IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 April 2023, accepted 6 May 2023, date of publication 15 May 2023, date of current version 2 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3276713

SURVEY

Forwarding Strategies for Named Data Networking Based IoT: Requirements, Taxonomy, and Open Research Challenges

NAEEM ALI ASKAR[1], ADIB HABBAL[1], (Senior Member, IEEE), FERAS ZEN ALDEN[2], XIAN WEI[3], (Senior Member, IEEE), HASHEM ALAIDAROS[4], JIELONG GUO[3], AND HUI YU[3]

[1]Computer Engineering Department, Faculty of Engineering, Karabük University, 78050 Karabuk, Turkey
[2]Department of Informatics and Software Engineering, Faculty of Engineering, Cihan University-Erbil, Erbil 44001, Iraq
[3]Institute of Research on the Structure of Matter, Chinese Academy of Science Fujian, Fuzhou 350002, China
[4]Cybersecurity Department, School of Engineering, Computing and Design, Dar Al-Hekma University, Jeddah 22246, Saudi Arabia

Corresponding authors: Adib Habbal (adibhabbal@karabuk.edu.tr) and Jielong Guo (gjl@fjirsm.ac.cn)

This work was supported in part by the Fujian Science & Technology Innovation Laboratory for Optoelectronic Information of China under Grant 2021ZZ120, and in part by the Fujian Science and Technology Plan under Grant 2021T3003.

ABSTRACT The Internet of Things (IoT) aims to efficiently connect various entities, including humans, machines, smart devices, physical environments, and others, so they can communicate and exchange data in real time. However, due to the massive amount of data transferred, the presence of devices with limited resources, heterogeneity, and mobility support would make it difficult to create a robust network with respect to performance in an IoT context. In order to efficiently disseminate the enormous volume of automated data, Named Data Networking (NDN), a viable networking design for the future Internet, has been proposed. NDN has shown great potential for IoT because it has built-in support for naming, caching, mobility, and security. Forwarding strategies play an important role in the successful deployment of NDN-based IoT. In this article, we introduce NDN-based IoT forwarding emphasizing on IoT characteristics and requirements. We classify NDN-based IoT forwarding strategies and then discuss in detail certain exemplary schemes. Additionally, we compare several aspects of current forwarding methods that are now in use, including the types of forwarding strategy, particular issues, type of solution, assessment metrics, and simulation platform. We wrap up our contribution by outlining the major open research issues that can guide future investigations in this area. We anticipate that this survey will help the community of NDN-based IoT researchers' understanding of forwarding strategies in IoT environments.

INDEX TERMS Forwarding strategy, IoT, NDN, ICN, CCN.

I. INTRODUCTION

Information-Centric Networking (ICN)/ NDN can also be seen as one of the technologies that will enable the Internet of Things (IoT), a network of billions of connected devices where content distribution will be a major issue [1], [2], [3]. However, in an IoT environment, where information is sent between end-to-end hosts, content distribution is reliant on the TCP/IP architecture. The host-centric Internet paradigm poses problems as a result of the exponential growth in heterogeneous devices and the massive transfer data in the IoT system [4], [5]. For effective data dissemination throughout the Internet, factors like mobility, scalability, network management, and security are paramount [6], [7], [8].

In NDN, the data consumer or receiving end, controls every communication. A customer sends the network an Interest with an identifying name, as shown in Figure 1, in order to get the desired material. This name is used by routers to send the Interest to the producer(s) [9], [10], [11]. Once the Interest reaches a node on the forwarding path which has the requested Data, that is, the Interest packet name matches the Data packet name or the Data name prefix, the router

The associate editor coordinating the review of this manuscript and approving it for publication was Sathish Kumar.

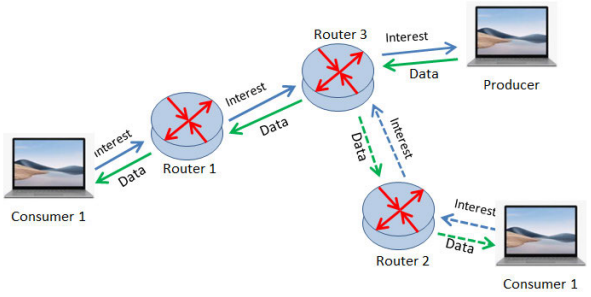

FIGURE 1. Processing the packet in NDN communication [12].

will retrieve the Data that includes the name and the content, as well as a signature made with the producer's key. This Data travels in the opposite direction of the Interest to return to the asking customer [12], [13], [14].

Different from IP, typical multicast suppression techniques in NDN allow many routers to take advantage of the same information to share transmissions over a broadcast medium since both Interest/Data can uniquely identify the content being sent. As a result, as compared to IP, NDN must entail a significant re-engineering of the router's forwarding plane, which deploys three tables: the Forwarding Information Base (FIB), the Pending Interest Table (PIT), and the Content Store (CS). Among them, CS maintains the forwarding information for Interests to enable effective packet forwarding, PIT monitors the Interest passed upstream to assure the return of the Data, and FIB caches the packet buffers to support in-network caching.

Due to unstable and constrained wireless links, mesh networks have problems with packet forwarding and content distribution. The main components of the NDN design are the End-to-End principle, plane separation of routing and forwarding, stateful forwarding, integrated security, and user choice enabler. The NDN is made safe for communication through the establishment of a trust anchor and a practical trust management solution. The producer signature function, which is pre-installed in data packets, ensures the confidentiality and security of the messages. If an application needs in-order INTEREST delivery, we must discover a forwarding mechanism that will successfully shield it from packet loss and congestion. A new network forwarding plane created by the NDN paradigm can effectively avoid failure links, avoid prefix hijackers, and use multipath to reduce congestion. Large-scale forwarding tables, per-packet DATA status updates, and quick, variable-length, hierarchical name-based lookups are all necessary for NDN. Scalable packet forwarding continues to be a difficult topic. The three main features of NDN forwarding are quick name lookup, intelligent forwarding strategies (preferred route), and caching rules. The classification and in-depth discussion of NDN-based IoT forwarding methods can be found in a few review papers, though. A thorough survey is now required due to the significance of forwarding in NDN-based IoT and the large number of forwarding solutions that are currently accessible. This study's objectives are to present a thorough overview, make comparisons, and pinpoint some potential research topics. Below is a summary of the paper's overall message and its main contributions.

- First, a general overview of NDN in an IoT environment, IoT characteristics and requirements, NDN architecture, and moving toward an NDN-based IoT, are given.
- Additionally, a full and in-depth survey study of IoT improvement based on NDN forwarding method, as well as an overview of NDN forwarding strategies with new taxonomy, is provided.
- Then, a thorough evaluation of the available solutions in the literature is offered with regard to a variety of factors, including forwarding strategies, evaluation metrics, specifics problem, and simulation platform.
- Open issues and important challenges in the area are identified, and discussion is held regarding how to solve them.

II. IoT AND NDN

Designing a network architecture which connects a sizable ecosystem, where elements may be resource-constrained, mobile, and/or have highly varied traffic patterns, provides significant issues. Among the needs that IoT must satisfy are agile network design and management, security, scalability, robustness, and reliability [15], [16]. When deploying the IoT, NDN functionalities offer a number of benefits. For instance, the majority of IoT apps do not demand that two devices establish end-to-end connectivity. Instead, they rely on locating the content and extracting it [17]. We believe that NDN can solve a number of IoT requirements by directly controlling a number of functionalities (naming, data aggregation, security, etc.) at the network layer due to its inherent features [18], [19], [20].

A. INTERNET OF THINGS

The Internet of Things (IoT) has created several opportunities for managing many applications in the future in a more effective, simple, and intelligent manner. Connecting any device in our environment to the Internet and enabling intelligent features on it, is the fundamental tenet of the IoT [21], [22]. Multiple technologies are combined to let actuators and sensors to sense and gather useful information, communicate and cooperate, deliver smart data analysis, and make decisions without human involvement. However, it has also made it more difficult to achieve various goals, such as universal access, improved scalability, increased robustness, and unquestionably increased security [23], [24], [25].

1) IoT CHARACTERISTICS

Internet of things are dependent on the following characteristics, what were published in [26], [27], [28], [29], and [30].

a: SENSING

Numerous IoT application cases, including healthcare, smart mobile devices, climate monitoring, industrial control, etc., can make use of the sensing features. Sensors enable the

device to communicate with the outside world and humans by measuring environmental characteristics in a context-aware manner.

b: OBJECT-RELATED SERVICES

IoT offers object-related services by taking into account a device's restrictions, such as privacy and semantic integrity, between actual objects and the virtual objects that go along with them.

c: HETEROGENEITY

IoT is enabled by a variety of hardware platforms and operating systems. In order to enable seamless data flow, this complex ecosystem must permit connections across diverse devices and services.

d: DYNAMIC CHANGES

IoT devices have dynamically changing statuses, such as location, speed, sleeping and awakening, connectedness, and others. As a result, the number of devices may fluctuate.

e: LARGE SCALE

The number of IoT devices is growing while they need to be maintained, and there will be orders of magnitude more communication interactions than there are now with IoT devices connected to the current Internet.

f: SAFETY AND SECURITY

Since IoT devices may have an impact on the physical world; safety is one of the most crucial factors that must be taken into account. Additionally, security procedures must be developed that can extend across nodes, networks, and the data transferred across them in order to secure them.

g: CONNECTIVITY

IoT enables network compatibility and accessibility. Compatibility grants everyone the same ability to consume and create data, whereas accessibility requires joining a network.

2) IoT REQUIREMENTS

The components of the proposed IoT architecture must take into account a number of requirements due to the resource constraints of linked IoT devices and the unreliability of their communication methods, as reported by [26], [28], [31], [16], and [30].

a: NAMING

Every node, with generated data, as well as its offered services, must be given a distinct name in order for IoT designs to be widely used. Considering the dynamic characteristics of IoT networks, such a naming scheme must be durable (mobility, failures, energy depletion, etc.). Additionally, it needs to be brief in order to account for the limitations of storage, communication, and processing. The naming scheme should also be comprehensive in order to reflect the complexity of IoT contexts.

b: SECURITY AND PRIVACY

Security becomes a significant concern since IoT nodes make associated physical items accessible over the Internet. IoT systems do, in fact, encompass crucial infrastructures, such as electricity and industrial systems, as well as crucial data from smart healthcare systems that directly affect human lives. This emphasizes how important security and privacy are in IoT situations. In fact, failure to safeguard and secure IoT devices could delay or even prohibit adoption.

c: SCALABILITY

The proposed IoT architectures must employ dependable and adaptable methods that can handle the massive increase in generated data traffic, while scaling with the number of linked devices.

d: LIGHTWEIGHT DESIGN AND ENERGY EFFICIENCY

The computing, bandwidth, memory, energy, and storage capabilities of the nodes that make up the IoT environment vary greatly. As a result, it is necessary to develop lightweight proposals and algorithms that can operate under these constraints in order to protect network resources and increase network lifetime.

e: STORAGE AND CACHING

The caching techniques help IoT networks improve dependability, data availability, and response time while reducing latency. Additionally, storage resources might be needed for medium term and larger information collecting, with pre-selected network storage nodes chosen to minimize computational and administrative overheads.

f: SUPPORT FOR MOBILITY AND QUALITY OF SERVICES

IoT architectures must enable connection failures, Quality of Service (QoS), and mobility in such diverse networks in addition to being able to provide dependable data transmission in both ad hoc and infrastructure modes [17].

g: DATA AVAILABILITY

In the existing TCP/IP-based architecture, anytime a node switches from one place to another, information that was previously considered to be available is no longer available. The same occurs when a device's battery runs out and it is unable to transmit data. Additionally, a Denial of Service (DoS) assault prevents Internet users from receiving data at once. DoS happens as a result of the inability of the current Internet architecture to examine or inspect data in response to requests made during data transmission. As a result, techniques like in-network caching are necessary to ensure that information is always available.

B. NDN

Named Data Networking (NDN) is a new paradigm for the future generation of the Internet, making an effort to view network contents as first-class entities instead of being restricted to a supplementary device or location. This indicates that NDN changes the focus from the endpoint to the data or information, in contrast to the conventional host-centric Internet, that employs IP addresses to establish connections among the endpoints involved in information exchange. The network nodes in the NDN architecture treat each piece of data and each packet as a unique, self-employing data unit that has a persistent, self-authenticating, and location-independent name. Consumers can access content by name directly, disregarding the IP address and location of the producer [32], [33]. Because its straightforward communication style, and native support for, in-network caching, simpler data sharing, scalability, and security, NDN shifts the host-centric model to ICN, that implies many benefits to IoT [34]. Content centric networking (CCN) focuses on content rather than providing endpoints with communication channels [35], [36], [37].

NDN uses public-key cryptography to assure security, just like other ICN methods [38]. Each entity in a NDN environment has the same name along with a cryptographic key, and anything over an NDN is thought of as an entity. Each name becomes an identity once it has received an NDN certificate. In addition to digital keys, NDN also employs the trust policy and NDN certificate methods for content security [39]. Identity reliability is determined by the application in terms of trust policy. Additionally, producers decide on the names for data packets, and consumers will only receive data packets with the correct name formats. Using interest packets, the NDN certificate approach retrieves NDN certificate data packets that contain public key information [40], [41].

