IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 31, 2018, accepted November 13, 2018, date of publication November 22, 2018, date of current version December 27, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2882811

Leveraging Named Data Networking for Fragmented Networks in Smart Metropolitan Cities

OMAIR AHMAD KHAN[1], MUNAM ALI SHAH[1], IKRAM UD DIN[2], (Senior Member, IEEE), BYUNG-SEO KIM[3], (Senior Member, IEEE), HASAN ALI KHATTAK[1], (Member, IEEE), JOEL J. P. C. RODRIGUES[4,5,6], (Senior Member, IEEE), HALEEM FARMAN[7], AND BILAL JAN[8]

[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 44550, Pakistan
[2]Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[3]Department of Software and Communications Engineering, Hongik University, Sejong 30016, South Korea
[4]Post-Graduation, National Institute of Telecommunications (Inatel), Santa Rita do Sapucaí–MG 37540-000, Brazil
[5]Covilhã Delegation, Instituto de Telecomunicações, 1049-001 Lisbon, Portugal
[6]PPGIA, University of Fortaleza (UNIFOR), Fortaleza 90811-905, Brazil
[7]Department of Computer Science, Islamia College Peshawar, Jamrod Road, University Campus Peshawar 25120, Pakistan
[8]Department of Computer Science, FATA University, Dara Adam Khel FR Kohat 26000, Pakistan

Corresponding author: Byung-Seo Kim (jsnbs@hongik.ac.kr)

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government. (No. 2018R1A2B6002399). The work of Joel Rodrigues was supported by the National Funding from the FCT - Fundação para a Ciência e a Tecnologia through the UID/EEA/500008/2013 Project; by Finatel through the Inatel Smart Campus project; by Finep, with resources from Funttel, grant no. 01.14.0231.00, under the Radiocommunication Reference Center (Centro de Referência em Radiocomunicações - CRR) project of the National Institute of Telecommunications (Instituto Nacional de Telecomunicações - Inatel), Brazil; by Brazilian National Council for Research and Development (CNPq) via Grant No. 309335/2017 − 5.

ABSTRACT A fragmented network is a phenomenon caused when a metropolitan area network is affected due to some natural calamities such as fire, earthquake, flood, and so on. A reliable communication among nodes in the fragmented network is a vital research issue. Different solutions have been proposed to establish communications among nodes in such a fragmented network. One such solution is to make the use of named data networking (NDN). The NDN with the help of content store, pending interest table, and forwarding information base, establishes the communication with other nodes based on the names of contents, rather than the nodes themselves. However, these solutions are inefficient in the case of fragmented networks. In this research, we propose an NDN-based technique which uses the satisfied interest table (SIT) along with the push-based special alert message to communicate with other nodes to overcome such issues. We also use the Nonce phenomena to avoid loops during communications. The use of SIT helps a node to find the relative information quickly in the fragmented networks. By using this technique along with the SAM, we achieved better efficiency and response time.

INDEX TERMS Fragmented networks, named based network (NDN), satisfied interest table (SIT), metropolitan area network (MAN).

I. INTRODUCTION

The Internet of Things (IoT) has the ability to provide feasible and extendable solutions of scalable connectivity around the globe. Consequently, in the process of building homogeneous and heterogeneous device communications, IoT plays a promising role to examine, maintain, monitor, and control these devices. The frequent use of smart devices and connectivity along each other is one of the major reasons that researchers are being attracted towards the IoT. Through IoT, numerous smart applications are being evolved such as smart health-care [1]–[3], intelligent grid [4], intelligent homes [5], [6], smart campus [7], and intelligent city [8], [9]. One of the impact applications of IoT is Disaster Management Scenario (DMS) that mainly occurs due to flood, earthquake, fire, and storms.

