Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.058607

ARTICLE

SEF: A Smart and Energy-Aware Forwarding Strategy for NDN-Based Internet of Healthcare

Naeem Ali Askar[1,*], Adib Habbal[1,*], Hassen Hamouda[2], Abdullah Mohammad Alnajim[3] and Sheroz Khan[4]

[1]Department of Computer Engineering, Faculty of Engineering, Karabük University, Karabük, 78050, Türkiye

[2]Department of Management Information Systems, College of Business Administration, Majmaah University, Al-Majmaah, 11952, Saudi Arabia

[3]Department of Information Technology, College of Computer, Qassim University, Buraydah, 51452, Saudi Arabia

[4]Department of Electrical Engineering, College of Engineering and Information Technology, Onaizah Colleges, Qassim, 51911, Saudi Arabia

*Corresponding Authors: Naeem Ali Askar. Email: naeem.askar@uod.ac; Adib Habbal. Email: adibhabbal@karabuk.edu.tr

Received: 16 September 2024 Accepted: 11 November 2024 Published: 19 December 2024

ABSTRACT

Named Data Networking (NDN) has emerged as a promising communication paradigm, emphasizing content-centric access rather than location-based access. This model offers several advantages for Internet of Healthcare Things (IoHT) environments, including efficient content distribution, built-in security, and natural support for mobility and scalability. However, existing NDN-based IoHT systems face inefficiencies in their forwarding strategy, where identical Interest packets are forwarded across multiple nodes, causing broadcast storms, increased collisions, higher energy consumption, and delays. These issues negatively impact healthcare system performance, particularly for individuals with disabilities and chronic diseases requiring continuous monitoring. To address these challenges, we propose a Smart and Energy-Aware Forwarding (SEF) strategy based on reinforcement learning for NDN-based IoHT. The SEF strategy leverages the geographical distance and energy levels of neighboring nodes, enabling devices to make more informed forwarding decisions and optimize next-hop selection. This approach reduces broadcast storms, optimizes overall energy consumption, and extends network lifetime. The system model, which targets smart hospitals and monitoring systems for individuals with disabilities, was examined in relation to the proposed strategy. The SEF strategy was then implemented in the NS-3 simulation environment to assess its performance in healthcare scenarios. Results demonstrated that SEF significantly enhanced NDN-based IoHT performance. Specifically, it reduced energy consumption by up to 27.11%, 82.23%, and 84.44%, decreased retrieval time by 20.23%, 48.12%, and 51.65%, and achieved satisfaction rates that were approximately 0.69 higher than those of other strategies, even in more densely populated areas. This forwarding strategy is anticipated to substantially improve the quality and efficiency of NDN-based IoHT systems.

KEYWORDS

Energy efficient; forwarding strategy; health information system; internet technologies; IoHT; people with disabilities; reinforcement learning; Q-learning

1 Introduction

The Transmission Control Protocol/Internet Protocol (TCP/IP) design emphasizes strong end-to-end connectivity in communications, with IP addresses facilitating communication between devices in the Internet of Healthcare Things (IoHT). However, IoT healthcare devices often have limited energy and power resources [1,2]. With advancements in information and communication technologies, such as wireless sensor networks and fifth-generation wireless communication, connecting and monitoring millions of devices has become increasingly challenging, with content security being a critical concern [3]. An Internet of Things (IoT) network consists of numerous wirelessly connected objects that interact with their physical environment to collect environmental data and provide various services via the Internet. The driving force behind IoT is the use of intelligent devices to enable and automate a wide range of services, allowing the creation of smart applications such as smart hospitals, smart cities, smart homes, smart buildings, and smart campuses (SCs) [4].

The Internet of Healthcare Things (IoHT) is crucial for enhancing the accuracy, reliability, and efficiency of medical devices in the healthcare sector. By connecting medical tools and healthcare services, researchers are advancing the development of digital healthcare systems. All medical technology and software capable of gathering, analyzing, and exchanging data online are part of the IoHT submarket within the Internet of Things. Biomedical sensors can monitor data such as respiration rate, blood pressure, electrocardiograms (ECG), and body temperature, which can then be managed through edge devices like smartwatches, computers, smartphones, or specialized embedded devices [5,6]. Additionally, the IoHT can track environmental factors, such as room conditions, laboratory transition times, treatment durations, and patient-to-staff ratios.

The current IP architecture is unsuitable for an IoT-based Internet of Healthcare Things (IoHT) for several reasons [7], including inconsistencies in privacy measures, high power, and memory consumption on small IoT devices due to the heavy use of TCP/IP, excessive bandwidth usage, inadequate addressing for IoT devices, content security issues, and a lack of support for network fragmentation [8]. Over the past two decades, significant advancements in networking have been made to overcome the limitations of the existing IP architecture and to address the needs of emerging technologies. In this context, a new architecture called Named Data Networking (NDN) has been proposed.

In NDN-based architectures, communication between devices is conducted through name-based content rather than IP addresses [9]. The advent of NDN allows IoT applications to utilize naming for smart devices, with the NDN architecture serving a crucial role in both IoT sensors and actuators by treating them as named content instead of assigning IP addresses. In fact, managing IoT infrastructure through a TCP/IP architecture, as opposed to a content-centric approach, introduces ambiguity. Given that NDN provides robust content security, it is the ideal choice for IoT environments.

The concept of Named Data Networking (NDN) is largely driven by the shortcomings of the existing Internet architecture [10]. In an NDN network, data delivery is managed by three key components: the Forwarding Information Base (FIB), which handles data forwarding by determining the appropriate routes for Interest packets; the Pending Interest Table (PIT), which tracks ongoing data requests and their states during the data retrieval process; and the Content Store (CS), which stores data chunks within the network to reduce retrieval time by serving data from the cache instead of fetching it from the original source.

In [11,12], a high-level NDN–IoT architecture was developed. The NDN–IoT architecture is comprised of three layers: the things layer, the NDN layer, and the application layer. Fig. 1 illustrates the NDN–IoT architecture. The things layer represents the vast array of devices within the Internet

of Things. The NDN layer, also known as the networking layer, shields users from the complexity and diversity of IoT (Internet of Things) applications. The NDN layer in the NDN–IoT architecture consists of two primary components: the management/control plane and the data plane. The control plane manages the operational functions of Interest packets and Data packets, including security, naming, caching, and strategies that effectively meet IoT requirements.

The forwarding strategy in Named Data Networking (NDN), typically considered part of the strategy layer (as shown in Fig. 1), plays a crucial role in determining how data is routed through the network. When applying NDN to IoT, the forwarding strategy is adapted to the specific characteristics and requirements of IoT environments [13,14]. NDN's Interest-driven approach enables selective and efficient data retrieval, allowing devices to fetch data based on actual interest and reducing unnecessary data transmissions. Additionally, NDN's security model provides content-based security, ensuring the authenticity and integrity of exchanged information in IoT applications. Unlike IP networks, name-based forwarding in NDN enables named data networks and the Internet of Things to communicate directly through packets. The IoT system's other features, such as delay-tolerant communication, fast local recovery, and hop-by-hop congestion control, can also be enhanced through name-based stateful forwarding.

Although the importance of NDN for IoT has been somewhat researched, very few studies have considered creating a communication plan that accounts for an IoT device's energy constraints. While Content Stores (CS) in NDN routers aid in caching frequently requested data, managing this cache and deciding when to retrieve data from the original source can impact energy consumption [14,15]. Inefficient caching strategies may lead to unnecessary data transmissions. Energy consumption is one of the most important factors in the placement of Internet of Things devices and sensors [16]. Optimizing energy consumption in IoT is challenging, as it involves not only minimizing the energy use of individual sensor nodes but also extending the overall network lifetime. The broadcast nature of the wireless medium in NDN-based IoT can aid in distributing Interest packets, allowing multiple neighboring nodes to receive a transmission from one node. Consequently, neighbors become potential recipients of requests or content, increasing the likelihood that a packet will reach producer or forwarding nodes that can provide cached content. However, this redundancy in forwarding candidates creates a broadcast storm issue, posing a challenge to the deployment of NDN-IoT [17,18].

A broadcast storm refers to the excessive broadcasting of packets in a network, especially in scenarios where many nodes simultaneously broadcast their messages. In the context of the Internet of Healthcare Things (IoHT), where devices are often resource-constrained and energy-sensitive, a broadcast storm can significantly degrade network performance. Broadcast storms are a major challenge in IoHT networks, impacting energy consumption, latency, network lifetime, and security. Addressing this issue is essential to ensure that NDN-based IoHT systems remain reliable, efficient, and secure, particularly in healthcare contexts, where the risks are high and the consequences of failure can be severe.

This paper introduces a novel Smart and Energy-aware Forwarding strategy (SEF) specifically designed for Named Data Networking (NDN) in the Internet of Healthcare Things (IoHT). By enhancing Geographic Interest Forwarding (GIF) with a reinforcement learning framework, SEF innovatively leverages both the energy levels and geographical distances between nodes to select the optimal path for Interest packet transmission. The unique application of Q-learning allows devices to dynamically assess and choose the most suitable node for forwarding at each decision point, addressing the critical challenges of broadcast storms and energy inefficiencies in resource-constrained IoHT environments. This strategic integration not only optimizes next-hop selection

but also significantly reduces overall energy consumption, thereby extending network lifetime and improving data delivery reliability. The proposed SEF strategy represents a significant advancement in the ability of IoHT systems to maintain efficient, responsive, and sustainable operations in high-stakes healthcare scenarios.

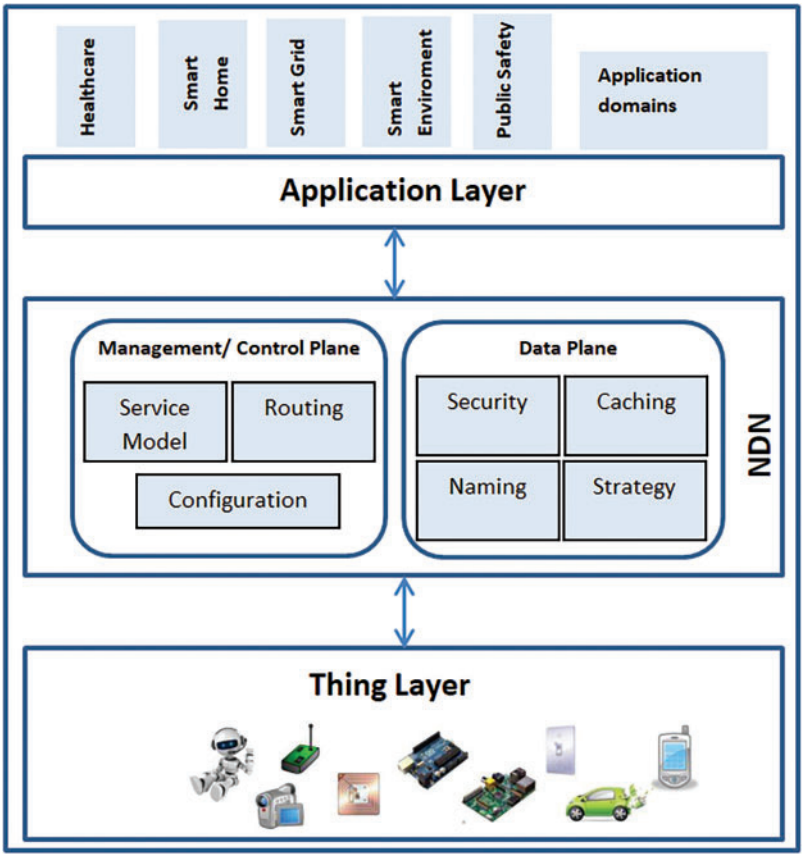

Figure 1: NDN-IOT architectural [19]

We conduct thorough evaluations to validate our strategy and demonstrate through simulations that it is suitable for various large-scale IoHT scenarios. The simulation results indicate that our solution significantly enhances network longevity while reducing energy consumption, improves Packet Delivery Ratio (PDR), sends fewer Interest packets, and reduces retrieval delays.

The remainder of the article is structured as follows: Related work is presented in Section 2. The suggested methodology is described in Section 3. Performance evaluation results in various communication scenarios are reported in Section 4. The article is concluded in Section 5, which also suggests some directions for future research.

2 NDN Based Internet of Healthcare Things (IoHT)

We provide an overview of the NDN-IoHT architecture and its main elements in this section. We describe the data forwarding mechanism that connects the producer and the sink, enabling content retrieval. After that, we explore the relevant literature on developments in forwarding strategies. We conclude this part by presenting the theories related to the forwarding techniques used in this study.