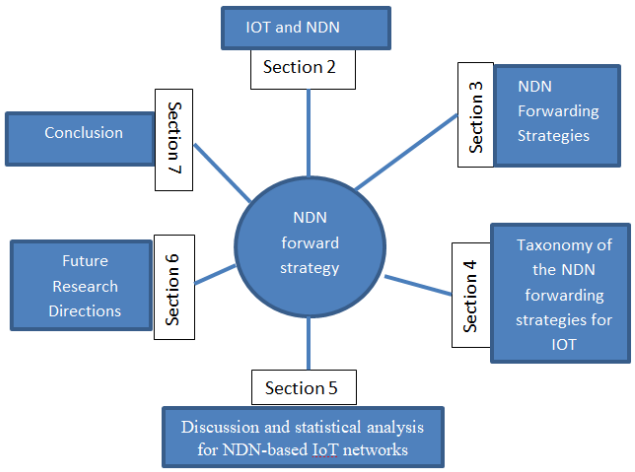

FIGURE 2. Organization of this paper.

1) NDN ARCHITECTURE

The concept of CCN is the foundation of the data-oriented networking paradigm known as NDN. Numerous problems

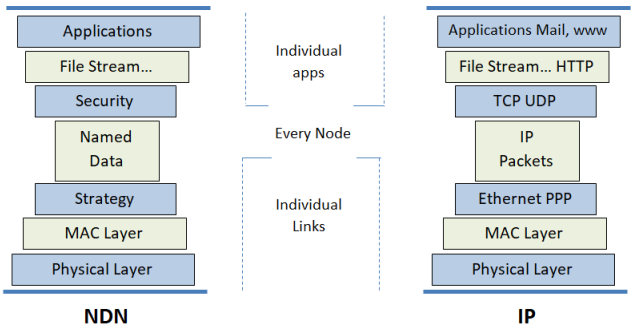

FIGURE 3. NDN and IP hourglass architectures [44].

with the present IP connection-oriented paradigm, such as network load distribution, IP depletion, and network overhead, are addressed by this architecture [42], [43]. As depicted in Figure 3, NDN's goal is to restructure the IP stack by leveraging multiple networking technologies below the waist to connect named data in place of the IP hourglass's waist [44], [45]. However, NDN may directly use some IP services like Domain Name Service (DNS) and inter-domain routing rules. NDN can be somewhat changed and adapted to using IP routing protocols such Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) [46], [47]. The strategy layer makes the best use of resources by choosing a link in a multi-homed device, for example. In accordance with the limitations of the access network and the needs of the application, it also enables the specification of various transport and forwarding services [48], [49]. The name data is subject to the security features handled by the security layer. Next, we'll briefly go over some of the fundamental elements of NDN architecture [42], [46], [50].

a: PACKETS

Receivers, or data consumers, drive communication in NDN through the exchange of two packet types: Interest and Data. Each type of packet has a name that designates the specific data that can be sent in the packet, as depicted in Figure 4.

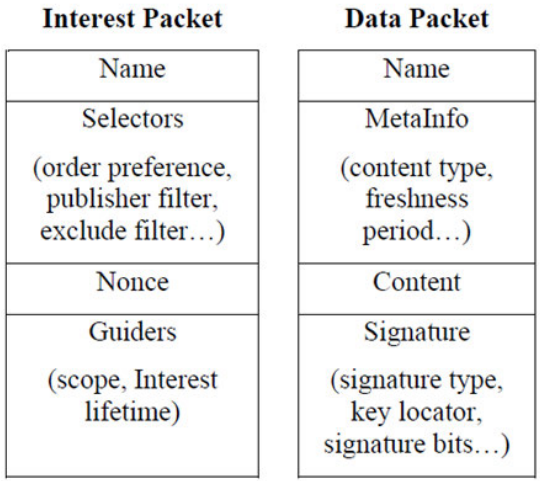

FIGURE 4. Packet format for NDN [43].

• Interest: A user creates an Interest packet and transmits it to the network with the name of a desired piece of data. This name is used by routers to send the Interest to the data producer(s).

• Data: When the Interest reaches a node with the requested data, the node will send back a Data packet that includes the name and content as well as a signature from the producer's key that ties the two together [51]. This data packet travels backwards along the route taken by the Interest to contact the asking customer [42], [52].

b: CONTENT NAMING

Despite the fact that researchers have proposed several ICN naming systems, names in NDN are hierarchical and resemble URLs [53]. The names do not refer to any particular place, and even the first part does not have to be readable by people. It implies that name space will be unlimited and that users and apps would need to be aware of their needs [54]. All material in NDN must have a name and can only be accessed using that name. The network will return the information that matches the user's chosen name when the user does prefix searching [55], [56].

c: CS

Content Store is one of the three basic components of network devices in NDN that handle Interest and Data packets. For named content, the CS is a sizable temporary storage facility akin to modern web cache servers [57]. When a router or node in NDN receives an Interest, it first checks its CS to see if there is a match; if so, the Interest is satisfied. In order to reduce response time and load, this means that each node in the NDN network handles a saved copy of that Data in network caching or CS, to satisfy any upcoming interest in the same content [58]. By using this process, the network's most well-liked content will spread to other nodes, improving network performance. ICN employs a number of tactics and replacement guidelines for specified information that has been cached to enhance data delivery [59].

d: PIT

This stores or keeps track of the record of content names and incoming faces, records all Interest packets that have been transmitted by the node or router, but have not yet been satisfied. As was previously mentioned, when a node receives an Interest packet, it first checks its CS to see if it has the necessary data. If not, the node or router creates an entry in the PIT with the content name of the Interest and the face identifier, and then forwards the Interest to the FIB table for additional processing. The face identification and content name saved in the PIT will eventually be utilized to transmit the Data packet utilizing the entry. It denotes that the entry of PIT will be dropped and the Data packet takes the alternative route to reach the intended node. Data packets that have not yet been entered into the PIT will be deemed unsolicited and dropped [60], [61].

e: FIB

The same name-prefix is used to forward the Interest packet through a table called the Forwarding Information Base (FIB), which also stores information about subsequent hops. In order to forward the Interest packet to the proper sources of data, FIB translates the output faces to the information names. The FIB can be updated using name-prefix depending on the routing protocols to ensure that precise information about the location of the requested data and the path that it will follow to get there is available [62], [63]. A list of upcoming hops and a name prefix make up each FIB entry. Routers can forward Interest packets to one or more hops in accordance with their forwarding strategies, thus providing a multipath forwarding scheme [46], [64], [65].

The fundamental NDN forwarding scheme for NDN nodes first examines its local content store after receiving an Interest packet. The data is therefore transmitted over the incoming face if the requested data is present in the CS. If not, the PIT entries are compared to the content prefix. The router adds the incoming interface of this Interest to the existing PIT entry if the content prefix is present in the PIT. A new entry will be added to the PIT and the node will transmit the Interest packet to all interfaces indicated in the FIB match, if the name in the PIT does not match. The node that has a copy of the requested data returns a Data packet with the requested content once the Interest has reached it. A router examines its local cache after receiving the Data packet. The information will be disregarded and deleted if it has already been stored. In every other case, the data follows the breadcrumbs left in the PIT to find the path back to the user, if a match is found in the PIT. All downstream interfaces indicated in the matched PIT entry are passed the Data. In addition to caching the Data in the CS, the router then deletes the PIT record linked to the Interest packet [66], [67]. The procedures involved in processing Interest and Data packets across the NDN data structures are summarized in Figure 5.

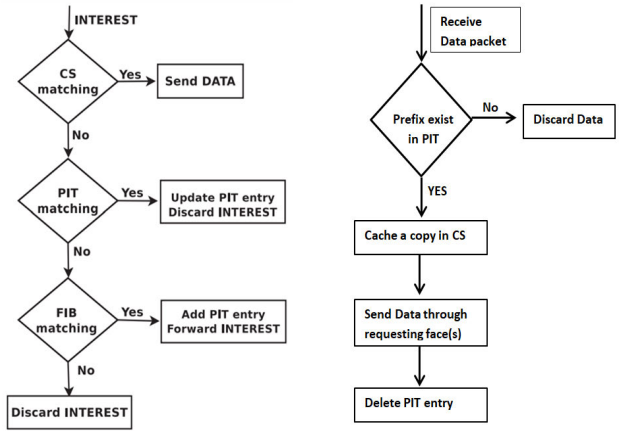

FIGURE 5. NDN interest and data processing [68].

2) TOWARDS NDN-BASED IoT

Depending on the application context, connected objects in the IoT are expected to have high requirements, particularly

in terms of QoS, mobility, and response time. NDN promises to provide good assistance in these areas because of its built-in characteristics. NDN can specifically take care of the following IoT requirements [69], [70]:

a: QUALITY OF SERVICE (QoS)

In IoT networks based on NDN, QoS is ensured by utilizing NDN's in-network capabilities, such as caching techniques and query aggregation, which serve to speed up response times and lower the rate of packet loss for all types of network traffic.

b: SCALABILITY

NDN can support IoT scalability through the network-level naming mechanism and content routing based on these names. Instead of providing a location, users can narrow the scope of their inquiries by targeting their search terms specifically, which helps to support the massive volume of queries for connected objects.

c: ENERGY EFFICIENCY

By putting the information close to the consumer, NDN caching strategies reduce the number of packets that must be transmitted and prevent congestion in the IoT network, allowing for energy savings.

d: SECURITY

NDN offers a crypto-signature, a secured object/name binding method, and enables the network and/or its components to verify integrity, access control, and confidentiality locally at the network layer, without the necessity for third-party services, vastly facilitating secure content sharing between many IoT nodes [71].

e: HETEROGENEITY

Due to NDN's established naming rules, which enable decoupling of the reception from transmitters, users can search for data by name, regardless of the device it is being hosted in or the routing service being used, thus overcoming inherent problems associated with the highly heterogeneous nature of the IoT ecosystem of gadgets.

III. NDN FORWARDING STRATEGIES

The optimum face to send an Interest through in NDN is determined by a forwarding strategy, which may be based on a routing protocol or on measures like link load and availability. Network performance is enhanced by effective forwarding, especially when it comes to services. Response times can be sped up and the workload distributed among service replicas by selecting the best face in the FIB for a service name [68], [72].

In NDN, the NDN Forwarding Plane supports three features: efficient caching processes, quick name lookup, and inelegant forwarding strategies [73], [74], [75]. A forwarding plane is logically made up of FIB, which is used to store all the data related to forwarding rules, PIT that is used to store pending interest requests, and CS that houses a packet data cache [55], [76], [77].

Effective caching policies correspond to the CS because it is a part of the content distribution process that supports it. Intelligent forwarding strategies are designed to select multiple outgoing interfaces by selecting the most efficient interface; the network environment is also taken into consideration when making this decision. Because NDN packets do not carry source and destination addresses like IP packets do, fast name search is a function that allows packets to be forwarded on NDN by using a lookup process based on the name of the content [78]. The forwarding approach is this study's main topic. The node's forwarding strategy is used to choose the appropriate face on the FIB table to forward packets of Interest [79], [80].

Application namespace is used by NDN routers in place of IP addresses to forward packets [81]. Routers use self-learning mechanisms or routing algorithms to update and publish their FIB entries [82]. In contrast to IP routers, NDN routers employ stateful forwarding, which means that they retain details about the requests they receive until they are fulfilled or time out [83]. Interest packets are forwarded using the forwarding technique in accordance with the FIB entries, local measurements, or additional per-namespace forwarding policies [45]. The destination interfaces are likewise picked by the forwarding strategy. Multi-path forwarding is another option that NDN routers have to ensure priority, load balancing, and prevent broken links. Only one Data packet can be included in each Interest packet, and each response follows the same path as the related request [84], [85], [86].

Broadcast: When a customer requests a certain piece of data, NDN uses a straightforward multicasting strategy, that is, the Interest packets are easily broadcasted to every interface listed in the forwarding of the interest packet, which is same as the required data name prefix, except for the requesting interface. Similarly, the broadcast characteristics of the wireless channel for data transfer enhances NDN implementations in WSN environments [87]. Consumers can simply broadcast their Interest in retrieving information in any direction, whenever they need to. Until it reaches a possible supplier, all nodes receiving this Interest packet will broadcast it as well. By quickly locating the closest cached copy without each node forwarding the Interest packet's continual update, it can address the intermittent connectivity issue and short link duration. However, when numerous nodes within the match transmission range discover an Interest packet, they all re-broadcast it [88]. This is typically expensive, causes severe network redundancy, packet collisions, congestion, significant, and a host of other issues with data transmission, including the broadcast storm problem, particularly in the case of dense networks. Researchers improved the default NDN forwarding plane as a result of these flaws to make it more compatible with the wireless environment. One of the various methods that have been investigated to stop the broadcast storm

issue is finding the most suitable node to rebroadcast the packet [89], [90], [80].

Deferred broadcast: Each node in a deferred broadcast system listens to the channel while delaying rebroadcasting the Interest packet for a set amount of time using a timer. When a node detects a packet being broadcast by a high priority neighbor, the deferred approach cancels a scheduled transmission. The broadcast storm is eventually reduced because only nodes with high priority engage in the Interest packet or Data packet forwarding process, which lowers the number of forwarding candidates and collision risks.

Unicast: Problems with broadcasting such packet duplication and collisions can reduce the network's efficiency. Only a small number of studies, however, supported unicasting throughout the content retrieval phase following the discovery of the content source using broadcast mode. When FIB cannot give forwarding direction, the goal of the content discovery phase is to establish routes among the customer and the content provider. Future requests are forwarded through unicast on the found pathways following the discovery phase. According to the FIB's criteria, intermediate nodes in the found path advance the Interest toward a single neighbor. As a result, each node only executes one interest communication.