In a particular domain of DMS through IoT, the research is being carried out by many organizations, such as ZIZMOS–funded by SBIR [10] and RIO setup center– sponsored

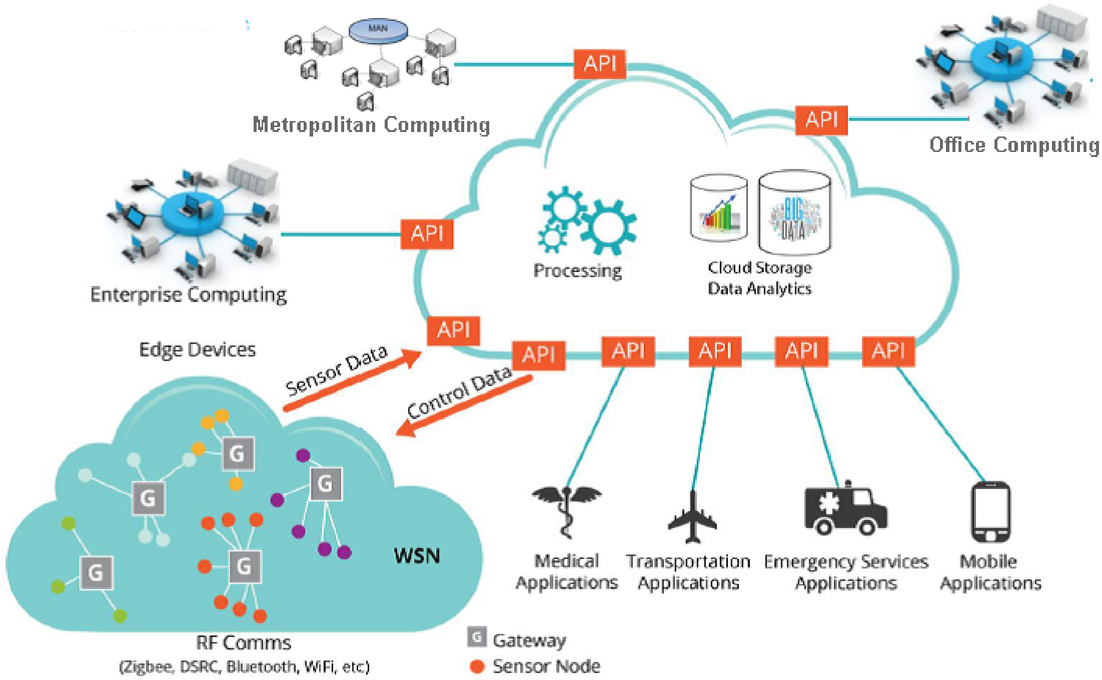


FIGURE 1. Overview of communications in the IoT network.

by IBM. The DMS, specifically for fire, is a promising application for the places which are overcrowded with smart devices, i.e., smart campuses, malls, and airports etc. Similarly, in the IoT perspective, the smart colony is also an important scenario where thousands of people are residing and the connectivity of devices is 24/7. However, this is quite hard to maintain because such scenarios are significantly difficult to protect and manage as one has to assure the protection of each and every device from disasters. In such scenarios, the main side-effect is the information loss when the infrastructure of a network is damaged [1]. In Metropolitan Area Network (MAN), IoT based DMS is the only solution which could be beneficial for the protection and maintenance of a smart colony. The IoT based DMS provides reliability, efficiency in memory and energy, and robustness among all IoT devices, which is the main motivation to work in the domain.

With the existing IP architecture, there are several shortcomings such as fool-proof security protection, shortage of IP addresses for IoT devices, real-time naming of bulks of information, no built-in support for mobile nodes, no mechanism for network fragments, excessive consumption of memory and power with heavier TCP/IP on tiny nodes, bandwidth consumption, and lastly, the large size of IP packets. These are among significant issues that make typical IP scheme unsuitable for the IoT based DMS [11]–[14].

To mitigate these issues in the existing IP architecture, Information Centric Networking (ICN) architectures are getting evolved from the last few years. So far, there are eight architectures of ICN, which are proposed for stationary as well as mobile networks. These architectures are NetInf, CCN, CONVERGENCE, COMET, MobilityFirst, PURSUIT, DONA, and NDN [15]. Irrespective of the IP architecture, ICN architectures mainly deal with content names instead of their respective hosting node and IP addresses. ICN naming plays a vital role by taking into account addresses of both IoT sensors as named-content accompanied by the information they provide as named content. The CCN is used in an IoT network replacing the host centric TCP/IP paradigm [13], [14], which is quite useful. Figure 1 presents the communication between among IoT devices which are part of a smart metropolitan, as shown in Figure 2.