2.1 NDN-IoHT Architecture

For IoT healthcare networks, the NDN-IoHT design utilizes the content-centric networking paradigm from NDN [20–22], as illustrated in Fig. 2. The essential elements are:

Content Store (CS): In an NDN-IoHT node, data packets are stored in the Content Store (CS), a local cache, according to their names or prefixes. The CS returns a data packet to fulfill the interest after examining it for a matching prefix when an interest packet arrives. With this functionality, the on-board cache can respond to repeated requests more quickly. However, due to the limited resources of IoT devices, the CS has a restricted amount of storage [23].

Pending Interest Table (PIT): The PIT monitors interest packets and the interface (InFace) from which they are received. Data packets are returned via the reverse path using this information. When data arrives, the PIT determines which downstream interface(s) to send it to in order to fulfill the initial data request based on its recorded entries.

Forwarding Information Base (FIB): The FIB oversees the forwarding of interests based on name prefixes. It acts as the forwarding table for name-based forwarding in NDN-IoHT and specifies which interfaces (OutFaces) to use for forwarding. The FIB is populated with various forwarding techniques and routing methods [24]. Based on its content name, the FIB lookup determines which interface to route an interest packet to the possible data sources. Two types of packets, interest packets and data packets are exchanged between consumers (doctors) and producers (patients) in NDN-IoHT. These packets are based on hierarchical content names rather than host IP addresses.

Interest Packet: This refers to the request packet that carries the client-to-data provider query. It includes the necessary identifier for the requested data and contains search parameters specified by the client, such as a preferred order, publisher name, or keywords.

Data Packet: This refers to the information packet. It contains a data identifier along with information to verify its validity, including the source's digital signature.

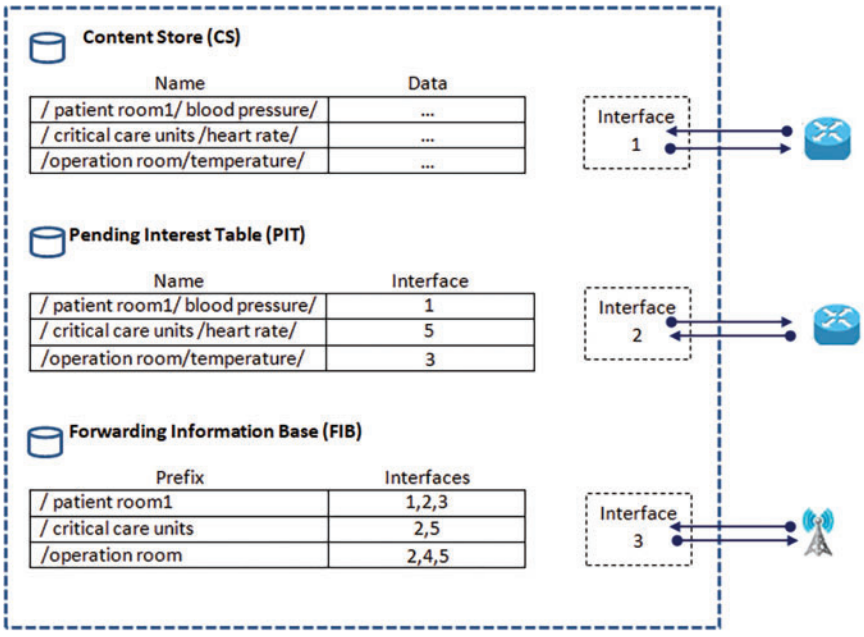

Figure 2: NDN Network architecture

2.2 Data Forwarding Process in NDN-IoHT

Data forwarding is a crucial part of the communication process in NDN-IoHT. In NDN-IoHT, the main goal of data forwarding is to ensure the effective and reliable transport of data packets from the source to the destination. The following is a description of the NDN-IoHT data forwarding process:

1. **Interest Generation:** A doctor (or nurse, or other practitioner) who desires to receive a particular piece of data creates an interest packet that contains the name of the requested data. The interest packet is then sent out over the network.
2. **Interest Propagation:** The interest packet travels from the sink to a node or from node to node until it reaches the producer node, which contains the desired data content.
3. **Data Packet Generation:** The name and substance of the data are included in a data packet created by the node (producer).
4. **Data Propagation:** Next, the data packet is propagated along a reverse path from node to node until it reaches the sink or consumer.
5. **Data Delivery:** The data packet is received and processed by the sink, which may be a doctor, nurse, or other practitioner. The data packet is then stored in the cache section (CS) of the destination node.

The standard NDN-IoHT architecture and data forwarding process are shown in Fig. 3, which highlights the major components of data transmission and the data forwarding process.

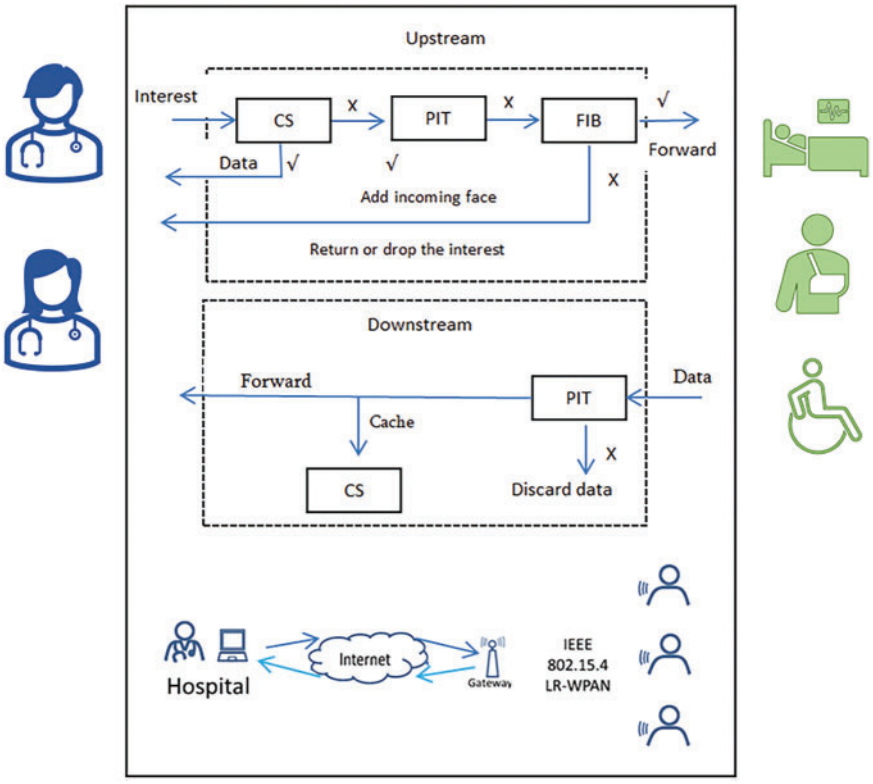

Figure 3: Data forwarding in typical NDN-IoHT architecture

2.3 Literature Review of NDN-Based IoT

NDN presents effective solutions for data communication in IoT and WSNs (Wireless Sensor Networks), attracting increasing research attention. The receiver-based service model of NDN aligns naturally with the data-centric nature of IoT and WSNs, making it suitable for many applications built on sensing modules. Recently, there has been a growing interest in applying NDN to WSNs and IoT. However, few studies have concentrated on forwarding and energy-efficient strategies in multihop network environments. This section highlights the key contributions to forwarding strategies in NDN-based wireless sensor and IoT networks. The named data network-based internet of things schemes that we have presented are analyzed and qualitatively compared in Table 1 based on specific criteria.

The provider-aware forwarding (PAF) scheme for *ad hoc* networks, which was suggested in [25]. In the PAF scheme, each node maintains a Distance Table (DT) that records the number of hops. The initial Interest packet is broadcast throughout the network via blind flooding. Upon receiving the request, a node responds with a Data packet that includes two additional fields. Nodes with a corresponding PIT entry for that Data packet store the packet ID (Identity document), name prefix, and the distance to the content producer in the DT table. As the Data packet is forwarded, each node increments the distance field by one until the packet reaches its destination. However, this strategy reduces the number of nodes involved in the forwarding process. However, it is inefficient in terms of energy consumption because, as the number of consumers increases, blind flooding becomes more frequent, leading to a shorter network lifespan.

The energy-efficient dual mode interest forwarding (DMIF) technique for NDN-based WSNs was suggested in [26]. DMIF uses several tactics to boost the recommended solution's efficacy and energy efficiency. Consists of two collaborative forwarding modes that incorporate various energy-efficient mechanisms, including flooding scope control, flexible mode shifting, packet suppression, broadcast storm prevention, and energy weighting factors, all designed to balance and conserve energy consumption. However, its limited size makes it unsuitable for big networks.

Geographic interest forwarding (GIF) was proposed in [27] for NDN based Internet of Things. The GIF strategy enhances the NDN model to meet the needs of IoT networks by incorporating push-based traffic support and a compact naming scheme for efficient data exchange management. It employs a greedy forwarding strategy to route Interest packets towards data producers. When a sink node requests data from a producer, the GIF scheme seeks the nearest neighbor to the destination and forwards the message accordingly. However, Extensive network discovery processes; it is not appropriate for small networks.

The named data networking disaster management (NDN-DM) system was proposed in [28], which adapts the NDN communication model to allow a producer to forward an alert message (AM) to neighboring consumers without first receiving an interest packet. To address the lack of push traffic support in NDN, a new customized interest packet, known as AM, is introduced. In a disaster scenario, each sensor or producer node that detects the event broadcasts an AM to its one-hop neighboring nodes. If the receiving node already has the AM in its Content Store (CS), it discards the packet; otherwise, it stores a copy of the data in the CS and further broadcasts it throughout the network. This proposed scheme was validated in a specific fire scenario, where mobile nodes on a university campus collaborate to manage the fire situation. However, it uses a broadcast scheme with caching capability rather than an NDN communication approach.

Table 1: A synopsis and comparative analysis of previous research on NDN-based Internet of Things

Ref.	Name (Year)	Techniques for optimizing energy consumption	Limitations	L2 protocol	Collision	Performance					
						Energy consumption	Network lifetime	Average retrieval delay	PDR	Total no. of interests	Average hop count
[25]	PAF 2015	Using the blind flooding strategy and distance metric to choose the optimal forwarder.	More packet duplication; broadcast storm issue occur.	802.11	High			✓		✓	
[26]	DMIF 2016	Using directive mode and flooding mode based on an energy weight factor enables controlled flooding while reducing network overhead.	Limited size; making it unsuitable for big networks.	802.15.4	Low	✓	✓				✓
[27]	GIF 2019	Using the geographical location to choosing next hop.	Extensive network discovery processes; it is not appropriate for small networks.	802.15.4	Low	✓	✓	✓			✓

(Continued)

Table 1 (continued)

Ref.	Name (Year)	Techniques for optimizing energy consumption	Limitations	L2 protocol	Collision	Performance					
						Energy consumption	Network lifetime	Average retrieval delay	PDR	Total no. of interests	Average hop count
[28]	NDN-DM 2020	Using the PUSH scheme instead of the PULL scheme helps prevent delays in packet transmission.	Communication overhead and PDR have been not considered.	802.11a	High	✓		✓			
[19]	EPF 2020	Using the SDN and priority message to minimize the broadcast of interest packet.	More message; more overhead.	802.15.4	High	✓	✓	✓		✓	
[29]	EMFM 2021	Using multipath to choose the path with the largest battery capacity and lowest PIT level.	Lacks Latency, security and PDR have been not considered.	802.11g	low	✓					
[30]	E-GIF 2022	Using the geographical location and energy level to selecting one forwarder at a time.	Failure to find the best path.	802.15.4	low	✓	✓	✓	✓		

(Continued)

Table 1 (continued)

Ref.	Name (Year)	Techniques for optimizing energy consumption	Limitations	L2 protocol	Collision	Performance					
						Energy consumption	Network lifetime	Average retrieval delay	PDR	Total no. of interests	Average hop count
[31]	IMDS 2021	Using the Fog computing technology to crucial for minimize the latency in e-healthcare systems.	High collision and energy consumption have been not considered.	No mention	High			✓	✓		
[32]	NDN-SDN	Using SDN to enhance user satisfaction and network performance across various metrics.	Security and energy consumption have been not considered.	802.15.4	low			✓			
[33]	INF-NDN	Using the natural language processing (NLP) to reduce the length of content names.	Security have been not considered.		High	✓		✓	✓		✓
SEF		Using Q-learning to select the best node between neighbors.		802.15.4	low	✓	✓	✓	✓	✓	✓

Energy efficient Priority Forwarding (EPF) was proposed in [19] to enhance high priority packet transmission while consuming less energy. In an NDN-IoT scenario, this approach utilizes the capabilities of the SDN (Software Defined Network) controller. For low priority packet transmission, a minimum energy barrier of 16% was established. By comparing the packet's priority with the name prefix, the defer window is used to forward the packet. Furthermore, successful mitigation of broadcast storms is achieved. The suggested method outperforms both floods and GIF in terms of Total Number of Interests, Content Retrieval Delay, and Average Energy Consumption. Nevertheless, a lot of messages used in this research lead to more overhead and high collision occurs, which will increase the energy consumption.