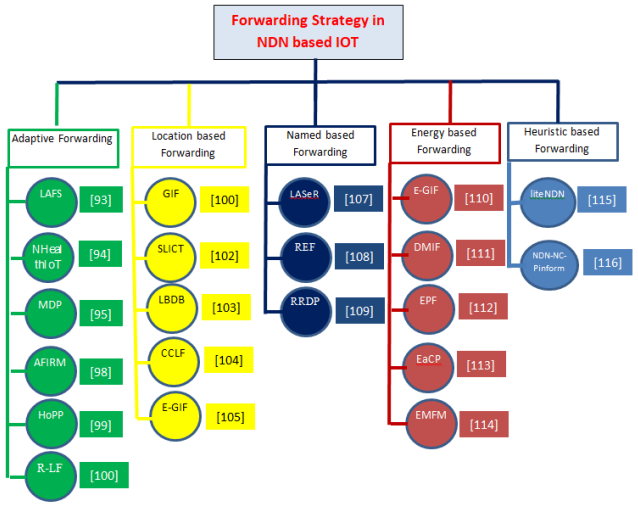

FIGURE 6. NDN forwarding strategies.

IV. TAXONOMY OF THE NDN FORWARDING STRATEGIES FOR IoT

A major problem with IoT networks is forwarding, and forwarding protocols are thought to be the primary cause of route discovery and maintenance. In this section, this paper looks at and provides a taxonomy of the many NDN-based IoT solutions (Figure 6) that have been put forth in the literature [50]. In adaptive forwarding, the Data packet's optimum route is found and used to send data efficiently and with the lowest amount of delay. The position data of nearby nodes or destination nodes are used in location-based forwarding to increase the effectiveness of forward search. Name based forwarding allows overriding the forwarding table and defining the outgoing or egress interface in accordance with particular criteria, such as the names of the consumer and producer or the kind of traffic. Interest and data packets are aware of a variety of factors in aware forwarding, including the next hop, neighbor nodes, and the network, the context in which the packet is communicating, which includes location, energy, and provider nodes. Meanwhile, heuristic based forwarding finds a better, albeit not necessarily optimal, route to a destination by employing particular methods. The software running on networking electronics can determine a different route to the desired destination via an alternative open path when a disruption in network topology occurs.

A. ADAPTIVE-BASED FORWARDING

A table providing a brief summary of all the adaptive-based forwarding strategies reviewed in this paper is presented in Table 1 and their detailed description are as follows.

In [91], the researcher propose the Learning-based Adaptive Forwarding Strategy (LAFS) as a forwarding strategy for NDN-based IoT networks. LAFS improves the performance of network when reducing resource consumption. The suggested technique depends on the learning process which offers the essential knowledge for network nodes to interact intelligently, and provide a lightweight and adaptable forwarding mechanism that is well suitable to IoT contexts. The LAFS protocol can be simulated in ndnSIM and evaluated by comparing to current NDN forwarding techniques. However, the proposed strategy has heavy bandwidth cost.

For the purpose of forwarding emergency events traffic of a NDN-based IoT healthcare network, Saxena and Raychoudhury [92] suggested an adaptive forwarding approach, named Cdf. In this research used three context parameters: prefix forwarding status, signal quality, and packet type, which are integrated and calculated as part of the forwarding process using the Cdf approach. Whether a packet is for an emergency event or a regular packet, the packet type indicates the sort of traffic. The Signal-to-Noise Ratio (SNR) can be used to determine resource availability by comparing the signal quality (low or high). Prefix forwarding status is provided for every forwarding of the Interest packet entry for each interface, and provides three status values (i.e., bad, good, or average) for representing link performance, according to Round-Trip-Time (RTT) for the specific forwarding Interest packet entry. The values of these parameters act as condition attributes for the execution of the related rule and the Cdf forwarding decision. In order to forward emergency event traffic, the authors set up a number of requirements based on the attribute values, such as sending emergency traffic to all interfaces with reasonable RTT regardless of the signal quality. This study used Sent Data, Sent Interests, Remaining energy, Hop count, Success rate and Retrieval time as a evaluation matrices for comparing to another NDN forward

TABLE 1. Forwarding strategy based on adaptive.

REF	Name (Year)	Specific Issue	Findings	Algorithm	Implementation	Limitations
[91]	LAFS (2021)	Broadcast storm problem	This study presented a Learning-based Adaptive Forwarding Strategy (LAFS) for NDN-based IoT networks.	Learning algorithm	Simulation using (ndnSIM)	The proposed strategy has heavy bandwidth cost.
[92]	NHealthIoT (2019)	Securing the sensors	The NHealthIoT uses pure-NDN-based M2M communication for capturing and transmission of raw sensor data to the home server which can detect emergency healthcare events using Hidden Markov Model.	Publish and subscribe and push	ndnSIM	In this strategy increase overhead of exchanged packets
[93]	MDP (2018)	Latency	This study proposed a Markov Decision Process (MDP) based Interest scheduling for IoT traffic with varying priorities and measure the performance with different traffic probabilities.	Push Model	Matlab	Mobility in this strategy has not been provided, because it is assumed that IoT devices are fixed
[96]	AFIRM (2018)	Mobility	The researcher proposed a novel and efficient forwarding algorithm named AFIRM in order to support producer mobility.	Link recovery, routing and signaling	OMNeT++	The proposed strategy has network overhead
[97]	HoPP (2018)	Mobility	This study contributed HoPP, a robust publish-subscribe scheme for typical IoT scenarios that targets IoT networks consisting of hundreds of resource constrained devices at intermittent connectivity.	Lightweight routing and publish-subscribe Approach	RIOT and CCN-lite	Latency during this strategy has been not considered.
[98]	R-LF (2019)	Reducing transmission overhead	This study presented a lightweight forwarding strategy for Named Data Networking (NDN) over IEEE 802.15.4. NDN is an ICN architecture with a great potential for the IoT and future Internet.	Reinforcement learning technique	OMNeT++ simulator	Energy consumption in this proposed work has been not considered.

strategy. However, the drawback of this study is Increase overhead of exchanged packets

A Markov Decision Process (MDP) based scheduler for the forwarding technique was proposed by Muralidharan et al. [93], [94], which takes into account the type of interest or requested message. The based scheduler satisfies the delay requirements by selecting good interfaces having low RTT values to fetch Data in accordance with the traffic information it has acquired. The forwarding strategy in [95] is likewise an MDP-based forwarding strategy that uses a comparable methodology to move Interests to the optimal interfaces in order to enhance QoS in NDN. The majority of IoT applications, however, require delay-tolerance, which was not taken into account. In order to overcome this problem, Muralidharan et al. in this research, the traffic Interests are divided into three categories: query-based traffic with medium priority, event-based traffic with low delay requirements, and periodic traffic without any latency requirements. The namespace contains the Interest packet type. The IoT traffic type, channel condition, delay precondition factor, and RTT are all taken into consideration by the scheduler when estimating the state transition probabilities. The scheduler adjusts the interface ranking, or applies the forwarding decision, for each message that is received. The MDP strategy was simulated in matlab and evaluation matrices used for this study are Packet type, prefix forwarding status and signal quality for comparing to another NDN forward strategy. However, the limitation of this strategy is mobility, because it is assumed that IoT devices are fixed.

An adaptive forwarding-based forwarding technique which tackles the problems of mobility and data availability is called adaptive forwarding based link recovery for mobility support (AFIRM) by Meddeb et al. in [96]. For NDN architecture, AFIRM is a completely distributed, adaptable, and content-driven algorithm. The packet loss brought on by the producers' motion is decreased by AFIRM. The AFIRM strategy was simulated in OMNET++ and evaluation matrices used for this study are Link recovery, routing and signaling for comparing to another NDN forward strategy. However, the drawback of this study is Network overhead.

Gündogan et al. in [97] propose HoP-and-Pull (HoPP), a reliable publish-subscribe method for common IoT situations that focuses on intermittently connected IoT networks made up of hundreds of resource-constrained devices. This method keeps the number of FIB to a minimum and provides reactivity in close to real time, mobility,

TABLE 2. Forwarding strategy based on location.

REF	Name (Year)	Specific Issue	Findings	Algorithm	Implementation	Limitations
[99]	GIF (2019)	Data retrieval latency	The researcher proposed a novel geographic interest forwarding scheme where add support for push-based traffic and different forwarding techniques.	Geographic Location	ndnSIM	In this strategy when each node shares its private information, the security barrier is breached.
[26]	SLICT (2016)	Secure forwarding	This study proposed an ICN-compliant and secures implementation of geographic forwarding for ICN.	Geographic forwarding mechanism	RIOT	SLICT's effectiveness is not measured in terms of the total number of Interest packets sent over the network
[101]	LBDB (2019)	Broadcast storm issue and broadcast collisions	In this study a Location-Based Deferred Broadcast (LBDB) scheme is introduced to improve the efficiency and performance of interest broadcast in ad-hoc NDN.	Deferred Broadcast	ndnSIM	Energy consumption and throughput decrease the satisfaction ratio
[102]	CCLF (2020)	Mobility	This study proposed a forwarding strategy called Content Connectivity and Location-Aware Forwarding (CCLF) for NDN-based MANETs.	Geographic Location	ndnSIM	The total number of Interest packets sent in the network is not used to measure the effectiveness of CCLF
[103]	E-GIF (2019)	Energy consumption	This study proposed a power saving extension for the Geographic Interest Forwarding (GIF) protocol.	Sleep mode function	ndnSIM	The total number of Interest packets transmitted over the network is not used to evaluate E-GIF efficiency
[104]	GIF (2016)	Network overhead	This study proposed a Geographic Interest Forwarding scheme called GIF, for NDN-Based WSNs.	Push and Pull-based mode	ndnSIM	In this proposed work, due to the extensive network discovery processes, it is not appropriate for small networks.

temporary network splitting, and data aggregation by default. With a variety of limited devices connected through IEEE 802.15.4 wireless LoWPANs on the IoT-Lab testbed, the protocol in a real-world deployment was experimentally assessed. Implementations facilitated experiments utilizing various single-hop and multi-hop situations built on CCNlite with RIOT, and the evaluation matrices used for this study are Performed well in the majority of experiments, robust, and resilient for comparing to another NDN forward strategy. However, the limitation of this strategy is latency.

Meanwhile, Abane et al. in [98] proposed an NDN-based low-end IoT forwarding approach that uses a reinforcement learning method to alter a forwarder node's waiting period before broadcasting the Interest packet. The protocol does not require any extra packets or data structures as a result, with the exception of a cost field which is loaded in both Interest and Data packets, and this indicates a node's distance from eligibility and the provider to send an Interest packet. This suggested approach uses a reinforcement learning algorithm at each forwarding node, that necessitates a large amount of processing power to maintain this machine learning algorithm (at every packet exchange). As a result, this strategy is not suggested for IoT devices with minimal processing capabilities. The R-LF strategy was simulated in OMNET++ and evaluation matrices used for this study are hop count, satisfaction-rate, and latency for comparing to another NDN forward strategy. However, the drawback of this study is energy consumption.

B. LOCATION-BASED FORWARDING

A table providing a brief summary of all the location-based forwarding strategies reviewed in this paper is presented in Table 2 and their detailed description are as follows.

Location aware: For NDN-based IoT, Aboud et al. suggested a greedy Geographic Interest Forwarding (GIF) system in [99]. A Producers discovery phase is started by content producers to introduce themselves to consumers via HELLO messages, providing the sender's ID and coordinates, while a Neighbors discovery phase is started by content producers to introduce themselves to consumers before executing Data searches. It is worth noting that the suggested forwarding technique requires node geo-coordinates in addition to an extra packet type (HELLO message), that can be resource-intensive, especially in the case of a mobile IoT network with limited resources. The proposed strategy was simulated in ndnSIM and evaluation matrices used for this study increased data delivery effectiveness and better use of network resources for comparing to another NDN forward strategy. However, the drawback of this study, when each node shares its private information, the security barrier is breached.

GEO aware: Secure Localized Information Centric Things (SLICT) is presented in [26], which is a method that performs secured forwarding depending on geographic location in IoT deployments. In order to ensure that packet communication only occurs with nodes that are permitted and trusted, SLICT is the method which associates and discovers the neighbors. SLICT is a secure beaconing system that manages

changes in topology and position. The SLICT naming method validates independent geographic interest forwarding through the network. A forwarding framework that operates in ICN-based WSN is taken into consideration by SLICT. The majority of geographic mechanisms is built on a forwarding strategy based on greed. This mechanism offers a greedy forwarding strategy based geographic routing method that is not included in the advanced toolkits of today, such as Contiki and RIOT. The GPSR employs a perimeter routing strategy to steer clear of nearby maxima. The coordinates of the node where the packet entered perimeter mode must be carried in the packet when using this technique. The SLICT program has a field called Type Length Value (TLV) that it stores coordinate data and a flag that indicates whether the GPS receiver is in perimeter mode or greedy mode. The SLICT method is employed in a variety of application settings, including dense deployment in big metropolitan structures and sparse deployment in expansive rural areas. The SLICT strategy was simulated in RIOT and evaluation matrices used for this study are Network overhead, memory and computation overhead, Total energy consumption. However, the SLICT's effectiveness is not measured in terms of the total number of Interest packets sent over the network

Ad hoc NDN networks are given a Location-Based Deferred Broadcast (LBDB) strategy proposed by Kuai et al. in [100]. In the Interest dissemination phase, a collision avoidance timer is employed to reflect the forwarding priority of a node and is mostly based on the forwarding node's location information and data sources. The objective is to reduce transmission overhead and hence delay in data delivery. It is believed that this proposed forwarding strategy contradicts the NDN concept, specifically the data-centric communication paradigm, because it is based on the location of the nodes, particularly the data sources. Geo-coordinates are also insufficient for IoT networks with limited resources. The proposed strategy was simulated in ndnSIM and evaluation matrices used for this strategy are Average Hops, Normalized Transmission Overhead, Average Delay, and Satisfaction Ratio for comparing to another NDN forward strategy. However, the drawback of this study is energy consumption and throughput decrease the satisfaction ratio.

