JIMMA UNIVERSITY

JIMMA INSTITUTE OF TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

Binding Name with Node Content to Improve Accessibility in IOT Using ICN Naming Scheme

By: Guyo Mamo

A THESIS SUBMITTED TO JIMMA UNIVERSITY'S FACULTY OF COMPUTING AND INFORMATICS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN COMPUTER NETWORKING

Jimma University
Jimma, Ethiopia
August, 2021

Declaration

This is to certify that Guyo Mamo's thesis titled: *Binding Name with Node Content to Improve Accessibility in IOT Using ICN Naming Scheme,* which was submitted in partial fulfillment of the requirements for the Degree of Master of Science in Computer networking, complies with university regulations and meets the accepted standards for originality and quality.

Approved by:

	Name	Signature	Date
External |Examiner:	Henock Muluget (Ph.D)		September 1, 2021
Internal Examiner:	Negasa Berhanu		
Advisor:	Dr.Melkamu Deressa (Ph.D)		10/08/2021
Co-advisor:	Berhanu Megerssa		10/08/2021
Chair-Person:	Sofia Alemu		
Chairman (CNOS chair):	Kebebew Ababu		

Abstract

The Internet of Things simplifies our everyday lives by connecting massive objects and creating a perfect environment for humans to easily access any required services and information at any time, from anywhere in the globe. IoT encompasses different sorts of devices that might be resource-constrained, influential, and virtualized things globally. Typically, an IoT system consists of a large number of infrastructure-less devices that may be deployed inside an infrastructure and are easily accessible over the Internet. A variety of contemporary IoT applications are widely accessible by using current TCP/IP protocols. On the other hand, there is a low-end device in the IoT that operates primarily with a built-in battery, small in size, and has limited resources. The connectivity of these resource-constrained devices is done using a low-power, lossy wireless network that provides communication with a sufficient data rate, adequate payload size, and some range. In resource-constrained devices, IoT communication takes the form of a request-response mechanism to save resources. To conserve resources, IoT communication takes the form of a request-response mechanism in resource-constrained devices. However, given the present Internet infrastructure, the request-response communication paradigm is unworkable. To make this sort of communication paradigm in IoT feasible, the IETF working group created numerous middleware technologies that made IoT more accessible to most users, but it resulted in extensions of TCP/IP protocols. As a result, the appearance of various other protocols between the application layer and network layer were introduced which has a significant impact on network performance. As a result, future Internet architectures such as Named Data Network (NDN) are becoming crucial in IoT system deployments. Receiver-driven, naming, in-network caching, and other inherent features of new Internet architecture have the capacity to meet IoT needs. It is clear that the ICN architecture was not created with the IoT architecture in consideration so still there were a number of challenges in their combination. Naturally, broadcast is a wireless network communication pattern that is used to inform devices about the overall network without the usage of any extra control mechanisms. Furthermore, it enables network path redundancy and data duplications. However, in the absence of a control mechanism, broadcast creates extraordinarily significant network overhead and needless packet duplication, particularly in areas with many transmission paths. In the new Internet architecture, routing is state-full, and a duplicated interest packet practically increases the chances of a collision. In today's wireless technology, no special protocol is used to filter packets, thus they are sent directly to the CPU, which is resource agonistic in constrained systems.

To address challenges raised by the usage of broadcast, the proposed a paper based on the NDN forwarding strategy, with an emphasis on path selection techniques that transmit incoming Interest packets based on the signal strength of each node that participating in the conversation. When a resource-efficient or a no with a better radio signal used in a route it improves data accessibility in a provided network. The proposed document use a node physical node indicator which have radio-enabled by default. When this method is applied into forwarder nodes or rely node, it first qualifies the node that has a good signal status to forward incoming packets to producers or data handler nodes. By doing so, the result acquired shows a decreased number of Interest packets lowered from a network by comparing inside the wireless communication model's default transmission. The number of data packets received that were duplicated was also decreased. Furthermore, sending identical Interest packets, receiving duplicate data packets, and service denial cost device's energy. Furthermore, not only does data packet duplication affect the network, but the procedure needed to produce the forwarding state wastes resources as well. Finally, using the optimum path in resource-constrained devices increases data accessibility as well as resource use, which is currently a bottleneck in the network.

Keywords: NDN, ICN, IoT, Broadcast, Wireless Networks, best path.

Acknowledgements

First and foremost, I would like to thank my almighty God for giving me the strength to complete this research. Next, I would like to express my gratitude to Jimma University for providing this opportunity. I would like to use this occasion to convey my heartfelt appreciation to my esteemed adviser, Dr. Melkamu Deressa Assoc.Prof.at Assosa University, and Berhanu Megersa, Lecturer at Jimma University in the Faculty of Computing and Informatics, for their invaluable assistance and suggestions in completing my thesis work. In addition, I would like to express my heartfelt gratitude to my coworkers and friends for their assistance with this research work. I must thank a number of persons with whom I communicated via email and who assisted me much with my research work. Finally, I cannot forget my family's support during this entire process, particularly my wife. I know, I have caused them enough uncertainty and disappointment along the way, but I am pleased I have finally caught up with them, to see them happy.

Table of Contents

List of Tables

List of Figures

Acronyms

ABE	Attribute-Based Encryption
ADU	Application Data Unit
AODV	Ad-hoc On-Demand Distance Vector protocol
BF	Blind Flooding
CCN	Content-Centric Network
CDN	Content Distribution Network
CF	Controlled Flooding
CoAP	Constrained Application protocol
CPU	Computer Processing Unit
CS	Content Store
DONA	Data Oriented Network
FDP	Forwarding Data Packet
FIB	Forwarding Information Base
FIP	Forwarding Interest Packet
4WARD/SAIL	Scalable and Adaptive Internet Solutions
ICN	Information Centric Networking
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPv4	Internet Protocol version four
IPv6	Internet Protocol version Six
ISR	Interest Satisfaction Ration
MAC	Media Access Control
MANETs	Mobile ad-hoc Network
MDMR	Max Diversity Most Recent
NDN	Named Data Network
NDNLP	Named Data Network Link Protocol
NIC	Network Interface Card
NRS	Name Resolution System
OSs	Operating Systems

PIT	Pending Interest Table
PSIRP/PURSUIT	Publish-Subscribe Internet Routing Paradigm
P2P	Point-to-Point
RONR	Reactive Optimistic Name-based Routing
RPL	Routing Protocol for Low-Power and Lossy Networks
RFID	Radio Frequency Identification
RSSI	Radio Signal Strength Indicator
RTT	Round-Trip Time
SDN	Software Define Network
SCS	Shared Caching System
6LoWPAN	IPv6 over-Low Power Wireless Personal Area Network
TCP/IP	Transmission Control Protocol/Internet Protocol
TLV	Type-Length-Value
URIs	Uniform Resource Identifiers
VANETs	Vehicular ad hoc networks
VIF	Vanilla Interest Flooding

CHAPTER ONE

INTRODUCTION

1.1 Background

A billion of small, an ordinary devices come together to form the IoT technologies (IoT), which provides a perfect environment for accessing services and information from anywhere in the world. This has been made possible by the widespread use of smartphones and laptops, as well as the relatively low cost of resource-constrained data gathering devices and associated wireless communication technologies. IoT devices, such as sensor devices, are becoming less expensive as a result of the physical and computer systems that they can support. As a result, they are four times less expensive than the Internet-connected devices that people previously utilized as stated in [1]. This change clearly had an effect on the market. From 656 billion dollars in 2014 to 1.7 trillion dollars in 2020, the Internet of Things is predicted to grow. As a result, the IoT's economic impact is expected to be significant. As a result, the IoT's annual economic impact might range from 3.9 trillion to 11.1 trillion dollars by 2025. IoT devices are battery-powered, compact in size, and have small in CPU speed and limited memory size. These limited devices connect directly with one another or with user applications over the Internet in an IoT system. This form of communication is made possible by the TCP/IP protocol suite, while wireless connection is made possible by low-power, lossy wireless technologies.

In this case, the IP protocol suite was built decades ago for a completely different purpose, and it did not contain IoT capabilities at the time of creation. As a result, IoT functionalities now expose the limits of IP. For example, most IP security protocols are based on communication channels, but the data itself need to be safe. Furthermore, IoT systems require effective resource identification and discovery, which is difficult to do with IP in limited infrastructures. IP architecture continues to enable IoT systems via modifications and middleware. As a result, technologies like as CoAP, 6LoWPAN, RPL, REST, and others are created to ease the integration of these two systems. However, the main work invested in present IP solutions is just to make IoT devices accept the existing IP protocol suite, while many other new capabilities must be included in devices. As a result, if communication support in devices could be simplified and made more robust, it would be a critical enabler for a global IoT ecosystem. Furthermore, simplifying connectivity choices for IoT applications would significantly reduce development costs.

Alternative architectures based on the Information Centric Networking (ICN) paradigm promise to natively satisfy growing Internet applications, but modifying IP for the IoT is considered as cutting corners. NDN is one of the potential ICN architectures that supported by the National Science Foundation (NSF) as part of the Future Internet Architecture (FIA) initiative. The most significant variable in NDN is the content. Names are used in networking activities, and hosts handle communication without logical addresses by requesting named-content directly from the network. This idea is accompanied by natural characteristics such as communication without creating end-to-end connections and name-to-address resolution. Furthermore, no consumer-provider path or session must be maintained, providing a natural support for connection disruption caused by mobility. NDN somehow mitigate the challenges occurred in the previous system which is waiting decades for the future Internet architecture. However, because of the NDN paradigm relies on content names rather than host addresses, significant changes must be made to current IP-based networking equipment, protocols, and applications. Furthermore, as long as present IP solutions function, persuading IP supporters and industrial players of the benefits of NDN will be challenging. Fortunately, numerous research have been conducted in recent years to examine the appropriateness of NDN for the IoT in order to make NDN stronger. With all of this energizing effort, real-world NDN deployments may now be imagined. Although NDN is not yet ready for widespread IoT deployments, real-world designs will enhance NDN experiments and aid in determining what is required to make NDN a reality. Nonetheless, despite the growing interest in NDN, the success of the NDN project, as well as other ICN projects, is not guaranteed. Indeed, NDN is now an academic initiative managed by students and institutions, with no corporate funding. As a result, while utilizing NDN for IoT, especially in the case of a thesis, extreme caution should be exercised. Therefore, enabling ICN principles by using NDN in current IoT designs is a more suitable approach than considering an isolated NDN solution for the IoT. Given the importance of constrained-devices in IoT systems, integrating NDN in low-end IoT devices using a low-power wireless technology is a good method to using NDN in the IoT. However, low-end IoT is still in a development stage even with IP, which provides an opportunity to make NDN an important part of IoT solutions in a short period. To evaluate this emerging system, we work on NDN deployment in the IoT. Small companies that often do not possess the financial resources to design and produce a market-ready IoT product from scratch develop IoT solutions.

1. Motivation

According to [2] goal of Internet of Things is to interconnect each and every devices to the Internet. The interconnection of these devices make easy accessibility at any time, at anywhere, at any place and by any path and it also enhance the existing Internet. Nevertheless, it not only enhance the existing Internet, it also introduced valuables and remarkable applications. IoT has addressed a wide range of real-world business activities and applications during the last two decades, including Smart Home, Smart Building, Digital Health, Smart Cities, smart parking systems, traffic monitoring and control, bike-sharing, and smart bus. Smart Home is a term used to automate home management devices such as Alexa and Google Home. Smart Grids used to distributed renewable energy generation and advanced metering infrastructure. Smart Transportation, which includes vehicle safety, traffic efficiency, and the ability to automate driving, and Smart Health, which includes remote health monitoring and accessibility for persons with impairments. As mentioned in [1,] many of these applications share several aspects in common, such as energy efficiency, interactivity, real-time data connection and analysis, and non-intrusive monitoring systems. The fundamental objective of IoT [3] is to enable applications, machines, humans, and objects to better understand their surrounding surroundings by connecting devices, collecting, and analyzing data. This enables services and applications to make quick decisions and adapt to dynamic changes in the environment, as a result improving our lives in a variety of ways such as reduced human effort, efficient resource use, real-time marketing, and data analysis. In order to provide these services and applications, IoT will require a massive network of interconnected nodes. As a result, all of these nodes create a large amount of contents. So because existing IPv4 addressing space is exhausted to handle the quantity of devices, and the available address space is imbalanced, all nodes that participate in a system need to be named or addressed. As a result, various challenges have arisen that must be addressed in this context, such as heterogeneous nature of devices and sensors, efficient data retrieval, energy and memory limitations, power consumption, mobility, scalability, security, and dynamic network topology, as stated in [4]. As IPv4 address space is not enough to address IoT devices accordingly IPv6 address space derived to overcome the issues of IPv4 address space shortage. Newly proposed address space have been sufficient available address, which could assigned to each devices, participate in the IoT network. However, this address is quite long length which less suitable for communication held throughout Constraint-oriented devices [1]. Although in future, addressing the IoT devices is not the only issues, but a large amount of data which is being produced by IoT devices needs better and efficient management systems. Therefore, Finding effective naming and addressing methods for these billions of linked devices is therefore critical. In order to deal with the dynamic changes, a new method to Internet communication has been developed in order to meet the problems and limits of the present system by design. Information Centric Networking (ICN), as described in [5,] has been proposed as a new network paradigm for the future Internet. It uses data/content names rather than network addresses is the fundamental feature of ICN. A content name should be unique, permanent, and location independent. The customer requests the content by name rather than the provider's address. As a result, in-network caching may be used during communication to enhance data retrieval and minimize network traffic by storing material closer to users. Because content is independent of location, ICN manages mobility natively by simply reissuing any unsatisfied requests. Furthermore, ICN enables simple data retrieval via a request-response exchange paradigm, content-based security by embedding all security-related information inside the content itself, and native multicast support. On the other hand, most communication patterns in IoT applications are fundamentally content-oriented [6]. IoT devices and users are interested in receiving the requested material from the network regardless of who offers/hosts it. Use cases such as retrieving sensed values from a sensor, updating a mobile application with recently published content (e.g., weather notification), or monitoring the status of a patient at home focus on the content as the main element rather than establishing a communication session with the content provider. Definitely, as [1], ICN architecture and characteristics can allow large-scale IoT implementation. ICN name abstraction, in particular, provides easy integration and interaction with IoT applications and devices. In-network content caching enhances network content availability and quality of service, while content-based security enforces security and privacy by focusing on the content rather than the communication route. Finally, the clean-slate ICN architecture and communication paradigm enhances network performance and scalability while also reducing device energy consumption. As a result, we think that ICN is a viable communication paradigm for IoT networks. Although ICN draws a wide range of academics, it is still in its early stages and will not be extensively adopted.

1.3 Statement of the problem

Today, we were in the era of many revived technologies, which improve our daily working environment. IoT is one of these technologies, which interconnect human being within the thing and it expected profoundly transform our environment. Currently, it is one of the hottest research areas and there are still many challenges, which needs a researcher's effort to improve. The major difficulties stem from the usage of delocalized data and the inability to obtain it via an end-to-end transport stream, content retrieval upon request, and a lack of an appropriate mechanism that can easily handle planned content changes. Recently, hop-wise replication and in-network caching have been developed to help with information dissemination in the IoT and to reduce the need for continuous connectivity. The main goal of this new architecture to transform the current Internet to a simpler and more generic architecture. ICN is defined as a new paradigm for naming content and putting information at the core of its architecture [71] rather than depending on IP host identification. Among this new architecture NDN approach has been widely adopted because of its simple communication model, scalability, light configuration, and management operations [72]. It has lately been proposed as a viable alternative networking solution for IoT**.** More particularly, it accommodates common IoT communication patterns such as content retrieval on demand and scheduled content updates, and benefit substantially from cache-assisted, hop-by-hop replication [4]. Thus, the NDN method in IoT give chances to improve data access efficiency through caching or error control, as well as minimize the complexity of auto-configuration mechanisms when compared to IP protocol approaches such as 6LoWPAN/IPv6/RPL. Despite the fact that the integration of ICN and IoT networks benefits resource-constrained devices by conserving energy and radio resources, improving availability, and reducing complexity, there are a number of issues that must be addressed[63].

Currently, NDN forwarding strategies are mostly based on the broadcast-and-learn method. This method employs a phase in which Interests are broadcasted until the content is discovered, after which following requests are routed more precisely based on the information gained throughout the broadcasting process. Therefore, employing broadcast is required in an NDN wireless network since broadcast is the natural communication pattern over wireless connections. However, utilizing broadcast in resource-constrained devices presents several difficulties. In contrast to unicast, broadcast at the link-layer lacks an acknowledgement mechanism to manage frame retransmissions. In other words, the absence of a control mechanism results in extremely high network overhead and unnecessary packet duplication. Furthermore, duplicated packets, particularly Interests, cause significant link-layer access contention and increase the risk of collisions. Due to there is no broadcast packet filtering mechanism in present wireless equipment, all incoming packets are handled by the CPU, which is an agonistic resource in constrained-devices. Additionally, the overhearing come at a cost of active listening to radio transmissions and consume significant amount of energy.

The name-to-MAC mapping method or unicast was created to alleviate the problems caused by broadcast in the NDN forwarding scheme. When compared to broadcast forwarding, unicast packet forwarding dramatically saves energy usage and processing time. However, unlike IP address communication, there is no clear mapping between a content name and a MAC address. As a result, it frequently leads to broadcast or multicast frames on the data connection layer. Furthermore, extraordinarily high packet losses occur in NDN unicast forwarding due to a lack of an efficient mechanism that drives a packet straight to the data's producer or data handler devices. Furthermore, if the known node fails, the unicast is obliged to search for another route. The cost of the route maintenance mechanism adds more overhead and processing to the network. Both approaches try to prevent the interest broadcast storms from the network with multicast strategy for interest forwarding through which nodes forward interest packets to content producer’s nodes. Despite their benefits, they add overhead to the current NDN architecture by adding extra controlling messages. This very disappointing state-of-the-art drives us to rethink the problem and research alternative solutions. Therefore, a lightweight forwarding strategy or efficient system is required to route interest packets to destination or content producer nodes without interfering with natural ICN features such as data duplication or in-networking caching, delocalization, use many route, and effective resource usage. We propose the system that based on each node signal strength and energy which use best path to forward interest packets to the destination. Therefore, based on this parameter our algorithm is going to identify the best forwarding path among the other path.

Generally, the proposed work tries to address the following research questions, which will focus on improving the accessibility of content without affecting the basic functionalities of the system.

- ✓ How can efficiently forward Interest packets without affecting the built-in wireless communication pattern?
- ✓ What is the basic issues that reduces the performance of Network of the combination of

NDN network and IoT constrained devices?