An energy-aware multipath forwarding mechanism (EMFM) is proposed by the researcher in [29] for advancing arriving Interest packets in order to reduce node energy consumption and increase network lifetime. EMFM considers nodes along with their corresponding battery and PIT size to predict the next forwarding hops in the overall packet transmission process. A simulation was conducted to develop and evaluate the EMFM and compare it with the on-demand energy-based forwarding strategy (OEFS) using the ndnSIM tool. Through an evaluation of EMFM's network performance in terms of data redundancy, content download time, and network energy consumption, the investigation's findings unequivocally demonstrated that EMFM can extend the network lifetimes of NDN wireless nodes. Nevertheless, the only comparison is with OEFS.

The researcher provides the enhanced geographic interest forwarding (E-GIF) in [30] an NDN over IEEE 802.15.4 communication system that meets the requirements for monitoring and controlling Internet of Things applications that need to have low power and low data rates. A sleep mode scheduling algorithm schedules the sleep/wake-up mode based on the node's function in the forwarding and path repair operations, while a dependable energy-aware forwarding strategy chooses the next hop forwarder based on its remaining energy level. The evaluation matrices used in this algorithm are the retrieval delay, delivery ratio, energy consumption, and scalability. Nevertheless, in this protocol, a lot of packets are dropped because the path mechanism fails to find the best path.

In [31], the researcher proposes a novel Intelligent Multimedia Data Segregation (IMDS) approach in the fog computing environment that separates multimedia data and the model used to determine the total latency (transmission, processing, and network) using machine learning (k-fold random forest). The data is first gathered by the model. Data collection is followed by pre-processing. Next, the data is separated into k-folds. In this case, k-fold cross-validation is used. The initial sample is divided into manageable k-chunks for the purpose of testing the model during the cross-validation procedure. The original data was divided into k-chunks using a random technique, but each chunk's size was always the same. In k-fold, the model is tested using the last chunk, and $k-1$ chunks are utilized for training.

In [32], the author proposes a source-driven forwarding technique in which the content sources reply to Interest queries in a decentralized fashion. All of the sources get the content requests, but the sources react probabilistically to reduce latency and costs associated with content retrieval. The approach allows the closest sources to establish a high likelihood of responding with the appropriate content. Conversely, in response, the remote sources offer to reduce transmission overhead. Additionally, as a crucial component of the source-driven scheme, a caching technique is put forth that caches various contents while allowing for the admission of fresh content, taking into account the time elapsed between subsequent copies and content availability.

One important research need is the intelligent examination of content names to identify a forwarding clue. It is essential to comprehend the interest name and obtain a forwarding clue in order

to accomplish intelligent communication. In order to close this gap, the researchers in [33] suggests the intelligent naming system INF-NDN (Intelligent Naming and Forwarding-Name Data Networking) IoT, which also has a correlation with a forwarding mechanism. By using natural language processing (NLP) techniques and choosing super nodes and ordinary nodes in the network, the proposed INF-NDN IoT enhances the NDN naming schemas. INF-NDN IoT marks content names and super nodes, which carry out the semantic forwarding, with semantic tags (forwarding clues). According to experimental findings, INF-NDN IoT performed better than previous research and produced superior outcomes in terms of hop count, retrieval time, name length, interest satisfaction rate, and name memory utilization. However, this research compares its performance with the scheme for data content objects in information-centric networks (SICN).

Table 1 presents a qualitative theoretical comparison and analysis of the NDN-based IoT schemes that we have offered based on certain standards. This table aids in the identification of a number of outstanding problems that must be resolved in order to effectively distribute data in NDN-based IoT. Our analysis reveals that the majority of forwarding solutions now in use, such as PAF and IMDS, do not optimize energy consumption. Table 1 further highlights the fact that, in contrast to the IEEE 802.11 protocol, only four protocols DMIF, GIF, EPF, and E-GIF have been implemented over the IEEE 802.15.4. The medium access control (MAC) protocol. This is a sensible and appropriate decision for our IoT environment. Additionally, a number of solutions including NDN-DM, PAF, and EPF—have a high collision rate as a result of their blind forwarding mechanism. Transmission latency, network availability, and energy usage are all negatively impacted by this behavior.

Generally, IoT constraints like low data rates and energy resources are not addressed by the current methods for applying the NDN communication model to IoT networks, which highlights the need to develop new effective and dependable IoT communications mechanisms. Therefore, the goal of this work is to build a communication solution that is both energy-efficient and lightweight, utilizing the IEEE 802.15.4 as well as the NDN communication paradigm. In addition to minimizing collision risk, the suggested approach should facilitate multihop communication.

2.4 Theories Pertaining Forwarding Strategy

This section focuses on the Theories pertaining to forwarding strategy for NDN-based IoHT, so geographic interest forwarding and reinforcement learning are discussed, respectively.

2.4.1 Geographic Interest Forwarding

NDN provides workable IoT and WSN solutions. An increasing amount of research is being done on NDN-based networks [10]. In actuality, the majority of use cases that can be built on top of sensing components are compatible with the Named Data network receiver based service approach, which seamlessly integrates into data-centric wireless sensor network and Internet of Things. Interest in using the NDN with WSNs and the Internet of Things has increased [34]. Only a small number of works, nevertheless, concentrated on routing and forwarding solutions in multi-hop network environments. Geographic Interest Forwarding (GIF) [34] is one of the earliest works that investigates the possible application of the named data network paradigm to wireless sensor network and the Internet of Things. It is modeled after the GPSR (Greedy Perimeter Stateless Routing) protocol. In order to accommodate the various demands and limitations of the Internet of Things, GIF expands the NDN model by incorporating push-based traffic support, a compact naming scheme for data exchange, and a producer discovery mechanism.

The GIF scheme's researcher suggests an Interest forwarding algorithm with producer awareness that is built around three stages: data exchange, producer awareness, and neighbor discovery. The GIF scheme routes messages to content creators using an energy-aware, greedy forwarding strategy. By providing each node with the necessary data, the first two phases of the network's setup the producers' discovery and the neighbors' discovery are used to set everything up. In the first stage, known as neighbor discovery, every pair of nodes will communicate with one another by sending a Hello packet that includes the identity, geographical location, and residual energy of each node. The producer discovery phase is the second stage, in which each producer sends a "push-interest" [35] containing the producer's ID, location, and data name to the sink node. Following the setup stage, the GIF scheme looks for the neighbor nearest the destination with the highest remaining energy and sends the message to that node whenever a sink needs data from a producer.

2.4.2 Reinforcement Learning

Reinforcement learning (RL) is a robust algorithm that identifies the optimal policy through direct interaction with the environment, without needing a predefined model. It uses an agent that, by interacting with its surroundings, learns the value function associated with a given policy and leverages this to predict an optimal solution. Based on the learned value function, the agent continuously adapts and refines its approach to achieve the best policy devices to adapt to network dynamics, such as mobility and energy levels, thereby enhancing routing decisions [36].

The most widely used model-free RL method is Q-learning, as shown in Fig. 4. By using previous experience, RL allows machines or agents to learn how to act optimally in specific scenarios. An RL-based model collects data to complete a task and learns through ongoing interaction with the environment. Q-learning, an off-policy RL algorithm does not require a model and helps the agent discover the most advantageous course of action. This learning algorithm stores state-action pairs in a Q-table, where each state-action pair entry produces a Q-value. The objective of Q-learning is to maximize this Q-value, with the agent updating its action strategy based on environmental feedback. The agent evaluates the effectiveness of different actions in the current state to determine better choices for subsequent iterations [37]. Q-learning consists of the following components [38,39]:

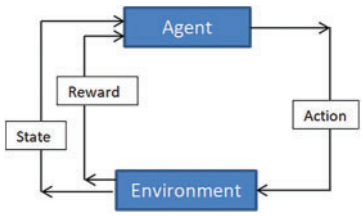

Figure 4: The components of a Q-learning [39]

State: This current situation of a node within the network. In SEF, the state consists of two key factors: geographical distance (D) and energy levels. Geographical distance (D) indicates the distance between the current node and its neighbors, while energy levels encompass the residual energy (RE_j) and initial energy (IE_j). of neighboring nodes. These factors together define the state of the node, providing critical context for making forwarding decisions.

Action: An action is a decision made by the node based on its current state, such as selecting the next-hop neighbor for packet forwarding in SEF. This choice considers both the geographical distance to the destination and the energy levels of neighboring nodes.

Q-value: This represents the expected utility or quality of taking a specific action in a given state, indicating how favorable it is to choose a particular action (e.g., selecting a next-hop neighbor) based on the current state.

The initial Q-value Q_0 is defined in (1). Where ResEn (n) is the current residual energy of the neighbor n, Dist (prod, n) is the distance between the producer and that neighbor, and w_1 and w_2 are respective weights. MaxDist is the maximum distance to the producer. The first portion is intended to prevent choosing a low-powered neighbor, while the second half is designed to save energy by reducing communication overhead.

$$Q_0(s,a) = w_1 * \left(\frac{D_{(s,j)}}{D_{(s,p)}}\right) + w_1 * \left(\frac{RE_j}{IE_j}\right) \tag{1}$$

Update Q-value: The Q-value is updated based on the reward received and the future expected rewards. The update process follows the standard Q-learning update rule in Eq. (2). This update mechanism ensures that the Q-value gradually reflects the optimal action for each state, leading to better decision-making over time. The learning of the Q function is done by the iteration of the Q-value.

$$Q_{t+1}(s,a) = (1-\alpha)\, Q_t(s,a) + \left[r_t + \gamma.\max Q_{t+1}(s,a)\right] \tag{2}$$

where s and a are the states and actions, t the current cycle, α the learning rate, r_t the current reward value, γ the discount factor, and max Q_{t+1} (s, a) the estimate of the optimal future of the Q-value. Each iteration process updates a new Q-value.

Reward: The reward is the immediate feedback received after taking an action, guiding the learning process of the algorithm. In SEF, the reward is calculated based on the Eq. (3). The reward function encourages the selection of neighbors that are closer to the destination and have higher remaining energy, thus optimizing the network's overall performance by balancing energy consumption and reducing unnecessary broadcasts.

The reward r_t is designed to reflect the learning about the residual energy and the geographical distance.

$$r_t = \left\{ \begin{array}{c} \left[(1-\alpha) * \frac{D_{(s,j)}}{D_{(s,p)}}\right] + \left[\alpha * \left(\frac{RE_j}{IE_j}\right)\right] \\ R_c \text{ if neighor is destination} \\ -R_v \text{ if no neighbor avilable} \\ -R_E \text{ if neighbor has energy low} \end{array} \right\} \tag{3}$$

The energy level of the neighbor node that could forward the packet and its distance to the sink are combined in the first item in (2). Selecting the neighbor node that has the max remaining energy and is closest to the sink results in the assignment of more reward, Where S denotes the sink that sent out the packet in the first place, p stands for the producer, j is one of node i's neighbor and denote the possible next hop which will receive the Interest packet from i's node, $D_{(S,j)}$ is the length between sink and the possible forwarder j, $D_{(S,p)}$ is the length between sink S and producer, RE_j is the neighbor node's remaining energy, and IE_j is the possible forwarder j's initial energy.

A high value of α indicates that the neighbor with the highest energy level has a higher chance of being chosen as the next-hop, while a high value of (1− α) indicates that the neighbor who is closest has a higher chance of being chosen. When a sender node is able to attach the producer in a single hop, the reward is the second item in Eq. (2). We take the producer's energy to be infinite. A constant RC is awarded to a node sender who is able to get in direct contact with the producer. In the third item in

the reward equation, the greedy forwarding strategy fails if a node is unable to locate a neighbor who is closer to the producer. Some nodes may not have enough energy, or node deployment may be the source of this issue. We suggest a Q-learning method, a node drops interest packets and notifies the sending node of a forwarding failure by sending a negative reward $-R_v$. The reward function's fourth item acts as a low energy alert by sending a negative ($-R_E$) reward to nodes.

3 Methodology

This section outlines the system model of our strategy and the design of the proposed NDN-based data dissemination scheme, called the Smart and Energy-Aware Forwarding Strategy (SEF). The primary objectives of this design are to ensure efficient data communication in NDN-based IoHT, reduce energy consumption, avoid packet losses, and extend the lifespan of the IoHT network. We propose a smart and energy-aware forwarding strategy (SEF) based on reinforcement learning for NDN-based IoHT. The SEF strategy depends on the geographical distance and energy levels of neighboring nodes, enabling devices to learn how to make better forwarding decisions and optimize next-hop selection.

Cloud computing typically involves transferring data to centralized servers that are geographically distant from IoT devices, introducing latency due to transmission time over wide-area networks (WANs). In NDN-based IoT systems, which often require real-time operation (such as health monitoring or emergency response), this latency can be a critical issue. Using local caching in the CS (Content Store) of NDN nodes significantly reduces delay by storing data closer to where it is consumed, eliminating the need for round-trip communication with distant cloud servers.