For NDN-based MANETs, Chowdhury et al. [101] suggested a forwarding technique known as Content Connectivity and Location ware Forwarding (CCLF). As that each node independently decides whether to forward packets based on per-prefix performance measures and any available geo-location data, CCLF broadcasts NDN packets. A density-aware suppression method is used by CCLF to cut down on pointless packet transmissions. For ad hoc links, CCLF employs a link adaption layer to fill the gap between CCLF and the actual link's capabilities. Each node that gets an Interest sets a forwarding timer, and when the timer expires, the Interest is forwarded. The timing is set up such that nodes with stronger interest-related content connectivity and closer proximity to the data location will have a higher likelihood of transmitting the Interest. Before its timer expires, if a node hears another node transmit the Interest, it will likely suppress its own forwarding with a probability proportionate to the number of neighbors within its transmission range. This concept, which aggregates intelligence without altering ICN fundamentals, is intriguing. The proposed strategy was simulated in ndnSIM and evaluation matrices used for this strategy are Protocol overhead, satisfaction ratio, and delay stretch for comparing to another NDN forward strategy. However, the total number of Interest packets sent in the network is not used to measure the effectiveness of CCLF.

Aboud et al. in [102] suggested an addition to the Geographic Interest Forwarding (GIF) protocol that saves power. A cross-layer technique is employed in the proposed E-GIF scheme to enable direct communication between protocols at dissimilar layers. In order to integrate the sleep mode into the forwarding decision of the sensor nodes that use the NDN protocol stack, the interactions between the MAC and routing layers are specifically and extensively exploited. The researcher provides wireless multi-hop communication capability to the ndnSIM simulator to test the proposed system. However, the drawback of this strategy is the total number of Interest packets transmitted over the network is not used to evaluate E-GIF efficiency.

For NDN-based WSNs, Aboud in et al. [103] proposed the Geographic Interest Forwarding (GIF) system. This plan is centered on avoiding flooding tactics because they are resource-blind, which can significantly reduce network overhead. Additionally, a number of energy-efficient strategies, such as packet suppression and broadcast storm avoidance, are suggested to reduce and balance energy consumption. The outcomes unambiguously demonstrate that in terms of data retrieval time, the GIF NDN-based system performs better than the directed diffusion NDN-based method. The findings further demonstrate that employing the GIF system minimizes the overall energy consumed because Interest packets are never inundated but are instead routed through the neighbor with the best combination of proximity to the destination and remaining sensor power. However, this study due to the extensive network discovery processes, it is not appropriate for small networks.

C. NAMING-BASED FORWARDING

A table providing a brief summary of all the naming-based forwarding strategies reviewed in this paper is presented in Table 3 and their detailed description are as follows.

Travis et al. [104] presented a reactive routing method that is comparable to RPL for IoT in another work named "LASeR: Lightweight authentication and secured routing for NDN IoT in smart cities". IoT makes this technique lightweight. The three steps in onboarding and routing are network discovery and authentication, node authentication, and path advertisement. In contrast to reactive systems, simulation results showed that LASeR solely employs broadcast for initial neighbor discovery. Although this study does not address routing between anchors and gateways, it is believed that alternate approaches, such as a link-state

TABLE 3. Forwarding strategy based on name.

REF	Name (Year)	Specific Issue	Findings	Algorithm	Implementation	Limitations
[105]	LASeR (2017)	Security	This study proposed and evaluated a novel, scalable framework for lightweight authentication and hierarchical routing in the NDN IoT.	Cryptographic materials and primitives and cryptographic materials and primitives	ndnSIM- Ns3	The limitation of this strategy is inefficient in packet retrieval time
[106]	REF (2021)	Data packets and interest packets being duplicated	This study proposed a new forwarding strategy: redundancy elimination forwarding (REF)	Redundancy elimination approach	ndnSIM	Energy consumption in this proposed work has been not considered.
[107]	RRDP (2022)	Redundant data packets	This study designed a data packet forwarding strategy suitable for NDMANET named Reduce Redundant Data Packets (RRDP) strategy.	Require ACK-Counters	ndnSIM	This strategy only compared with flooding strategy

protocol, will be adopted. The LASeR strategy was simulated in ndnSIM and evaluation matrices used for this study are Distance and Density. However, the limitation of this strategy is inefficient in packet retrieval time.

Meanwhile, Dehaghani et al. in [105] suggested a new forwarding method named Redundancy Elimination Forwarding (REF). The NDN node structure and how the data structure functions are changed in REF. Investigations were made into the issue of redundancy duplication in NDN wireless networks' forwarding techniques. REF, a new forwarding tactic, was introduced to accomplish two goals: (1) prevent the repetition of Interest packets, and (2) offer a quicker mechanism for packet processing and forwarding. The throughput, resource needs, and overhead of the network are all improved by these changes. The REF approach is simulated using ndnSIM in several scenarios, and the results reveal that it offers reliable performance in a range of settings. However, the drawback of this protocol is energy consumption.

Similarly, Zhang et al. proposed in [106] the Reduce Redundant Data Packets (RRDP) method, which is a data packet forwarding approach appropriate for NDMANET that tries to stop redundant packets from being forwarded at the intermediate node. On the assumption that the success rate of customer requests remains mostly unchanged, this method can reduce the transmission of redundant packets and reduce network traffic to the absolute minimum. This approach is more suited to NDMANETs with minimal node storage and constrained computation capacity because it is straightforward and inexpensive to deploy. The RRDP strategy was simulated in ndnSIM and evaluation matrices used for this study are consumer request successful ratio (CRSR) and total number of data packet transmissions (TDPT). However, this strategy only compared with flooding strategy.

D. ENERGY-BASED FORWARDING

A table providing a brief summary of all the energy-based forwarding strategies reviewed in this paper is presented in Table 4 and their detailed description are as follows.

In [107], the investigator demonstrates an NDN over IEEE 802.15.4 communication systems which satisfies the needs of monitor and control of IoT applications that require minimum power consumption and minimum data rates. A dependable energy-aware forwarding strategy selects the next hop forwarder based on its residual energy level, and a sleep mode scheduling algorithm plans the sleep/wake-up mode according to the function of the node in the forwarding and path repair operations. In this algorithm, the energy consumption, retrieval delay, delivery ratio, and scalability are employed as evaluation matrices. However, the drawback of this protocol is energy consumption.

Gao et al. in [108] for NDN-based WSNs presented an energy-efficient Dual Mode Interest Forwarding (DMIF) method. DMIF employs a number of strategies to raise the effectiveness and energy efficiency of the suggested solution. However, because it keeps track of every node that has been traversed and includes this information in each interest packet that is transmitted, the DMIF system does not scale effectively in large-scale networks. As a result, packet fragmentation is inevitable due to the 802.15.4 protocol's maximum allowed packet size. As a result, the suggested approach is not effective in packet retrieval time and is therefore inappropriate for real-time applications.

In order to improve high priority packet transmission and energy usage, Tariq et al. in [109] suggested an Energy efficient Priority Forwarding (EPF) their work. This method makes use of the SDN controller's capability in an NDN-IoT scenario. In the study, a 16% energy barrier was set as the minimum for low priority packet transmission. The packet is forwarded using the defer window, which

TABLE 4. Forwarding strategy based on energy.

REF	Name (Year)	Specific Issue	Findings	Algorithm	Implementation	Limitations
[107]	Energy aware forwarding strategy (2022)	Energy consumption	This study proposed interesting energy saving functionalities, to take full advantages of a reliable energy-aware forwarding strategy that selects the next hop forwarder based on its residual energy level and a sleep mode scheduling algorithm that schedules the sleep/wake-up mode.	Sleep mode	ndnSIM	Latency in this proposed work has been not considered.
[108]	DMIF (2016)	Broadcast storm and energy consumption	This study presented an energy-efficient Dual Mode Interest Forwarding (DMIF) method.	Hybrid algorithm	ndnSIM	Very specific static scenarios are evaluated and do not take mobility into consideration, and it is inefficient in packet retrieval time
[109]	EPF (2020)	Energy consumption and Broadcast storm problem	This study proposed an Energy efficient Priority Forwarding that take advantage of the combination of NDN and SDN in IoT environment	SDN	EPF in ndnSIM	Security performance has not been investigated
[72]	EaCP (2021)	Energy consumption	This study proposed an Energy-aware caching placement scheme (EaCP) that aims to maximize the energy-saving by trading-off between content transmission energy and content caching energy.	Energy-aware heuristic algorithm	Python language	The total number of interest packets transmitted over the network is not used to evaluate EPF efficiency
[110]	EMFM (2021)	energy consumption	This study is to propose a forwarding mechanism called EMFM to forward incoming interest packets in order to reduce the usage of energy.	Multipath Forwarding Mechanism	ndnSIM	This strategy only compared with OEFS (On-demand Energy-based Forwarding Strategy)

compares the priority of the packet with the name prefix. Additionally, effective broadcast storm mitigation is accomplished. In terms of Content Retrieval Delay, Total Number of Interests, and Average Energy Consumption, the proposed approach performs better than both floods and GIF. However, the limitation of this strategy has Security issues.

Meanwhile, the EaCP technique was suggested by Serhane et al. in [72] to increase the energy effectiveness of IoT-based ICN networks. In order to attain a higher position for content placement, EaCP often balances the cost of caching and the cost of transmission. In order to achieve this, the node position, content popularity, and content transmission and caching energy were taken into account. The distributed optimal placement setting is what the EaCP algorithm seeks to achieve. Additionally, taking into account several metrics were run through a thorough simulation. The findings collected demonstrated the efficacy of strategies in terms of energy conservation, cache utilization, and a significant increase in the cache hit ratio. It was observed that the EaCP approach can significantly minimize communication overhead while extending battery life of IoT devices. The next stage of this work focuses on adapting real-world conditions, such as mobility, in order to enhance the EaCP architecture. A clever deep learning model can be used in this circumstance to forecast and extract energy of IoT users' rewards for mobile nodes. However, the total number of interest packets transmitted over the network is not used to evaluate EPF efficiency is the limitation of this study.

Also, S. Hassan and M. Alsamman in [110] suggest an energy-aware multipath forwarding mechanism (EMFM) to advance incoming Interest packets in order to lower node energy consumption and prolong the lifespan of the network. In order to forecast subsequent forwarding hops in the overall packet transmission process, EMFM takes into account nodes and their associated battery and PIT size. Using the ndnSIM tool, a simulation was run to build and assess the EMFM and compared it to the on-demand energy-based forwarding strategy (OEFS). The results of this investigation clearly showed that EMFM can prolong NDN wireless nodes' network lifetimes by evaluating the network performance of EMFM in terms of data redundancy, content download time, and network energy consumption. However, it's compared only to OEFS (On-demand Energy-based Forwarding Strategy).

TABLE 5. Forwarding strategy based on Heuristic.

REF	Name (Year)	Specific Issue	Findings	Algorithm	Implementation	Limitations
[111]	liteNDN (2020)	Packet delivery time and network traffic	This study introduced liteNDN, a novel forwarding and caching strategy for NDN networks.	Most probable path (MPP)	Mini-NDN network emulator	Security and energy consumption have been not considered
[112]	NDN-NC-Pinform (2017)	Latency	This study proposed a probability-based multipath forwarding strategy for efficient distribution of escalating data volumes in a large-scale IoT application	Probability multipath forwarding	ndnSIM	Total number of Interest packets sent in the network is not used to measure in this strategy

E. HEURISTIC-BASED FORWARDING

A table providing a brief summary of all the heuristic-based forwarding strategies reviewed in this paper is presented in Table 5 and their detailed description are as follows.

M. Abdelaal et al. in [111] provide liteNDN, a cutting-edge caching and forwarding method for NDN networks.

In liteNDN, NDN routers cooperate to forward packets in the most efficient way possible by sharing their knowledge of data names and interfaces. Then, liteNDN makes use of this information to quickly acquire the required data by estimating the likelihood of each downstream path. Additionally, liteNDN uses heuristics like routing costs and data relevance to decide when to cache segmented packets as well as regular packets. The proposed method has undergone a thorough evaluation in terms of network usage, cache hit rate, and data retrieval latency. The findings demonstrated that liteNDN can lower the superfluous traffic, as well as significantly lessen delay and caching activities, as compared to traditional NDN forwarding and caching schemes. The proposed strategy was simulated by Mini-NDN network emulator and evaluation matrices used for this study are Throughput and data retrieval latency. However, the limitations of this study are security and energy consumption.

Meanwhile, Lei et al. in [112] created a probability-based multipath forwarding strategy for efficient distribution of escalating data volumes in a large-scale IoT application (e.g., video streaming in 5G), by investigating an NDN streaming media system implemented in the ndnSIM simulator that incorporates network coding. The experimental findings unequivocally show that network coding can considerably boost performance, reliability, and QoS in 5G NDN. In addition, this is a universal solution because it works with most cache techniques. More importantly, this strategy has great promise for offering expanding IoT applications, such as premium streaming video services. This strategy was simulated in ndnSIM and evaluation matrices used for this study are Network Transmission Efficiency and Cache Hit Ratio. However, the total number of Interest packets sent in the network is not used to measure in this strategy.

In table 6 a comprehensive performance analysis of existing solutions in literature is provided with respect to number of parameters such as performance, resource consumption, energy consumption, security, scalability, and mobility.