- ✓ How different forwarding strategies used in NDN improve accessibilities of data in request-reply driven communication methods?
- ✓ What happen if node energy and link stability of algorithms applied on the node?

1.4 Contributions

This thesis minimizes the propagation of an inappropriate interest packets throughout the network and affect overall network performance by holding packets that were waiting to send to the producers or to the data handler devices**.** The proposed approach not only decreases the number of unsatisfied interest packets in the network, but it also improves data accessibility by eliminating unwanted packets in the network and reduces network overhead as a result increases network efficient. When incoming packets are overheard, each node, whether it has a good, intermediate, or poor signal, begins to process and creates a PIT entry table. Because the responded data packet uses the constructed PIT entry table as a reverse route, they send the same data back to the requester. As a result, undesired data overrides the data that was intended to be stored in the supplied node for cache purposes. When our system reduces irrelevant interest packets, it also reduces duplicate data packet returned back to the consumers. In general, the quantity of interest satisfaction ration is higher than in earlier efforts such as broadcast and the name-to-MAC address mapping technique. Consequently, as the number of interest packets transmitted from the network reduced, so did the number of resources required to process those packets saved, network performance increased, and delay time also decreased.

1. 5 Objective

1.5.1 General Objective

The major goal of this thesis study is to demonstrate how alternative lightweight best-path techniques improve data accessibility in IoT resource constrained-devices by employing NDN forwarding strategy approaches as an alternate solution.

1.5.2 Specific objectives

The specific objectives help to achieve our ultimate objective. So, in order to meet our general objective the following specific objectives are defined:

- To analyze various efforts has been done as a resolution techniques which used in traditional Internet and IPv6 effective designed mechanism for IoT constrained-devices.
- Familiarized within the overall IoT design architecture and the ICN design architecture.
- To overview and analyze the lightweight mechanism improve accessibility of data in NDN network.
- To reduce the amount of Interest packets distributed throughout the network as a result of a lack of control mechanism.
- To decrease the number of duplicate data packets returned to the consumer or requester as a result of the PIT entry table that was generated.
- To examine the influence of the default NDN forwarding system on the path discovery transmission method in IoT devices.
- Compare energy consumption, and performance of the network after applying the path selection algorithm in NDN architecture.
- Finally, evaluate the final output and reports its impacts on the constrained devices.

1.6 Methodology

Methodology is a set of tools, tactics, and strategies used to complete the research of this thesis work. The study's general and particular objectives were fulfilled through the employment of diverse techniques. This technique allows us to implement NDN functionalities for IoT limited devices.

1.6.1 Literature Reviews

The first thing we conducted a comprehensive review of literatures to acquire a deeper understanding of the research area and its problem domains. Throughout this literature, we identify the importance of the previous efforts in the area ICN-IOT techniques. ICN was investigated as a communication enabler for IoT projects. In addition to the literature reviews, we refer to other resources such as books, reports, manuals, journals, and published and unpublished theses.

1.6.2 Selecting the right platform

Selecting the right simulation for the research is the most important task to accomplish our research. So that, to achieve what we proposed we used the following simulation tools, embedded Oss.

1.6.3 Embedded Operating System.

Several operating systems (OS) have been developed to allow smart IoT services on resource-constrained devices with limited processor, memory, space, and power. Among them, we utilize the software listed below.

1.6.4 ndnSIM Simulator

The ndnSIM simulator is based on the ns-3 network simulator. This ns-3 has previously offered numerous items that can be utilized for simulation inside ndnSIM: Although ndnSIM is implemented using a new network-layer protocol model, it may operate on top of any link-layer protocol model. The simulator's current implementation is version 2.8. The simulator implemented NDN forwarding and administration using NDN Forwarding Daemon (NFD) source code. Several forwarding techniques are provided in the simulator ndnSIM [18] through NFD. These techniques specify how Interests should be managed or discarded. The Best Route Strategy is activated by default, which passes Interests to the upstream with the lowest routing cost. The Interest is sent to all upstream nodes using the Multicast Strategy. There is another a technique known as Client Control Strategy, which allows a local consumer application to select the upstream for each Interest's forwarding. Finally, if desired, a new strategy may be implemented or an existing one can be overridden. The Random Approach is an example of a novel strategy that uses random load balancing.

1.7 Scope

The proposed work's main objective is to assess a lightweight forwarding technique for NDN in resource-constrained IoT devices. To determine if the ICN design is relevant and acceptable for IoT devices with limited resource

The proposed work's main objective is to assess a lightweight forwarding strategy for NDN in resource-constrained IoT devices. To evaluate if alternative path relevant and appropriate for IoT resource-constrained devices by ICN forwarding strategy. Just to observe if the NDN features overcome the problem come up with the long length of IPv6 in the IoT resource constrained devices. Which one is more suitable to safe the resource of the devices? Identify whether the content produced by producer node is provide for the next requester when the same request with the same content name come. In other way we also study, what will happen, when forwarding strategy applied on the consumer side and compare with built in wireless communication process.

Moreover, we look at if forwarding strategies of NDN is appropriate in low-end IoT devices and to observe if easily content is accessible by varying different strategy. Analyses what will happen when we alter the communication path and discuss energy it consumes during this process, if it reduces overhead. The proposed paper do not consider the cache strategy and security of the network.

1.8 Thesis organization

The thesis is divided into five chapters. In Chapter One, we cover the overviews of the Internet of Things, its connectivity, the relevance of IoT, and the effects it has on current systems like TCP/IP. How IoT highlight the limitation of existing system and our motivation. Chapter 2 introduces literature reviews. The reviewed paper on the IoT and it is architecture. We also emphasize the limitations of TCP/IP architecture and the significance of ICN for IoT. It also define ICN, as it is new architecture, its key features and its communication process. In this chapter we introduces why ICN for IoT and research done on these area, IoT-ICN challenges and issues which need further discussion and comparison it with IP protocols. We study related works by introducing what is current solution, which ICN architecture meets the needs of IoT. Chapter 4 presents our proposed design. How NDN forward in wireless network. Ends with the communication techniques of constrained network. In chapter five our experimental results. Tools we used and result we achieved throughout our work. Finally, in chapter 6 we write the conclusion and our future works.

CHAPTER TWO

LITERAURE REVIEW

2.1 Internet of Things

The Internet of Things has grown in popularity in recent years. According to [1], the establishment of a uniform Internet resulted in the connection of things. Objects can be humans or any type of smart device, as seen in the lower part of Fig. 2.1. As shown in the picture, objects may be connected in three ways: “machine-to-machine”, “machine-to-human”, and “human-to-human” when the connectivity in IoTs is represented in the upper section of the figure. Therefore, the concept of IoT has developed over time and experienced several modifications, which will undoubtedly continue with the evolutions of enabling new technologies.

The Internet of Things (IoT) connects billions of tiny computing devices known as things to offer access to services and information all around the world. This is achieved by linking cellphones and laptops, as well as primarily low-cost resource-constrained data collecting devices and wireless communication technologies. It is a development of the Internet that has become critical in giving global access to services and information. It has become possible through the interconnection of billions of small computing devices, which allow the physical world to has been monitored and controlled, and it facilitates to access at any time, at any place from any network **[1].** The Internet of Things includes a variety of devices that can be resource-constrained, powerful, and virtualize things. IoT encompasses things such as smart washing machines, smart refrigerators, smart microwave ovens, smartphones, smart meters, and smart cars, according to [1]. The Internet connectivity of these smart devices enables numerous beneficial and amazing applications such as smart home, smart building, smart transportation, digital health, smart grid, and smart cities. These tiny devices may be linked in billions and connected to the Internet, generating massive amounts of data which become an additional challenge on the existing system and out of control in the near future.

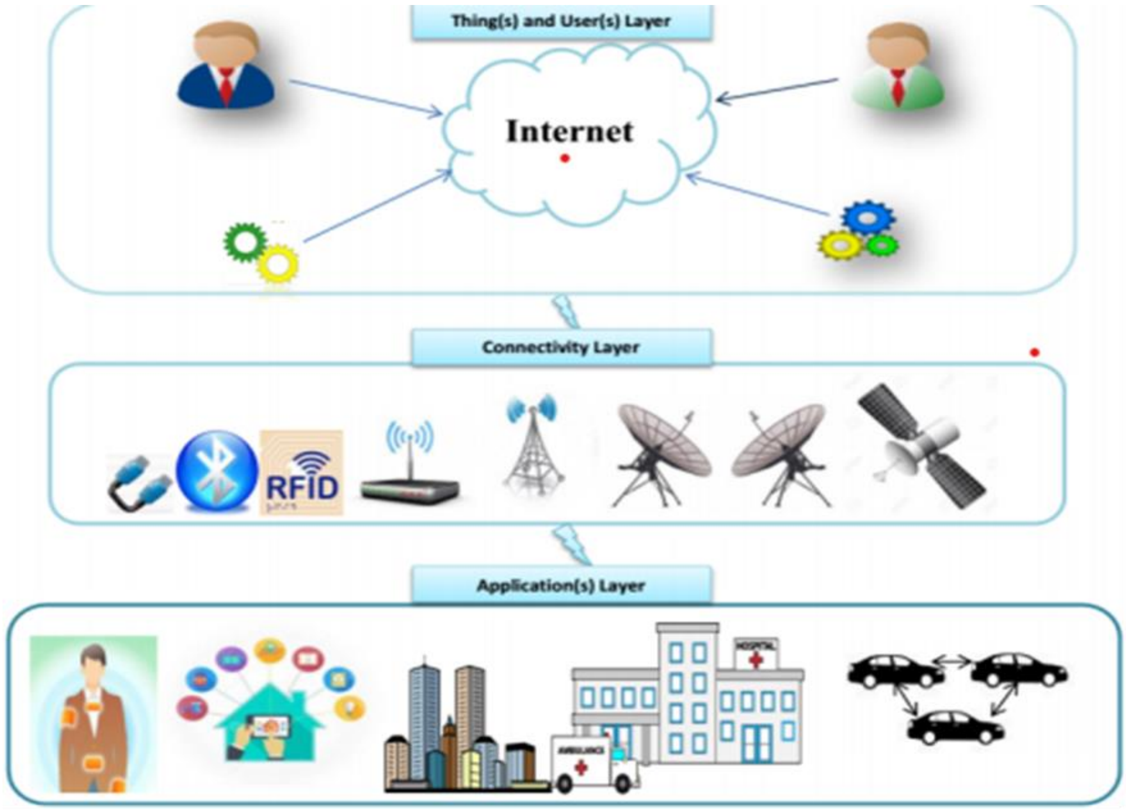

Figure 2.1. Internet of Things (IoTs) [1].

IoT devices can also be linked through traditional connection techniques, such as cable connections. Data from many sources and locations may be exchanged via a variety of different device kinds and communication techniques in the Internet of Things.

Practically, IoT devices are battery powered and can contains in thousands or ten thousands devices, which have limited resources such like memory. In this IoT system, these constrained devices communicate with one another or with user applications over the Internet. This communication achieved through the TCP/IP protocol. In another, wireless communication achieved with low power and lossy wireless technologies. IP protocol or current Internet architecture was designed decades ago for completely different purpose with many limitation such as security, resource naming and discovery issues. IoT architecture highlight the limitations of IP architecture where it support resource naming and discovery, which is impossible to deploy constrained infrastructure in IP. However, IP can support IoT system through adaptations and middleware. As mentioned in [62],Some protocols such as CoAP, 6LoWPAN, RPL, REST and other solution developed under IETF to support the coexistence of both architecture (TCP/IP and IoTs).

2.2 IoT Challenges

Due to vast scale of IoT infrastructure with a huge number of devices involved in developing a successful IoT application is not an easy task and have to face a lot of challenges. Some of these challenges are namely, mobility, reliability, availability identification, scalability, data integrity, management, energy management, interoperability, and security and privacy [64]. RFID, ICN, 6LoWPAN, and SDN are examples of enabling technologies that can be used to realize the Internet of Things.

To address these IoT problems, researchers attempt to resolve them using a variety of mechanisms, such as the integration of RFID with WSN, where RFID is based on hardware parts that allow readings of RFID-labeled items to acquire the needed item identification. IoT may localize information systems by utilizing these two integrations, while the system is built on communication standards and standard identified objects. As mentioned [68] the RFID resource addressing systems use addressing, which allows for the retrieval of the corresponding resource address via the resource name. So, in radio frequency identification technology, a code resolution system (CRS) is utilized for RFID public information systems to query the services address of the matching item information based on RFID tag information. The addressing technology of the EPC global network architecture and the uid center ubiquitous network architecture is mostly based on the domain naming system mechanism. Many difficulties have been highlighted in the RFID addressing system, including compatibility issues, security and efficiency, robustness, and imbalanced load.

IoT typically consists of the constrained devices in low-power and Lossy Network (LLN) and are limited in terms of reliability, throughput and energy. Implementing a centralized SDN architecture in IoT environment faces considerable challenges such as controlling traffic which subject to jitter due to unreliable links and network contention, overhead generated by SND can severely affect the performance of other traffic [69].

According to [67] to bridge the IoT challenges different technology are used. Naming the data and devices make ICN more suitable for IoT as it combines millions of devices and huge information content.

2.3 TCP/IP Architecture Limitations and the Importance of ICN for IoTs

All users require data without knowing who created it, which is especially important in IoT, since every one node functions as both a producer and a consumer at the same time [11-12]. A flash crowd is a phenomenon that occurs on the Internet when a high number of Internet users seek a certain piece of information, which is a result of today's Internet usage. Because of the flash mob, network traffic for any one server increased [15], causing data to become unavailable. To mitigate this type of issue, ICN provides an in-network caching technique that aids in reducing network traffic from the original provider. Therefore, by facilitating this approach ICN makes ideal for low power devices. Furthermore, with ICN, information or content is named independently of its location, allowing it to be located anywhere in the world. Naming data and devices makes ICN more suited for IoT since it covers billions of devices, each of which generates large amounts of data or content. Furthermore, ICN allows receiver-driven communication, with the receiver having complete control over all communication. As a result, with IoT, the receiver of information is more interested in the data than in its location, therefore this ICN characteristic might help them.

An alternative architecture that promises to natively meet developing Internet applications is the information-centric networking paradigm. When doing networking operations on names and hosts, the main entity is content (without logical addresses). It requests named-content from the network directly. This form of communication is based on name-to-address resolution and is established without end-to-end connections.

Today IoT applications is widely supported by the TCP/IP protocol suite. So that this IoT Big Data put more burdens on the underlying TCP/IP architecture while increase many important issues. Among this issues Naming or addressing every IoT devices [2-3].

As IPv4 addressing space is exhausted, IPv6 address space also may exhaust in the future and also it does not provide optimal name and addressing strategies for billions of devices and contents [1]. In another way, IPv6 address space is a quite long and this long length makes it less suitable for communication through constrained-oriented devices [17-18].

Devices diversity, which raise another issues of heterogeneity also the main burden in IP communication where every device has different constraints and specification. In fact, in IoT system those devices heterogeneous can be in terms of processing power capabilities, size, memory, battery life, and cost. Besides, of, their heterogeneity in this low memory and low battery life constraint-oriented devices data can be unavailable. To solve this issues in-network caching required to make data available is missing in IP-based networking.

Data sensitivity is another important point in IoT application where security and extra privacy required when these devices access data [19]. Moreover, some IoT application like VANETs, MANETs and smart transportation require better mobility handling which is impossible in IP protocol suites [20-21]. In the hand, from data perspective most of IoT application users interested in getting the updated information rather than knowing the address or location of where information originate (source). For instance, the collection of IoT devices may have specific purpose especially in a pointed domain to gather information [22], temperature sensors measure temperature from their surrounding and do not word processing task which general purpose computer does.

Considering TCP/IP as a network architecture for IoTs, which traditionally designed to connect limited number of computer and to share limited and expensive network resources through limited address space at network layer, which not designed to support or fulfill IoTs requirements. Not only this, IoTs huge data put additional requirements like data dissemination and scalability on the underlying architecture. To fulfill all these needs of IoTs Information Centric Networking (ICN), which would be a promising future Internet architecture introduced.

2.4 Information Centric Networking

Information-enteric Networking [13] has been proposed as a new design for the future Internet, solving several difficulties in existing IP-based networks such as routing, scalability, and content sharing performance [30].In order to provide effective data distribution and access, ICN combines all network operations around the name of the content rather than the network address. It is a potential communication model that differs significantly from the standard IP address-centric strategy. The ICN approach consists of the retrieval of content by unique names, regardless of origin server location (IP address), application, and distribution channel, thus enabling in-network caching or replication and content-based security.

Many methods, such as peer-to-peer (P2P) and CDN (Content Distribution Network), have been created in the past to facilitate content sharing and distribution over the Internet [31]. However, unlike P2P and CDN, ICN is a standardized protocol that operates at the network layer, whereas P2P is an application-specific protocol and CDN is a proprietary solution that operates at the application layer. Furthermore, P2P material is provided by end users, whereas CDN proprietary infrastructure is employed. However, with ICN, material may be supplied directly from the network infrastructure. The redesign with the concepts of what is the content rather than where the content location is improve the network performance, facilitate the content retrieval and replication using in-network content caching. Fig 2.2 shows the difference between IP and ICN communication architecture. Consumer 1 and 2 knows the address of the producer and they fetch individually the content through IP routed path. However, consumer 3 and 4 follows ICN-based communication and the consumers specify the requested content name without knowing the producer IP address. Here the requested content forwarded based on name-based routing rules until it reaches a device, which has a requested content. After the first consumer received requested content and satisfied another consumer requested the same content can satisfied from a node store a received content in the previous communication without worrying about the producer location.