Moreover, cloud computing raises concerns about data privacy and security, especially in sensitive IoT applications like healthcare. By storing data in the cloud, the system may expose sensitive information to third-party providers, which may not be acceptable in healthcare or smart home applications. In NDN, data is cached and served locally within the network, reducing the amount of sensitive data sent to external servers. Additionally, NDN inherently uses data-centric security, where data packets are signed, and offers enhanced privacy control at the network layer. Leveraging the CS in NDN nodes allows IoT systems to serve data directly from local caches, reducing overall network load and avoiding cloud-related bottlenecks.

Edge computing is often favored over cloud computing in NDN-based IoT systems because it brings computation and storage closer to the devices. NDN's caching mechanism aligns well with edge computing principles, allowing nodes to serve data directly from their content stores without frequent cloud interactions. This improves performance, reduces latency, and lowers energy consumption. Therefore, cloud computing is not used in this research.

3.1 System Model

In this section, we consider two scenarios in IoT healthcare systems including monitoring systems in smart hospitals and monitoring systems for people with disabilities, as follows:

1. Monitoring System in Smart Hospitals

In a smart hospital environment, various low-power sensor nodes are deployed to monitor patients' vital signs, such as heart rate, blood pressure, and oxygen levels. These sensor nodes are strategically placed in patient rooms, hallways, and critical care units. Each sensor node acts as a content producer, continuously generating data related to patient health. Fig. 5 shows the system model of the Monitoring System in Smart Hospitals.

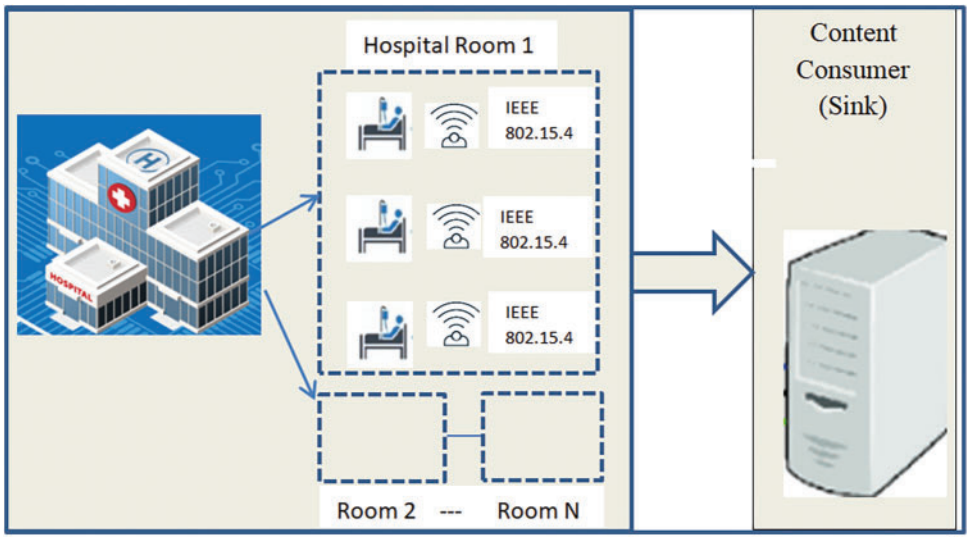

Figure 5: System model of monitoring system in smart hospitals

Sensor Nodes (Content Producers): Positioned in patient rooms, ICUs (Intensive Care Unit), and operating theaters, these sensors continuously generate data such as heart rate, blood pressure, temperature, and equipment status.

Sink Node (Content Consumer): Located in the hospital's control center, it collects data from sensor nodes and issues periodic Interest packets to query specific data from various content producers.

Multihop Communication: Sensor nodes forward Interest and Data packets through intermediate nodes, utilizing SEF based on Q-values to select optimal paths and conserve energy.

IEEE 802.15.4 Standard: Provides low-power, reliable communication between sensor nodes.

SEF Strategy: The SEF algorithm optimizes the forwarding of packets by considering the geographical distance between sensor nodes and the energy levels of neighboring nodes, ensuring efficient data transmission and reducing energy consumption.

2. Monitoring System for People with Disabilities

This scenario focuses on a Healthcare Monitoring System for Individuals with Disabilities, the Elderly, and managing pandemics. The system comprises static sensor nodes strategically placed in different rooms of the house to monitor various parameters such as movement, fall detection, heart rate, and other vital signs, in Fig. 6 shows the system model of Monitoring System for People with Disabilities.

Quarantine Centers; Infected individuals in quarantine can be monitored remotely, reducing the need for physical contact and the risk of virus transmission.

Sensor Nodes (Content Producers): Positioned in different rooms of the house, these sensors continuously generate data such as heart rate, blood pressure, temperature, and equipment status.

Sink Node (Content Consumer): Located in the hospital's control center, it collects data from sensor nodes and issues periodic Interest packets to query specific data from various content producers.

Multihop Communication: Sensor nodes forward Interest and Data packets through intermediate nodes, utilizing SEF based on Q-values to select optimal paths and conserve energy.

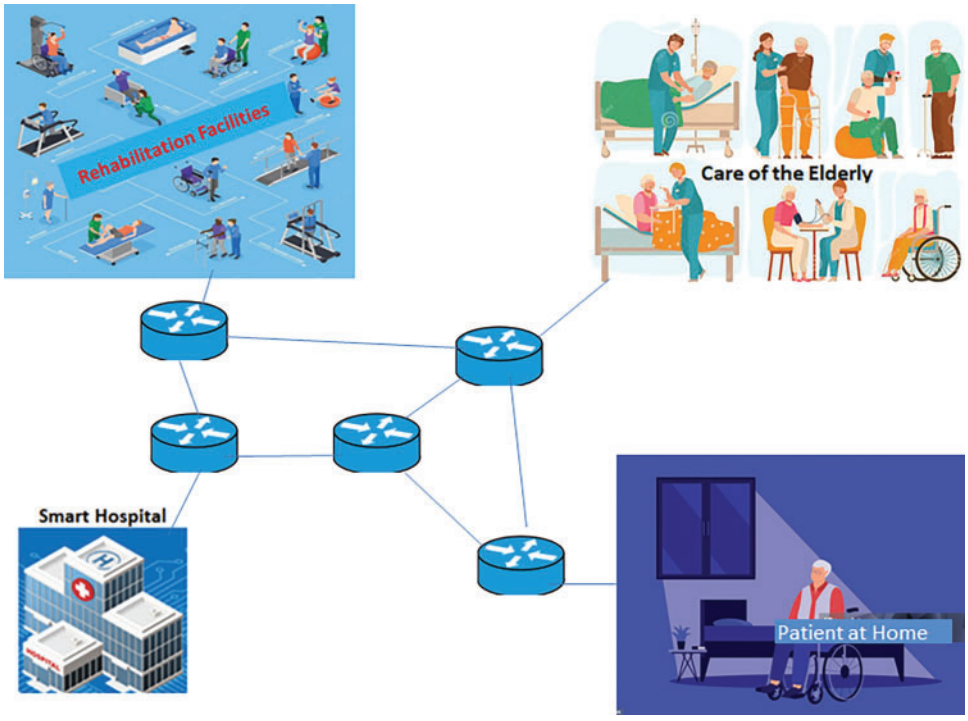

Figure 6: System model of monitoring system for people with disabilities

IEEE 802.15.4 Standard: Provides low-power, reliable communication between sensor nodes.

SEF Strategy: The SEF algorithm optimizes the forwarding of packets by considering the geographical distance between sensor nodes and the energy levels of neighboring nodes, ensuring efficient data transmission and reducing energy consumption.

The primary aim of our strategy is to ensure continuous and energy-efficient monitoring of patients, minimizing packet loss and delays, while maximizing network lifetime and ensuring timely data delivery to healthcare professionals. Lastly, we suppose which sensors are stationary, aware of their own positions, and aware of the locations of the sink node.

3.2 Smart and Energy-Aware Forwarding Strategy Design

In accordance with the NDN communication model, the sink must explicitly request content by sending an Interest packet that includes the prefix of the requested data. We developed a smart and energy-aware forwarding technique (SEF) based on reinforcement learning for NDN-based IoHT to efficiently route Interest packets to content producers. To minimize traffic overhead, prevent collisions, and maximize energy efficiency, only one node forwards the Interest packet at each hop. Additionally, this selection is based on the residual energy level and position of neighboring nodes to extend network lifetime and reduce packet delivery delay. The proposed forwarding module consists of three stages: the forward selection stage, the data delivery stage, and the initial network setup stage. The following sections provide more details on the operation of each stage.

3.2.1 Initial Network Setup Stage

Before broadcasting the Interest packet, each pair of nodes exchanges their ID, residual energy, and position by sending a short 'Hello packet' message to all neighboring nodes, as shown in Fig. 7a. It is important to note that this process is performed only once to reduce energy consumption and network congestion. Each node saves the information gathered during the 'Initial Phase' stage in a new structure called the 'Neighbors Table'.

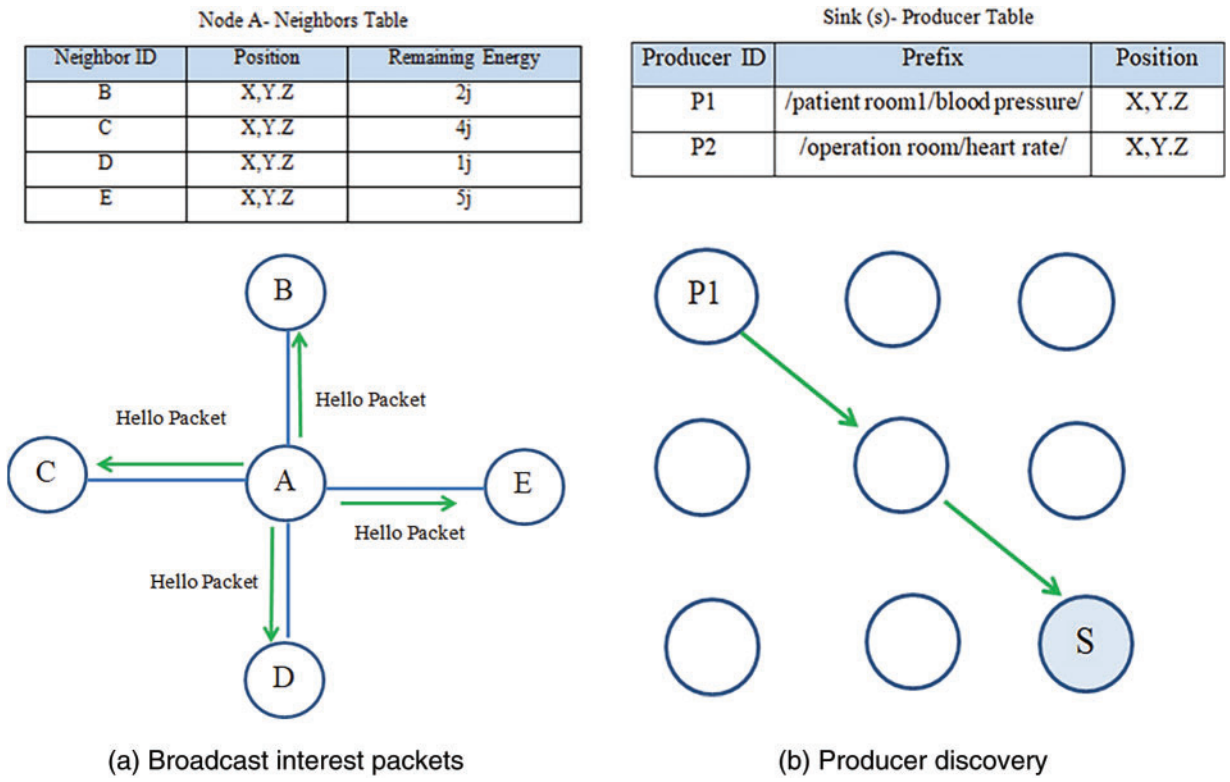

Figure 7: Initial network setup stage

Instead of periodically exchanging these details among neighbors, the proposed approach piggybacks energy information onto each Interest packet received, forwarded, or sent by sensors, allowing nodes to update their 'Neighbors Table' while minimizing energy consumption. Importantly, each node stores data only about its direct neighbors, not the entire network. Specifically, only small amounts of data—such as each neighbor's ID, location, and energy level—are saved. This keeps the overall size of the Neighbors Table small, ensuring it remains suitable for the memory constraints of targeted Internet of Things devices.

