 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.

Since the NDN packets do not consider a specific node but instead only the content, most of the above solutions do not support pushing data to a predefined destination. 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.

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

3.1 Information Centric Networking and IoT

ICN, as a new model for the future internet, can bring various benefits to IoT due to its simple communication model, support for mobility, in-network caching, security and scalability. Many projects with various designs are exploring the ICN theme. However, most of these share the same structure such as; retrieving data by name instead of IP address, defining two types of interest and data packets to exchange solicitation and actual data, Content Store (CS) to cache the content corresponding to an interest, Pending Interest Table (PIT) to keep an entry for previously forwarded interests until they are satisfied and Forwarding Information Base (FIB) to retain data about next hop.

In ICN, when a node receives an interest, its first lookup is its content store; if a match is found, then the interest will be satisfied with data. Otherwise, a PIT entry is created and interest is forwarded to the Forwarding Information Base for further processing. Data packets with no entry in PIT will be assumed to be unsolicited and therefore dropped. The data packet follows the reverse path in order to be delivered to the appropriate node and the PIT entry will be canceled.

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. 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.

3.2 Our Proposed Architecture

Considering named node networking [3], we classify the taxonomy of our architecture into four layers, as shown in Fig. 1. They are the healthcare sensors layer, Local Processing Unit (LPU) layer, Central layer and Operational layer. We further divide the network traffic into two categories: local area traffic and wide area traffic.

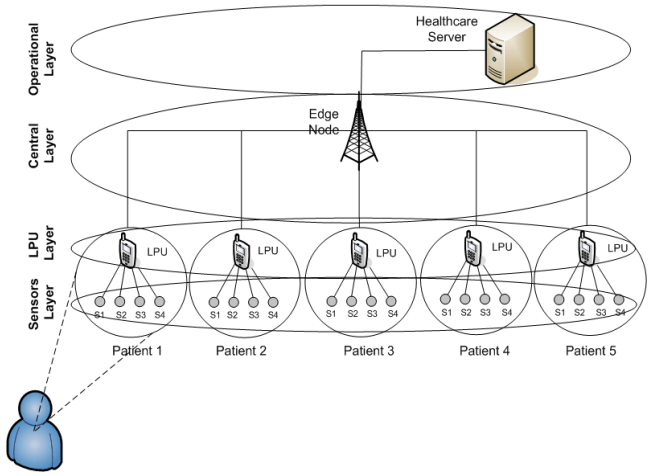

Fig 1. Simulation Topology

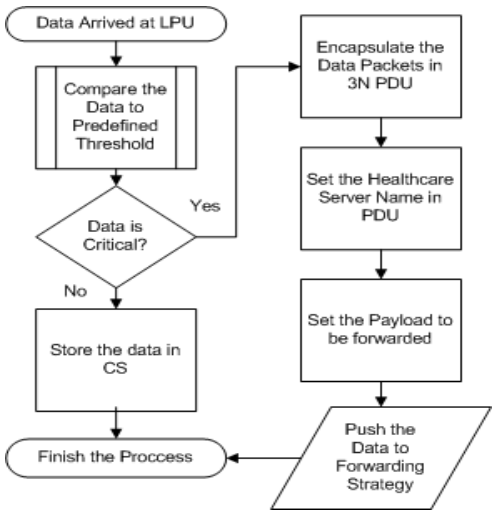

Fig 2. Data Processing at LPU on data arrival from Sensors

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 the entire 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. The LPU sends regular interest packets to the sensors and pushes the data to the wide area after the process shown in Fig. 2. 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.

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. The names in the Node name

namespace will be called 3N names.

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. Every node in this architecture uses the Node Name Signature Table (NNST) 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.

The central layer encompasses the edge and other intermediate nodes between the LPU and the operation layers. 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 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. The naming process ends through the generation of an acknowledgment PDU, called an Acknowledge the Enroll Node (AEN), by the new node after receiving the OEN. 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. In addition, override of the PIT decisions is required, since pushing is a form of one-way data transmission with no prior PIT entry and it would thus be assumed to be unsolicited data in ICN. To fulfill this, we used a 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, 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. 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.