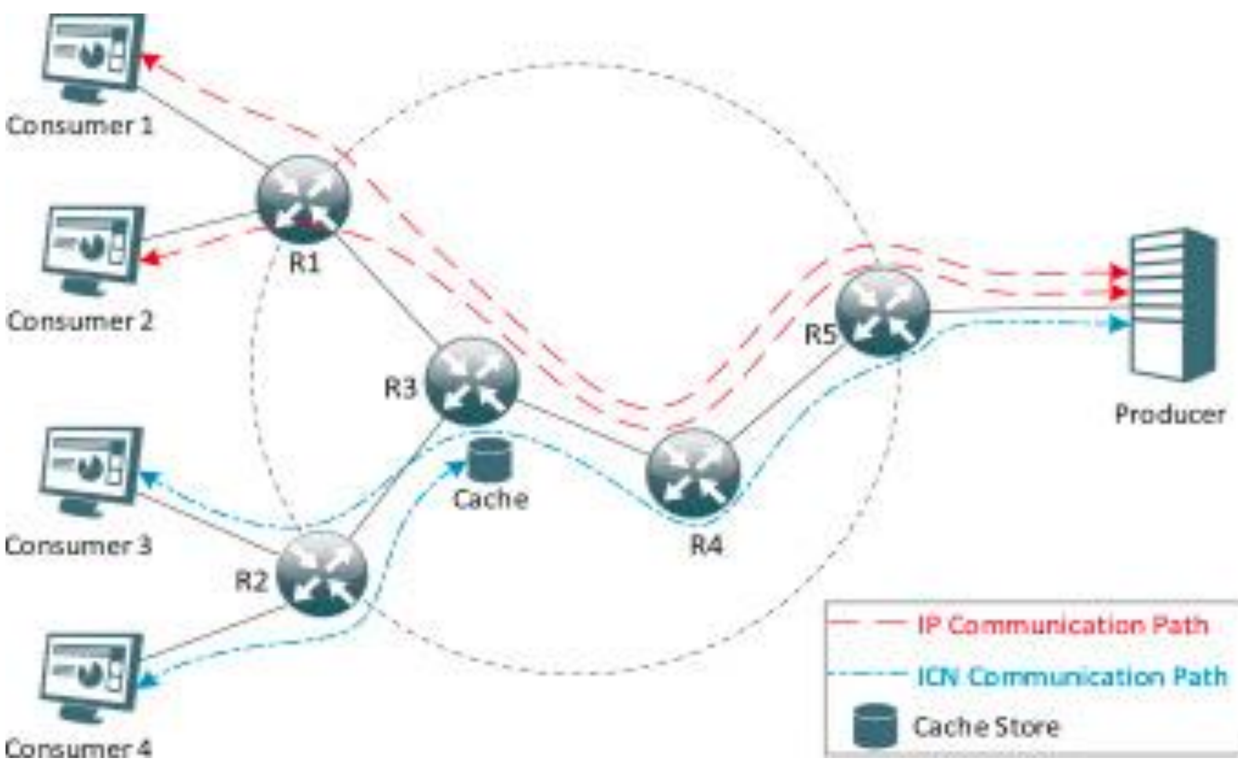

Figure 2.2 IP vs. ICN based Content retrieval [65]

2.5 Key Features ICN

ICN characteristics are appeal it to the future Internet architecture. It recently attract the attention of networking researchers as an alternative architecture to the traditional IP based networking. It promises to replace the current host-centric communication model by leveraging the content as the key network elements.

2.5.1 Content naming

The essential element of ICN is the content name [10], which uniquely identifies the material itself. It should be small, persistent, and capable of validating material. The naming strategy chosen must be scalable and allow for name aggregation. ICN has recommended four different sorts of naming systems.

- **Hierarchical Names:** They are made up of several components [32] that are used to identify the content and define the application/services. Its structure is similar to that of existing Uniform Resource Identifiers (URIs), and it may produce user-friendly and relevant names for users. Because name prefixes may be pooled, hierarchical naming improves scalability, but it can also be long.
- **Flat Names:** They are generally produced through the use of hash algorithms on content [33]. There is no structure to the name. As a result, it is unfriendly to humans and cannot be applied to dynamic content that has not yet been published. One difficulty with flat naming scalability is that it does not enable routing aggregation.
- **Attribute-Value based Names:** The attribute-value based naming scheme [34] consists of a series of attributes, each with a name, a type, and a set of potential values (creation date/time, content type, location, version, and so on). They represent a single piece of content and its characteristics as a group. This naming method facilitates easy searching by utilizing well-known content keywords. However, ensuring name uniqueness is difficult since multiple distinct contents may have the same characteristics.
- **Hybrid Names:** A hybrid-naming system [35] combines at least two of the preceding methods, if not all of them. It tries to leverage the best features given by the base scheme to increase network scalability and speed while also improving security and privacy. For

example, using name aggregation to improve the lookup process, flat names with set lengths to conserve space, and attribute values to offer keyword searching and security/privacy.

Furthermore, instead of providing hop-by-hop name-based routing, ICN utilizes the Name Resolution System (NRS). The interest packet is sent to the NRS server, which resolves the desired name and forwards the request to the content producer.

2.5.2 Routing and Forwarding

When names are used to identify content, name-based routing [24] is introduced to discover and deliver the content to the requester. Because of the receiver-driven design, a consumer initiates a request for content by naming it. The discovery process begins by searching for content only by name. The request is sent hop by hop via a forwarding or routing table until it reaches the original or a replica node containing the requested content, at which point the content is delivered to the requester.

2.5.3 In-network Caching

In-network caching [26] may be used during ICN communication since the content names are location-independent and each data packet is self-consistent. As illustrated in Figure 2.2, each ICN node can store the material and provide it for future requests. Caching enhances network performance by lowering latency and facilitating content retrieval.

However, still determining what kinds of content would cached in ICN network needs many metrics including popularity and freshness. It needs to know consumer demands and detail analysis of network topology is important as well as considering devices capabilities such as the cache memory and processing. In addition removing the old cached content and replacing it with new content introduces the need for replacement algorithms and most used content which have less changes in the cache store [37].

2.5.4 Content–based security

In content security, mechanism applied to content itself rather than the communication channel. ICN emphasis content based security [26]. To ensure this different trust models developed based on network services. Any data in this communication each data packet is self-authenticating based on the original contents security-related information. For instances, the publisher public/secret keys and signature [27-29].

2.5.5 Mobility

According to ICN [12] [14], the material is independent of its original location, and only the desired content name is utilized to discover and transmit it to the customer. When a node switches from one network to another, it can re-issue any unfulfilled requests, and the producer responds with the required data without the requirement for a new address.

2.6 ICN Proposed architecture

2.6.1 Data-Oriented Network Architecture

It is one of the first ICN designs to identify information items using permanent flat names. Names contains the ciphered hash of the content owner's public key and uniquely identifies one of the contents with regard to the same owner. As an object identifier, the content publisher employs a cryptographic hash, and subscribers may simply verify the material's integrity by hashing it and comparing the results.

2.6.2 Scalable and Adaptive Internet Solutions

SAIL and its precursor 4WARD (Architecture and Design for the Future Internet) [39, 40] are generic architectures since they incorporate PURSUIT and NDN characteristics. SAIL employs self-certifying flat names with explicit aggregation of the form ln: /A/L, where A is the authority portion and L is the local part with respect to the authority, and each component can be any sort of string, ranging from a URL to a hash value.

2.6.3 Publish Subscribe Internet Technology

This project was inspired by its forerunner, the Publish-Subscribe Internet Routing Paradigm (PSIRP) [38]. In creating its ICN architecture, it takes a completely clean-state approach, employing a publish/subscribe stack instead of an IP protocol stack. It employs self-certifying flat names that include scope and rendezvous components (scopes organized hierarchically).

2.6.4 Convergence

This solution incorporates some elements from the NDN architecture. Names in this context can be self-certifying and flat in the form name space ID: name, similar to the P: L pair of DONA, or hierarchical, as in NDN.

2.6.5 Mobility First

This project is primarily concerned with developing a mobility solution. The naming method used here is self-certifying and flat, with a worldwide unique identifier (GUID). This GUID is separated by its location, which is an IP address for the URI. In other words, even if a GUID and a network address are separated, the Mobility First design maintains a mapping between the two. As a result, it employs two routing schemes: GUID-based and network-address-based.

2.6.6 Content Centric Networking

The PARC (Palo Alto Research Center) initiated and manages the content Centric Networking (CCN) [1] project, which aims to develop a flexible, simple, and universal next-generation communication architecture. One of the primary goals of CCN architectural design was to shift from host-centric to content-centric communication. In this content-centric communication, the requester, known as a consumer, sends an Interest to the network, and any node that has the requested data can send it back to the consumer through the same channel.

In CCN "Interest" and "data", messages [9] are fundamental used to achieve the pull-based communication process. Along with two messages, some data structures PIT, FIB and CS maintained at each node to properly forward interest data messages in the network.

2.6.7 Named Data Networking

Currently, NDN [40] is one of the most active architectures in ICN research that has forked from CCN architecture in 2010. It comes up with some principles, which need to common network protocol for all applications:

- Universality: fetch unique name (Data-Centricity)
- Data Immutability: Data packet should be secure whether the packets are in motion or at rest (Secured Data Directly).
- Packet should carry hierarchical names (Hierarchical Naming).

- Interest should use incomplete names to retrieve data packets (In-Network Name Discovery) and
- One Interest packet should bring back more than one Data packet (Hop-to-Hop Flow Balance).

The communication happened in NDN is somewhat seem like the HTTP's request model running at the network layer. The main difference of HTTP and NDN is that NDN supports the request-response pattern through packets carrying names as the main information where all the networking operations operate on those names, not on binary network addresses. Additionally, Data packets in NDN are immutable which means ones Data should produce with a certain name it cannot modified. Producer generate new Data with new name when needed. In other way, every Data packet is carrying a digital signature that binds its name to its content (Self-secured).

Naming and Packets

NDN and IP different in packet format where NDN encoded in the TLV (Type-Length-Value) and the packets are no header and protocol. A TLV block consists on a sequence of bytes starting with a predefined number (Type), followed by its Length and its Value. Two type of packets defined in NDN to perform communication: Interest and Data. Both packets contain a name and may carry additional information according to the defined fields described below. Although Interest and Data packets have, default and optional fields respectively but they do not have predefined packet size or field sizes.

Figure 2.3 Interest and Data fields [67]

Names: a content identified through hierarchical name that contains a sequence of name components. In each packet there an elements of Name.

Name can be written this *"/AB/room/1/lab/8/temp"* which identifies the temperature value related to the class which has Id (8) locate in room 1. Here, names hierarchically structured and the same data type related to another lab, which in another room can be named *"/AB/room/4/lab/2/temp"*.

Naming schemes defined by the applications, which provides flexible in the way the content named and requested. One important things this naming schemes come up all names are opaque to the network, which makes routers access name components separately for routing, and forwarding purposes and it no interpret the whole name. This approach allows application developers and users to design the name that suits their needs without the need to maintain a mapping between network requirements and application configuration.

Packets

Some application use units of information, which represent data they handle in the most appropriate form. This unit's information commonly designated as Application Data Unit (ADU). In NDN, applications are communicate by exchanging Interest and Data packets, which identifies the provided data names.

The segment in TCP numbering system does not match with the NDN ADU boundaries, which is the major difference between the two approach (TCP/IP and NDN). Packet fragmentation in NDN causes two major problem. First, packet fragmentation cause extra computation, large header size and increases latency, especially in the resource-constrained devices. Second, since each chunk is signed Data packets splitting content into multiple chunk can become computationally expensive for both producers and consumers. This Packet fragmentation and reassembly needs should avoided as much as possible.

Interest Packet

Requested Interest by consumers might be includes CanBePrefix, MustBeFresh, InterestLifeTime and ForwardingHint parametric as optional which give more information on Interest matching or forwarding. Nonce also include in the Interest packet and used to detect looping Interest. The consumer node sends the interest messages if it requires any content and the provider node replies with the data message with the content or fragment of the content.

Data Packet

A response, which sent back to a requested part, represents a Data and contains needed content. There is actual data and other arbitrary sequence of bytes in a content. Intermediate node receives data message handle the copy of the content message depending on a caching policy implemented. Figure 2.4 shows interest and data forwarding planes in NDN. When a node in NDN receives, an interest packet it checks its local CS, if the requested data already exists in the cache it means replies the needed content and the node known as a replica node. Therefore, data packet will sent back using the same face where interest the interest have received. Whether no material is found in the local CS, it will check in PIT to see if a comparable request has already been submitted upstream. NDN will add the PIT entry or aggregate interest to the face where the interest was received; otherwise, if the name is not the same as the current one, a new PIT entry with the name of the desired content and the name of the face will be generated. Then it consults FIB to determine the next hop to the content provider. In reverse path, when an NDN node receives a data packet it checks it's PIT. If there is no match found in the PIT entry table, which means there is no request that has sent before, then the node discards the data packet by considering it as an unwanted packet else it will forward the data packet to all the faces saved in the PIT table. Here, at the same time based on the cache policy implemented the nodes along the data path store or cache the content.

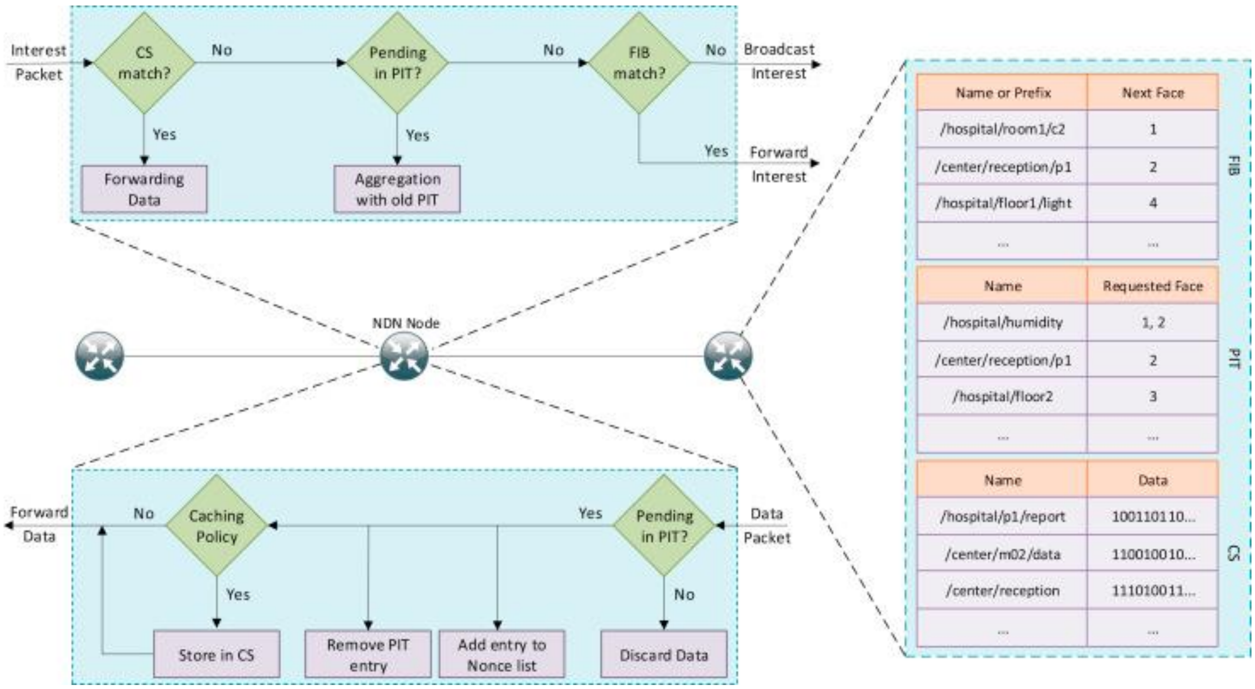

Figure 2.4 NDN Operational Logic and Table structure [66].

2.7 NDN Communicational Process

In NDN, each node requires three data structures to process packets and uses "interest" and "data" messages to simplify communication.

- **Pending interest table (PIT):** A data structure, which stores unsatisfied interests with content name, incoming face from where the interest message received and record, received time. The table keeps sent interest until response time or duration of interest message ended. An entry created in the PIT when a node receives an interest message that it cannot satisfy with the requested content which means that the content is not available in the CS. A typical entry contains the Interest, its incoming interface(s), the interface(s) to which it will be forwarded and expired time. The "nonce" used uniquely identify interest message. Its value stored in the PIT to detect the interest loop. If a node receives an interest with similar-value nonce it drop that interest and no further action is required.
- **Forwarding Information Base (FIB)**: Contains information about reachability of the content. When interest is unsatisfied by received node which means if there is no matching content in CS and no entry in the PIT then the interest forwarded toward providers by using FIB. Every entry in FIB has a tuple of name prefix and outgoing face(s). Single prefix entry

may have more than one outgoing face associated with it. The content name in the interest searched within the FIB using longest-prefix matching.

- **Content Store**: It is cache used to store full or partial contents or data packets. It is not persistent storage and the stored content is stored according the cache policy, which satisfy the future request. Data packets are self-secured and not related to specific hosts so each data packet can reused to satisfy other Interest requesting the same content. This approach is a native in-network caching and managed by CS.

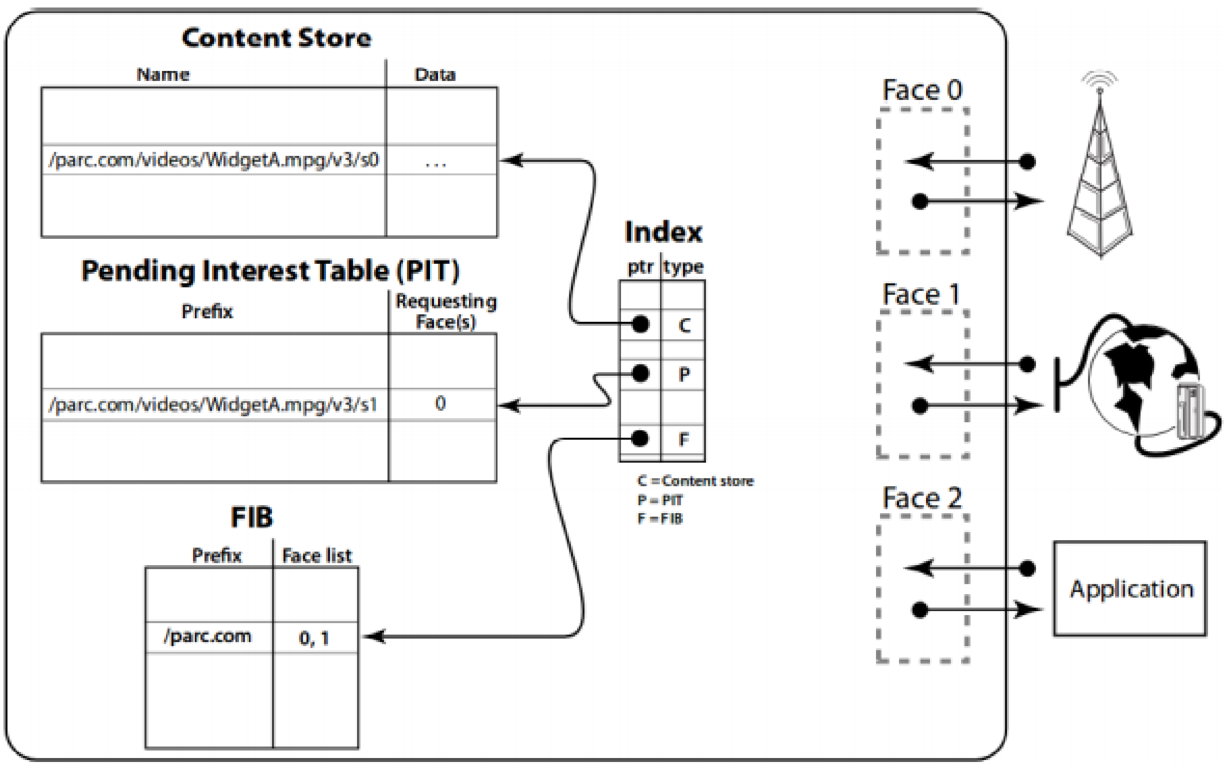

Figure 2.5 NDN node and data structures [9].