V. DISCUSSION AND STATISTICAL ANALYSIS FOR NDN-BASED IoT NETWORKS

The existing schemes are compared and statistically analyzed in this section. The factors used, such as the specific challenge, assessment metrics, network simulation, and publishing year, can be used to enhance the IoT data networking forwarding strategy.

A. BEST REAL-WORLD IoT SCENARIOS

Adaptive-based forwarding is best for smart Grid and Traffic Monitoring because it's able to transmit data effectively and with the least amount of delay, the best route for the Data packet is identified and used.

Location-Based Forwarding is best for transportation and healthcare, this category uses the position data of neighboring nodes or destination nodes to improve the efficiency of forward search.

Naming-Based Forwarding is best for Smart Home, Wearables, this approach enables to override the forwarding table and define the outgoing or egress interface based on specific criteria such as the names of the consumer and producer or the type of traffic.

Energy-based forwarding is best for health care, smart farming, and industrial IoT-based scenarios, this strategy enables to reduce the energy consumption of the nodes and thus increases the lifetime of the network; therefore, more nodes have enough power and transmit more data packets.

Heuristic-based forwarding is best used in smart city scenarios because that knowledge to estimate the probability of each downstream path to swiftly retrieve the requested data. Additionally, it's exploits heuristics, such as routing costs and data significance, to make proper decisions about caching normal as well as segmented packets.

B. BY SPECIFIC CHALLENGE

Numerous issues exist with NDN implementation in the IoT environment, such as network overhead, latency, mobility, the

TABLE 6. Performance analysis in forwarding strategy.

Taxonomy	REF.	Name	Objectives					
			Performance	Resource consumption	Energy consumption	Security	Scalability	Mobility
Forward strategy based on Adaptive	[91]	LAFS (2021)	L	L	L	NM	H	NM
	[92]	NHealthIoT(2019)	L	NM	NM	H	H	Yes
	[94]	MDP (2018)	L	NM	NM	H	L	NM
	[96]	AFIRM (2018)	L	H	H	H	H	Yes
	[97]	HoPP (2018)	L	H	H	H	L	Yes
	[99]	R-LF (2019)	L	H	H	H	H	Yes
Forward strategy based on Location	[26]	GIF (2019)	L	L	L	L	H	NM
	[26]	SLICT (2016)	H	L	L	H	H	NM
	[100]	LBDB (2019)	L	H	H	NM	L	Yes
	[101]	CCLF (2020	L	H	H	H	L	No
	[102]	E-GIF (2019	L	L	L	L	H	NM
	[103]	GIF (2016)	L	L	L	L	H	Yes
Forward strategy based on Name	[104]	LASeR (2017)	L	L	L	H	H	NO
	[105]	REF (2021)	L	L	L	H	H	Yes
	[106]	RRDP (2022)	L	L	L	NM	H	Yes
Forward strategy based on Energy	[108]	Energy aware forwarding strategy (2022)	L	L	L	L	H	No
	[109]	DMIF (2016)	H	L	L	NM	H	No
	[109]	EPF (2020)	L	L	L	L	H	No
	[72]	EaCP (2021)	NM	L	L	NM	L	Yes
	[110]	EMFM (2021)	L	L	L	NM	H	Yes
Heuristic based on Forwarding	[112]	liteNDN (2020)	L	H	H	L	L	No
	[112]	NDN-NC-Pinform (2017)	L	NM	NM	NM	H	NM

H: High, L: Low, NM: No Mentioned

broadcast storm problem, security, and redundant data. The distribution of potential issues in NDN-based IoT networks is depicted in Figure 7. We can see that 22% of the NDN-based

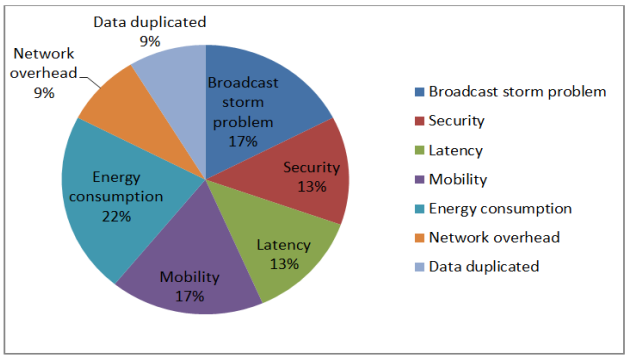

FIGURE 7. Distribution of specific challenges.

IoT system research covered in this study deal with the energy consumption issue. This is followed by both the broadcast storm problem and mobility problem with 17%, both latency and security with 13%, and only 9% deal with network overhead and data redundancy. This can be justified by the fact that in IoT NDNs, broadcast is the simplest and most popular strategy for content distribution. As a result, the majority of articles seek to mitigate the issue of energy consumption by offering a method to control the broadcast. It is important to note that the routing issue in NDN-based IoT system is associated to both the broadcasting and network environment as well.

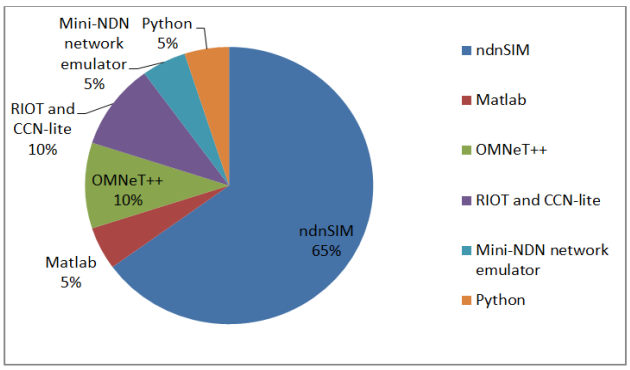

FIGURE 8. Evaluation metrics distribution in this study.

C. BY METRICS

The distribution from the most popular metrics in simulation evaluation studies for NDN-based IoT network forwarding protocols is shown in Figure 8. The biggest problem with IoT applications, especially those that require timely data, is retrieval delay. Due to this, a lot of research studies concentrate on assessing how forwarding technique affects data retrieval delay. It can be observed that data retrieval delay is used as a parameter in 20% of the reviewed publications to assess the proposed NDN-based IoT. Since achieving energy consumption is the primary objective of any NDN-based IoT, it is represented by 16% of the reviewed works. The NDN-based IoT systems research also evaluated the effectiveness of NDN-based IoT forwarding mechanisms by taking another

metrics into account, like hop count with a percentage of 12%, followed by the number of interest packets, interest lifetime, and retrieval time with 10% each, and network overhead with a figure of 8%. Throughput, remaining energy, and success rate are all about 4% each.

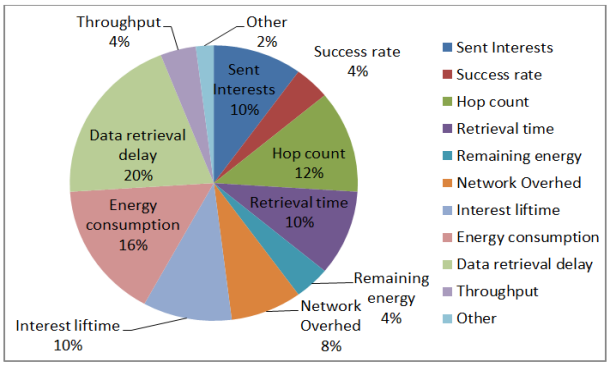

FIGURE 9. Simulators network distribution.

D. BY SIMULATION

This paper's analysis leads to the conclusion that, as indicated in Figure 9, the majority of the surveyed publications (65%) employ the ndnSIM simulator. It may be supported by the fact that ndnSIM is the only simulator that comes pre-implemented with the NDN primitives, is open source, and is simple to use. In addition to ndnSIM, 10% of the articles surveyed in this survey also used NDN-based IoT algorithms built on OMNeT++. In addition, three more simulators, Matlab, Mini NDN, and Python, are used in 5% of NDN-based IoT investigations.

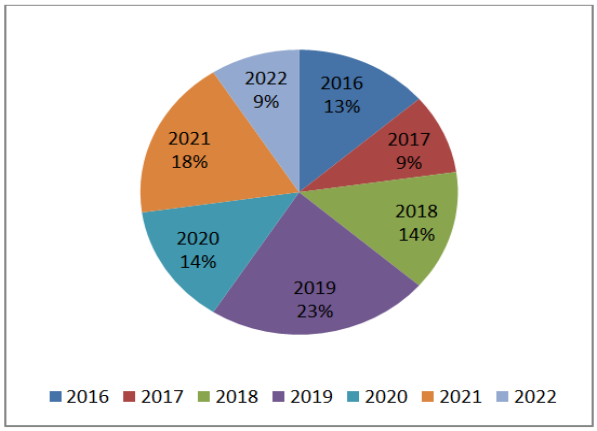

FIGURE 10. Publications distribution per years.

E. BY PUBLICATION

Many attempts have been made to modify and enhance NDN architecture in IoT systems to enable communications effectively when the Internet transitioned from being connection-driven to content-driven. As shown in Figure 10, only 13% of papers that were assessed in 2016 suggested a better forwarding method for NDN-based IoT. In 2017, this percentage dropped by 4% from 2016. Since then, the research community has been aware of the forwarding difficulty associated with installing NDN over IoT, and the percentage has climbed, reaching 14% in 2018 and 23% in 2019. However, as compared to 2018, the number is similar in 2020. This is because a sizable portion of the research community has turned its attention to other NDN-based IoT network problems that present design challenges for concrete NDN-based IoT architectures, such as security, caching, and naming. In 2021, this percentage increased by 4% from 2020. Additionally, in 2022, publications will make up 9% of the total. Given that forwarding continues to pose a barrier to the design of an effective and reliable communication in NDN-based IoT networks, in the upcoming years, we anticipate more study papers to be generated by the research community.

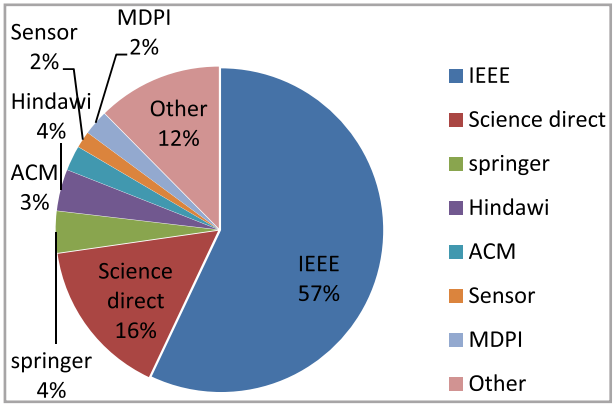

FIGURE 11. Publications distribution per journal type.

Moreover, this paper utilized 120 references in this survey. As shown in Figure 11, only 57% of the papers were published in IEEE journals, 16% in Science direct journals, 3% is assessed in ACM conferences, both Hindawi and Springer journals only published 4%. MDPI and sensor both make up only 2%. In addition, 12% were gathered from other journals in this paper.

VI. FUTURE RESEARCH DIRECTIONS

In this section, this paper highlights the crucial areas where various research and regulatory groups must participate and contribute in order to enhance the overall NDN forwarding strategy.

A. OPEN ISSUES

The key benefit of using NDN as a communication mechanism for the IoT is the expansion of content accessibility within the network. A significant issue still exists in designing an effective message forwarding system for IoT via NDN. It has taken a lot of work to improve the NDN-based IoT forwarding strategy and effectively enable enhanced communications. However, there are still some issues with NDN-based IoT forwarding that need to be addressed. These

issues need the research community's attention. The issues are presented, discussed, and some potential remedial actions are highlighted in the sections that follow.

1) Energy and power of mobile and sensor nodes: Developing a generic forwarding approach for all types of wireless networks involves yet another challenge. IoT is increasingly energy-constrained as a result of the denser deployment of sensor nodes. After such a massive deployment, power consumption of the sensor nodes is a significant problem. The sensor network batteries cannot be recharged or changed. In order to increase the network's overall efficiency, it is essential to design energy and power efficient sensor nodes. Energy threshold limitations can control energy consumption in particular situations, whereas energy harvesting techniques are sometimes utilized for energy efficiency.
2) Channel restrictions: Interest packets are broadcast from consumer nodes, thus broadcast storms are quite likely. It is necessary to have a bandwidth-efficient and reliable channel in order to support mitigation techniques and guarantee fault-free transmission.
3) Data producer mobility: When a user switches from one network to another, they may just re-request any content they may have missed. However, the content provider's mobility is a difficult problem.
4) Security: IoT services are not accessible to the general population for information retrieval. Therefore, using access-control over the object, authenticated consumer interests should be applied in this situation. Additionally, the majority of IoT devices have limited CPU and memory capacities due to resource constraints, making it challenging to use public key cryptography. Thus, adaptable and lightweight cryptosystems with affordable confidence models are needed.

B. FUTURE DIRECTION

Despite these obstacles, NDN forwarding strategy-based IoT adoption is growing, as more individuals become aware of the research and development being done in this field. IoT built on the NDN forwarding approach will develop further. The following is a list of some IoT future detections based on NDN forward strategy:

1) EDGE/FOG COMPUTING

The way that companies gather, store, handle, and move data is changing as a result of decentralization in computing. Emerging architectures are placing compute and storage resources outside of the data center and closer to the locations where data is gathered, as opposed to housing everything in a single large data center [113], [114].

The main idea of using NDN-based IoT with edge/fog devices is that IoT devices should regularly gather and upload sensed and captured data to edge devices for processing and caching. Other IoT devices can take advantage of NDN's benefits in this way to swiftly retrieve data from the best edge/fog device, i.e., using FIB and request aggregation of NDN to reduce the costs and delays associated with data communication. IoT devices have the ability to exchange data from a middle device handling request aggregation.