Table 1

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

4 Simulation Results and Discussions

To evaluate the performance of our proposed architecture, we simulate our architecture 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. 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. In the simulation the following performance metrics are analyzed.

4.1 Network Delay

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. 3 shows the network delay for push-based critical data forwarding using the named node network architecture. Likewise, Fig. 4 shows the network delay for a pull-based network architecture using NDN.

The outcome shows that the interest propagation using smart flooding forwarding strategy for various data in the pull-based NDN architecture is not proportional. This may cause more network delay as the variety of data and the number of sensors increases while the push-based named node network architecture performs better network delay.

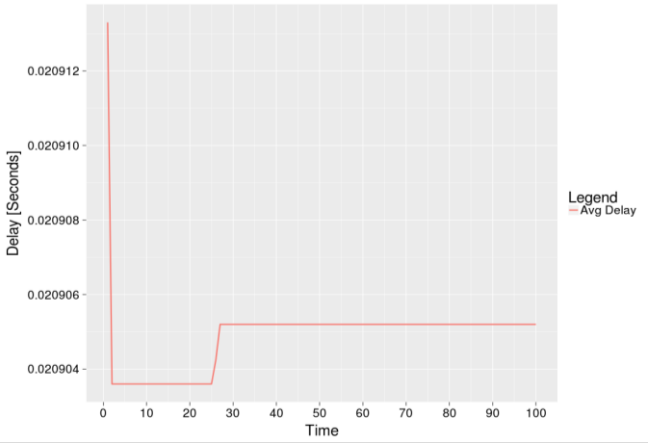

Fig 3. Average Network Delay in Push-Based Critical Data Forwarding Using Name Node Network Architecture

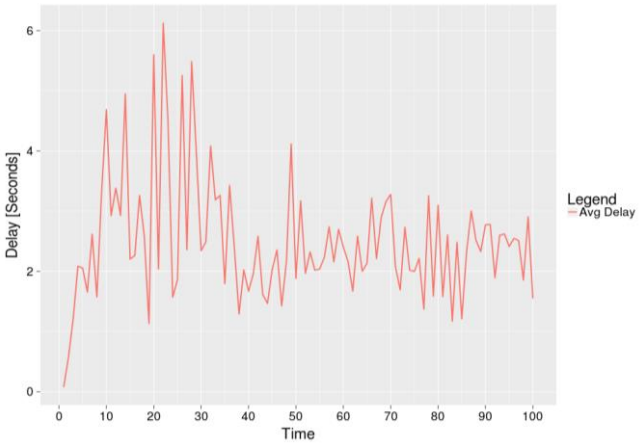

Fig 4. Average Network Delay in Pull-Based Architecture Using NDN

4.2 Network Data Rate

Data rate is considered to be the other important metric in networks. Fig. 5 shows the network data rate for push-based critical data forwarding using named node network architecture while Fig. 6 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 affects the network data rate and performance. As shown in Fig. 7 and Fig. 8 the flooding forwarding strategy for various data performs better in NDN, however, it introduces network congestion in the large-scale networks and may cause many packet drops if the network bandwidth is congested.

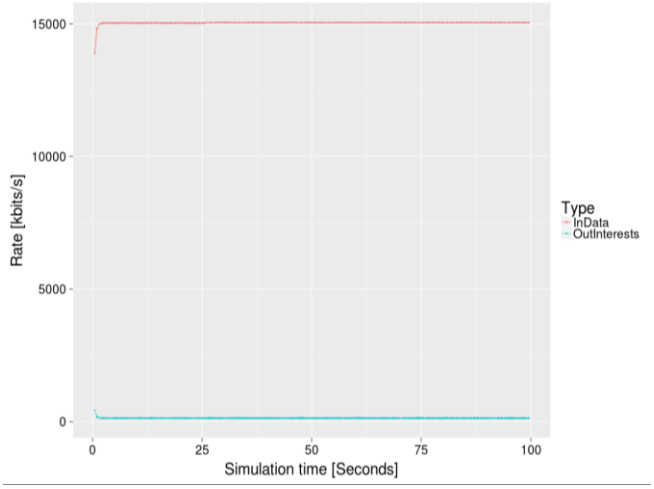

Fig 5. Average Network Data Rate in Push-Based Critical Data Forwarding Using Named Node Network Architecture