NDN uses two types of packet (interest and data) when interest and data packets carry the name of the requested content. NDN architecture is a named-based network where the routing achieved by using names. It uses hierarchical name, human-readable, and structured which like URL names. Moreover, NDN maintains three data structures: Cache Store (CS), Pending Interest Table (PIT), and Forwarding Information Base (FIB). Figure2.8 shows interest and data forwarding planes in NDN. When a node in NDN receives an interest packet, it first checks a content in its local CS. If the requested data already exists in the cache, it means this node is a replica node. In such case, a data packet will sent using the same face where the interest has received on. Otherwise, it will check in PIT if a match for similar request has already forwarded upstream. In this case, NDN will append the face where the interest has received to the PIT entry (interest aggregation); otherwise, a new PIT entry will created that has the name of the requested content and the name of the face. Then it checks FIB to find the next hop toward the content provider. In reverse path, when an NDN node receives a data packet, it checks its PIT. If no match found, which means there is no request that has sent before, the node discards the data packet by considering it as an unsolicited packet. Otherwise, it will forward the data packet to all the faces saved in the PIT table. At the same time, based on cache policy, the nodes along data path may cache content.

1.7.1 Why ICN for IoT?

In the past, networks utilized Internet Protocol (IP) to develop the Internet that utilized now. According to [1,] IP networking was not intended for its current capabilities. The paper comprehend IP limits by examining IoT aspects by summarizing the evolution of the Internet and its current state. It was created with a lot of constraints. As a result, explore how IP design supports IoT systems and identify solutions and shortcomings.

As stated in [64] articles, IoT is primarily based on the connectivity of many heterogeneous devices, and IoT systems rely on TCP/IP protocols, especially the IPV6 protocol. Unfortunately, it may be inadequate for effectively supporting IoT applications. One of the primary issues with IPv6 is the 40-byte header length, as well as the IPv6 specification, which mandates networks to support a minimum MTU size of 1280 bytes. Low power restricted connections, on the other hand, are frequently based on very small MTU, which has been taken into account by 6loWPAN. A 6loWPAN is an adaption layer between the network layer and the link layer that provides a compression mechanism for the IPv6 header, extension, and UDP headers by relying on link layer fragmentation, which introduces overhead and increases network stack complexity. Among IoT requirements security is one, indeed the IP security model is based on the security of the communication channels which is not suitable for IoT environment for several reasons [67]. In order to solve this problems, ICN is proposed as an alternative communication techniques for IoT application.

In addition to the exponential rise in traffic, user expectations have played a role. Users attempt to obtain data by connecting to various fixed or mobile devices in diverse contexts. Because of the rapid growth and user expectations, a unique communication strategy is required. A few workarounds to most of the new traffic pattern have been proposed, such as Content Distribution Networks (CDN) and peer-to-peer (P2P) overlays, however these do not provide adequate answers to the fundamental challenges caused by the existing Internet design. Both techniques are overlaid on top of the existing network architecture. With such rapid growth in both content and users, incremental improvements or solutions to the present Internet infrastructure will struggle to keep up with the Internet's progress. As a result, various efforts have been made in recent years to design a “Clean Slate” solution for the future Internet's architecture. The Information Centric Networking (ICN) concept underpins these innovative alternative designs. This new architecture differs from the previous one in the following ways: naming system and in-network caching, where requested items are addressed by their unique name and can be supplied by any cache holding. Consequently, caching content will impact the life time of the IoT device’s batteries, a request may be satisfied by any an active node, while the information producers are remain in their sleep mode. Moreover, ICN also address the security requirement and targets to secure the contents themselves rather than securing the cannels connecting the equipment with each other. It also a promising candidate for the IoT environment since it can natively support IoT scenarios while improving data dissemination and reducing network complexity.

Today users need data without knowing the producers of data in both Internet and IoT. Especially, in IoT where one node acts as a producer and consumer at the same time. At this moment when large number of users request a particular information network traffic increased and as a result, data can become an available due to some interruption may be occur in a network. Low-end IoT devices is very sensitive when traffic overload take place they become out of services. An adequate approach not derived yet which can handle when this kind of problem is happened both in the previous system. However, ICN provides and supports in-network caching which have able to minimizes traffic load on the original data producers by putting data on intermediate devices or store more closer to the requests. This ICN in-network caching makes it ideal for low power devices. Moreover, in ICN information or content named independent from its location so that it can be locate anywhere globally. Naming the data and devices make ICN more suitable for IoT due to it may be combine billions of devices and huge amount of information. In another way, the communication or receiver-driven makes the ICN under full control of receiver. Therefore, as stated in previous IoT users need only data but do not care about data location. So, IoT benefit from this type of communication approach. Furthermore, data can accessed whenever a receiver clearly requests a data. Opaqueness communication between sender and receiver make more secure. Finally, the significance of ICN/NDN networking approaches that satisfy IoT needs. To integrate IoT with ICN architecture the researcher proposed [41] node Architecture which supports NDN-IoT architecture which consists application layer, NDN layer and things layer. This node architecture holds contents name instead of IP address enabling network.

2.8 Research done in the ICN for IoT fields

There are many scientific publications which covered the ICN for IoT research field. From these paper reviews seven is used as the main tops on IoT.

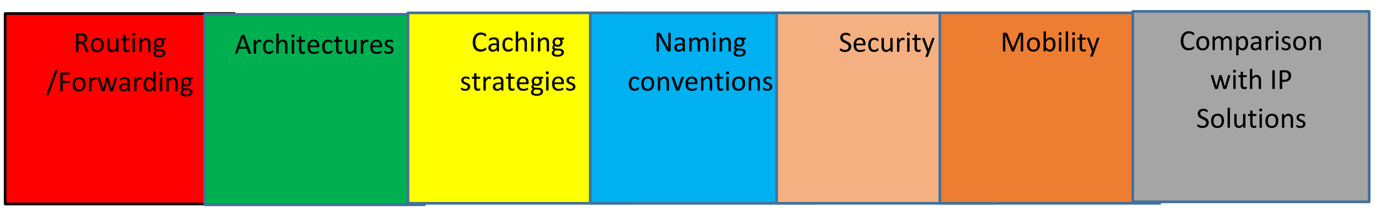

Figure 2.6 Identifies research categories in the ICN for IoT field

2.8.1 Routing and Forwarding

ICN installations necessitate the use of specialized routing and forwarding algorithms capable of determining the best next hops for each Interest message. ICN routing systems must identify the optimal route to one or more producers/caches for each data name rather than discovering routes to particular hosts as in IP. Routing and forwarding research in the ICN for IoT sector is primarily focused on developing energy efficient routing and forwarding methods that may be employed on limited IoT devices. Authors generally concentrate on establishing the most energy-efficient balance between signaling traffic and the usage of traffic flooding, particularly in mesh networks. This work may be divided into two categories: blind forwarding and conscious forwarding [42]. Blind forwarding techniques usually rely on computationally cheap (controlled) data flooding through a network with little signaling cost. Routing and forwarding methods that employ aware forwarding seek to acquire higher level information about, for example, the network topology and use this knowledge to execute efficient forwarding, generally at the expense of increased signaling overhead [42] and [43] are examples of conscious forwarding strategy suggestions. The authors of [42] propose GRMR: Greedy Regional Multi-cast Routing, a technique that employs local multicast tree constructs to identify the most effective routes. The authors of [44] offer a mix of conscious and blind forwarding. Vanilla Interest Flooding (VIF), which floods interests throughout the network, and Reactive Optimistic Name-based Routing (RONR), which produces FIB entries after a single interest flooding, are suggested in [45]. This paper [46] describes an adaptive forwarding method that allows IoT nodes with the highest battery charge to execute flooding operations.

2.8.2 Architecture

Many articles on ICN for IoT research have been written about the development of new architectures. The researchers want to create methods that will allow them to apply and adapt the ICN paradigm to a specific, generally pre-existing scenario or technology. Most of the time, these designs are loosely based on Van Jacobson's [47] concepts of information centric networking. To support a specific use case, the authors suggest fundamental modifications to the ICN paradigm, such as removing ICN's one-Interest one-Data principle. In these instances, the writers usually concentrate on high-level design rather than extensive testing with the newly suggested architecture**.** An architecture was designed in [48] to facilitate the implementation of ICN for the IoT. The authors create a managed Shared Caching System (SCS) for Fixed and Mobile Converged (FMC) networks. Another intriguing idea is [49], which introduces designs integrating ICN, SDN, and IoT. Several designs that integrate ICN and SDN into Sensing as a Service (SAAS) [50] cloud paradigms are examined.

2.8.3 Caching strategies

A least number of research paper developed which focuses on the optimization of caching strategies for the IoT. Caching design is not be seen as an ICN-specific research challenges as caching already studied and adopted in a wide range of applications. Caching strategies for IoT applications can be customized to unique IoT characteristics like as traffic patterns and device limitations. Caching strategies may be divided into two categories: cache decision strategies and cache replacement strategies. A cache determination strategy determines whether incoming Data messages must be cached. This choice may be made based on specified criteria, such as randomly, the popularity of a certain Data message, or the current contents of the cache. A probabilistic method is given in [46], which allows incoming data caching to be determined based on a random variable. The technique provided here was compared to the usual ‘cache everything' strategy. A more complex caching approach is described in [51], in which the choice to cache a specific piece of data is based on a weighted total of battery life, cache occupancy, and the remaining time until the Data is considered stale. The cache replacement strategies are the second component of caching strategies. When a cache exceeds its maximum capacity, certain regulations take effect. When a new Data message comes, and the cache decision strategy decides to cache that data, this packet may need to replace one that was previously cached. Based on some established logic, the cache replacement strategy must choose which Data message to replace. Article [52] proposes Max Diversity Most Recent as an example of a cache replacement method for IoT applications (MDMR). The MDMR approach seeks to optimize data availability from many producers in a single cache.

2.8.4 Naming Conventions

How data messages should be titled remains an unresolved problem for ICN applications in general, and IoT apps in particular. Typically, authors note the naming conventions design challenge but leave it for future development. Some major research difficulties for defining names in IoT applications are mentioned in [53], such as: "How to deal with the generally lengthy names in IoT applications?" ”, “Should data be named based on metadata?” as well as “How should it deals with dynamic data that changes over time?” ”. Many of these issues are currently unaddressed in ICN for IoT proposals.

2.8.5 Security

The most popular research article created in this field. ICN does not use protected connections like IP, but instead employs content-based security, in which individual data packets can be encrypted and self-verified. This necessitates the creation of new security technologies and procedures. Because IoT devices may collect sensitive private information, the adoption of solid security solutions is extremely crucial in IoT applications.

In the literature, a wide range of security concerns have been addressed, ranging from authentication and authorization processes of new ICN-enabled IoT nodes [54-56] to entire NDN security architectures [56-57]. The ‘OnboardICNg' authentication and authorization protocol, which employs a central authentication server, is given in [55]. The authors of [54] compare the ‘OnboardICNg' protocol to an authentication system that uses asymmetric encryption and does not require a central authentication server. It has been demonstrated that this benefit comes at the expense of increased latency and energy consumption due to the more resource-intensive cryptographic procedures.

According to [58], Attribute-Based Encryption (ABE) for IoT applications is presented, which enables multiple users to access cached encrypted Data packets. When a Data message is encrypted at the Producer, ABE can be used to indicate which users (with which characteristics) must be allowed to decode the message from the sensor node. This technique enables many users to retrieve and utilize encrypted Data messages from network caches.

2.8.6 Mobility

Mobile nodes are used in a variety of IoT use cases. When tracking the position of an item, for example, a tracking device may switch between various connection points several times. Consumer mobility is natively supported by ICN. When a consumer attaches to a new point of attachment, it may simply retransmit its interest and continue to receive and request data along the new channel. The ICN architecture does not inherently enable producer mobility. When a producer relocates, the routing information in FIBs must be updated. Otherwise, ICN nodes will send interests to old producer locations that are still present in their FIBs. Producer mobility support is a fundamental challenge of the ICN architecture and is therefore not specific for IoT applications. In survey paper [59], an overview given of multiple proposed solutions. The authors identify four types of solutions to support producer mobility in ICN.

- **Mapping-based solutions**: These methods make use of a rendezvous, which keeps track of the producer's present position. When a producer relocates, he or she must notify the RV of the new point of attachment. A consumer may then consult the RV to obtain the mobile producer's new location/name.

- **Tracing-based solutions**: Tracing-based solutions utilize an RV as well as NDN's state-full forwarding plane to update the producer's location. Interests in the mobile producer's data provided to the RV to recover these pending Interests, the mobile producer sends special trace command, interest messages to the RV on a regular basis.

- **Data spot**: A data spot method can be utilized in some specialized situations. This method use ICN names, which are linked to geographical places. /Datacenter/Room4/hz/Temp, for example, asks the current temperature in a data center. This request can be fulfilled by any node that is currently at this location.
- **Data depot**: This mobility technique uses a central depot, which stores all data of mobile producers. Mobile producers will send all generated data to this fixed depot node. The data depot satisfies all Interests for mobile producer data messages.

Although producer mobility is not an IoT-specific issue, effective mobility solutions for resource-constrained nodes should be created. Support for producer mobility in IoT systems is currently a relatively untapped research area.

2.9 IoT-ICN Challenges and Issues

In this section, the most challenges and issues of with current solutions for ICN-IOTs listed-out. During ICN architecture enabled for IoT, systems there are a lot of problem, which phased developer. Among these challenges:

2.9.1 Naming

More of the ICN-based IoT naming research conducted for CCN/NDN hierarchical naming. Due to CCNx have a fixed header it is a challenge to apply this it to IoT low power and constraint-oriented devices as well as header compression techniques can be needs to support small data packets. However, NDN packet have variable length header, which has small data packets. Especially, IoT applications have short length data to transmit in a response of a query or to send command towards any sensor or to just acknowledge the command to or to send current state of any sensor, so that NDN packet formats with variable length headers provide good support for IoT's applications. Names are follow hierarchical structure which may have long and variable lengths names so this long name might be utilize to see a specific person health information. In its nature, IoT WSN supports 127 bytes payload and this long name may raise the problem. In another way, this hierarchical name is human readable, which is need other security mechanism to assure user information. In addition to this name to MAC address mapping has sever negative impact when content broadcasted in layer two address. Additionally, managing for length-varying names expected to be complex. Therefore, it is quite stimulating and difficult to design such a lookup system for IoT constraint-oriented device. Therefore, still there is looking for a general and appropriate naming scheme that can solve all identified constraints.

2.9.2 In-Networking Caching

The main advantage of ICN for IoT has been recognized as in-network caching. The researchers have given ICN-IoT caching a lot of thought. ICN caching in IoT may conserve network bandwidth, reduce data latency, and extend the battery life of IoT devices. Most ICN-based caching techniques require that the freshness value of the material be considered when choosing whether or not to cache the content. While content popularity has been included in the in-caching decision in [51], there is still a need to investigate content popularity utilizing a simple technique.

Many studies have been done on caching placement techniques, with the majority of studies recommending LRU as a suitable cache replacement approach [51]-[52]. As mentioned in [52] it creates and carefully analyzes a cooperative caching system that maximizes sleeping cycles while minimizing energy usage of restricted IoT nodes. They demonstrate in theory and experience that a clever replication method may save considerable resources while enhancing content availability throughout a wireless IoT system. Cache protocols are absent from today's Internet and have a lot of promise for IoTs. In general, there is no full cache management solution in the existing literature. As a result, the cache management system should handle IoT node duties about sharing limitations in order to maintain the privacy and security of IoT applications, as well as the authenticity of data in a node.

2.9.3 Content Routing and Information /Content Delivery

Data routing and forwarding methods in ICN-IoTs began when the consumer node was far away from the production node or was indirectly linked in a multi-hop fashion. ICN designs enable content name, but some research in ICN-IoTs fails to provide naming of IoT devices. To enable routing for multiple sorts of names, either the content name or the device name can be resolved using the Name Resolution System (NRS) to find the requested content.

2.9.4 Mobility

Mobility is employed in both producer and consumer mobile nodes. The majority of ICN architectural designs assert that consumer mobility is intrinsically supported, but producer mobility is not fully stated. In ICN, mobile data consumers signal that they want to re-issue an Interest message, and the network transmits this Interest to the nearest and most reliable data provider or to the cached data. In contrast, with ICN-IoTs, the majority of nodes can function as information providers/producers. Vehicles in IoT applications such as VANETs function as information producers regarding road conditions, such as information about accidents and road construction, and can also act as information providers when these vehicles cache data to send to other vehicle nodes. Producer mobility may be divided into four ways for IoT scenarios: tracking and mapping mobile producers, moving data to a nearby location, or regenerating data from other mobile producers in that region. Furthermore, a proactive method for the IoTs environment may be studied. A first draft provided a straightforward and easy-to-maintain anchor-less solution to dealing with provider mobility in ICN.

2.9.5 Privacy and Security

The majority of the possible study area for both user requests and data responses in ICN-IoTs applications is filled. ICN offers content-level authentication and access control, however content requests are kept in ICN inter-mediate routers and may be traced by attackers. Thus, privacy algorithms are necessary to ensure privacy at the router level between user and producer. Furthermore, it is not yet standardized to determine if intermediate routers will be included in ICN-IoTs applications.

Moreover, public key infrastructure (PKI) is very difficult to implement for constraint-oriented devices as it requires much power during implementation of trust management and key generation consequently, light cryptography and light hash function can evaluated and hence modified for constraint-oriented devices. Keys generation and management that include both key revocation lists and key distribution processes still needed to explore further for IoTs applications. In addition, a significant research area is control access strategies in which user authentication, their corresponding access privileges, cache access, and updates needed to investigate for IoTs applications. Moreover, security of sensitive information, spoofing and sniffing highly needed to explore and addressed. ICN-based safety has been studied in healthcare applications and can be investigated for other IoT applications such as smart home, smart grid, and smart traffic. All in all, a comprehensive system assuring both privacy and security for IoT data and applications is currently lacking. As a result, there is a significant need to create a comprehensive solution in this regard.