2) BLOCKCHAIN TECHNOLOGY

Blockchain technology, which is well-known for being a technological revolution, is generating exceptional optimism and attention. The account of all transactions is kept in the distributed digital ledger, which is made up of blocks of encrypted, signed transactions. By providing copies of records to each participant, the Blockchain approach does away with the need for a centralized authority [115].

The flexibility and effectiveness of the NDN are significantly influenced by the forwarding strategy. A set of guidelines and regulations for the transfer of Data and Interest packets are known as forwarding strategies. When certain circumstances exist, such as when the uplinks are crowded or when it is questioned whether a particular Interest packet is a component of a DoS assault, the forwarding strategy may also decide to drop the packet of Interest. Therefore, using blockchain technology in NDN forwarding strategy can resolve this issue.

3) SDN

The optimal solution for supplying the NDN networks' lacking intelligent centralized control and programmability is Software-Defined Networking (SDN) [116].

Incoming Interests are efficiently redirected to off-path routers that have the desired content cached by the SDN controller after an analysis of network status. By enabling both NDN consumer and NDN routers to fetch the content from numerous off-path locations dependent on the network conditions, utilizing SDN with NDN forwarding strategy can improve the data retrieval process in some circumstances. Additionally, by dispersing Interests across a variety of open pathways, it assures congestion avoidance on a particular path.

4) MACHINE LEARNING

Systems can closely scrutinize data using machine learning (ML), which allows for knowledge to be inferred that goes beyond merely studying or extracting it for use and development over time [117], [118]. Grouping, classification, regression, and rule extraction are just a few of the different issue types that machine learning can be used to solve.

Recently, there has been a lot of interest in NDN's machine learning-enabled growth. Some study uses machine learning techniques for forwarding or routing purposes. Implementing machine learning in NDN may be able to address issues like interest flooding overhead, increased maintenance costs for routing information, network intricacy, a variety of application demands, etc [119], [120].

The NDN system still occasionally has issues, despite being touted as an alternative to IP-based design. These

issues are more concerned with the architecture's efficiency. To address new or current issues that arise at NDN, particularly in the routing and forwarding mechanisms, ML-based NDN is now available. The topics have a lot of potential for growth. By enabling ML-based NDN, NDN's efficiency could be improved and optimized.

VII. CONCLUSION AND FUTURE WORK

This paper provided a comprehensive analysis of forwarding techniques for NDN-based IoT literature. Then, we began the introduction of IoT ecosystems and its primary requirements. The NDN paradigm and NDN forwarding strategy have been proposed as a possible IoT alternative. A new taxonomy of NDN forwarding strategy for IoT literature was then suggested. An extensive comparative review of the current forward strategy for NDN-based IoT studies was conducted based on the suggested framework. After that, we compared and statistically analyzed the existing strategies. Despite the fact that there were fewer comparison parameters introduced than anticipated, the parameters used still offer sufficient data that can be used to enhance forwarding elements of IoT-NDN, while getting rid of some redundant solutions, and providing additional inspiration for developing a new protocol in NDN-based IoT systems. We observed which publications included in this research addressed the energy use (22%) in great detail. Additionally, ndnSIM was the most popular simulator (65%). As a result, this paper makes suggestions on open research issues that demand the community's attention. Future work in this field should concentrate on the drawbacks of various NDN forwarding strategies so that readers can generate suggestions for developing a de facto NDN forward architecture that can overcome the most severe inadequacies in existing NDN routing techniques.

The finding of our paper can be summarized into four main points. First, NDN-based IoT can be used healthcare, smart city, smart home, traffic monitoring, smart Grid, smart farming and industrial scenarios that are required. Second, NDN-based IoT forwarding strategy can classify into five categories: Adaptive-based forwarding, location based forwarding, name based forwarding, energy based forwarding and Heuristic-based forwarding. Third, We observed which publications included in this research addressed energy use (22%) in great detail. Additionally, ndnSIM was the most popular simulator (65%). Finally, several technical challenges must be overcome to increase the adoption of NDN-based IoT.

REFERENCES

[1] M. Meddeb, A. Dhraief, A. Belghith, T. Monteil, and K. Drira, "Producer mobility support in named data Internet of Things network," *Proc. Comput. Sci.*, vol. 109, pp. 1067–1073, Jan. 2017, doi: 10.1016/j.procs.2017.05.385.

[2] S. K. Datta and C. Bonnet, "Interworking of NDN with IoT architecture elements: Challenges and solutions," in *Proc. IEEE 5th Global Conf. Consum. Electron.*, Oct. 2016, pp. 1–6, doi: 10.1109/GCCE.2016.7800509.

[3] M. Amadeo, C. Campolo, and A. Molinaro, "Information-centric networking for connected vehicles: A survey and future perspectives," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 98–104, Feb. 2016, doi: 10.1109/MCOM.2016.7402268.

[4] 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, Apr. 2019, doi: 10.1109/JIOT.2018.2873343.

[5] 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, pp. 122–140, Mar. 2017, doi: 10.1016/j.adhoc.2016.12.004.

[6] K. Shah and Z. Narmavala, "A survey on green Internet of Things," in *Proc. 14th Int. Conf. Inf. Process. (ICINPRO)*, Dec. 2018, pp. 2347–2376, doi: 10.1109/ICINPRO43533.2018.9096789.

[7] M. M. F. Hamdi, A. Habbal, N. H. Zakaria, and S. Hassan, "Evaluation of caching strategies in content-centric networking for mobile and social networking environment," *J. Telecommun. Electron. Comput. Eng.*, vol. 10, nos. 2–4, pp. 1–6, 2018.

[8] A. A. Barakabitze, T. Xiaoheng, and G. And Tan, "A survey on naming, name resolution and data routing in information centric networking (ICN)," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 3, no. 10, pp. 8322–8330, 2014, doi: 10.17148/ijarcce.2014.31055.

[9] 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," *Sustainability*, vol. 12, no. 8, p. 3088, Apr. 2020, doi: 10.3390/SU12083088.

[10] A. Habbal, S. I. Goudar, and S. Hassan, "Context-aware radio access technology selection in 5G ultra dense networks," *IEEE Access*, vol. 5, pp. 6636–6648, 2017.

[11] R. Ullah, M. A. U. Rehman, M. A. Naeem, B.-S. Kim, and S. Mastorakis, "ICN with edge for 5G: Exploiting in-network caching in ICN-based edge computing for 5G networks," *Future Gener. Comput. Syst.*, vol. 111, pp. 159–174, Oct. 2020, doi: 10.1016/j.future.2020.04.033.

[12] Z. Li, Y. Xu, B. Zhang, L. Yan, and K. Liu, "Packet forwarding in named data networking requirements and survey of solutions," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1950–1987, 2nd Quart., 2019, doi: 10.1109/COMST.2018.2880444.

[13] B. Hao, G. Wang, M. Zhang, J. Zhu, L. Xing, and Q. Wu, "Stochastic adaptive forwarding strategy based on deep reinforcement learning for secure mobile video communications in NDN," *Secur. Commun. Netw.*, vol. 2021, pp. 1–13, Apr. 2021, doi: 10.1155/2021/6630717.

[14] R. A. Rehman, S. H. Ahmed, and B.-S. Kim, "OEFS: On-demand energy-based forwarding strategy for named data wireless ad hoc networks," *IEEE Access*, vol. 5, pp. 6075–6086, 2017, doi: 10.1109/ACCESS.2017.2684912.

[15] M. A. Hail, "IoT-NDN: An IoT architecture via named data netwoking (NDN)," in *Proc. IEEE Int. Conf. Ind. Artif. Intell., Commun. Technol. (IAICT)*, Jul. 2019, pp. 74–80, doi: 10.1109/ICIAICT.2019.8784859.

[16] M. Alabadi, A. Habbal, and X. Wei, "Industrial Internet of Things: Requirements, architecture, challenges, and future research directions," *IEEE Access*, vol. 10, pp. 66374–66400, 2022, doi: 10.1109/ACCESS.2022.3185049.

[17] B. Nour, H. Ibn-Khedher, H. Moungla, H. Afifi, F. Li, K. Sharif, H. Khelifi, and M. Guizani, "Internet of Things mobility over information-centric/named-data networking," *IEEE Internet Comput.*, vol. 24, no. 1, pp. 14–24, Jan. 2020, doi: 10.1109/MIC.2019.2963187.

[18] M. Amadeo, C. Campolo, A. Iera, and A. Molinaro, "Named data networking for IoT: An architectural perspective," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2014, pp.1–4, doi: 10.1109/EuCNC.2014.6882665.

[19] O. Hahm, E. Baccelli, T. C. Schmidt, M. Wahlisch, and C. Adjih, "A named data network approach to energy efficiency in IoT," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2016, pp. 1–12, doi: 10.1109/GLOCOMW.2016.7848819.

[20] A. Habbal, S. A. Abdullah, E. O. C. Mkpojiogu, S. Hassan, and N. Benamar, "Assessing experimental private cloud using web of system performance model," *Int. J. Grid High Perform. Comput.*, vol. 9, no. 2, pp. 21–35, Apr. 2017.

[21] A. Habbal, S. I. Goudar, and S. Hassan, "A context-aware radio access technology selection mechanism in 5G mobile network for smart city applications," *J. Netw. Comput. Appl.*, vol. 135, pp. 97–107, Jun. 2019.