Next comes the 'Patient Data Discovery' phase, in which each sensor used to collect data from patients sends its patient_ID, patient's position, and the type of data it produces to the sink node. The data sent by the producers will be stored in a new table called the 'Producers Table', as shown in Fig. 7b. It is important to note that this new data structure requires memory only in the sink node, meaning that intermediate Internet of Things (IoT) devices are unaffected.

Additionally, we were able to reduce the memory requirements for implementing the NDN structure, as the Neighbors and Producers tables replaced the NDN forwarding information base (FIB). By using these tables, each IoT device can operate without implementing a FIB table.

3.2.2 Data Delivery Stage

During this stage, whenever the sink needs to retrieve data from a patient, it broadcasts an Interest packet containing the prefix of the requested patient data. To prevent all neighboring nodes from transmitting the same Interest multiple times, the Interest sender specifies the ID of the neighbor designated to forward the Interest. A new field, named "Next-Hop-ID," has been added to the Interest header to carry this information (Fig. 8 illustrates the Interest header structure).

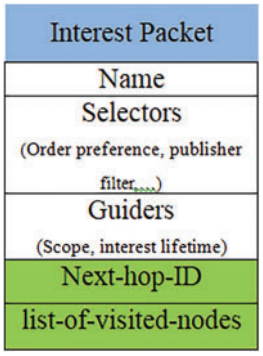

Figure 8: Interest packet

Upon receiving an Interest packet, sensor nodes can confirm whether they were selected as the forwarder by checking the "Next-Hop-ID" field. A node will discard the Interest packet if it is not the designated forwarder. Additionally, by using this field, we can prevent multiple neighbors from transmitting the same Interest, thus avoiding collisions and retransmissions that would otherwise negatively impact bandwidth, energy consumption, and latency.

We limited the size of this field to four bytes to reduce the overhead caused by adding a new field to the Interest message. The IEEE 802.15.4 standard allows for a maximum frame size of 127 bytes. Therefore, even after including the "Next-Hop-ID" field in the Interest message, the total size remains well below the standard limit. Additionally, using this field helps prevent multiple neighbors from transmitting the same Interest twice, thereby avoiding collisions and retransmissions, which have a far greater negative impact on bandwidth, energy consumption, and latency than a four-byte increase in the Interest message size.

3.2.3 The Forwarder Selection Stage

Before issuing an Interest packet, the sender node selects a potential next-hop forwarder from its neighboring nodes. This decision is guided by the Q-learning algorithm, which considers the geographic distance and remaining energy of each neighbor. The primary objective is to prioritize the neighbor that is closest to the destination and has the maximum remaining energy.

Each IoHT device continuously monitors its own residual energy level, and this information, along with the node's ID, is included in the transmitted packets. This ensures that receiving nodes have up-to-date information about the sender's energy status. We integrated a Q-learning algorithm based on Reinforcement Learning (RL) into the forwarding decision-making process. RL operates

on the principles of trial-and-error learning and delayed rewards. An IoHT node receives a reward after selecting an action, and through repeated episodes, it gradually learns more about the targeted parameters, adjusting its strategy based on accumulated rewards. The Q-learning algorithm uses an evaluation function to calculate these cumulative rewards.

We developed a Q-function that evaluates the Q-value based on two factors: residual energy and geographical distance. The forwarding decision is made using this Q-function, with the goal of selecting the next hop that has the maximum Q-value, thereby favoring the neighbor closest to the destination with the highest residual energy. Specifically, each node initiating or forwarding an Interest packet calculates a Q-value based on the residual energy and geographic position of its neighboring nodes, following Algorithm 1.

Algorithm 1: //Pseudocode for next-hop forwarding decision using Q-learning

// Initialize Q-table (Q [s,a] represents the Q-value for state s and action a)
Initialize Q-table with random values or zero
// Parameters
α = learning rate
γ = discount factor
w1 = weight for energy factor
w2 = weight for distance factor
R_c = positive reward for reaching destination
R_v = negative reward for no neighbor available
R_E = negative reward for low energy neighbor
// Function to select next-hop neighbor based on Q-learning
function select_next_hop(current_node, neighbors, producer, sink):
best_q_value $= -\infty$ // Initialize with a very low value
next_hop = null // Placeholder for best neighbor
// Get the current state (geographical distance and energy levels)
for each neighbor in neighbors:
// Compute the geographical distance from the sink to neighbor j
D_sj = calculate_distance(sink, neighbor)
// Compute the geographical distance from the sink to the producer
D_sp = calculate_distance(sink, producer)
// Get the neighbor's remaining energy RE_j and initial energy IE_j
RE_j = neighbor.remaining_energy
IE_j = neighbor.initial_energy
// If the neighbor has low energy, continue to next neighbor
if RE_j is too low:
continue
// Compute the current reward value for the neighbor

$$r_t = \left[(1-\alpha) * \frac{D_{(s,j)}}{D_{(s,p)}}\right] + \left[\alpha * \left(\frac{RE_j}{IE_j}\right)\right]$$

// If the neighbor is the destination, add a constant reward R_c
if neighbor == producer:
$r_t = R_c$
// Calculate the Q-value update using the Q-learning update rule

(Continued)

Algorithm 1 (continued)

```
current_q_value = Q[current_node][neighbor]
max_future_q_value = max(Q[neighbor][next_neighbor] for next_neighbor in neighbor.neighbors)
// Update Q-value
new_q_value = current_q_value + α * (r_t + γ * max_future_q_value − current_q_value)
Q[current_node][neighbor] = new_q_value
// Select neighbor with the highest Q-value, if not already visited
if new_q_value > best_q_value and neighbor not in list_of_visited_nodes:
best_q_value = new_q_value
next_hop = neighbor
// If no valid neighbor found, assign a negative reward R_v
if next_hop == null:
assign_reward(current_node, R_v)
// Return the selected next hop
return next_hop
// Function to handle Interest packet forwarding
function forward_interest_packet(current_node, producer, sink):
while current_node != producer:
// Get the list of neighboring nodes
neighbors = get_neighbors(current_node)
// Select the next hop based on Q-learning decision
next_hop = select_next_hop(current_node, neighbors, producer, sink)
if next_hop is null:
break // Stop if no valid next hop found
// Forward Interest packet to the next hop
send_packet_to(next_hop)
// Add current node to the list of visited nodes to prevent loops
list_of_visited_nodes.append(current_node)
// Update current node to the next hop
current_node = next_hop
// If producer is reached, return success
if current_node == producer:
return "Success"
```

To prevent looping during the search for the next hop, we added a new field in the Interest packet called 'list-of-visited-nodes'. This helps reduce packet drops and ensures reliable access to the producer. Before selecting the node with the highest Q-value as the next hop forwarder, the node must first check the list of visited nodes. If the node has already been visited, it should be ignored, and the next highest Q-value node among its neighbors should be chosen instead.

We can explain the problem with the following scenario illustrated in Fig. 9. Suppose we have a sink (S), a producer (P), and intermediate nodes A, B, C, and D between S and P. In this situation, the sink sends the Interest to A and B. Assume node B selects the next hop (which has the best Q-value), and node A sends the Interest packet to its neighbors (A, C, and D). If node A has the best Q-value compared to nodes C and D, node A will be chosen as the next hop. After that, node A will send the Interest packet to all its neighbors (B, C, and D). Here, if node B has a maximum Q-value, a loop

problem will occur. The Interest will keep being forwarded from A to B without reaching the producer. Therefore, node A must choose the second-best Q-value among its neighbors.

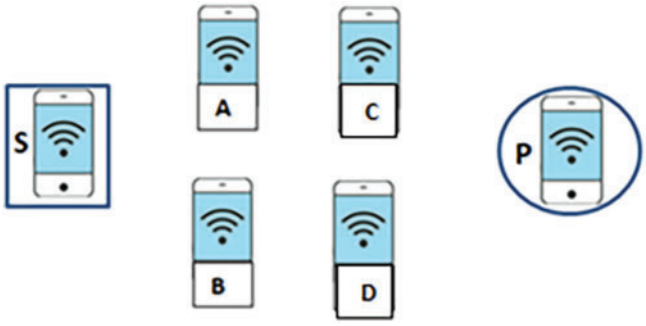

Figure 9: Loop problem

Hop by hop, each intermediate node performs the same steps until reaching the data producer, which then uses the reverse path to return the requested data. Upon receiving the data packet, the first intermediate node neighboring the producer calculates its reward value r_t using Eq. (3). This new value is inserted into the data packet before it is transmitted to the next relay device. The next device extracts this information to update the Q-value of its neighbor. It also calculates its reward value and inserts it into the data packet before transmission. This technique guarantees the continuity of the Q-learning process, as IoT devices update the required information about their neighbors with each delivered data packet. The detailed operation of the SEF strategy is depicted in the flowchart shown in Fig. 10.

4 Performance Evaluation

We evaluate a case study involving a large-scale sensor network designed for an NDN-based IoHT system. Our strategy includes seven scenarios with varying numbers of nodes: 9, 25, 121, 225, 625, 1089, and 4225. For instance, we deploy 9 nodes in a home for individuals with disabilities, 121 nodes in a building for elderly care, and 625 nodes in a clinic. Additionally, we utilize 625 nodes in quarantine centers to remotely monitor infected individuals, reducing the need for physical contact and the risk of virus transmission. In a large rehabilitation center for patients recovering from surgery, injuries, or other conditions, we deploy 1089 nodes to monitor patients' progress, activity levels, and rehabilitation exercises. Lastly, we use 4225 nodes in a smart hospital complex, which requires real-time monitoring of thousands of patients, staff, and medical equipment across multiple buildings. Each room, hallway, and department is equipped with multiple sensors to track various parameters, resulting in a high node count. The transmission network's range varies from 200 to 3550 m^2.

In the simulation, there is only one sink node positioned in the center of the topology, as shown in Fig. 11. It is assumed that the sink periodically transmits an Interest packet for a specific task. Different monitoring task loads are reflected in the variation of message intervals, which are set to 1, 3, 5, and 7 s. The broadcast mode with Carrier-sense multiple accesses with collision avoidance (CSMA/CA) MAC layer configuration adheres to IEEE 802.15.4 specifications. The initial energy of the nodes is set at 50 joules, and each node's transmission range is configured to 50 m. Most of the parameters utilized in our simulations are listed in Table 2.

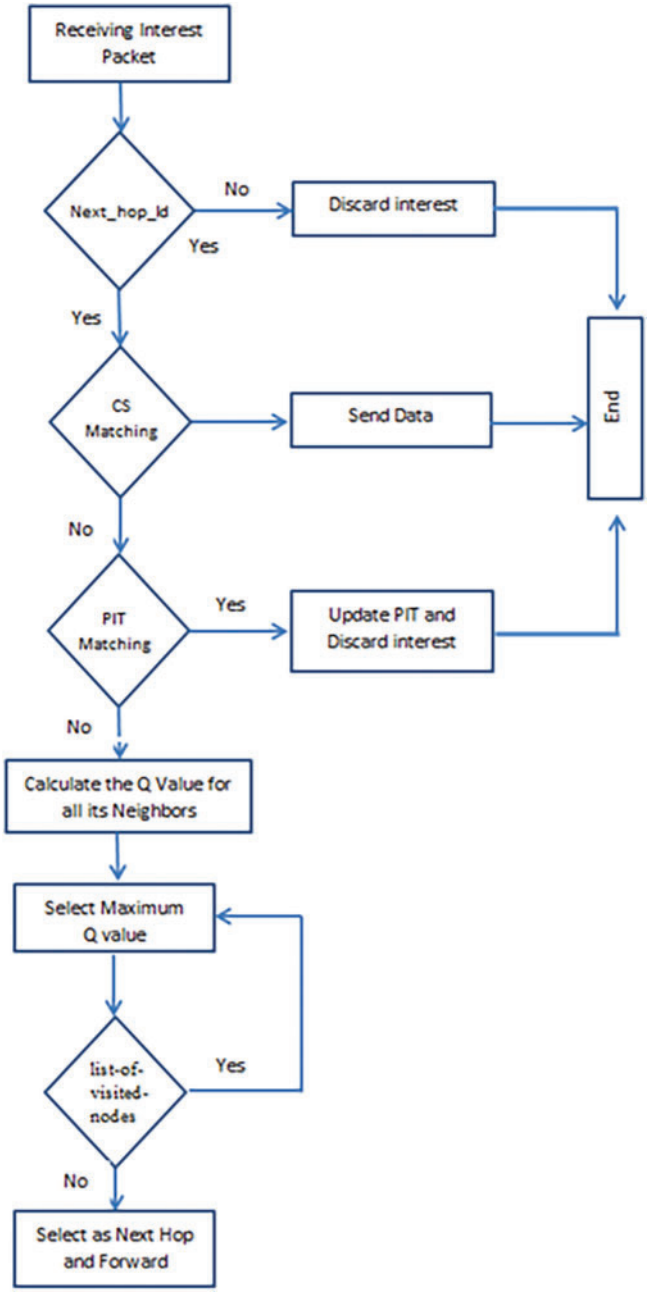

Figure 10: Flowchart of SEF strategy

4.1 Performance Metrics

In this section, each scenario is run 20 times with seed variation to assess whether the proposed forwarding strategy can reduce energy use without compromising the overall effectiveness of the data distribution process in terms of packet delivery ratio (PDR), efficient forwarding, and delay. We compared our Smart and Energy-aware Forwarding strategy (SEF) with three of the best NDN-IoT forwarding schemes: Enhanced Geographic Interest Forwarding (E-GIF), EPF, which is based

on an SDN-NDN-IoT system, and the flooding strategy. Table 2 displays the parameters of the simulation. Next, we utilized the official NDN simulation module for ndnSIM [40–42] and evaluated its performance against the E-GIF, EPF algorithm, and the native flooding mechanism of NDN using six metrics: energy consumption, average data retrieval delay, total number of Interests, network lifetime, average hop count, and packet delivery ratio (PDR). The following are the definitions of the evaluation metrics:

Figure 11: Network topology

Table 2: Simulation parameters

Parameters	Value
Node number	Varying from 9 to 4225
Transmission range	50 m
Simulation time	3600 s
Area size	Varied from (200 × 200) to (3550 × 3550)
Monitoring interval	1,3,5,7 s
Initial energy	5j
Node deployment	Grid deployment
Number of sinks	One sink
Number of producers	4 producers

Total Power Consumption: As many IoT devices rely on batteries and have limited power resources, energy consumption is an important indicator to monitor. Including the energy used for sending, receiving, and processing Interest and Data packets, this metric represents the overall energy used by the network nodes during the simulation period. Since it increases the lifespan of IoT devices, lower energy consumption leads into higher performance.

$$E_{total} = \sum_{i=1}^{n} (TX_i + RX_i) \tag{4}$$

$$TX_{ij} = \epsilon_{elec} \times k + \epsilon_{amp} \times d_{ij}^2 \times k \tag{5}$$

$$RX_i = \epsilon_{elec} \times k \tag{6}$$

TX_{ij} represent the energy consumption for sending packets from node i to node j. RX_i represent the cost of energy for node i that receives a packet. ϵ_{amp} is Energy consumed per bit to amplify the signal and it is equal to 100 pj/bit/m^2, ϵ_{elec} is Energy consumed per bit to run the transmitter and receiver circuitry and it is equal to 50 μJ/bit. d_{ij} is the distance between nodes i and j, and k is the number of bits in the packet.

Network Lifetime: The term network lifetime refers to the amount of time that passes between the initial node's energy exhaustion and its eventual shutdown. It illustrates how the forwarding approach is sustainable and energy-efficient. In IoT applications where node replacement or recharging is challenging, extending the network lifetime is essential. Longer network lifespans provide dependable and stable network performance over time. The amount of time that passes before the first node in the network runs out of energy is known as its lifetime.

Data Retrieval Delay: The data retrieval delay quantifies the amount of time wanted to complete the monitoring task, from the moment the sink sends the Interest packet until the needed data is received. As a result, the average time needed that obtain a wanted data set is known as the average-data-retrieval-delay (Avg. Delay), A lower retrieval delay indicates more efficient data transmission within the network, and it can be computed using the formula below:

$$\text{Avg.Delay} = \frac{1}{N} \sum_{i=1}^{N} \text{Data Retrieval Delay}_i \tag{7}$$

N denotes the total number of data packets that the sink has received, and the following equation provides the value of Data Retrieval Delay_i:

$$\text{Data Retrieval Delay}_i = DRT_i - ITT_i \tag{8}$$

where DRT_i is the Data-Reception-Time and denotes the moment the sink receives the ith requested Data packet, and ITT_i is the Interest-Transmission-Time, denoting the time when the sink transmits the ith Interest packet.

Packet Delivery Ratio (PDR): PDR is the ratio of all the Interest packets sent by the sink node to all the Data packets that were successfully delivered to the sink node. It shows how well the forwarding approach retrieves the needed data. A greater PDR denotes dependable data delivery, which is essential to guaranteeing that Internet of Things applications obtain the data they require to operate as intended. Enhancing PDR lowers data loss and raises system dependability. PDR is computed with the following formula:

$$PDR = \frac{\text{Total data Packets Received}}{\text{Total Interest packets sent}} \times 100 \tag{9}$$

Hop Count: The average number of hops (intermediate nodes) that Interest and Data packets make between the content producer and the content consumer (sink node) is represented by the average hop count. Because fewer nodes are engaged in packet forwarding, lower average hop counts minimize energy consumption and delays in data retrieval. The forwarding strategy's overall effectiveness is

increased by optimizing the hop count. Averaging the number of hops taken by each successful Interest-Data exchange over the course of the assessment period yields the average hop count.

Sent Interests: This metric counts the total number of Interest packets generated, sent, and received within the network. In the NDN architecture, Interest packets are used to request data from specific content providers. The total number of Interest packets reflects the overhead generated by the forwarding strategy. Fewer Interest packets suggest improved efficiency, as they indicate reduced energy consumption and lower network congestion. The total number of Interest packets is determined by counting each Interest packet generated and transmitted during the evaluation period.

4.2 Simulations Results

We measured the energy efficiency of the E-GIF, EPF, flooding strategy, and SEF strategy in the simulations that were run. By assessing the impact of increasing the network density and changing the monitoring interval, we were able to compare their overall energy consumption, network lifetime, retrieval time, Packet Delivery Ratio (PDR), total number of Interest packets, and hop count.

Fig. 12a shows the measurement of total energy consumption as a function of the number of nodes. The total energy consumed in the network is reduced by 27.11% when using the SEF strategy compared to the E-GIF strategy, and by 82.23% and 84.44% compared to the EPF and flooding strategies, respectively, for varying network sizes and densities. Similarly, Fig. 12b shows that the SEF algorithm enhances energy consumption by an average of 40.12%, 82.65% and 85.78% compared to the E-GIF, EPF, and flooding strategies, respectively, for different monitoring intervals. These findings verify that, even in larger networks, the SEF scheme performs better in terms of power savings than the E-GIF, EPF, and flooding strategies. This is expected, as the E-GIF algorithm drops many packets due to the path mechanism's failure to find the best path. Similarly, the EPF algorithm uses many messages, leading to more overhead, and broadcasting in the flooding strategy results in a high number of collisions. All these problems contribute to increased energy consumption.

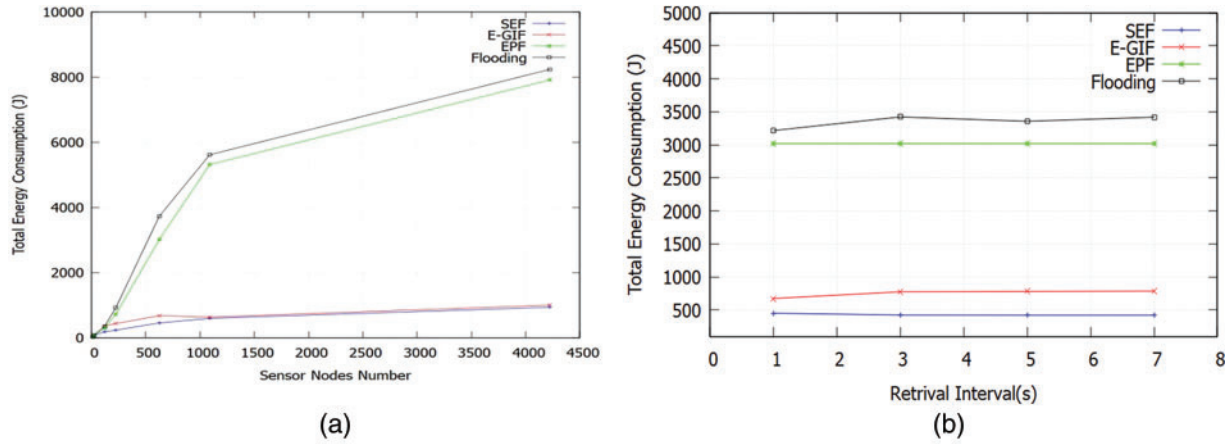

Figure 12: (a) Energy consumption *vs*. sensor nodes number; (b) Energy consumption *vs*. retrieval interval

The proposed research demonstrates greater energy efficiency than the E-GIF, EPF, and flooding strategies, as shown in Fig. 13a, which compares network lifetime across different network sizes. The network lifetime is directly impacted by reduced energy consumption and minimized retrieval time.

The SEF algorithm's network lifetime has increased by an average of 25.35%, 41.98%, and 65.52%, outperforming the E-GIF, EPF, and flooding strategies, respectively.

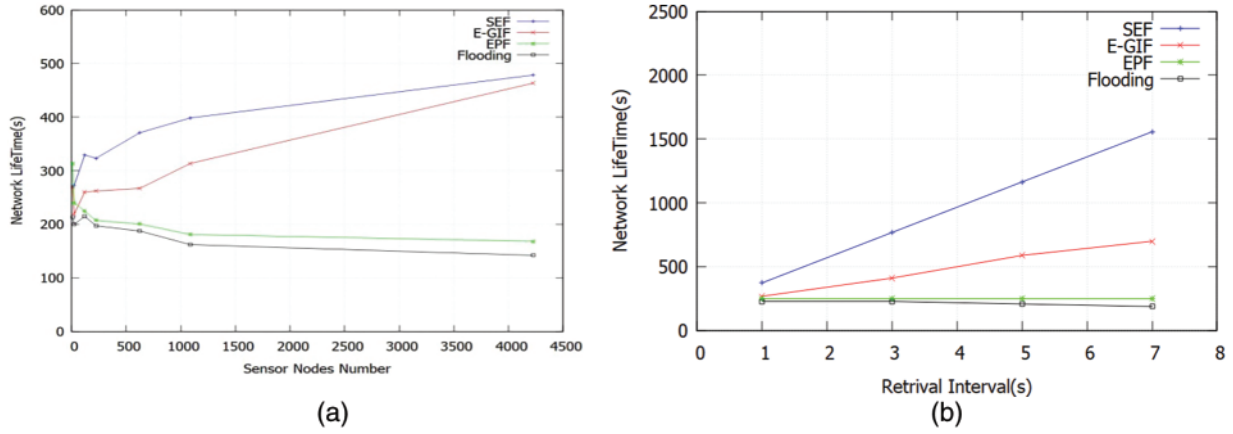

Figure 13: (a) Network lifetime *vs*. sensor nodes number; (b) Network life time *vs*. retrieval interval

Similarly, Fig. 13b shows the results of network time as a function of the Interest-sending interval. We observe that as the sending interval increases, the overall network lifetime significantly increases for both our proposal and E-GIF. At the same time, the flooding forwarding strategy and EPF show the worst values. The SEF strategy increases the network lifetime by an average of 92.78% compared to the E-GIF strategy.

As shown in Fig. 14a, the average retrieval time varies with different numbers of sensor nodes. This is due to a lower chance of collisions and a higher probability of successful delivery, which result in shorter retrieval times. The average retrieval time for the SEF algorithm has decreased by 20.23%, 48.12%, and 51.65% compared to the E-GIF, EPF, and flooding forwarding strategies, respectively. As a result, it is clear that the SEF algorithm forwards packets between sensor nodes and sink nodes more quickly. The results demonstrate that the SEF algorithm's learning mechanism plays a major role in the improvements in retrieval time.

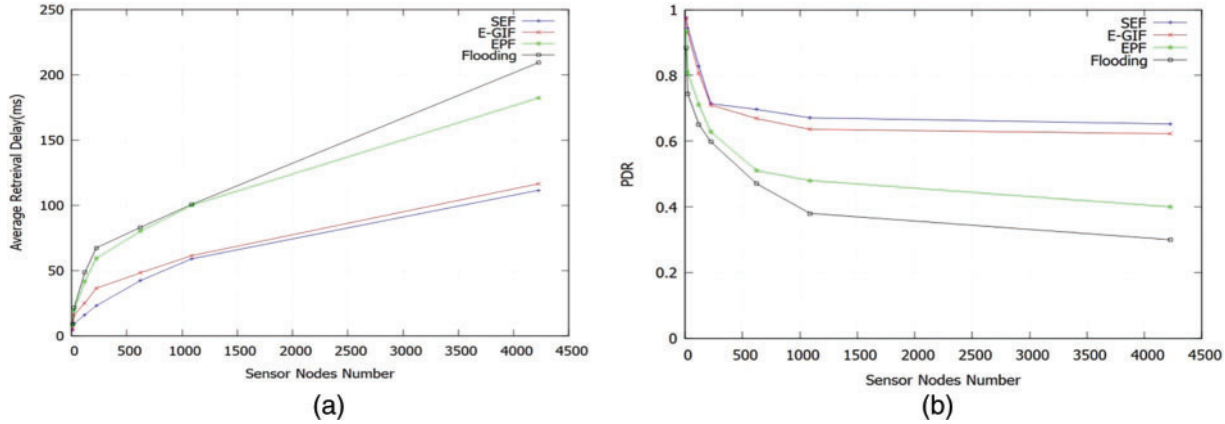

Figure 14: (a) Average retrieval time *vs*. sensor nodes number; (b) PDR *vs*. sensor nodes numbers

Fig. 14b makes it clear that the SEF algorithm outperformed the E-GIF, EPF, and flooding strategies in terms of delivery rate. This indicates that our proposed work has reduced the chance

of collisions by selecting the best Q-value from all neighbors as the next hop to forward the packet. Compared to E-GIF, EPF, and flooding strategies, it is evident that the Packet Delivery Ratio increased as the number of nodes increased. Our solution achieved a satisfaction rate that was about 0.69 higher than that of the other three strategies, despite the denser population. Furthermore, the larger network population results in lower satisfaction percentages for E-GIF, EPF, and flooding. As a result, it was able to lower overall energy consumption without negatively impacting the Packet Delivery Ratio.