2.9.6 Content Discovery

In ICN, the producer publishes material by entering the matching name into the nearest ICN-based router, and the content is kept in the router to satisfy future consumer inquiries. Consumer demands in ICN-IoTs can be met in two ways: first, by content given via the nearest router, and second, by material retrieved directly from the content producer. In the second scenario, consumer devices may require data including certain parameters such as freshness. To enable efficient content accessibility over ICN, packet formats must be established and re-designed to meet such demands. In order to allow push-type communication in ICN-IoTs, the Interest Message and Data Message need be changed [56]. For this, name-based aggregation can provide improved latency and efficient information lookup. Name-based aggregation can help with this by reducing latency and increasing the efficiency of information search. However, one of the problems with content discovery is determining which needs to address these queries. How should continually create material be named in order to offer efficient look-up? How to effectively handle content discovery in highly dynamic contexts VANETs? In addition, How to map and search contents from named-devices corresponding to content requests efficiently?

2.10 Comparison ICN with IP solutions

A few papers compare ICN with IP for IoT use cases to see whether ICN truly enhances network performance in IoT applications [45] [60]. In [45], a very simple topology was utilized for comparison, and NDN was compared to an IP-based protocol stack that is not suited for IoT applications. NDN is compared to a typical IoT optimized IP stack in [45], although only one fictional use case is presented. Both publications are devoid of any explanations of the traffic patterns and popularity distributions that are in use. Furthermore, both papers only address a single use case. Most importantly, no scenario considered where multiple IoT deployments interconnected via the realistic internet-like topologies. Therefore, it can concluded that a thorough comparison of ICN and IP for IoT applications is still missing in literature.

The uniqueness and complexity of IoT requirements raise challenges that require adaptations to the design of ICN protocols. The [70] articles explore the uniqueness of ICN in IoT and handle it through the use of naming schemes, security, caching, discovery and delivery, and morphing.

CHAPTER THREE

RELATED WORK

3.1 Introduction

Internet of Things gathers a diverse set of various nodes. For this paper our focus on low-end IoT devices, based on hardware resource of class two [8] which is connected via radio, and powered by battery. This devices is benefit from ICN specifically from NDN where the lightweight NDN networking stack requires less memory which it compared to current IoT stack standardized in IETF

3.2 Current Solution

The current IoT wireless devices can filter a packet only by using their MAC address due to there is no appropriate matching solutions like in current Internet which bind IP address of devices with link layer address in order to safe a packet from being broadcasted. ICN network architecture use name content instead of IP address to communicate with other devices in the network. There is no appropriate mechanism, which serve ICN approaches specially NDN packets to map with its link layer address like IP architecture. Due to there is no suitable mechanism which map content name within its layer address NDN broadcast a packet throughout the network. As result all packets processed by the CPU, which causes extreme load on resource constrained devices as well as generates network overhead.

Due to adaption of IP for the IoT is not straight forward as needed other architectures based on the Information Centric Networking (ICN) paradigm satisfy emerging IoT applications. Among this architecture, NDN [15] towards evaluating NDN for IoT is one, which mainly centered on the content entity. Under NDN network processes are performed on names, hosts (without logical addresses) request named-content directly from the network. Recently, the studies investigates the suitability of NDN for the IoT.

3.3 NDN meets IoT

NDN an alternative architecture which is not specifically designed for the IoT architecture as it was stated in [62]. However, there many NDN proposals and study which illustrate its advantage in IoT functionalities. In this section, some of the studies that either technically improve the NDN support for IoT, or propose designs and visions to enable a viable NDN solution for IoT is presented. Obviously, not all the NDN studies which related to IoT are presented but only focused on those that were stimulating, encouraging or the main solutions that can be address challenges identified in this document. Table 3.1 illustrate architecture mapping of between ICN features and IoT requirements.

To improve reliability [11] introduces NDN broadcast protocols, which try to minimize collision. Here, it helps to reduces interferences on the data link layer by placing content nearest to the sink, which reduces number of hosts count and minimize packet loss at application layers. Broadcast, simplifies content distribution however, it introduces two major problems. In NDN, frames are not filter by existing drivers or network interface card (NIC). Therefore, devices CPU that rises a conflict in devices, which has limited hardware resources, process these frames. In both approaches increase packet delivery ration but the packet processed by CPU until independent NDN service bound to the broadcast packet developed or available. There are various challenges phased when enable the IoT over NDN. First, Naming with multiple hierarchical, second, Routing over infrastructure-less environment and third, implementation for highly constrained devices.

Another approach discovered the ICN-based approach for the IoT through real-world experiments using NDN features. For instance, the CCN-lite implementation on top of RIOT is used. The experiment based on a deployment of 60 IoT devices distributed in different rooms, floors, and buildings. Each node is equipped with a radio chip and sensors provide temperature and humidity measurements. The advantages of using NDN analyzed and an experimental comparison with 6LoWPAN/RPL/UDP provided. Positive results obtained, which show that NDN can be an alternative to build an IoT architecture. The most interesting result is the comparison between the

ROM and RAM sizes of the binaries compiled for NDN and 6LoWPAN/RPL stacks in the RIOT and Contiki platforms. According to those measurements, the ICN/NDN approach can significantly outperform common IoT protocols in terms of ROM size (down to 60% less) and RAM size (down to 80% less). To improve reliability in [11] is introduces NDN broadcast protocols which try to minimize collision. Here, it helps to reduces interferences on the data link layer by placing content nearest to the sink, which reduces number of hosts count and minimize packet loss at application layers. As broadcast simplifies content distribution, however it introduces two major problems. In NDN, frames are not filter by existing drivers or network interface card (NIC). The researcher wants modify the device driver of NIC to support frame filtering based on the same names rather MAC addresses. It achieve good performance in the final output but the solution needs to update hardware of devices, which makes it unusual with current popular IoT devices. Therefore, devices CPU that rises a conflict in devices, which has limited hardware resources, process these frames. In all approaches, it increases packet delivery ration as well as increase the packet processed by CPU. So, need proper and independent NDN service which bind the broadcasted packet with relevant name will be developed or alternative path to broadcast should designed.

Another approach in [4] proposed name-based filters on the NIC. They try to filter names at device driver level of the network interface card and to improve the implementation names maintained in the bloom filter table, which shows good performance results. However, layer violation issues occurred. The data, which is structure to implement filter, is specific to NDN approach, which implemented at layer three or network and above link layer. In another way, not all ICN naming scheme is the same [12]. Due to there is no the same naming scheme when this naming scheme change is changed it needs to update device drivers which limit the deployment of upcoming approaches. It also distributes data or content on layer 2 broadcast frame approach and does not benefit from layer services such as error handling, retransmission and acknowledgments.

Another approach which is different from adaptation of the link layer or device driver are presented by [10] [7] articles. In this paper unicast, faces mechanism is introduced which has similarity with the TCP/IP approach. It assigns unicast MAC address to NDN faces dynamically. Initially, Interests, which has a unicast source MAC address of sender, will be became broadcasted. Based on this receiver take the sender address to assign a unicast face. This allows MAC based filtering and benefits from error handling on the data link layer and it is suitable only in some approach. However, it is not applicable in nodes, which are not in a same broadcast domain. In another way, unicast traffic reduces caching capabilities and data redundant. So deep analysis of link layer unicast and broadcast of NDN node is still need detail investigation. The paper, reconsider alternative approach of NDN-MAC Layer mapping to forwarding interest packet.

Approach	Description	Draw back	Related work
Adaptation layer	Additional layer between link layer and NDN which support ACK, retransmission	In this approach the adaptation was focused: • On the overlay system. The integration of CCN/NDN on IP. Still it based on the end-to-end route set-up, which need control between overlay nodes, as a result induce high control overhead. • The overlay design forces point-to-point communications; therefore, in-network caching not performed.	[12]
Unicast mapping	Mapping between NDN names and MAC addresses	• It requires more resources and generates overhead. • Miss path redundancy and in-network caching, additional memory required to maintain name-to-MAC mapping. • It does not follow the NDN vision.	[4]
		• It requires re-engineering a part of the hardware, which makes it unusable with	

Hardware-based	Name based filtering at NIC	current popular IoT devices. • In current IoT the name created dynamically, therefore it requires a permanent version of NIC, which maintain dynamic name with the MAC addresses.	[17]
Broadcast reduction	Delayed retransmissions and packet overhearing	• In order to identify the legitimacy of the incoming data additional components added to the packet. This addition packet make the communication complex and as a result complex operation, which introduces overhead. • It use the aggregation of corresponding the same name prefix so that computational overhead is required to perform prefix aggregation, which is infeasible for constrained devices.	[11]
NDN-OMNET framework	To evaluate the internal interaction of a system which provide good visualizations of NDN communications at network system level.	• It uses the scenario used in unicast mapping. • The forwarding strategy they used still focused on the addresses, which based on point-to-point communication, which is not compliant with NDN according to ICN enthusiasts. • It does not select the best path to retrieve contents. Sometimes the source of content is very not clear.	[62]

Table 3.1: *Summary of Related Work*

NDN wireless forwarding techniques are all in all based on a broadcast-and-learn process in which interests are broadcast until content is located. Then, depending on the information gained during broadcast, following requests are routed more precisely. This accurate forwarding information is accomplished if the identical requests originate before the expiration of the generated state, such as PIT and FIB information, otherwise it is forced to rebroadcast. The interest broadcast should be considered as it increases content dissemination efficiency, but introduces another disadvantages in the communication process. The frames are not filtered by common by devices driver like IP address, but it processed by the CPU, which conflicts with the limited hardware resources. In another way, a common link layer technologies such as 802.15.4 do not support error handling of broadcast frames and introduces significant impacts on the data link layer compared to the unicast communication type. As a result, the NDN goal of retrieving content without needing a host address is easily met by a broadcast technique. However, the large overhead caused by the Interest broadcast requires a careful design to reduce unnecessary Interest transmission.

Recent initiatives that attempt to link the name of the content to the address of the producer. This type of communication pattern is artificially enabled at the equipment level by frame filtering based on destination addresses. This communication pattern is incompatible with the NDN vision since there is no wireless forwarding based on content names without any host identification such as MAC addresses. The communication patterns in IoT suggests that the communications can involve more than two identified hosts as the same content can be shared between multiple nodes.

Both approaches are try to prevent interest packet broadcast storms from the network. However, in spite of their benefits they put additional overhead to current NDN architecture. For this reason, the solution which based on the nodes energy efficient and signal strength (best-path selection) system is proposed. This proposed system consists of a multi-cast based interest forwarding method that takes into account when relying considers residual energy and signal strength of nodes in deciding whether to forward interest packets.

CHAPTER FOUR

PROPOSED SOLUTION

4.1 Overview

As discussed in literature reviewed, IoT constrained-node is one of the most serious network, which need focus in the IoT architecture or system. These type of network needs treatment or appropriate management to extend the network lifetime so long as. Small device with limited resource such as CPU, memory and power resources or constrained devices such as sensors, actuators, smart objects or smart devices can form a constrained network and becoming constrained nodes in that networks. The network itself may exhibits constraints in the form of unreliable or loss of channel, limited and unpredictable bandwidth, and dynamically change in topology. IoT devices uses NDN architecture to forward in a low-rate mesh network by using IEEE 802.15.4 networks. These NDN wireless forwarding low-end IoT devices is one the main features supported. These forwarding strategies generally performed based on a broadcast and learn mechanism. In this approach, Interest packets will broadcasted up to the content found. As a result, the next requests processed based on the information learnt in the previous forwarding methods. So that, blind flooding or broadcast is necessary in NDN wireless network. It has a potential, which can improve performance of application scenarios, which connect devices through lossy media such as radio. NDN services to compensate radio interferences or devices overhear which performed at data link layer. It places contents closer to the sink and reduces number of hop which Interest packet pass through when look up the contents in the network. In another term packet, loss also reduced. However, opposite to IP communication there is no clear mapping between content name and a MAC address in NDN, which enforces the packet to broadcast on the data link layer. Consequently, it needs an actual or smart mapping of content name with link layer address, which keep from bound to the broadcast in the network. Therefore, the evaluation result reported later should be bolded that the broadcast is the most resistant transmission method to handle disseminating, mobility and caching and identify its major drawback in the network.

4.2 NDN forwarding Strategy

In NFD, the forwarding strategy acts as a decision maker, determining when and where to transmit incoming Interests packets. The motivation of having multiple strategy to show the difference between single fixed strategies, which cannot fit the needs of for all applications. For example, some applications may require to multicast Interests to all available Faces to retrieve any matching copy of the Data as much as possible, while the other may want to retrieve Data only from locations pointed by the routing system. Per-namespace selection of the specific strategy used when a decision about Interest forwarding needs to be made. The Interest forwarding decision points can forwarded based on the built-in strategies. The existing forwarding strategy in the combination of ICN and IoT communication path has its own advantages and disadvantages based on the communication parameters used.

4.3 Properties of best path selection.

There are many routing path in NDN network. This routing path determine the speeds of accessing the demanded data. Therefore, when packet request is income they may broadcast it or unicast based on the existing parameter. In the area, which has no control the packets, disseminated in all existing path. This type of communication parameter extremely affects the network as well as the devices resource. Here, the interest broadcast only causes extra computation without improving network performance. Typically, the link quality of all node is not the same sometime the shortest path in network may have no good link. As a result, the request lifetime may be expire where the packet replied to the requested side. In order to minimize this tricky the paper use a link quality indicator as a metric to select the most appropriate path, which consider resources they have.

4.4 Select best Path based on Link quality

In IoT constrained, objects take part in the communication are energy constrained. There are processes in energy efficient forwarding methods that minimize the energy consumption of participating nodes while increasing network efficiency. To retrieve the Data packets the best possible path should selected and emphasizes the performance of access time (it reduces delay time). Using best path in the routing rapid flooding of unsatisfied Interest packets are reduced as a result network performance increased. The main advantages improved in this communication pattern is that, it reduce the flooding of Interest packets and increases network efficiency. It reduces duplicate data packet replied as well as avoid multipart communication process. The rapid flooding of unsatisfied Interest packets leads the network overloads. Due the routing process in NDN stateful, every node start process if a packet is perceived during communication.

The residual energy of active NDN node also considered this scheme and Interest message forwarding scheme is rely on the nodes energy status. A consumer may transmit an Interest packet with the name of the content, and the recipient node must first determine the packet's legitimacy. Based on the instruction in the Interest packet it may be dropped or inspect for further process. For the first time the node, check if the requested content is in the content store. After CS and PIT entry checks, if no entry found in any of CS or PIT then the NDN node examine the energy of each node and a node within better energy than the others would be forward the incoming Interest packet to the destination or to the producers.

Node stabilities in a network can result in rapid flooding of unsatisfied Interest packets so that it leads to network overloads. A link stability based Interest forwarding decreases the number of Interest and data packets distributed in the networks. To forward Interest packet it rely on the signal quality estimation method. Sometimes, for some reason a link become unreliable. Therefore, our thesis based on the efficient transmission of path selection scheme of a routing protocol depends on the accuracy of link quality, which increase accessibility. In order to choose a best path among the others the paper use the link quality indicator approach, which proposed in [61]. In this article link, quality indicator categorized as good, intermediate and bad. In our algorithm, it chooses only good and intermediate as our parameter. The intermediate approach used to choose alternative path in case if there is no node with a good link quality. So, if the content not found locally forwarding decision performed based on this stated parameters.

Each network node relies on the quality of signal to make interest-forwarding decisions. Its value computed locally and consists of average elapsed time between forwarding an Interest packet and receiving its corresponding data packet (round-trip time). The algorithm 4.1 shows the operation performed on receiving an Interest packet by any forwarding node in the network. When a code receives an Interest packet it first confirms the signal strength of the node and compare with the others.

The node validate the signal status of node and if a node signal is in a good status it send an incoming Interest packet. Unfortunately, if there is no node with good signal strength in the network then it checks nodes with an intermediate status. Thus, drops an interest packet, which have bad status, and no longer participates in the content searching process. Therefore, the time between sent Interest packet and send content back to the consumer is too short to wait. To demonstrate the value of path selection, a simple technique was utilized to minimize unwanted transmissions when flooding an interest packets on a broadcast channel, which can create packet collisions, high overhead, and redundancy. To increase packet delivery performance, the forwarding strategy should be set using time-based packet suppression techniques that require a node that accepts the delayed packet to discard it if the identical packet is overheard across a channel. This is the Pseudo code of overall communication process of our proposed document.

Psuedo Code: Communication Process Monitor

IneterestPacketReceived (InterestPacket):

Step 1: Function ***ProcessInterest ()*** // Consumer need some content

Step 2: **Interest Packet.** *Consumer start application and generate Interest name based*

Step 3: *First, the node validate the name, then lookup the content in its local storage if cached applied.*

Step 4: *If Content is* **NOT** *in CS, then check if this name is in the Pending Interest Table (PIT).*

Step 5: *if Name NOT in PIT, then Check Link Quality Indicator (RSSI)*

Step 6: *if Link Quality Indicator status is good then*

Step 7: *Send Interest Packet, Update PIT (Register IterestPacket, IncomingInterface)*

Step 8: *if Link Quality Indicator status is not good then*

Step 9: *Validate if Link Quality Indicator status is Intermediate then*

Step 10: *Send Interest Packet, Update PIT (Register IterestPacket, IncomingInterface)*

Step 11: *If Link Quality Indicator is neither good nor intermediate then*

Step 12: *Drop Interest Packet* |

Figure 4.2 Communication process of the nod

Starting Simulation Algorithm

This algorithm is applied in each NDN node for the sake of best path selection

```
Algorithm 1 Function
    InterestPacketReceived (InterestPacket)
Let N.RSSI =good
Let N.RSSI =intermediate
       If Content  != CS then
            If Name !=  PIT
                  If N.RSSI = good       //  RSSI <4
                        SEND(InterestPacket)
                      UPDATEPIT (InterestPacket, OutInterface)
                  elseif N.RSSI   != good
                       if N.RSSI =intermediate // RSSI 4 - 10
                            SEND(InterestPacket)
                          UPDATEPIT (InterestPacket, OutInterface)
                      end
                  else
                      DROPINTEREST(InterestPacket)
              end
           else
              UPDATEPIT (incoming interface)
          end
        else
          SENDDATA (data)
      end
    end
Output: Interest Packet is sent on the best path among the path.
```

Algorithm 4.1 Each Node configuration setting.