ICN based models (such as NDN) have interest and information messages that are used to obtain a reply from the IoT network [15]. To give better security, these two messages are marked by subscribers and publishers of the contents. Furthermore, the publication of any data is started on the receipt of purchaser's demand for the arrangement of information, which makes it additionally secure. Furthermore, the existing cellular architectures can be used to re-enroll data from IoT devices with new adjacent devices. Note that an IoT device in an NDN can store information locally and make it available to other nodes when the data is not available in disaster situations. The existing ICN architectures offer the availability of data in dynamic ways [15]. It can be observed that NDN is more appropriate to construct than an IoT based DMS model. In this paper, we propose an NDN-based DMS model that utilizes satisfied interest table (SIT) alongside push-based signal messages to group with other nodes. The utilization of SIT causes the node to rapidly locate the required data in disaster scenario. The results show that better accuracy

FIGURE 2. Various application scenarios in smart metropolitan cities.

and response time can be achieved by using an NDN based model.

Furthermore, the paper provides an in-depth overview of NDN and its applications in the IoT domain. This technical paper presents the significance of NDN in fragmented networks where connectivity may be scarce or unreliable. Being extended from Khan *et. al.* [16], one of the main contributions of this paper is to provide a proof of concept through the implementation of NDN based DMS. The DMS uses the SIT with Beacon and Nonce phenomenon to provide an optimum performance. The rest of the paper is organized as follows: in Section II, the background of IoT, ICN, and ICN based NDN are analyzed in broader perspectives. Most recent technological advancements related to NDN enabled IoT are described through DMS prototype in Section III. Section IV is about the NDN based communication model for fragmented networks and performance evaluation of the applications of NDN in fragmented networks. In Section V, we provide the proof of concept for NDN based DMS in fragmented networks along with configurations and setup. Finally, Section VI provides an overview of results and presents performance of the proposed technique. The paper is concluded along with future works in Section VII.

II. BACKGROUND

A. INTERNET OF THINGS (IoT)

Internet of Things (IoT) is a term first coined in 1999 by Ashton [17]. In today's terminology, IoT is an interconnection of different objects such as sensors, humans, computation devices, and other gadgets. All these objects are called smart devices and mostly these devices have a built-in wireless connectivity. All these devices are configured with some network configurations so that they can pass data to other devices. The purpose of this network connectivity among different objects is to monitor, analyze, and pass-on data to other devices so that they can make a decision, perform a specific user-defined task, and update their status value so that other objects can make decisions and take actions accordingly [18], [19]. Figure 2 represents an IoT scenario where different devices and objects are sending and receiving data.

IoT is the new extent of research where every smart object is connected to other object while sharing information. Through IoT connectivity among different smart objects, we can perform our daily tasks more easily, efficiently, and accurately [20]. According to a recent survey, 12 billion smart devices are connected that share information. According to this survey, 26 billion smart devices will be connected to the Internet by 2020 [21]. As the number of IoT objects is increasing everyday, it is expected that there will not be a single object remaining which is not part of the IoT revolution. This is the reason IoT will affect on our social and personal life [22]. There are different application areas of the IoT which are being developed and enhanced. We have categorized the application areas in Figure 3.

Traditional IP based infrastructures are different from layer based IoT infrastructures. As previously mentioned, IoT is the combination of interconnected smart objects where these

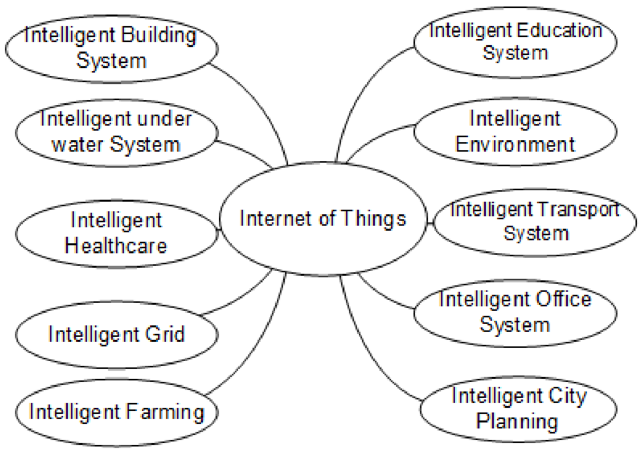


FIGURE 3. Application categorization for IoT.

objects are assigned unique addresses. For better connectivity and addressing, the IoT infrastructure is divided in the following four layers [23].