We assess the performance of the total number of Interests in Fig. 15a, comparing the overall number of Interests with the total number of nodes. This performance graph shows that the SEF algorithm outperforms the E-GIF, EPF, and flooding strategies in terms of performance. By enabling the Q-learning algorithm to choose the best Q-value among neighbors, the controller reduces the number of interests by addressing the broadcast storm problem, which benefits the SEF algorithm.

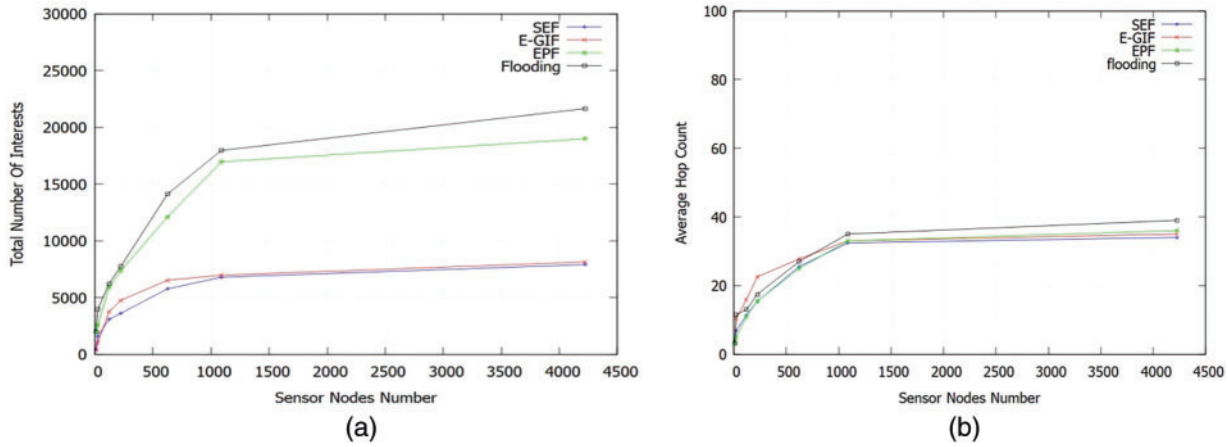

Figure 15: (a) Total number of interests *vs*. sensor nodes number; (b) Average hop count *vs*. sensor nodes number

The average hop results with different numbers of nodes are displayed in Fig. 15b. We find that the SEF algorithm consistently produces the lowest hop count, demonstrating its continuous search for the shortest path to the producer. An intriguing observation is that the number of hops increases as the number of nodes increases. This indicates that more interests require more hops to be satisfied, even though more interests can be fulfilled by the cache.

4.3 Security Analysis

The IoHT brings many advantages to healthcare, enabling smart hospitals and monitoring systems for people with disabilities to function efficiently through interconnected devices. Given the sensitivity of patient data, it is critical to ensure both security and privacy in the context of healthcare IoT systems. Unauthorized access or disclosure of such information may have serious repercussions and jeopardize patient privacy and confidence. Advanced Persistent dangers (APT), Distributed Denial of Service (DoS) attacks, and side-channel attacks are some of the biggest dangers to healthcare IoT systems. These threats can seriously impair service availability, which is a major worry in smart hospitals. In these settings, Internet of Things devices continuously check the vital signs of patients and manage life-saving medical devices. Any vulnerability in these systems' availability or integrity could lead to potentially fatal circumstances, highlighting the necessity of strong security measures to protect both data and services.

A DoS attack is one of the most significant threats in healthcare IoT systems, where service availability is paramount. In smart hospitals, IoT devices monitor patients' vital signs and control critical equipment. If these devices become unresponsive due to DoS attacks, patient safety can be at risk. For people with disabilities, interruptions in their monitoring systems can result in a loss of critical real-time data, leading to delays in emergency interventions. SEF reduces unnecessary traffic by preventing broadcast storms, which is one common vector for launching DoS attacks. This reduces the chances of overwhelming the network infrastructure. SEF's ability to optimize resource usage prevents resource exhaustion, a common method used in DoS attacks to render devices non-functional. By ensuring efficient energy use, SEF helps devices operate longer under load, making it harder for attackers to disable devices via resource-intensive attacks.

In IoHT, APTs are particularly dangerous as they can operate undetected for long periods, gathering sensitive healthcare data or compromising system integrity. Attackers typically aim to exfiltrate patient data or manipulate device behavior in smart hospitals or monitoring systems for people with disabilities. The reduction of network traffic in SEF complicates attackers' ability to conduct reconnaissance, a crucial stage for APTs. SEF limits the volume of network metadata available to adversaries, making it harder to map the network topology or discover critical devices.

Side-channel attacks in IoT healthcare environments could exploit timing information, electromagnetic emissions, or power usage to extract sensitive information. Medical devices used in patient monitoring, for instance, could leak encryption keys or other sensitive data through side-channel vulnerabilities. SEF's energy optimization strategies lead to more predictable and uniform power usage patterns, making it harder for attackers to exploit fluctuations in power consumption for side-channel attacks. By maintaining steady energy profiles across devices, SEF reduces the chance of information leakage via these indirect channels.

In IoT healthcare systems, devices may be deployed in accessible areas where they are vulnerable to physical tampering or theft. For example, patient monitoring devices in hospitals or wearables used by people with disabilities can be physically tampered with, compromising data integrity and availability. By optimizing energy use, SEF minimizes the need for frequent physical interventions (such as battery replacements), thereby reducing opportunities for physical tampering. Devices remain in operation longer without requiring manual service, making physical attacks less likely. SEF's network efficiency can support real-time monitoring of device health. If physical tampering alters the energy consumption profile or communication patterns, healthcare administrators can detect this abnormality and act promptly.

Zero-day vulnerabilities are particularly problematic in healthcare IoT environments because these systems often rely on proprietary software with limited security updates. A zero-day attack could compromise the confidentiality, integrity, or availability of critical systems. SEF's traffic optimization creates a more controlled and predictable environment, making it easier to spot irregular network behavior that may result from exploiting a zero-day vulnerability. Anomalous activity can be detected more quickly, allowing for faster responses before significant damage occurs. By minimizing unnecessary communication and optimizing resource usage, SEF indirectly reduces the system's attack surface, offering fewer vectors for attackers to exploit unknown vulnerabilities.

In an IoHT context, privacy is as critical as security. Patient data is highly sensitive, and any unauthorized access or exposure could lead to severe consequences. SEF reduces the amount of traffic and data exchanged between devices, minimizing the exposure of sensitive patient information in transit. By only sending essential information, SEF reduces the risk of data interception or

unauthorized access. SEF can potentially support secure, encrypted communication between devices, ensuring that even if data is intercepted, it remains inaccessible to attackers.

The SEF strategy offers promising contributions to mitigating several key threats in IoT healthcare systems, including DoS attacks, APTs, side-channel attacks, physical attacks, and zero-day vulnerabilities. Its ability to reduce unnecessary traffic and optimize resource usage provides a solid foundation for enhancing security in sensitive healthcare environments. However, while SEF indirectly addresses several security concerns, there is a need for more explicit integration with advanced security mechanisms, such as intrusion detection systems, physical tamper detection, proactive zero-day defenses, and privacy-preserving technologies.

4.4 Discussion

The energy efficiency results clearly show that the SEF strategy reduces energy consumption by up to 85% compared to the flooding strategy and by approximately 42% compared to E-GIF. This significant improvement is attributed to SEF's use of Q-learning, which enables nodes to make informed decisions based on their neighbors' energy levels. The selection of the optimal next hop based on energy availability and geographic proximity reduces redundant transmissions and packet collisions, leading to more efficient energy utilization. In larger networks, SEF's ability to consistently minimize energy consumption highlights its scalability. Moreover, by preserving node energy, the SEF algorithm extends the network lifetime, enhancing the overall longevity of the network. The observed increase in network lifetime, particularly for larger networks and longer retrieval intervals, demonstrates that SEF minimizes unnecessary packet forwarding and ensures that devices enter energy-saving states when appropriate.

SEF also excels in terms of average retrieval time. The Q-learning-based approach reduces retrieval time by selecting the most efficient paths, which minimizes the number of hops required to reach the sink. SEF outperforms E-GIF by 19% and EPF by over 50%, indicating that it consistently forwards packets faster, even in larger networks where other strategies struggle with increased collisions and delays. As network size increases, the PDR of SEF remains higher than that of the alternative strategies. SEF's use of Q-learning to select the best next hop based on the Q-value ensures more reliable packet forwarding. Even in dense network conditions, SEF maintains a PDR that is 0.68 higher than that of other strategies, demonstrating its robustness in avoiding collisions and packet loss.

The total number of Interest packets generated in the network is significantly lower for SEF than for the other strategies. This reduction can be attributed to SEF's intelligent decision-making, which minimizes redundant Interest transmissions and reduces the likelihood of broadcast storms. By controlling the broadcast behavior, SEF lowers the number of Interests, improving overall network efficiency. Finally, the average hop count confirms that SEF consistently finds the shortest path between sensor nodes and the sink. Although the number of hops increases with larger networks, as expected, SEF maintains the lowest hop count among the tested strategies, further validating its ability to efficiently route packets. The cache mechanism also plays a role in reducing hops, as more Interests are satisfied locally.

In contrast, this research assumes that both sensor and sink nodes are stationary, which simplifies the design of the forwarding and energy-aware routing mechanisms. However, real-world IoT scenarios, especially in healthcare, often involve mobile elements like wearable devices. Future work should investigate the impact of node mobility on network performance, energy consumption, and the learning process of reinforcement learning algorithms. Furthermore, while this study focuses on optimizing energy efficiency and data forwarding, it does not directly address the critical issues of security

and privacy. In IoT-based healthcare systems, where sensitive health data is transmitted, ensuring data privacy is essential. Future research should explore the integration of security mechanisms into energy-aware routing protocols while minimizing any additional energy overhead. Additionally, although the simulation results demonstrate that the proposed SEF strategy outperforms other approaches; real-world deployment and testing in actual IoT systems are needed to validate these findings. Factors such as hardware constraints, environmental interference, and deployment challenges could affect performance in ways that simulations may not fully capture.

Lastly, it's important to highlight that our method does not significantly increase network overhead. The Neighbors Table structure, wherein each sensor maintains limited-size information about its neighbors, is introduced by the SEF method to reduce storage overhead. Since this structure does not store data pertaining to every node in the network, we believe it does not require a lot of space. Its size grows with the number of one-hop neighbors rather than the total number of nodes in the network; therefore, our solution's scalability is not negatively impacted by the storage overhead this structure introduces. Regarding communication overhead, it is important to note that the suggested forwarding module attaches itself to the outgoing Interest packets by using control information specifically, the remaining energy that it needs to function. This behavior greatly decreases communication overhead, making it independent of the number of nodes. Furthermore, in terms of overall bandwidth usage, the communication overhead increases more slowly than the data flow. These characteristics suggest that our forwarding technique will remain effective even as the network's size or workload increases.

5 Conclusion

In this paper, we propose a novel forwarding strategy for the NDN-based IoHT communication model. Our solution, SEF, incorporates geographical distance and the energy levels of neighboring nodes into the Q-learning algorithm to optimize the Interest-forwarding path. To enable efficient multihop communication while reducing communication overhead and collisions, we have developed a robust forwarding strategy. By combining NDN with the IEEE 802.15.4 standard, we harness the benefits of both approaches: the streamlined, lightweight forwarding process of Named Data Networking and the energy efficiency of IEEE 802.15.4. This makes our approach particularly well-suited for low-data-rate, low-power-consumption monitoring and control applications.