Flow Chart for proposed Solution

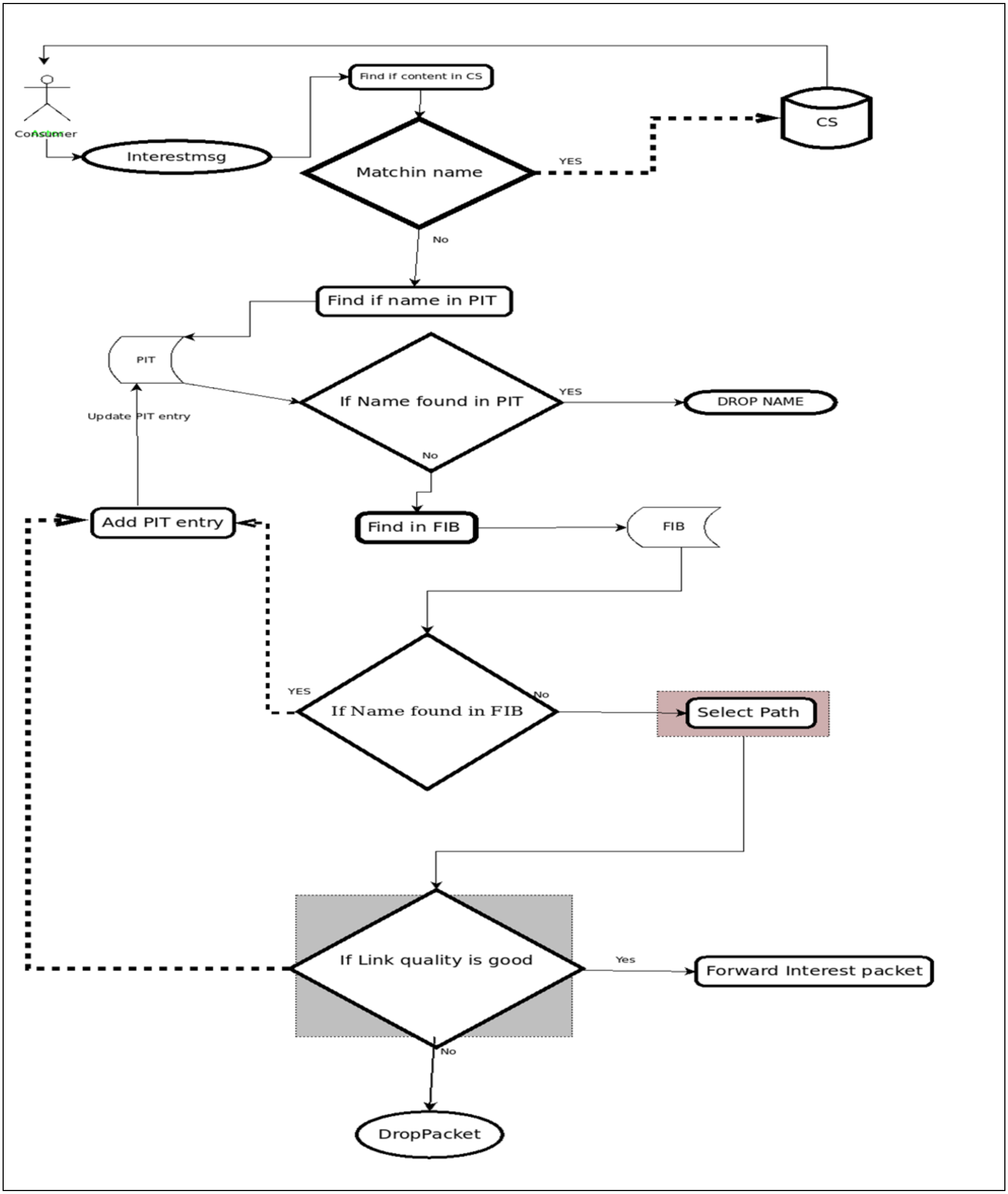

Figure 4.2 Flow chart for Proposed Solution.

4.5 Process for received interest packet in path selection

The processing of interest packet at relay node can be explained in the following steps.

1. When a node receives a packet, it checks to see if it is an interest packet.
2. In the case of an interest packet, it first checks its nonce and lifetime value. If a packet is a duplicate or expired packet, then the node discards it.
3. The node looks up its CS to find the desired data packet. If it is found, the node defer and listens to the channel for data time.
    a. If the same data packet is detected during this time, then the node discards its own data packet
    b. Otherwise it forwards the packet and discards the corresponding entry from the PIT
4. If the data packet is not in its CS, it looks up its PIT for any existing entry.
5. If an entry is found in its PIT (which means that some other nodes have already requested the same data message packet), then the node discards the packet.
6. In the case of no PIT entry, the node checks the node's residual energy (E_{res}).
    a. $E_{res,}$ is less than $E_{thres,}$ the node is in the danger state. It adds the corresponding entry to its PIT entry and discards the interest packet for further transmission.
    b. Otherwise, the node is in the safe state. It inserts the PIT entry, waits, and listens to the channel for interest message time.
        i. If the same interest message or data message time is received (defer) during this time, the node discards the current packet.
        ii. Otherwise, it forwards the interest packet to the other nodes.

4.6 Process for Received Data packet in Path selection

When a relay node receives a data packet, it follows the following process.

1. When a node receives a packet, it checks to see if it is a data packet.
2. In the case of a data packet, the node looks up its PIT for any corresponding entry related to the packet
3. If there is no other entry, the data packet is supported to be marked as unsolicited and it is discarded.
4. Otherwise, the node saves the current data packet in its CS.

5. The node looks up its PIT to check the pending requests from other nodes.
    a. If all requests for the interest packets are satisfied, it discards the corresponding entries from PIT.
    b. Otherwise, it defers and listens to the channel for data message time.
        i. If the same data packet with the same time is detected during this process, the node gives up its own transmission.
        ii. Otherwise, it forwards the data packets to other nodes.

To request Interest packet it follows the following procedures. The consumer that requests the needed data initiates the NDN communication. The customer can start an application from his or her smartphone to request data by submitting an Interest including the data's name.

When a packet reaches a node an Interest, it first checks to see whether matching Data already exists in its CS. If the relevant Data is discovered, it is returned as a response from its local CS without further forwarding the Interest. When there is no matching data in the CS, the router checks the PIT entry to determine whether there is an Interest in the table for the same information. This is true if the request is made before the content's expiration date. If this is the case, the new Interest will not be sent, and just the originating interface will be added to the current PIT record for Interest filtering. If no matching data is found in the CS and no equivalent Interest exists in the PIT, the Interest is sent. As a result, the Interest is routed based on the longest prefix match (LPM) against the FIB records. For instance, in this Interest name, FIB may find possible LPMs like "/Building", "/Building/floor/1" and even "/Building/floor/1/room/21", and the longest one is chosen.

The router then records the Interest in the PIT and sends it to the appropriate interface. If there is no match, the Interest is either flooded to all outbound interfaces or discarded, depending on the forwarding method. The Data packet containing the requested material is delivered back when the Interest reaches the content producer (the sensor) or an intermediary cache node. As a result, the Data packet takes the opposite path of the Interest, following traces left in each router's PIT.

When a Data packet arrives at a router, it is routed to the interfaces where the relevant Interests are received. The router then discards the entry from the PIT and saves the most recent Data packet in its CS. If no matching record for the Data packet exists in the PIT as a consequence of the Interest lifespan having ended, the Data is discarded.

CHAPTER FIVE

5 IMPLEMENTATION AND EVALUATION

In this section, the evaluation of the data accessibility of the content from producers done. So it mainly focuses on the Interest packet generated and exchanged between consumers and producers nodes by using named data network. Moreover, the proposed document investigate the benefits of selecting the best path in order to, efficiently access the content data produced by producer in the network when demanded. In our investigation selection of the best path, identify more performance than the existing forwarding system. In our case, to forward an incoming packet the node first check the link, which have better quality among the other path. The obtain result is a better when compared to name-to-MAC address and broadcasting forwarding strategy approaches in terms of packet drop rate, accessibility time, and energy consumption. Using a basic IoT scenario to demonstrate the effects of NDN-MAC mapping on forwarding performance. Only the MAC address may be used to filter a packet in current IoT wireless devices. The side effects of broadcast is that, the NDN packets processed by the CPU, which extremely consumes a node energy as well, create more loads on devices, which causes network overhead. In order to reduce burdens from the node and network using the effective forwarding strategy is a best solution which keeping broadcasting advantages.

5.1 Environmental Setup

5.1.1 Hardware Technology

Experiments are conducted on HP Desktop computer, which runs Ubuntu 20.04 platform with the Long-term support. The laptop has 4GB RAM and Intel® Core ™ i7-6500U CPU@2.50GHz 2.50GHz processor. For the purpose of our experiment, the ndnSIM 2.8 installed on Ubuntu 20.04 LTS HP Desktop computer.

To deploy on a real environment the IoT low-end devices is used. These devices have single-board microcontrollers and typical exact example of constrained-devices, which has a low power, a slow-speed CPU, and a few kilobytes of RAM and Flash (storage). These devices intended to support NDN stack implementation and run a simple NDN producer application, which generate Interest packet, which has content name and Data packets.

IEEE 802.15.4**.** This technology uses 27 non-overlapping channels which including 16 in the 2.4 GHz and 11 in the sub-GHz bands. The 2.4 GHz band has a bit rate of 250 kbps. The MTU is typically 127 bytes, and frames protected with a 16-bit CRC. It is widely used in the research area and features many different MAC layers such as Carrier Sense Multiple Access (CSMA), and Time Slotted Channel Hopping. With CSMA, nodes keep their radio always on, operate on a single channel, and access the medium through a contention algorithm, CSMA, in a slotted or un slotted mode. In unicast transmissions, link-layer acknowledgments used to confirm reception and enable retransmissions. Using NDN directly on the link-layer layer is a wise choice in wireless networks. This raises various questions on how to design forwarding strategies. First, it needs to figure out whether unicast MAC addresses must mapped to NDN names or a broadcast forwarding is more efficient. Second, while a forwarding strategy supported at the NDN network layer, it may affect the underlying link-layer components such as the CSMA algorithm.

5.1.2 Software Technology

The software platform is based ndnSIM 2.7. An ns-3 module implements Named Data Networking (NDN) communication module, which is a clean slate Internet design. The experiments include single consumer and more than one producer situations, which describe in more detail next to the analysis of our experiments. Our results represent averages over multiple runs with the same parameter settings.

5.2 Metrics used in our proposed solution

Routing metrics are classified into two types: node metrics and link metrics.

Node metrics include node consumption, node location, node energy remaining, and hop count metrics, whereas link or signal metrics concern the route between nodes. To evaluate the output the proposed system use the following four performance metrics:

- Forwarded data packet (FDP). It uses to indicate the number of data packets transmitted in response to the interest packets from the consumers. This metrics help to evaluate the capacity of offload node traffic.
- Rate of interest satisfaction (ISR).This is the percentage of interest packets that were successfully transmitted throughout the transmission duration. It counts the number of Interest packets provided as delivered content.

- Interest packet forwarded (FIP). It calculates the average number of interest packets sent by all nodes when retrieving data. It is used to assess the resource consumption of a PIT.
- Round-trip travel time (RTT). This is used to define the time in seconds between the consumer sending the Interest packet and the arrival of material in response to the requested Packet.

5.3 Simulation Topology

For the sake of our experiment, 3x3-grid topology is used, which holds nine nodes. A single consumer node and a variable number of producer nodes are randomly chosen. The amount of unique and static content elements on the producer node varies. The consumer node requests existing content items from the producer node at random. The document verify that all nodes are physically reachable, and consumers must have routing entries that allow them to contact producers directly. To evaluate the impacts of flooding interest packet throughout the network default-forwarding strategies were enabled in all nodes. The NDN stack generates and send out Interest packet, which includes two-option parameter in the command. First, the prefix name, which is mandatory in the Interest packet, sent without optional parameter like layer address. Therefore, the Interest packet enforced to broadcast. Then after, the number of node wakeups counted and the devices CPU load measured. The Figure 5.2 illustrate the expected simulation topology of the experiment. To analyze the output three procedures used. First, on all nodes, install a common prefix route, which decide forwarding strategy of all content names, and sent packets to every eligible face (there is no specified face) so the broadcast address is used.

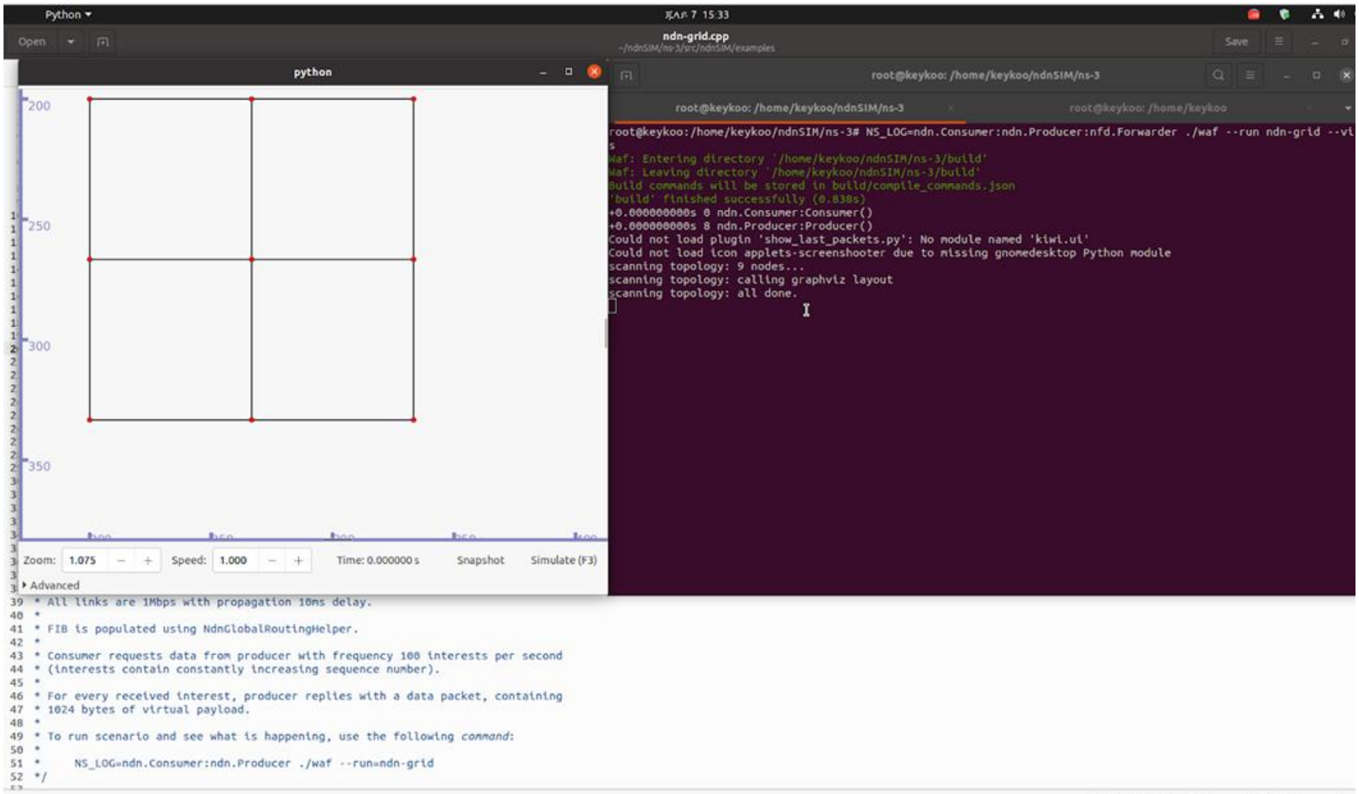

Figure 5.1 simulation topology setup

Second, install dedicated FIB entries solely on the specified consumer, which might be either the producer's unicast address or the broadcast address. The network size is altered and load by adjusting the number of producer nodes or the amount of content items per producer in a predetermined network size for further analysis. The number of content items per node is fixed and different network sizes is used, but increase the number of producers with different parameter settings by fixing the average content request rate per producer, and increase the number of Interests sent by consumers, which is directly proportional to the number of nodes in the network. Furthermore, while the number of nodes limited and varying the amount of contents items used in each node. A constant pace of content request per customer is used.

5.4 Simulation Parameters

To simulate our proposed system, 9-node in grid architecture is used while a consumer nodes equipped with NDN forwarding information. The goal of this simulation is to see if the forwarding method reduces the impact of the broadcast on the network.

The forwarding strategy intended for usage in IoT device local networks. As a result, a network of nine nodes was selected as a typical local network size to evaluate communication. In practice, wireless NDN should not use logical topology-based host identification. The IEEE 802.15.4 characteristics are mirrored in the MAC layer configuration. Table 5.1 reports the relevant simulation parameter.

Parameter
Interest Packet (using parameter)
Data packet size (to see by varying)
Payload size(it set 90 Kbytes content)
Number of nodes(to use 9 nodes)
RSSI (To check the signal strength)
Time (to know the time interval of Interest and data)

Table 5.1: Used parameters

5.5 Traffic generated

After the user, apply a following command:

```
~/ns-3# NS_LOG=ndn.Consumer:ndn.Producer:nfd.Forwarder ./waf --run ndn-grid --vis
```

The following figures shows that how NDN construct the path using link quality indicator and forward Interest packet in our simulation. Assume the distance between each node is the same.

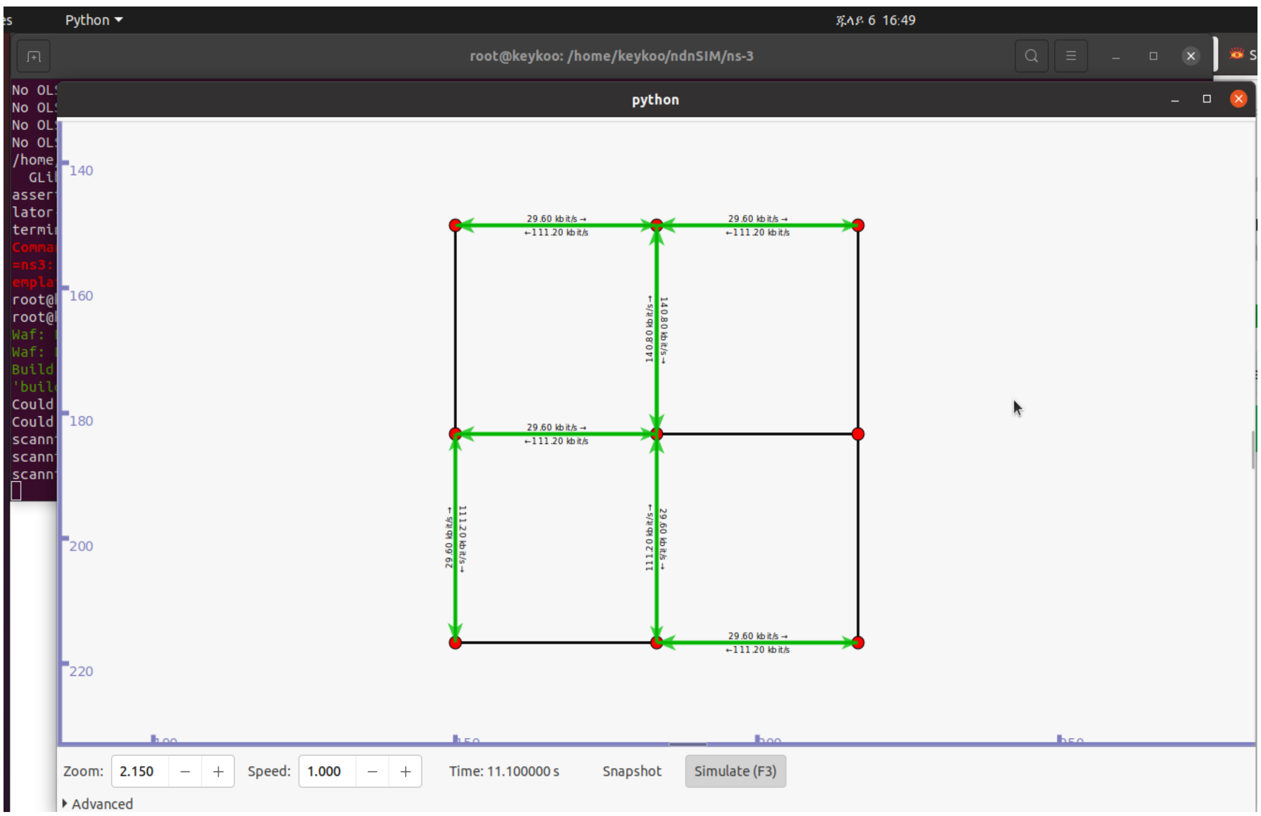

Figure 5.2: Simulation Start**.**

5.6 Result Discussion

A single consumer and a single content provider in our simulation utilized. Typically, the basic configuration for consumers is configured to fetch content items from the producer node on a regular basis by adjusting the interest number in different time values.