1) **Application layer:** All applications that support IoT infrastructure are run and managed by the application layer.
2) **Controlling Services:** This layer performs management roles, i.e., minimizes the data redundancy and processes the information by applying different process management methodologies.
3) **Network layer:** This layer controls fragmentation in the network and provides continuous connectivity.
4) **Sensor inter-connectivity and physical layer:** Sensors are tiny components that are attached to smart devices or dispersed in the real environment. The layer is responsible for the integration of data from these devices as well as processing and analyzing data.

The IoT is bringing a change in every aspect of life and we are becoming more dependent on IoT devices. However, IoT devices are constrained because of limited size, memory, and power. Several organizations are working towards different dimensions of the IoT.

1) Organizations and technologies include IPv-6, CORE, IETF, 6LowPAN, and ROLL groups [24] working on IP based IoT solutions and projects.
2) Different IP based projects are RH3, IPv6, CoAP, Media Type etc.

The classical IP infrastructures are facing different issues like system security, memory drainage, low addressing space and no caching etc. [25]. Due to these limitations, we need modifications and enhancements to make the IoT capable of meeting ever growing demands of users [24].

B. INFORMATION CENTRIC NETWORK (ICN)

To address limitations of the classical IP infrastructures, different solutions have been proposed such as Information Centric Network (ICN), which is an IP-less mechanism. It is a name based architecture that implies the phenomenon through which we can get required information and data (content) based on names instead of an IP. ICN is free from various overheads like assigning IP addresses to servers, router data, complex calculations, packet order of data, security of the channel and so on [12].

The ICN, CCN, and NDN models are investigated by the industry, for example, (DONA and NetInf) [15]. Some of the salient fetatures of these projects are their naming convention, API control, and security etc. [15]. A typical ICN is comprised of the following parameters:

1) Name object (NO): This parameter keeps track of different objects by their unique assigned names other than storing other parameters such as storage, address, and location etc.
2) Security along with Naming: It is the key element in this architecture to protect from different attacks, for example, DoS and Trojan.
3) Application Programming Interface (API): In the ICN architecture, API is different for requester and NO.
4) Routing and Forwarding implementation: There are two main approaches followed to handle routing implementation, i.e., NO requests (from the requester) and reply to the requester.
5) Caching: In ICN, every node has the ability to use cache with respect to CS.

There are many advantages of the ICN architecture when compared with traditional IP structure. For example, i) nodes in an ICN can reach other nodes through names, ii) ICN keeps track of those paths which are more frequently used, and iii) multicasting provision is available in this architecture. For the complete operation, ICN needs a small number of fields to generate requests. ICN makes use of sensors for different requests. These sensors are time-based and temperature based. Due to the implementation of different multi-hop and multicasting mechanisms, ICN has improved quality of services (QoS) [12], [15].

In Figure 4, we present a communication architecture for the ICN. Firstly, a subscriber, named 'A', floats a message to its nearby router, namely 'Router 1'. A request for the data packet is made on the bases of a unique name. The request then moves through different content routers. Each receiving node checks if the request can be entertained by finding an exact match in the PIT. The flow of this request is represented through red arrows in the figure. If the match is found, the required data is sent back through the same path where the request was generated along with the data packet. The reply to the request is shown with green colour arrows.

C. ICN-NDN

Different ICN architectures have been proposed in recent years, but Named Data Networking (NDN), is very prominent due to its salient features such as data structure, security, application interface, routing strategy, efficient content retrieval, and better bandwidth consumption. It is best suited for a network where mobility occurs as well as for a disconnected network [26]. The NDN architecture has been used in several scenarios, for example, smart home or smart campus,