We implemented this strategy using the ndnSIM framework and conducted extensive experiments to evaluate its performance. The results show that SEF effectively conserves energy in intermediary IoHT devices while maintaining a short and efficient Interest-forwarding path, which extends network lifetime and sustains high satisfaction rates and retrieval speeds. Comparisons with other state-of-the-art solutions indicate that our approach surpasses alternatives across multiple key metrics. In future work, we plan to perform real-world experiments to further validate our system's effectiveness. Additionally, we aim to support node mobility and investigate the impact of incorporating security features, such as authentication and data encryption, into the SEF strategy, while ensuring that energy efficiency remains uncompromised.

Acknowledgement: The authors extend their appreciation to the King Salman Center for Disability Research for funding this work through Research Group No. KSRG-2023-335.

Funding Statement: This study was funded by the King Salman Center for Disability Research through Research Group No. KSRG-2023-335.

Author Contributions: Naeem Ali Askar: Designed the model and methodology, carried out the implementation and analyzing, investigation, writing original draft; Adib Habbal: Conceptualization, investigation, supervision, writing—review and editing; Hassen Hamouda: Formal analysis, data curation, reviewed the results; Abdullah Mohammad Alnajim: Resources, review and editing; Sheroz Khan: Validation, review and editing. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data used to support the findings of this study are included within the article.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest to report regarding the present study.

References

[1] 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 Things J.*, vol. 6, no. 2, pp. 2128–2158, 2019. doi: 10.1109/JIOT.2018.2873343.

[2] L. Atzori, A. Iera, and G. Morabito, "Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm," *Ad Hoc Netw.*, vol. 56, no. 6, pp. 122–140, 2017. doi: 10.1016/j.adhoc.2016.12.004.

[3] L. Farhan, R. Kharel, O. Kaiwartya, M. Quiroz-Castellanos, A. Alissa and M. Abdulsalam, "A concise review on Internet of Things (IoT)-problems, challenges and opportunities," in *2018 11th Int. Symp. Commun. Syst. Netw. Digit. Signal Process. (CSNDSP)*, Budapest, Hungary, Jul. 2018. doi: 10.1109/CSNDSP.2018.8471762.

[4] I. Ud Din, A. Almogren, M. Guizani, and M. Zuair, "A decade of Internet of Things: Analysis in the light of healthcare applications," *IEEE Access*, vol. 7, pp. 89967–89979, 2019. doi: 10.1109/ACCESS.2019.2927082.

[5] N. A. Askar, A. Habbal, A. H. Mohammed, M. S. Sajat, Z. Yusupov and D. Kodirov, "Architecture, protocols, and applications of the Internet of Medical Things (IoMT)," *J. Commun.*, vol. 17, no. 11, pp. 900–918, 2022. doi: 10.12720/jcm.17.11.900-918.

[6] M. H. Shahid, A. R. Hameed, S. Ul Islam , H. A. Khattak, I. U. Din and J. J. P. C. Rodrigues, "Energy and delay efficient fog computing using caching mechanism," *Comput. Commun.*, vol. 154, no. 3, pp. 534–541, 2020. doi: 10.1016/j.comcom.2020.03.001.

[7] M. Faran Majeed, S. Hassan Ahmed, S. Muhammad, H. Song, and D. B. Rawat, "Multimedia streaming in information-centric networking: A survey and future perspectives," *Comput. Netw.*, vol. 125, no. 3, pp. 103–121, 2017. doi: 10.1016/j.comnet.2017.05.030.

[8] K. Haseeb, N. Islam, A. Almogren, and I. Ud Din, "Intrusion prevention framework for secure routing in WSN-based mobile internet of things," *IEEE Access*, vol. 7, pp. 185496–185505, 2019. doi: 10.1109/ACCESS.2019.2960633.

[9] W. Shang, Y. Yu, L. Zhang, and R. Droms, "Challenges in IoT Networking via TCP/IP Architecture," NDN Technical Report NDN-0038, 2016. Accessed: Oct. 10, 2024. [Online]. Available: http://named-data.net/wp-content/uploads/2016/02/ndn-0038-1-challenges-iot.pdf

[10] S. Mejri, H. Touati, and F. Kamoun, "Hop-by-hop interest rate notification and adjustment in named data networks," *IEEE Wirel. Commun. Netw. Conf. WCNC*, pp. 1–6, 2018. doi: 10.1109/WCNC.2018.8377374.

[11] M. Amadeo, C. Campolo, A. Iera, and A. Molinaro, "Named data networking for IoT: An architectural perspective," in *2014 Eur. Conf. Netw. Commun.*, 2014. doi: 10.1109/EuCNC.2014.6882665.

[12] M. Meddeb, A. Dhraief, A. Belghith, T. Monteil, K. Drira and S. Gannouni, "AFIRM: Adaptive forwarding based link recovery for mobility support in NDN/IoT networks," *Future Gener. Comput. Syst.*, vol. 87, no. 2, pp. 351–363, 2018. doi: 10.1016/j.future.2018.04.087.

[13] M. Amadeo, C. Campolo, A. Molinaro, and N. Mitton, "Named data networking: A natural design for data collection in wireless sensor networks," *IFIP Wirel. Days*, 2013. doi: 10.1109/WD.2013.6686486.
[14] N. A. Askar *et al.*, "Forwarding strategies for named data networking based IoT: Requirements, taxonomy, and open research challenges," *IEEE Access*, vol. 11, pp. 78363–78383, 2023. doi: 10.1109/ACCESS.2023.3276713.
[15] R. Alubady, M. Al-Samman, S. Hassan, S. Arif, and A. Habbal, "Internet protocol MANET vs named data MANET: A critical evaluation," in *4th Int. Conf. Internet Appl. Protoc. Serv.*, 2015, pp. 70–76.
[16] A. Tariq, R. A. Rehman, and B. S. Kim, "Forwarding strategies in NDN-Based wireless networks: A survey," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 68–95, 2020. doi: 10.1109/COMST.2019.2935795.
[17] A. Djama, B. Djamaa, M. R. Senouci, and N. Khemache, "LAFS: A learning-based adaptive forwarding strategy for NDN-based IoT networks," *Ann. Telecommun.*, vol. 77, no. 5–6, pp. 311–330, 2022. doi: 10.1007/s12243-021-00850-2.
[18] M. Kuai and X. Hong, "Location-based deferred broadcast for ad-hoc named data networking," *Futur Internet*, vol. 11, no. 6, 2019, Art. no. 139. doi: 10.3390/fi11060139.
[19] A. Tariq, R. A. Rehman, and B. S. Kim, "EPF—An efficient forwarding mechanism in sdn controller enabled named data IoTs," *Appl. Sci.*, vol. 10, no. 21, 2020, Art. no. 7675. doi: 10.3390/app10217675.
[20] D. Saxena, V. Raychoudhury, and N. SriMahathi, "*SmartHealth-NDNoT*: Named data network of things for healthcare services," in *MobileHealth 2015—Proc. 2015 Work. Pervasive Wirel. Heal. Co-Located MobiHoc*, 2015, pp. 45–50. doi: 10.1145/2757290.2757300.
[21] M. Amadeo, G. Ruggeri, C. Campolo, A. Molinaro, V. Loscrí and C. T. Calafate, "Fog computing in IoT smart environments via named data networking: A study on service orchestration mechanisms," *Futur Internet*, vol. 11, no. 11, pp. 1–21, 2019. doi: 10.3390/fi11110222.
[22] R. Alubady, S. Hassan, and A. Habbal, "Pending interest table control management in Named Data Network," *J. Netw. Comput. Appl.*, vol. 111, pp. 99–116, 2018. doi: 10.1016/j.jnca.2017.11.002.
[23] S. Hassan, I. Ud Din, A. Habbal, and N. H. Zakaria, "A popularity based caching strategy for the future Internet," in *2016 ITU Kaleidoscope: ICTs Sustain. World (ITU WT)*, IEEE, 2016, pp. 1–8.
[24] I. Ud Din, S. Hassan, and A. Habbal, "SocialCCNSim: A simulator for caching strategies in information-centric networking," *Adv. Sci. Lett.*, vol. 21, no. 11, pp. 3505–3509, 2015. doi: 10.1166/asl.2015.6575.
[25] M. Amadeo, C. Campolo, and A. Molinaro, "Forwarding strategies in named data wireless *ad hoc* networks: Design and evaluation," *J. Netw. Comput. Appl.*, vol. 50, no. 1, pp. 148–158, 2015. doi: 10.1016/j.jnca.2014.06.007.
[26] S. Gao, H. Zhang, and B. Zhang, "Energy efficient interest forwarding in NDN-Based wireless sensor networks," *Mobile Inf. Syst.*, vol. 2016, pp. 1–15, 2016, Art. no. 3127029. doi: 10.1155/2016/3127029.
[27] A. Aboud, H. Touati, and B. Hnich, "Efficient forwarding strategy in a NDN-based internet of things," *Cluster Comput.*, vol. 22, no. 3, pp. 805–818, 2019. doi: 10.1007/s10586-018-2859-7.
[28] Z. Ali, M. A. Shah, A. Almogren, I. Ud Din, C. Maple and H. A. Khattak, "Named data networking for efficient IoT-based disaster management in a smart campus," *Sustainable*, vol. 12, no. 8, 2020, Art. no. 3088. doi: 10.3390/SU12083088.
[29] S. Hassan, S. Hamdi, and M. Alsamman, "Energy-aware multipath forwarding mechanism for named data network in wireless environment," in *6th Int. Conf. Internet Appl., Protocols, Serv. (NETAPPS2020)*, 2021, pp. 43–49.
[30] H. Touati, A. Aboud, and B. Hnich, "Named data networking-based communication model for Internet of Things using energy aware forwarding strategy and smart sleep mode," *Concurr. Comput. Pract. Exp.*, vol. 34, no. 3, pp. 1–17, 2022. doi: 10.1002/cpe.6584.
[31] A. Kishor, C. Chakraborty, and W. Jeberson, "A novel fog computing approach for minimization of latency in healthcare using machine learning," *Int. J. Interact. Multimed. Artif. Intell.*, vol. 6, no. 7, pp. 7–17, 2021. doi: 10.9781/ijimai.2020.12.004.
[32] M. M. H. Iqbal, S. Md Asif, and Asaduzzaman, "A source-driven probabilistic forwarding and caching strategy in NDN and SDN-based NDN," *Int. J. Commun. Syst.*, vol. 35, no. 6, 2022, Art. no. e5093. doi: 10.1002/dac.5093.

[33] G. Musa Raza, I. Ullah, M. Salah Ud Din, M. Atif Ur Rehman, and B. S. Kim, "INF-NDN IoT: An intelligent naming and forwarding in name data networking for Internet of Things," *IEEE Access*, vol. 12, pp. 114319–114337, 2024. doi: 10.1109/ACCESS.2024.3444903.

[34] A. Aboud and H. Touati, "Geographic interest forwarding in NDN-based wireless sensor networks," in *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. (AICCSA)*, Agadir, Morocco, 2016. doi: 10.1109/AICCSA.2016.7945683.

[35] M. Amadeo, C. Campolo, and A. Molinaro, "Internet of Things via named data networking: The support of push traffic," in *2014 Int. Conf. Netw. Futur. (NOF)*, Paris, France, 2014. doi: 10.1109/NOF.2014.7119766.

[36] S. Ryu, I. Joe, and W. T. Kim, "Intelligent forwarding strategy for congestion control using Q-learning and LSTM in named data networking," *Mob. Inf. Syst.*, vol. 2021, 2021. doi: 10.1155/2021/5595260.

[37] V. K. Mutombo, S. Lee, J. Lee, and J. Hong, "EER-RL: Energy-efficient routing based on reinforcement learning," *Mobile Inf. Syst.*, vol. 2021, 2021, Art. no. 5595260. doi: 10.1155/2021/5589145.

[38] S. Padakandla, "A survey of reinforcement learning algorithms for dynamically varying environments," *ACM Comput. Surv.*, vol. 54, no. 6, pp. 1–15, 2021. doi: 10.1145/3459991.

[39] Z. Mammeri, "Reinforcement learning based routing in networks: Review and classification of approaches," *IEEE Access*, vol. 7, pp. 55916–55950, 2019. doi: 10.1109/ACCESS.2019.2913776.

[40] S. Mastorakis, A. Afanasyev, and L. Zhang, "On the evolution of ndnSIM: An open-source simulator for NDN experimentation," *Comput. Commun. Rev.*, vol. 47, no. 3, pp. 19–33, 2017. doi: 10.1145/3138808.3138812.

[41] S. Mastorakis, A. Afanasyev, I. Moiseenko, and L. Zhang, "ndnSIM 2.0: A new version of the NDN simulator for NS-3," NDN Technical Report NDN-0028, pp. 1–8, 2015.

[42] A. Afanasyev, I. Moiseenko, and L. Zhang, "ndnSIM: NDN simulator for NS-3," NDN Technical Report NDN-0005, pp. 1–7, 2012.