5.6.1 Interest Satisfaction Rate (ISR)

It was utilized to demonstrate the effectiveness of our techniques in providing the material requested by consumer nodes. Finally, broadcasting gave the greatest results, especially in small nodes, but also used a lot of network resources by sending duplicated Interest packets as well as duplicated data packets (duplicated data packet sent) since all nodes created a PIT entry during transmission. The unicast forwarding strategy is similar with broadcasting strategy in some condition but FIP and FDP is significantly in some scenario reduced. In our case, the Interest satisfaction rate is better than the aforementioned approach because our algorithm checks first received nodes' signal strength before transmitting incoming Interest packet. Therefore, the node with best signal strength transmit incoming packet without consuming resources of the devices have less resources. It sends both Data packet and Interest packet based on the path, which have the best signal strength among other path in the network. It reduced dissemination of Interest packet throughout the network and protect duplicated data packet replied.

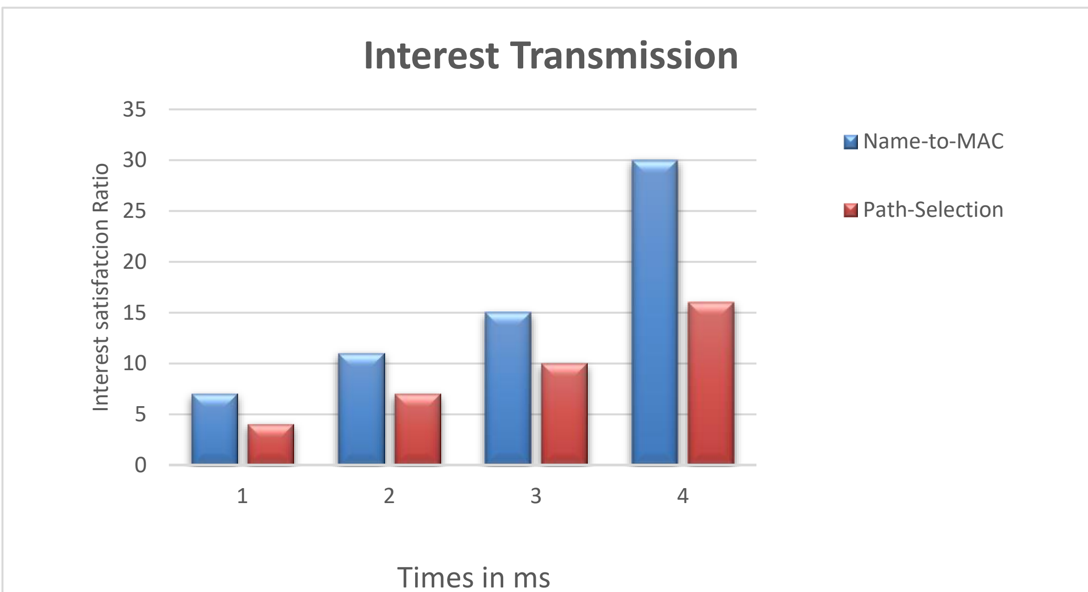

Figure 5.3 Interest Satisfaction Ration

5.6.2 Forwarding Interest Packets (FIP)

The aim of including a connection quality indicator into an NDN forwarding strategy is to decrease the total number of forwarding Interest packets (FIP). As it shown on the figure 5.6 the proposed solution reduced the number of interest distributed in a network and had a better results where compared to the other approaches. Regarding the blind forwarding strategy, best path selection reduced forwarding Data packet. Here, as soon as number of node increased the output of RSSI produced a better Interest packet forwarding than the native broadcasting approach and name-to-

MAC address (unicast) approach used. The total number of Interest packet reception rate is determined at the Producer level and represents the average of successfully received interest.

$$IRR = \frac{\text{Number of received interest packets}}{\text{Number of sent data packts}} \times 100 \text{ -- (Eq.1)}$$

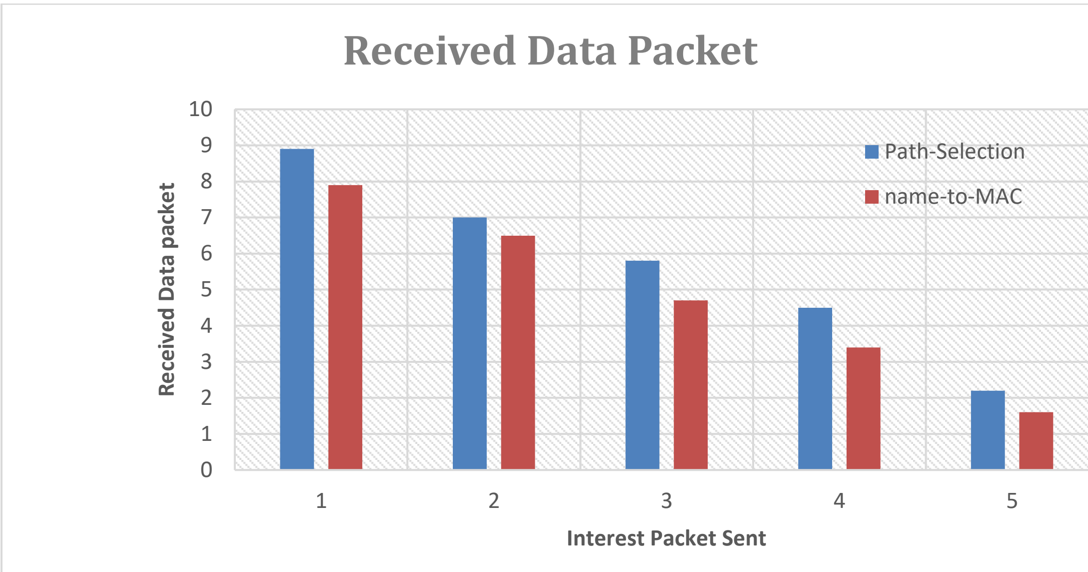

Figure 5.4 Forwarding Interest packet

5.6.3 Data Packet Forwarding (DPF)

The NDN forwarding technique only sends interest packets to one of the network's nodes. It was expected that the method will alleviate the load of intermediary or adaption technology from IoT devices. Currently, NDN forwarding architecture used the native wireless forwarding and the forwarding scenario recently tested as name-to-MAC (unicast). The goal of our proposed system, which transmit based on the path selection strategy, would reduce the number of data packet forwarded back to the requestor or consumer. In NDN each node create a PIT entry when they forward a packet to upstream so when data replied back it uses this created path as a route. So in the previous forwarding strategy data replied through each node, which have active PIT entry. However, in our proposed solution only a node, which have a good signal strength, is create a PIT table. Therefore, data replied only through this entry. The total number of data packet received calculated at the consumer side.

$$DPR = \frac{\text{Number of received data packets}}{\text{Number of transmitted interest packets}} \text{ -- (Eq.2)}$$

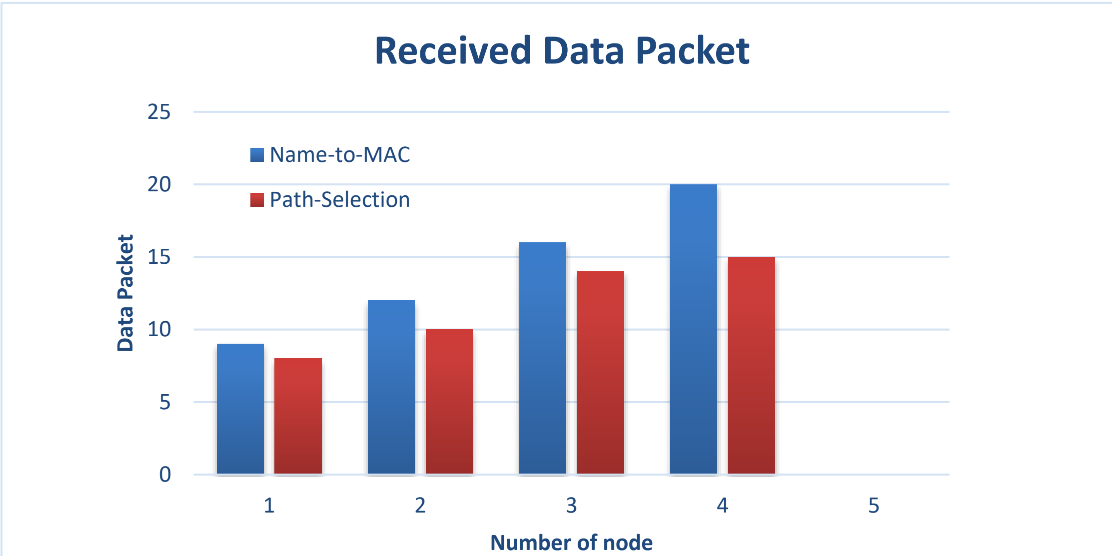

Figure 5.5 Data packet forwarding

5.6.4 Round-Trip Time (RTT)

The number of transmitted interest over the network indicates if the broadcast effect is attenuated and the RTT is used to check that waiting delays. In NDN has a built-in loop free packet forwarding which allows the forwarding strategy in NDN to freely make a forwarding decision based on the real time. FIB associates the content name with the list of interfaces in FIB entry. The state information such as round-trip time of these interfaces is maintained by FIB. It measured the round-trip time for an interest-data exchange. When compared to alternative techniques, forwarding incoming interest packets depending on connection quality not only supplied material requested by customers but also in a good RTT. The results demonstrate that the use of link quality is efficient, since the number of Interest packets and Data packets on the network has decreased. When compared to the broadcast method, the latency between the Interest packet and the Data packet is quite short, with a little difference when compared to unicast. An ideal improvement is the reduction of round-trip time by eliminating waiting delays while keeping the lowest number of both Interest and Data transmissions.

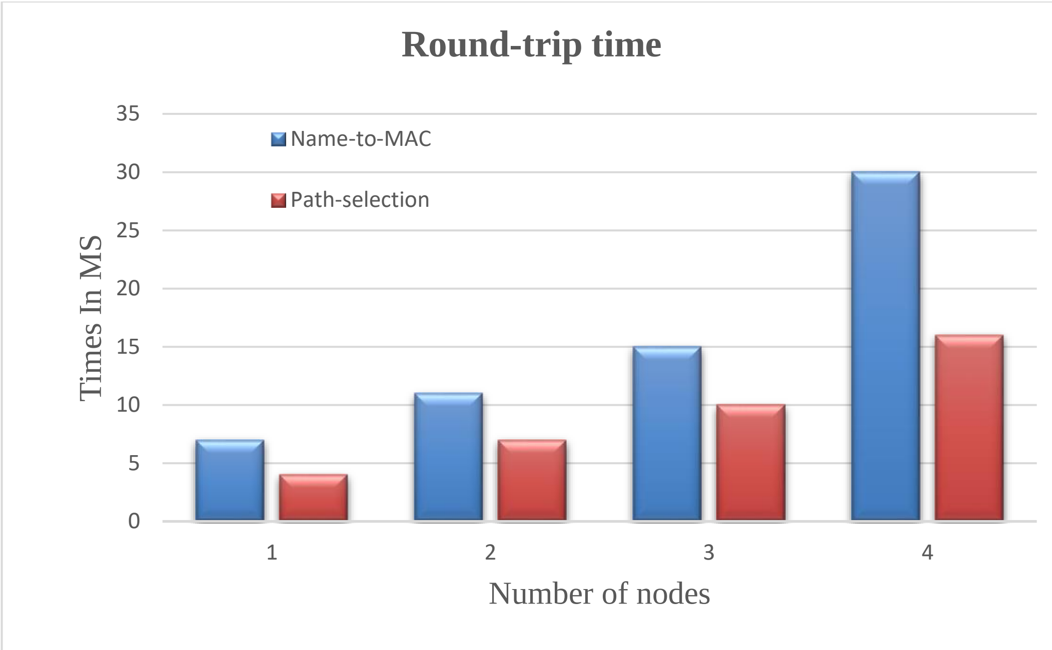

Figure 5. 6 Round-Trip Time

The RSSI forwards expected that it would reduce the number of received data packets from the network. According to figure 5.6, the best path decrease a number of received data packet in our scenario compared to the other forwarding strategy. As the number of Interest packet sent increases, the data packet replied back to the consumer decreased due to the network is overhead. A node receives an interest packet perform eligibility of the node to forward the incoming packet.

5.7 Energy Consumption

Network transmissions, including content labeling, network flooding, and wireless broadcast, have a significant influence on energy usage. In IoT devices, routing information is performed via names and prefixes that are dynamically auto-configured. The resultant overhead is determined not only by the routing protocols, but also by the number of names to be processed in ICN packets. In our studies, the default flooding of both interest and data packets which had a significant impact on the network is discovered, with each node in the network repeating each flooded packet on any interface. Each flooding needs O (n) packet broadcasts and O (nm) packet receptions, where n is the number of nodes in the network and m is the average node degree.

5.7.1 Using Residual energy as a routing metrics

The communication between the resource-constrained devices are battery powered so that there is a need to improve the energy efficiency of these resource-constrained devices. To improve energy efficiency of the network, energy efficient routing metrics is used. Actual parameters used to calculate energy consumption of each node is shown in Eq. (2). The formula consists of energy value (number of ticks, which CPU is running), current, and voltage (consumed by CPU) and RTIMER_SECOND (constant number of ticks in platform).

Current energy with each node is calculate by the following equation:

$$\text{Energy Consumption} = \frac{\text{Energy value} * \text{Curent} * \text{Voltage}}{\text{RTIMER}_{\text{SECOND}}} \text{...} (1)$$

$$E_{current\_energy} = E_{initial\_energy} - E_{consumed\text{-}energy} \text{...} (2)$$

Where:

$E_{initial\_energy}$ and $E_{current\_energy}$ means the energy of the nodes.

The initial energy of the node needs to be assigned. Current energy of the nodes needs to be calculated based on the above Eq. (2). Then, based on this initial energy and current energy remaining energy or residual energy of the node will be calculated using the following Eq. (3).

$$RE = \frac{Initial\_Energy}{Current\_Energy} \text{...} (3)$$

5.8 Analysis

Both forwarding data packet and Interest satisfaction results are better than the default routing strategy. Because only a node with a greater signal strength constructs a PIT entry table and a node with a better signal strength satisfies Interest, only a small number of data packets are transmitted back to the consumer. Forwarding Interest packet metrics also shows a better results compare to the other forwarding strategies. By maintaining an appropriate level of Interest satisfaction ratios, it greatly decreases the amount of Interest packets transmitted without negatively impacting the network with data packet duplication. Therefore, it can be concluded that using signal strength provides:

- Better network resources utilization due to a few number of node are involved
- Reduce a number of interest packets.
- Reduce a duplicate data packet to reply

- A short response time compared to the others forwarding system.

CHAPTER SIX

CONCLUSION AND RECOMMNDATION

6.1 Conclusion

The ICN approaches, is a network design architecture identified as a potential alternative network paradigm for the IoTs requirements which are challenged in the current Internet architecture. Among these IoT requirement that need to be addressed are answered by integrated both NDN and IoT network architecture and shown a potential solution in security, naming content and devices, in-network caching, and having maintenance routing path. In order to identifies the advantages of the combination of both system many efforts are done by researchers community, however, the currently approaches done to minimize overhead produced in the network but unsatisfied Interest packets reduced at the costs of additional data structure upon the NDN architecture that need additional memory and use extra controlling messages. Despite their benefits, all of them add overhead to current NDN architecture by adding new data structures, which need addition space and controlling mechanism. So in the resource-constrained devices overhead extremely consume the devices resource and shorten the life of those devices. Individual node life has its own impacts on over all networks performance as well continuity. In some scenarios to access small amount of data, the system cost it valuable resource. So that it is very crucial point to develop a system that assist NDN network forwarding system, which able to keep a valuable resource and increase accessibility of demanded data. In order to avoid these tricky the path selection algorithm or the proposed solution focused on the node's signal strength and nodes residual energy to evaluate the reduction of interest packets of NDN network from the network. Sometimes to access a small amount of data from the producers lose many resources especially in the resource-constrained devices as well as constrained network. So efficient resource utilization technique, which can keep the network as well as individual node's lifetime. The combination of NDN and IoT benefits are need proper management that forwarding interest packet to the destination. Therefore, the work done in this system is to examine whether the network is effective increased or not when individual node energy and signal participate in the network. The experiment is conducted to shows the interaction between the NDN which operate at network layer and the underlying data link layers. By using both metrics the amount of interest packet distributed in the network is decreased compared to the previous forwarding system such as blind forwarding and name-to MAC address mapping. Due to there is no controlling mechanism or designed protocol, which properly redirect the incoming packet to the destination devices or producers packets are, disseminated in the network to discovery the producers. Each packet consume the nodes resource in order to find a path to producers' node. Not only path discovery costs the node but they consume their energy during process unused data. Energy loosed for listening incoming interest packet, PIT entry creation, and transmission of duplicated data packet reduced as interest packet minimized from rebroadcasted. In IP network stack, which map IP addresses to the unicast MAC addresses of the destination devices and by using this mechanism packet prevented from broadcasted throughout the network. However, unlike IP address there is no clear mapping mechanism, which map consumer interest packet in the NDN by default, which prevent that incoming packet from flooding in low-end IoT solutions. The experiment is conducted to shows the interaction between the NDN which operate at network layer and the underlying data link layers. The document approve that link layer broadcast should be reduced in specific deployment scenarios especially in IoT without contradicting the principle concept of NDN as link layer broadcast conflicts with limited hardware resources in terms of processing, memory, and energy. The connection of NDN faces to unicast or broadcast MAC addresses and computed the resource overhead of using.