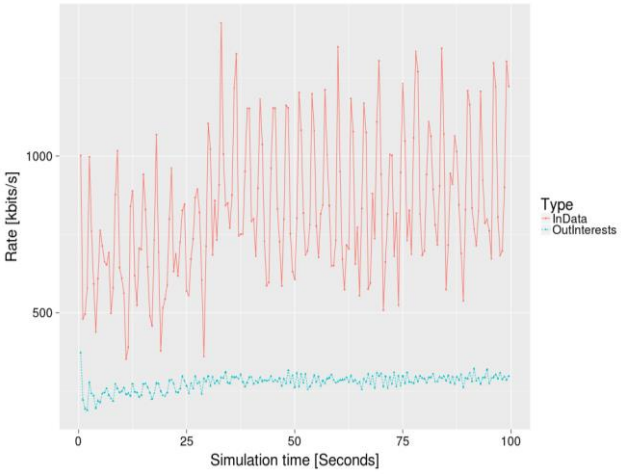

Fig 4. Average Network Data Rate in Pull-Based Architecture Using NDN

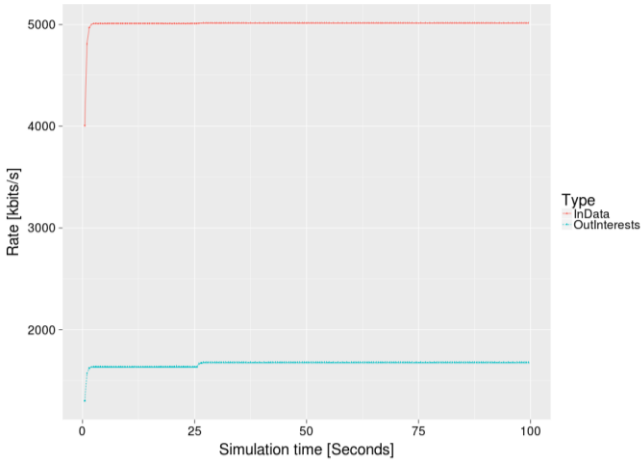

Fig 7. Average Network Data Rate in Pull-Based NDN Architecture Using Flooding Forwarding Strategy

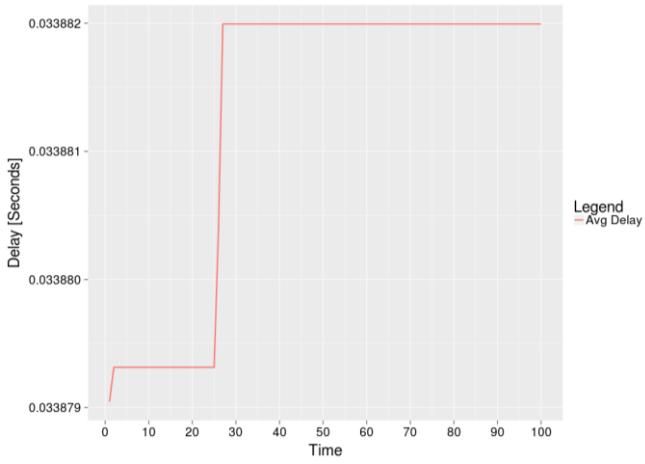

Fig 8. Average Network Delay in Pull-Based NDN Architecture Using Flooding Forwarding Strategy

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] 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.