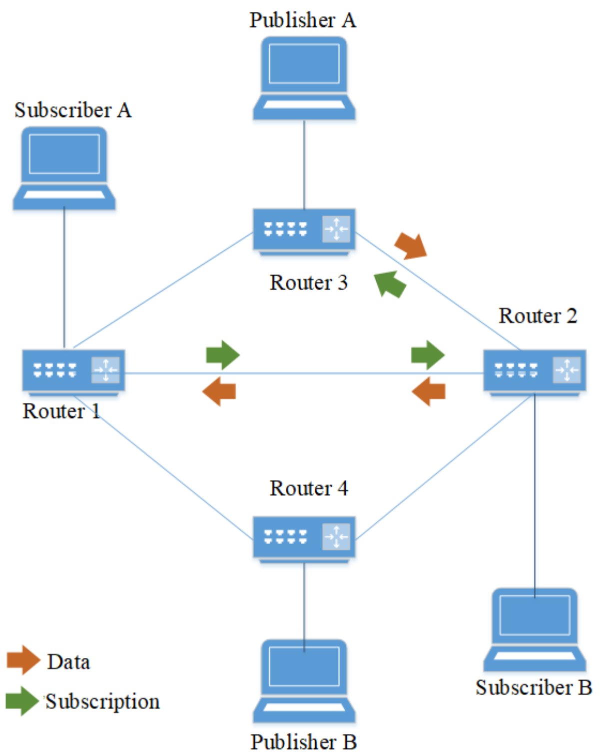


FIGURE 4. ICN based communications architecture.

as discussed in Section I. In NDN, there are two types of packet transmissions, i.e., interest packets and data packets. There is also a unique node structure that contains CS, PIT, and FIB. Each architecture has its own special features and functionalities [27].

CS contains cache information that can be retrieved when any interest packet satisfies the content interest. PIT contains the tracks of pending interest messages. This means that interest has been forwarded but the content is not arrived and is waiting for a match of that data [28]. FIB contains the record of all interest packets that is sent to other routers to get the data packet [29]. Whenever an interest packet satisfies the interest, the data packet is sent back. It follows exactly the same route where the interest packets come through. A unique security signature is used to incorporate the security. The architecture is well demonstrated in the domain of smart building, which is discussed in [5] and [30].

Currently, many organizations are working on various NDN-IoT based projects. These are listed below [31]:

1) NDN based video online learning.
2) NDN based system for partially disconnected networks.
3) NDN based virtual reality.
4) NDN based unscrupulous network.

In NDN, mainly three types of data structures are used:

1) Content Store (CS)
2) Pending Interest Table (PIT)
3) Forwarding Information Base (FIB)

In this architecture, the node has data and interest packets. In the traditional architecture of IP, we have addresses containing IPs instead of names. In NDN, these tiny data and interest packets are used to retrieve information. In interest packet, we have [*data name*] and in data packet, we have [*data name, unique sign in encrypted form and the data*].

D. ICN-IoT

ICN based IoT is a new direction of research where different smart devices and sensors generate information. ICN creates a new research venue where we retrieve the sensor data through names of contents rather old-style IP structure [12]. Summarized information about different IoT-ICN based applications is given in Table 1.

ICN-IoT aims to provide scalability, security, and efficiency where the data is in huge amount. There are different vulnerabilities such as internal and external attacks, and verification issues. A context-aware implementation of distributed policy along with security features is described in [7]. ICN-IoT based applications are provided in Figure 5.

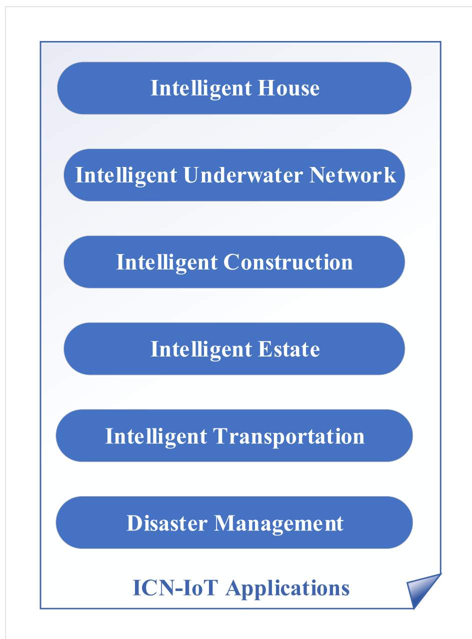


FIGURE 5. ICN-IoT applications taxonomy.