[22] M. Alhowaidi, B. Ramamurthy, B. Bockelman, and D. Swanson, "Enhancing the SDTMA-NDN architecture for transferring the scientific data software using named data networking," *Comput. Netw.*, vol. 166, Jan. 2020, Art. no. 106954, doi: 10.1016/j.comnet.2019.106954.
[23] S. Chatterjee, "A survey of Internet of Things (IoT) over information centric network (ICN)," 2018, p. 18, doi: 10.13140/RG.2.2.27799.47524.
[24] N. A. Askar, A. Habbal, A. H. Mohammed, M. S. Sajat, Z. Y. Z. Yusupov, and D. Kodirov, "Architecture, protocols, and applications of the Internet of Medical Things (IoMT)," *J. Commun.*, vol. 2022, pp. 900–918, Jan. 2022, doi: 10.12720/jcm.17.11.900-918.
[25] F. Salleh, S. Hassan, A. Habbal, and E. Mkpojiogu, "Internet of Things applications for smart campus," in *Proc. 6th Int. Conf. Internet Appl., Protocols Services*, vol. 121, Dec. 2020, pp. 93–103, doi: 10.1007/978-3-030-97516-6_5.
[26] M. Enguehard, R. Droms, and D. Rossi, "SLICT: Secure localized information centric things," in *Proc. 3rd ACM Conf. Inf.-Centric Netw.*, Sep. 2016, pp. 255–260, doi: 10.1145/2984356.2988519.
[27] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms," *Comput. Secur.*, vol. 94, Jul. 2020, Art. no. 101863, doi: 10.1016/j.cose.2020.101863.
[28] A. Djama, B. Djamaa, and M. R. Senouci, "Information-centric networking solutions for the Internet of Things: A systematic mapping review," *Comput. Commun.*, vol. 159, pp. 37–59, Jun. 2020, doi: 10.1016/j.comcom.2020.05.003.
[29] S. M. Karım, A. Habbal, S. Ashraf, and Azeem, "A review on the Internet of Vehicle security, all in one," *Secur. Commun. Netw.*, vol. 135, pp. 97–107, Jun. 2019.
[30] D. Mars, S. M. Gammar, A. Lahmadi, and L. A. Saidane, "Using information centric networking in Internet of Things: A survey," *Wireless Pers. Commun.*, vol. 105, no. 1, pp. 87–103, Mar. 2019, doi: 10.1007/s11277-018-6104-8.
[31] A. Djama, B. Djamaa, and M. R. Senouci, "TCP/IP and ICN networking technologies for the Internet of Things: A comparative study," in *Proc. Int. Conf. Netw. Adv. Syst. (ICNAS)*, Jun. 2019, pp. 1–6.
[32] F. Zen Alden, S. Hassan, A. Habbal, and X. Wei, "An adaptive social-aware device-to-device communication mechanism for wireless networks," *Ad Hoc Netw.*, vol. 137, Dec. 2022, Art. no. 102955.
[33] M. Arifuzzaman, Y. Keping, Q. N. Nguyen, and S. Takuro, "Locating the content in the locality: ICN caching and routing strategy revisited," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2015, pp. 423–428, doi: 10.1109/EuCNC.2015.7194111.
[34] Y. I. Kaiiali, A. Iliyasu, A. S. Wazan, A. Habbal, and Y. I. Muhammad, "A cloud-based architecture for mitigating privacy issues in online social networks," *Int. Arab J. Inf. Technol.*, vol. 16, no. 5, pp. 879–888, Sep. 2019.
[35] R. Alubady, S. Hassan, and A. Habbal, "Adaptive interest lifetime in named data networking to support disaster area," *J. Telecommun. Electron. Comput. Eng.*, vol. 10, nos. 2–4, pp. 29–34, 2018.
[36] I. U. Din, S. Hassan, M. K. Khan, M. Guizani, O. Ghazali, and A. Habbal, "Caching in information-centric networking: Strategies, challenges, and future research directions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1443–1474, 1st Quart., 2018, doi: 10.1109/COMST.2017.2787609.
[37] S. Dulal, N. Ali, A. R. Thieme, T. Yu, S. Liu, S. Regmi, L. Zhang, and L. Wang, "Building a secure mHealth data sharing infrastructure over NDN," in *Proc. 9th ACM Conf. Inf.-Centric Netw.*, Sep. 2022, pp. 114–124, doi: 10.1145/3517212.3558091.
[38] Z. Zhang, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyev, and L. Zhang, "Security support in named data networking," Tech. Rep., 2018. [Online]. Available: https://named-data.net/wp-content/uploads/2018/03/ndn-0057-1-ndn-security.pdf
[39] B. Nour, K. Sharif, F. Li, and Y. Wang, "Security and privacy challenges in information-centric wireless Internet of Things networks," *IEEE Secur. Privacy*, vol. 18, no. 2, pp. 35–45, Apr. 2010.
[40] F. A. Karim, A. H. M. Aman, R. Hassan, and K. Nisar, "A survey on information-centric networking with cloud Internet of Things and artificial intelligence," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–11, Jun. 2022, doi: 10.1155/2022/7818712.
[41] Aroosa, S. S. Ullah, S. Hussain, R. Alroobaea, and I. Ali, "Securing NDN-based Internet of Health Things through cost-effective signcryption scheme," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–13, Apr. 2021, doi: 10.1155/2021/5569365.
[42] O. Humraz and A. S. Haris, "Push-based critical data forwarding mechanism for IoT in healthcare using named node networking," in *Proc. Int. Conf. Comput., Power Commun. Technol. (GUCON)*, Sep. 2018, pp. 193–197, doi: 10.1109/GUCON.2018.8674892.
[43] M. Hussaini, S. A. Nor, and A. Ahmad, "Producer mobility support for information centric networking approaches: A review," *Int. J. Appl. Eng. Res.*, vol. 13, no. 6, pp. 3272–3280, 2018. [Online]. Available: http://www.ripublication.com
[44] A. Tariq, R. A. Rehman, and B. Kim, "Forwarding strategies in NDN-based wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 68–95, 1st Quart., 2020, doi: 10.1109/COMST.2019.2935795.
[45] F. A. Karim, A. H. M. Aman, R. Hassan, K. Nisar, and M. Uddin, "Named data networking: A survey on routing strategies," *IEEE Access*, vol. 10, pp. 90254–90270, 2022, doi: 10.1109/ACCESS.2022.3201083.
[46] A. Benmoussa, C. A. Kerrache, N. Lagraa, S. Mastorakis, A. Lakas, and A. E. K. Tahari, "Interest flooding attacks in named data networking: Survey of existing solutions, open issues, requirements, and future directions," *ACM Comput. Surv.*, vol. 55, no. 7, pp. 1–37, Jul. 2023, doi: 10.1145/3539730.
[47] C. Sarros, V. Demiroglou, and V. Tsaoussidis, "Intermittently-connected IoT devices: Experiments with an NDN-DTN architecture," in *Proc. IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2021, pp. 1–9, doi: 10.1109/CCNC49032.2021.9369578.
[48] S. Sajid Ullah, S. Hussain, A. Gumaei, and H. AlSalman, "A secure NDN framework for Internet of Things enabled healthcare," *Comput., Mater. Continua*, vol. 67, no. 1, pp. 223–240, 2021, doi: 10.32604/cmc.2021.014413.
[49] S. M. Asif Iqbal and Asaduzzaman, "Adaptive forwarding strategies to reduce redundant interests and data in named data networks," *J. Netw. Comput. Appl.*, vol. 106, pp. 33–47, Mar. 2018, doi: 10.1016/j.jnca.2018.01.013.
[50] A. Aboodi, T. Wan, and G. Sodhy, "Survey on the incorporation of NDN/CCN in IoT," *IEEE Access*, vol. 7, pp. 71827–71858, 2019, doi: 10.1109/ACCESS.2019.2919534.
[51] D. Gupta, S. Wadhwa, and S. Rani, "On the role of named data networking for IoT content distribution," in *Proc. 6th Int. Conf. Commun. Electron. Syst. (ICCES)*, Jul. 2021, pp. 544–549, doi: 10.1109/ICCES51350.2021.9488946.
[52] W. Shang, A. Bannis, T. Liang, Z. Wang, Y. Yu, A. Afanasyev, J. Thompson, J. Burke, B. Zhang, and L. Zhang, "Named data networking of things," in *Proc. IEEE 1st Int. Conf. Internet-Things Design Implement. (IoTDI)*, Apr. 2016, pp. 117–128, doi: 10.1109/IoTDI.2015.44.
[53] A. N. Ngaffo, W. El Ayeb, and Z. Choukair, "Information-centric networking challenges and opportunities in service discovery: A survey," in *Proc. IEEE 8th Int. Conf. Commun. Netw. (ComNet)*, Oct. 2020, pp. 1–8, doi: 10.1109/ComNet47917.2020.9306088.
[54] X. Guo, M. J. Zhang, A. Ngaboyindekwe, J. L. Fang, and J. Wang, "MPR based secure content routing scheme for NDN-MANET," *J. Internet Technol.*, vol. 20, no. 5, pp. 1625–1636, 2019. [Online]. Available: https://jit.ndhu.edu.tw/article/view/2143, doi: 10.3966/160792642019092005026.
[55] K. S. Joseph, "NDNoT?: Name based routing in IoT networks—A survey," *Int. J. Adv. Res. Comput. Sci. Technol.*, vol. 6, no. 1, 2018.
[56] M. A. Naeem, R. Ullah, Y. Meng, R. Ali, and B. A. Lodhi, "Caching content on the network layer: A performance analysis of caching schemes in ICN-based Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6477–6495, May 2022, doi: 10.1109/JIOT.2021.3110977.
[57] D. Saxena, V. Raychoudhury, and N. SriMahathi, "SmartHealth-NDNoT: Named data network of things for healthcare services," in *Proc. Workshop Pervasive Wireless Healthcare*, Jun. 2015, pp. 45–50, doi: 10.1145/2757290.2757300.
[58] K. T. Ko, H. H. Hlaing, and M. Mambo, "A PEKS-based NDN strategy for name privacy," *Future Internet*, vol. 12, no. 8, pp. 1–22, 2020, doi: 10.3390/FI12080130.
[59] B. Nour, K. Sharif, F. Li, S. Biswas, H. Moungla, M. Guizani, and Y. Wang, "A survey of Internet of Things communication using ICN: A use case perspective," *Comput. Commun.*, vols. 142–143, pp. 95–123, Jun. 2019, doi: 10.1016/j.comcom.2019.05.010.
[60] M. R. Rotinsulu, B. Susilo, A. Presekal, E. Pramono, and R. F. Sari, "Measuring quality of services (QoS) of several forwarding strategies on named data networking (NDN) using ndnSIM," in *Proc. IEEE Int. Conf. Cybern. Comput. Intell. (CyberneticsCom)*, Nov. 2017, pp. 45–49, doi: 10.1109/CYBERNETICSCOM.2017.8311713.

[61] 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, Jun. 2018, doi: 10.1016/j.jnca.2017.11.002.

[62] A. Abane, M. Daoui, S. Bouzefrane, S. Banerjee, and P. Muhlethaler, "A realistic deployment of named data networking in the Internet of Things," *J. Cyber Secur. Mobility*, vol. 10, pp. 1–8, Nov. 2019, doi: 10.13052/JCSM2245-1439.911.

[63] A. S. Wazan, R. Laborde, D. W. Chadwick, F. Barrere, A. Benzekri, M. Kaiiali, and A. Habbal, "Trust management for public key infrastructures: Implementing the X.509 trust broker," *Secur. Commun. Netw.*, vol. 2017, pp. 1–23, Jan. 2017.

[64] Y. Yang and T. Song, "Energy-efficient cooperative caching for information-centric wireless sensor networking," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 846–857, Jan. 2022, doi: 10.1109/JIOT.2021.3088847.

[65] T. Liang, J. Shi, Y. Wang, and B. Zhang, "On the prefix granularity problem in NDN adaptive forwarding," *IEEE/ACM Trans. Netw.*, vol. 29, no. 6, pp. 2820–2833, Dec. 2021, doi: 10.1109/TNET.2021.3103187.

[66] D. Marques, C. Senna, and M. Luís, "Forwarding in energy-constrained wireless information centric networks," *Sensors*, vol. 22, no. 4, pp. 1–21, 2022, doi: 10.3390/s22041438.

[67] K. Hasan and S.-H. Jeong, "Fast eHealth information delivery in the ICN-based mobile networks," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2021, pp. 1617–1619, doi: 10.1109/ICTC52510.2021.9621123.

[68] 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, pp. 148–158, Apr. 2015, doi: 10.1016/j.jnca.2014.06.007.

[69] L. Gameiro, C. Senna, and M. Luís, "ndnIoT-FC: IoT devices as first-class traffic in name data networks," *Futur. Internet*, vol. 12, no. 11, pp. 1–21, 2020, doi: 10.3390/fi12110207.

[70] M. Amadeo, C. Campolo, J. Quevedo, D. Corujo, A. Molinaro, A. Iera, R. L. Aguiar, and A. V. Vasilakos, "Information-centric networking for the Internet of Things: Challenges and opportunities," *IEEE Netw.*, vol. 30, no. 2, pp. 92–100, Mar. 2016, doi: 10.1109/MNET.2016.7437030.

[71] S. M. Karim, A. Habbal, S. A. Chaudhry, and A. Irshad, "Architecture, protocols, and security in IoV: Taxonomy, analysis, challenges, and solutions," *Secur. Commun. Netw.*, vol. 2022, pp. 1–19, Oct. 2022, doi: 10.1155/2022/1131479.

[72] O. Serhane, K. Yahyaoui, B. Nour, and H. Moungla, "Energy-aware cache placement scheme for IoT-based ICN networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2021, pp. 1–6, doi: 10.1109/ICC42927.2021.9500341.

[73] S. Ahdan, A. Nurhayati, G. N. Nurkahfi, and N. R. Syambas, "Adaptive forwarding strategy in named data networking: A survey," in *Proc. 15th Int. Conf. Telecommun. Syst., Services, Appl. (TSSA)*, Nov. 2021, pp. 1–6, doi: 10.1109/TSSA52866.2021.9768238.

[74] S. Ahdan, H. Situmorang, and N. R. Syambas, "Forwarding strategy performance in NDN network: A case study of palapa ring topology," in *Proc. 3rd Int. Conf. Wireless Telematics (ICWT)*, Jul. 2017, pp. 20–25, doi: 10.1109/ICWT.2017.8284131.

[75] M. Z. Ahmed, A. H. A. Hashim, A. M. Hassan, O. O. Khalifa, A. H. Alkali, and A. M. Ahmed, "Performance evaluation of best route and broadcast strategy for NDN producer's mobility," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 1, pp. 3671–3677, Oct. 2019, doi: 10.35940/ijeat.A2712.109119.

[76] J. Wu, X. Sun, J. Wu, and G. Han, "Routing strategy of reducing energy consumption for underwater data collection," *Intell. Converged Netw.*, vol. 2, no. 3, pp. 163–176, Sep. 2021, doi: 10.23919/icn.2021.0012.

[77] R. Mayasari and N. R. Syambas, "Machine learning on named data network: A survey routing and forwarding strategy," in *Proc. 14th Int. Conf. Telecommun. Syst., Services, Appl. (TSSA*, Nov. 2020, pp. 1–5, doi: 10.1109/TSSA51342.2020.9310909.

[78] B. Alahmri, S. Al-Ahmadi, and A. Belghith, "Efficient pooling and collaborative cache management for NDN/IoT networks," *IEEE Access*, vol. 9, pp. 43228–43240, 2021.

[79] B. Lewis, I. Smith, M. Fowler, and J. Licato, "The robot mafia: A test environment for deceptive robots," in *Proc. 28th Mod. Artif. Intell. Cogn. Sci. Conf.*, 2017, pp. 189–190.

[80] W. T. Ariefianto and N. R. Syambas, "Routing in NDN network: A survey and future perspectives," in *Proc. 11th Int. Conf. Telecommun. Syst. Services Appl. (TSSA)*, Oct. 2017, pp. 1–6, doi: 10.1109/TSSA.2017.8272942.

[81] K. Ahed, M. Benamar, and R. E. Ouazzani, "Content delivery in named data networking based Internet of Things," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 1397–1402, doi: 10.1109/IWCMC.2019.8766526.

[82] H. B. Abraham and P. Crowley, "Forwarding strategies for applications in named data networking," in *Proc. Symp. Archit. Netw. Commun. Syst.*, Mar. 2016, pp. 111–112, doi: 10.1145/2881025.2889475.

[83] H. Yuan, T. Song, and P. Crowley, "Scalable NDN forwarding: Concepts, issues and principles," in *Proc. 21st Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2012, pp. 1–11, doi: 10.1109/ICCCN.2012.6289305.

[84] M. Shafiq, Z. Tian, A. K. Bashir, A. Jolfaei, and X. Yu, "Data mining and machine learning methods for sustainable smart cities traffic classification: A survey," *Sustain. Cities Soc.*, vol. 60, Sep. 2020, Art. no. 102177, doi: 10.1016/j.scs.2020.102177.

[85] M. Bidollahkhani, O. Dakkak, A. S. M. Alajeeli, and B.-S. Kim, "LoRaline: A critical message passing line of communication for anomaly mapping in IoV systems," *IEEE Access*, vol. 11, pp. 18107–18120, 2023, doi: 10.1109/ACCESS.2023.3246471.

[86] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for Internet of Things in smart city," *Future Gener. Comput. Syst.*, vol. 107, pp. 433–442, Jun. 2020, doi: 10.1016/j.future.2020.02.017.

[87] A. Zapletal, K. Ueda, and A. Tagami, "Evaluation of forwarding strategies for NDN-based multi-access edge computing," in *Proc. IEEE Global Commun. Conf.*, Dec. 2020, pp. 2–7, doi: 10.1109/GLOBECOM42002.2020.9322485.