6.2 Recommendation

The current work discusses about NDN forwarding strategy improvements of data accessibility by reducing unwanted interest packet from the network. Future work should focus on covering other IoT scenarios, for example, scenarios where different real low-end IoT technologies are used. Short name of content and devices make efficient the link layer broadcasted path selection strategies. Intelligent mechanism, which immediate modify a routing path when the consumer unfortunately need data packet in the network without affecting the other node resources. Dynamic name based routing protocols is a good opportunity to design which immediately adapt congestion and topology changes. In another way, forecast combination of various technology with IoT architecture and compare with their output.

Reference

[1] S. Arshad, M. A. Azam, M. H. Rehmani and J. Loo, "Recent Advances in Information-Centric Networking-Based Internet of Things (ICN-IoT)," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2128-2158, April 2019, doi: 10.1109/JIOT.2018.2873343.

[2] S. Arshad, M. A. Azam, M. H. Rehmani and J. Loo, "Recent Advances in Information-Centric Networking-Based Internet of Things (ICN-IoT)," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2128-2158, April 2019, doi: 10.1109/JIOT.2018.2873343.

[3] “Bluetooth LE,” https://www.bluetooth.com/specifications.

[4] P. Kietzmann, C. Gündoğan, T. C. Schmidt, O. Hahm, and M. Wählisch, “The need for a name to MAC address mapping in NDN: Towards quantifying the resource gain,” *ICN 2017 - Proceedings of the 4th ACM Conference on Information Centric Networking*, pp. 36–42, 2017, doi: 10.1145/3125719.3125737.

[4] Nour B, Sharif K, Li F, etal“ICN Publisher Subscriber Models: Challenges and Group based Communication” [J].IEEE Network (SCI, IF: 7.503). 2019, 33(6): 156163. (DOI:10.1109/MNET.2019.1800551).

[5] Nour B, Sharif K, Li F,et al.“A Survey of Internet of Things Communication using ICN: A Use case Perspective”[J].Computer Communications(SCI IF: 2.766).2019, 142 143: 95–12. (DOI:10.1016/j.comcom.2019.05.010).

[6] Nour B, Sharif K, Li F,et al.“A Survey of Internet of Things Communication using ICN: A Use case Perspective”[J].Computer Communications(SCI IF: 2.766).2019, 142 143: 95–12. (DOI:10.1016/j.comcom.2019.05.010).

[7]. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015, doi: 10.1109/COMST.2015.2444095.

[8]Amadeo M, Campolo C, Quevedo J, et al. Information centric networking for the internet of

things: challenges and opportunities [J]. IEEE Network, 2016, 30(2): 92–100.

[9] M. James, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, and D. Aharon, “The Internet of Things: Mapping the value beyond the hype,” McKinsey Global Institute, p. 3, 2015.

[10] M. F. Bari, S. R. Chowdhury, R. Ahmed, R. Boutaba, B. Mathieu, A survey of naming and routing in information-centric networks, IEEE Communications Magazine 50 (2012). doi:10.1109/MCOM.2012.6384450.

[11] S. Arshad, M. A. Azam, M. H. Rehmani, and J. Loo, “Recent advances in information-centric networking-based internet of things (ICN-IoT),” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2128–2158, 2019, doi: 10.1109/JIOT.2018.2873343.

[12] Lucas Wang, Alexander Afanasyev, Romain Kuntz, Rama Vuyyuru, Ryuji Wakikawa, and Lixia Zhang. 2012. Rapid Traffic Information Dissemination Using Named Data. In Proc. of 1st ACM Workshop on Emerging Name-Oriented Mobile Networking Design - Architecture, Algorithms, and Applications (NoM). ACM, New York, NY, USA, 7–12.

[13] G. Xylomenos, C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos,X. Vasilakos, K. V. Katsaros, G. C. Polyzos, A survey of information-centric networking research, IEEE Communications Surveys & Tutori-als 16 (2014) 1024–1049. doi:10.1109/SURV.2013.070813.00063.

[14] I. Abdullahi, S. Arif, S. Hassan, Survey on caching approaches in Information Centric Networking, Journal of Network and Computer Applications 56 (2015) 48–59. doi:10.1016/j.jnca.2015.06.011.

[15] I. Ari, B. Hong, E. L. Miller, S. A. Brandt, and D. D. Long, “Managing flash crowds on the internet,” in Modeling, Analysis and Simulation of Computer Telecommunications Systems, 2003. MASCOTS 2003. 11th IEEE/ACM International Symposium on. IEEE, 2003, pp. 246–249.

[16] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013

[17] W. Shang, Y. Yu, R. Droms, and L. Zhang, "Challenges in iot networking via tcp/ip architecture," NDN Project, Tech. Rep. NDN0038, Tech. Rep., 2016.

[18] E. Borgia, "The internet of things vision: Key features, applications and open issues," Computer Communications, vol. 54, no. 1, pp. 1–31, 2014.

[19] J. A. Stankovic, "Research directions for the internet of things," Internet of Things Journal, IEEE, vol. 1, no. 1, pp. 3–9, 2014.

[20] V. Varadharajan and S. Bansal, "Data security and privacy in the internet of things (iot) environment," in Connectivity Frameworks for Smart Devices. Springer, 2016, pp. 261–281.

[21] R. Silva, J. S. Silva, and F. Boavida, "Infrastructure-supported mobility in wireless sensor networks — a case study," in Proc. IEEE Int. Conf. Industrial Technology (ICIT), Mar. 2015, pp. 1895–1900.

[22] Y. Al-Nidawi, H. Yahya, and A. H. Kemp, "Impact of mobility on the iot MAC infrastructure: IEEE 802.15.4e tsch and lldn platform," in Proc. IEEE 2nd World Forum Internet of Things (WF-IoT), Dec. 2015, pp. 478–483.

[23] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," Communications Surveys & Tutorials, IEEE, vol. 17, no. 4, pp. 2347–2376, 2015.

[24] Bari M.F., Chowdhury S.R., Ahmed R., Boutaba R., Mathieu B. **A survey of naming and routing in information-centric networks** IEEE Commun. Mag., 50 (12) (2012), 10.1109/MCOM.2012.6384450

[25] Abdullahi I., Arif S., Hassan S. **Survey on caching approaches in information centric networking** J. Netw. Comput. Appl., 56 (2015), pp. 48-59, 10.1016/j.jnca.2015.06.011

[26] Zhang Z., Yu Y., Zhang H., Newberry E., Mastorakis S., Li Y., Afanasyev A., Zhang L. **An overview of security support in named data networking** IEEE Commun. Mag., 56 (11) (2018), pp. 62-68, 10.1109/MCOM.2018.1701147

[27] Yu Y., Afanasyev A., Clark D., Jacobson V., Zhang L., *et al.* **Schematizing trust in named data networking** ACM International Conference on Information-Centric Networking (2015),

pp. 177-186, 10.1145/2810156.2810170

[28]. He P., Wan Y., Xia Q., Li S., Hong J., Xue K. LASA: Lightweight, auditable and secure access control in ICN with limitation of access times IEEE International Conference on Communications (ICC) (2018), pp. 1-6, 10.1109/ICC.2018.8422829

[29] Fotiou N., Alzahrani B.A. **Rendezvous-based access control for information-centric architectures** Int. J. Netw. Manag., 28 (1) (2018), pp. 1-11, 10.1002/nem.2007

[30] D. P. Arjunwadkar, Introduction of NDN with Comparison to Current Internet Architecture based on TCP/IP, International Journal of Computer Applications 105 (2014) 31–35. Doi: 10.5120/18376-9536.

[31] Passarella A. **A survey on content-centric technologies for the current internet: Cdn and p2p solutions** Comput. Commun. 35 (1) (2012), pp. 1-32, 10.1016/j.comcom.2011.10.005

[32] S. Arshad, B. Shahzaad, M. A. Azam, J. Loo, S. H. Ahmed, S. Aslam, Hierarchical and Flat based Hybrid Naming Scheme in Content-Centric Networks of Things, IEEE Internet of Things Journal 5 (2018) 1070–1080. doi:10.1109/JIOT.2018.2792016.

[33] M. Baugher, B. Davie, A. Narayanan, D. Oran, Self-verifying names for read-only named data, in: IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2012, pp. 274–279.doi:10.1109/INFCOMW.2012.6193505.

[34] O. Ascigil, S. Ree, G. Xylomenos, I. Psaras, G. Pavlou, A keyword-based ICN-IoT platform, in: ACM Conference on Information-Centric Networking (ICN), 2017, pp. 22–28. doi:10.1145/3125719.3125733.

[35] B. Nour, K. Sharif, F. Li, H. Moungla, Y. Liu, and M2HAV: A Standardized ICN Naming Scheme for Wireless Devices in Internet of Things, in: International

Conference on Wireless Algorithms, Systems, and Applications (WASA), Springer, 2017, pp. 289–301. Doi: 10.1007/978-3-319-60033-8_26.

[36] Koponen T., Chawla M., Chun B.-G., Ermolinskiy A., Kim K.H., Shenker S., Stoica I.

A data-oriented (and beyond) network architecture ACM SIGCOMM Comput. Commun. Rev., Vol. 37 (2007), pp. 181-192, 10.1145/1282427.1282402

[37] C. Bernardini, T. Silverston, A. Vasilakos, Caching Strategies for Information Centric Networking: Opportunities and Challenges, arXivpreprint arXiv: 1606.07630 (2016).

[38] Fotiou N., Nikander P., Trossen D., Polyzos G.C. **Developing information networking further: From PSIRP to PURSUIT** Conference on Broadband, Springer (2010), pp. 1-13, 10.1007/978-3-642-30376-0˙1

[39] Garcia G., Beben A., Ramon F.J., Maeso A., Psaras I., Pavlou G., *et al.* **COMET: Content mediator architecture for content-aware networks** Future Network Mobile Summit (2011) Google Scholar

[40] Melazzi N.B., Salsano S., Detti A., Tropea G., Chiariglione L., Difino A., *et al.* **Publish/subscribe over information centric networks: A standardized approach in convergence** Future Network Mobile Summit (2012)

[40] Zhang L., Afanasyev A., Burke J., Jacobson V., Crowley P., Papadopoulos C., Wang L., Zhang B., *et al.* **Named data networking** ACM SIGCOMM Comput. Commun. Rev., 44 (3) (2014), pp. 66-73, 10.1145/2656877.2656887

[41] Y. Zhang, D. Raychadhuri, L.A. Grieco, E. Baccelli, J. Burke, R. Ravindran, G. Wang, A. Lindgren, B. Ahlgren, O. Schelen, Design Considerations for Applying ICN to IoT, Internet-Draft, Internet Engineering Task Force, 2017, , Work in Progress, Accessed: 2018-05-18. Google Scholar

[42] M. Amadeo, C. Campolo, A. Molinaro, and G. Ruggeri, "Content-centric wireless

networking: A survey," Computer Networks, vol. 72, pp. 1 – 13, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128614002497

[43] S. Sun, L. Han, and S. Han, "GRMR: greedy regional multicast routing for wireless sensor networks," IEICE TRANSACTIONS on Information and Systems, vol. 99, no. 1, pp. 21–29, 2016. 5960 Bibliography

[44] S. Gao, H. Zhang, and B. Zhang, "Energy Efficient Interest Forwarding in NDN-Based Wireless Sensor Networks," Mobile Information Systems, vol. 2016, 2016.

[45] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, and M. Wählisch, "Information centric networking in the IoT: Experiments with NDN in the wild," in Proceedings of the 1st International Conference on Information-centric Networking. ACM, 2014, pp. 77–86.

[46] M. A. M. Hail, M. Amadeo, A. Molinaro, and S. Fischer, "On the performance of caching and forwarding in information-centric networking for the IoT," in International Conference on Wired/Wireless Internet Communication. Springer, 2015, pp. 313–326.

[47] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in Proceedings of the 5th international conference on Emerging networking experiments and technologies. ACM, 2009, pp. 1–12.

[48] Z. Li, J.-C. Point, S. Ciftci, O. Eker, G. Mauri, M. Savi, and G. Verticale, "ICN based shared caching in future converged fixed and mobile network," in 2015 IEEE 16th International Conference on High Performance Switching and Routing (HPSR). IEEE, 2015, pp. 1–6.

[49] A. El-Mougy, M. Ibnkahla, and L. Hegazy, "Software-defined wireless network architectures for the Internet-of-Things," in 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), Oct 2015, pp. 804–811.

[50] C. Perera, A. Zaslavsky, C. H. Liu, M. Compton, P. Christen, and D. Georgeakopoulos, "Sensor search techniques for sensing as a service architecture for the Internet of Things," IEEE Sensors Journal, vol. 14, no. 2, pp. 406–420, Feb. 2014.

[51] M. A. Hail, M. Amadeo, A. Molinaro, and S. Fischer, "Caching in Named Data Networking for the wireless Internet of Things," in 2015 International Conference on Recent Advances in

Internet of Things (RIoT). IEEE, 2015, pp. 1–6.

[52] O. Hahm, E. Baccelli, T. C. Schmidt, M. Wahlisch, and C. Adjih, “A named data network approach to energy efficiency in IoT,” in Globecom Workshops (GC Wkshps), 2016 IEEE. IEEE, 2016, pp. 1–6.

[53] A. Lindgren, F. B. Abdesslem, B. Ahlgren, O. Schelén, and A. M. Malik, “Design choices for the IoT in information-centric networks,” in 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2016, pp. 882–888

[54] A. Compagno, M. Conti, and R. Droms, “OnboardICNg: A secure protocol for on-boarding IoT devices in ICN,” in Proceedings of the 3rd ACM Conference on Information-Centric Networking, ser. ACM-ICN ’16. New York, NY, USA: ACM, 2016, pp. 166–175.

[55] M. Enguehard, R. Droms, and D. Rossi, “On the Cost of Secure Association of Information Centric Things,” in Proceedings of the 3rd ACM Conference on Information-Centric Networking, ser. ACM-ICN ’16. New York, NY, USA: ACM, 2016, pp. 207–208.

[56] J. Suarez, J. Quevedo, I. Vidal, D. Corujo, J. Garcia-Reinoso, and R. L. Aguiar, “A secure IoT management architecture based on Information-Centric Networking,” Journal of Network and Computer Applications, vol. 63, pp. 190 – 204, 2016.Bibliography 61

[57] L. Breslau, P. Cao, L. Fan, G. Phillips, and S. Shenker, “Securing instrumented environments over content-centric networking: The case of lighting control and NDN,” in IEEE INFOCOM NOMEN Workshop, 2013.

[58] A. M. Malik, J. Borgh, and B. Ohlman, “Attribute-Based Encryption on a Resource Constrained Sensor in an Information-Centric Network,” in Proceedings of the 3rd ACM Conference on Information-Centric Networking, ser. ACM-ICN ’16. New York, NY, USA: ACM, 2016, pp. 217– 218.

[59]. Zhang, A. Afanasyev, J. Burke, and L. Zhang, “A survey of mobility support in Named Data Networking,” in 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), April 2016, pp. 83–88.

[60] J. Quevedo, D. Corujo, and R. Aguiar, “A case for ICN usage in IoT environments,” in 2014 IEEE Global Communications Conference, Dec 2014, pp. 2770–2775.

[61] Renner, C.; Ernst, S.; Weyer, C.; Turau, V. Prediction Accuracy of Link-Quality Estimators. In Proceedings of the 8th European Conference on Wireless Sensor Networks, Bonn, Germany, 23–25 February 2011; pp. 1–16.

[62] A. Abane, P. Muhlethaler, S. Bouzefrane, M. Daoui, and A. Battou, "Towards evaluating Named Data Networking for the IoT: A framework for OMNeT++," vol. 56, no. September, pp. 73–61, 2018, doi: 10.29007/dqr1.

[63] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, and M. Wählisch, "Information centric networking in the IoT: Experiments with NDN in the wild," *ICN 2014 - Proceedings of the 1st International Conference on Information-Centric Networking*, pp. 77–86, 2014, doi: 10.1145/2660129.2660144.

[64] D. Mars *et al.*, "Using Information Centric Networking in Internet of Things : A Survey To cite this version : HAL Id : hal-02393632 Using Information Centric Networking in Internet of Things : A survey," 2020.

[65] B. Nour *et al.*, "A survey of Internet of Things communication using ICN: A use case perspective," *Computer Communications*, vol. 142–143, no. May, pp. 95–123, 2019, doi: 10.1016/j.comcom.2019.05.010.

[66] B. Nour, "ICN Communication Optimization for Internet of Things Boubakr Nour To cite this version : HAL Id : tel-02883232 ICN Communication Optimization for Internet of Things Candidate Name : School or Department : Faculty Mentor : Chair , Thesis Committee : Degre," 2020.

[67] A. Abane, "A realistic named data networking architecture for the Internet of things Amar Abane To cite this version : HAL Id : tel-02447084," 2020.

[68] Z. Huo, T. Liu, T. Li, and H. Zhong, "Research on Addressing Technology of Internet of Things Unique Resources Based on RFID," *Journal of Physics: Conference Series*, vol. 1982, no. 1, p. 012184, 2021, doi: 10.1088/1742-6596/1982/1/012184.

[69] M. Baddeley, R. Nejabati, G. Oikonomou, M. Sooriyabandara, and D. Simeonidou, "Evolving SDN for Low-Power IoT Networks," *2018 4th IEEE Conference on Network Softwarization and Workshops, NetSoft 2018*, pp. 212–216, 2018, doi: 10.1109/NETSOFT.2018.8460125

[70] M. Amadeo *et al.*, "Information-centric networking for the internet of things: Challenges and opportunities," *IEEE Network*, vol. 30, no. 2, pp. 92–100, 2016, doi: 10.1109/MNET.2016.7437030.

[71] D. Mars *et al.*, "Using Information Centric Networking in Internet of Things : A Survey To cite this version : HAL Id : hal-02393632 Using Information Centric Networking in Internet of Things : A survey," 2020.

[72] L. Zhang *et al.*, "NDN Project 2010," *Relatório Técnico NDN-0001, Xerox Palo Alto Research Center-PARC*, vol. 157, no. October, pp. 1–24, 2010, [Online]. Available: http://www.named-data.net/techreport/TR001ndn-proj.pdf.