[88] S. Ahdan, A. Nurhayati, G. N. Nurkahfi, and N. R. Syambas, "Adaptive forwarding strategy in named data networking : A survey," in *Proc. 15th Int. Conf. Telecommun. Syst., Services, Appl. (TSSA)*, Nov. 2021, pp. 1–6, doi: 10.1109/TSSA52866.2021.9768238.

[89] K. Ahed, M. Benamar, A. A. Lahcen, and R. E. Ouazzani, "Forwarding strategies in vehicular named data networks: A survey," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 5, pp. 1819–1835, May 2022, doi: 10.1016/j.jksuci.2020.06.014.

[90] N. Aloulou, M. Ayari, M. F. Zhani, L. Saidane, and G. Pujolle, "Taxonomy and comparative study of NDN forwarding strategies," in *Proc. 6th Int. Conf. Commun. Netw. (ComNet)*, Mar. 2017, pp. 1–8, doi: 10.1109/COMNET.2017.8285592.

[91] 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, nos. 5–6, pp. 311–330, Jun. 2022, doi: 10.1007/s12243-021-00850-2.

[92] D. Saxena and V. Raychoudhury, "Design and verification of an NDN-based safety-critical application: A case study with smart healthcare," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 5, pp. 991–1005, May 2019, doi: 10.1109/TSMC.2017.2723843.

[93] S. Muralidharan, A. Roy, and N. Saxena, "MDP-IoT: MDP based interest forwarding for heterogeneous traffic in IoT-NDN environment," *Future Gener. Comput. Syst.*, vol. 79, pp. 892–908, Feb. 2018, doi: 10.1016/j.future.2017.08.058.

[94] S. Muralidharan, A. Roy, and N. Saxena, "MDP-based model for interest scheduling in IoT-NDN environment," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 232–235, Feb. 2018, doi: 10.1109/LCOMM.2017.2764889.

[95] J. Su, X. Tan, Z. Zhao, and P. Yan, "MDP-based forwarding in named data networking," in *Proc. 35th Chin. Control Conf. (CCC)*, Jul. 2016, pp. 2459–2464, doi: 10.1109/ChiCC.2016.7553733.

[96] 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, pp. 351–363, Oct. 2018, doi: 10.1016/j.future.2018.04.087.

[97] C. Gündogan, P. Kietzmann, T. C. Schmidt, and M. Wählisch, "HoPP: Robust and resilient publish-subscribe for an information-centric Internet of Things," in *Proc. IEEE 43rd Conf. Local Comput. Netw. (LCN)*, Oct. 2018, pp. 331–334, doi: 10.1109/LCN.2018.8638030.

[98] A. Abane, M. Daoui, S. Bouzefrane, and P. Muhlethaler, "A lightweight forwarding strategy for named data networking in low-end IoT," *J. Netw. Comput. Appl.*, vol. 148, Dec. 2019, Art. no. 102445, doi: 10.1016/j.jnca.2019.102445.

[99] 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, Sep. 2019, doi: 10.1007/s10586-018-2859-7.

[100] M. Kuai and X. Hong, "Location-based deferred broadcast for ad-hoc named data networking," *Future Internet*, vol. 11, no. 6, pp. 1–18, 2019, doi: 10.3390/FI11060139.

[101] M. Chowdhury, J. A. Khan, and L. Wang, "Leveraging content connectivity and location awareness for adaptive forwarding in NDN-based mobile ad hoc networks," in *Proc. 7th ACM Conf. Inf.-Centric Netw.*, Sep. 2020, pp. 59–69, doi: 10.1145/3405656.3418713.

[102] A. Aboud, H. Touati, and B. Hnich, "Power saving extension for the NDN-based GIF protocol for the Internet of Things," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 525–530, doi: 10.1109/IWCMC.2019.8766775.

[103] A. Aboud and H. Touati, "Geographic interest forwarding in NDN-based wireless sensor networks," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2016, pp. 1–4, doi: 10.1109/AICCSA.2016.7945683.

[104] T. Mick, R. Tourani, and S. Misra, "LASeR: Lightweight authentication and secured routing for NDN IoT in smart cities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 755–764, Apr. 2018, doi: 10.1109/JIOT.2017.2725238.

[105] N. N. Dehaghani, R. Sadeghi, and S. M. F. Imani, "REF: A novel forwarding strategy in wireless NDN," *Wireless Pers. Commun.*, vol. 117, no. 2, pp. 1025–1042, Mar. 2021, doi: 10.1007/s11277-020-07909-8.

[106] L. Zhang, S. Li, and D. Li, "Reduce redundant data packets forwarding strategy for named data mobile ad-hoc network (NDMANET)," in *Proc. 4th Int. Conf. Adv. Comput. Technol., Inf. Sci. Commun. (CTISC)*, Apr. 2022, pp. 1–6, doi: 10.1109/ctisc54888.2022.9849753.

[107] 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," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 3, pp. 1–17, Feb. 2022, doi: 10.1002/cpe.6584.

[108] 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, Jan. 2016, doi: 10.1155/2016/3127029.

[109] A. Tariq, R. A. Rehman, and B.-S. Kim, "Energy efficient priority aware forwarding in SDN enabled named data Internet of Things," in *Proc. Int. Conf. Electron., Inf., Commun. (ICEIC)*, Jan. 2020, pp. 16–19, doi: 10.1109/ICEIC49074.2020.9051371.

[110] S. Hassan and M. Alsamman, "Energy-aware multipath forwarding mechanism for named data network in wireless environment," Tech. Rep., 2021.

[111] M. Abdelaal, M. Karadeniz, F. Durr, and K. Rothermel, "LiteNDN: QoS-aware packet forwarding and caching for named data networks," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 10–13, doi: 10.1109/CCNC46108.2020.9045742.

[112] K. Lei, S. Zhong, F. Zhu, K. Xu, and H. Zhang, "An NDN IoT content distribution model with network coding enhanced forwarding strategy for 5G," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2725–2735, Jun. 2018, doi: 10.1109/TII.2017.2781372.

[113] A. Sallam, A. A. Almohammedi, A. S. A. Gaid, S. Y. A., M. Sadeq, S. E. Abdulaziz, S. Abduasalam, Y. Abdulhaleem, and V. Shepelev, "Performance evaluation of fog-computing based on IoT healthcare application," in *Proc. Int. Conf. Technol., Sci. Admin. (ICTSA)*, Mar. 2021, pp. 4–9, doi: 10.1109/ICTSA52017.2021.9406542.

[114] M. Raeisi-Varzaneh, O. Dakkak, A. Habbal, and B.-S. Kim, "Resource scheduling in edge computing: Architecture, taxonomy, open issues and future research directions," *IEEE Access*, vol. 11, pp. 25329–25350, 2023, doi: 10.1109/ACCESS.2023.3256522.

[115] A. N. Ozalp, Z. Albayrak, M. Cakmak, and E. Ozdogan, "Layer-based examination of cyber-attacks in IoT," in *Proc. 6th Int. Conf. Internet Appl., Protocols, Services*, Jul. 2022, pp. 1–4, doi: 10.1109/HORA55278.2022.9800047.

[116] M. Elweddad, M. Güneşer, and Z. Yusupov, "Designing an energy management system for household consumptions with an off-grid hybrid power system," *AIMS Energy*, vol. 10, no. 4, pp. 1–15, 2022, doi: 10.3934/energy.2022036.

[117] H. Alhumyani, I. Alrube, S. Alsharif, A. Afifi, C. B. Amar, H. S. El-Sayed, and O. S. Faragallah, "An efficient internet traffic classification system using deep learning for IoT," *Comput., Mater. Continua*, vol. 71, no. 1, pp. 407–422, 2022, doi: 10.32604/cmc.2022.020727.

[118] H. C. Altunay, Z. Albayrak, A. N. Özalp, and M. Çakmak, "Analysis of anomaly detection approaches performed through deep learning methods in SCADA systems," in *Proc. 3rd Int. Congr. Hum.-Comput. Interact., Optim. Robotic Appl. (HORA)*, Jun. 2021, pp. 1–6, doi: 10.1109/HORA52670.2021.9461273.

[119] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: A malicious Bot-IoT traffic detection method in IoT network using machine-learning techniques," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3242–3254, Mar. 2021, doi: 10.1109/JIOT.2020.3002255.

[120] A. Salh, L. Audah, N. S. M. Shah, A. Alhammadi, Q. Abdullah, Y. H. Kim, S. A. Al-Gailani, S. A. Hamzah, B. A. F. Esmail, and A. A. Almohammedi, "A survey on deep learning for ultra-reliable and low-latency communications challenges on 6G wireless systems," *IEEE Access*, vol. 9, pp. 55098–55131, 2021, doi: 10.1109/ACCESS.2021.3069707.

NAEEM ALI ASKAR was born in Duhok, Iraq. He received the bachelor's degree in computer science from Salahaddin University, Iraq, and the M.Sc. degree in electrical and computer science from Universiti Sains Malaysia (USM), Malaysia. He is currently pursuing the Ph.D. degree with the Department of Computer Engineering, Karabük University, Turkey. His research interests include the Internet of Things and named data networking.

ADIB HABBAL (Senior Member, IEEE) received the Ph.D. degree in computer science (specializing in networked computing) from Universiti Utara Malaysia (UUM), Malaysia. He is currently a Professor (Associate) in computer engineering and the Founding Head of the Innovative Networked Systems (INETs) Research Group, Karabük University, Turkey. Before joining Karabuk University, in 2019, he was a Senior Lecturer with UUM (ten years) and the Head of InterNetWorks Research Platform (three years). He was also an IEEE UUM Student Branch Founding Counselor and an Executive Council Member of the Internet Society Malaysia Chapter. His research projects have been funded by several organizations, including IEEE R10, the IEEE Malaysia Section, Internet Society, the Chinese Academy of Science, Malaysian Ministry of Higher Education, and UUM. He has authored/coauthored 100 refereed technical publications in journals and conference proceedings in the areas of future internet and wireless networks. He has received a number of international recognitions for his outstanding educational and research activities, including UUM Excellent Service Award (2010), UUM Best Research Award (2014), and the UUM-SOC Prolific Writer Award (2016). He was a recipient of Internet Society Fellowship to the Internet Engineering Task Force (IETF), the IEEE Malaysia Section Best Volunteer Award, and the Asia–Pacific Advanced Network (APAN) Fellow to APAN35. His professional experience includes being a speaker at a number of renowned research conferences and technical meetings, such as ACM SIGCOMM, APAN, APRICOT, IEEE, and internet2, an editor for top-tier and refereed journals, a technical program committee for international conferences on computing networks, and an examiner for postgraduate scholars in his research areas. His research interests include future internet protocols and architecture, next generation mobile networks, WEB3, and blockchain technology and digital trust.

FERAS ZEN ALDEN received the bachelor's degree in telecommunication engineering from IPU University, Syria, in 2008, and the master's degree in information communication technology (ICT) and the Ph.D. degree from Universiti Utara Malaysia, in 2012 and 2020, respectively. He is currently a Lecturer with the Department of Informatics and Software Engineering, Cihan University-Erbil, Iraq. Previously, he was a Lecturer with the Information Technology Department, Faculty of Business and Technology (FBT), Unitar International University, Malaysia. His research interests include future networks deployment and integration with other technologies.

XIAN WEI (Senior Member, IEEE) received the M.S. degree in computer science from Shanghai Jiaotong University, Shanghai, China, and the Ph.D. degree in computer engineering from the Technical University of Munich, Munich, Germany. Currently, he is a Research Professor with the Software Engineering Institute (SEI), East China Normal University, Shanghai. He has been a Principal Investigator (PI) with the Fujian Institute of Research on the Structure of Matter, Chinese Academy of Sciences (CAS), since July 2017. He has authored over 90 publications in refereed journals and conference proceedings. His research interests include machine learning, geometric optimization, and time series analysis. The applications include multi-sensor fusion for intelligent car, robotic vision, images and point clouds modeling, synthesis, recognition, and semantics. He is a Senior Member of IET, INSAI, and CCF.

HASHEM ALAIDAROS received the Ph.D. degree in computer science (specializing in networked security) from Universiti Utara Malaysia (UUM), Malaysia. He is currently the Chair of the Cybersecurity Department and an Assistant Professor with Dar Al-Hekma University (DAH) University. He has over 15 years consulting and training in cyber security, risk management, auditing, and business continuity fields. He is also certified in a CISA, CRISC, and ISO 27001 Lead Auditor, an Implementer, the ISO 31000 Senior Risk Manager, and a CEH.

JIELONG GUO received the M.S. degree in biomedical engineering from South-Central Minzu University, Wuhan, China. Since 2017, he has been the Machine Learning and Pattern Recognition Laboratory, Fujian Institute of Research on the Structure of Matter, Chinese Academy of Sciences, China, as an Engineer. His research interests include geometric machine learning and manifold learning. The applications include medical image processing, robotic vision, intelligent driving, and semantics.

HUI YU received the Ph.D. degree in electrical engineering from the University of Strathclyde, U.K. He is currently an associate researcher. His research interests include modeling, analysis and optimization of complex dynamic systems, and their engineering applications in biochemical complex systems. His long-term in-depth research in the field of dynamic system model optimization and optimal experimental design. Recently, he mainly explores the theoretical combination of artificial intelligence and physical system modeling, constructs an AI-based optimal experimental design theoretical framework, combines deep learning technology, and system modeling optimization technology. He focuses on the research and development of automation and system accurate identification of complex system model construction optimization new method. He has published more than ten SCI journals and conference papers in the field of system process control, five invention patents, and two utility model patents.