III. NDN BASED DISASTER MANAGEMENT METHODOLOGIES

Smart cities have several integral applications in place where we intend to provide better services to improve daily life. Several systems have been proposed, which leverage state of the art technologies and make the use of information gathered for the service enhancement [32]. Vehicular NDN (VNDN) is another example of the NDN. In VNDN, if some necessary information is lost when needed, an NDN operation will be disturbed. This issue can be handle through PUSH based beacon message could be used.

In another research, Yaqub *et. al.* [36], consider vehicular ICN (VICN) strategies. They have also used PUSH messages for fast network convergence. In this framework, data structure includes 'content ID' which is communicated through

TABLE 1. Future of IoT-ICN applications.

IoT Application	Ref.	Purpose	Procedure	Evaluation Factors	Results
Intelligent house	[30]	NDN based naming scheme architecture along with functional model	Propose NDOMUS framework that consists of data and management planes.	Interleave exchange packets	NDOMUS provides better throughput
	[14]	ICN based cloud framework on the basis of ICN architecture.	Propose ICN-I Sapiens three layered architecture	N.A	N.A
	[1]	Focus on mobility of nodes and its hierarchy architecture.	Propose NDN based smart home architecture that consists of (HS and PC).	ISR Incremental Data fetching delay	NDN outperforms as compared to legacy IP architecture.
Intelligent city	[8]	Smart objects like building, transport, home	Three Layer implementation stages. Discovery stage Protection Initialization stage Provision Usage stage	N.A	N.A
Intelligent Estate	[7]	Naming schemes	Proposed hybrid-NDN naming methodology for IoT-SC	N.A	Evaluate NDN-IoT SC with respect to ISR
Intelligent structure	[30]	Focus on security features of naming schemes	NDN-building-management system.	N.A	N.A
Intelligent Transport	[32]	routing strategies, movement of nodes in VNDN	Beacon based PUSH support for forwarding critical data	Latency b/w data portions	PUSH support is robust and reliable than the PULL support.
DMS	[33]	Efficient memory utilization in disaster scenarios.	Evaluate ICN interest messages in dispersed manner, especially in disaster situations.	Zipf Dissemination Content popularity and weight. Content occurrence	Proposed DICIA outperforms in terms of efficient memory utilization than Reference Algo. (RA)
	[34]	Modification in CCN architecture. Reliable caching retrieval mechanism	SIT data structure is proposed to retrieve cache content when network is partially or completely disseminate	ISR rate Mean Absorption time Min. Hop Distance b/w nodes Node traffic overhead rate	SIT data structure performs better than the legacy flooding mechanism, especially in the situation of disaster case.
	[35]	Mobility of nodes	NDN based emergency message forwarding mechanisms for ETS by ABE support architecture.	N.A	N.A

LONGEST PREFIX MATCH in the FIB. Delay and disruption tolerant network (DTN) is a new type of networking architecture that also uses PUSH notification and beacon messages in case of a disaster [37]. Seedorf *et. al.* use the same beacon message phenomenon in the DTN [35], [38] by utilizing the ICN architecture. ICN-NDN based disaster application taxonomy is provided in Figure 6.

The objective of this paper [37] is to present a framework that uses NDN for disaster management. In disaster conditions, network fragments are formed and interest messages are exchanged with other nodes [39]. Seedorf *et al.* [37] proposed that certain parameters need to be gathered such as location in case of a disaster. Jabbar *et. al.* [40] proposed a lighter adaptation of HTTP called REST system for IoT applications.

Sourlas *et al.* [41] suggested an information flexibility system for CCN/NDN router design. It alters the existing

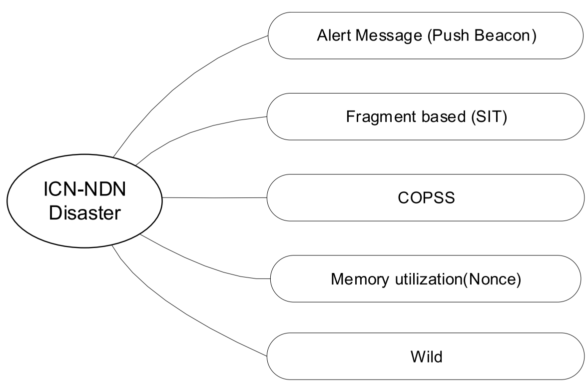


FIGURE 6. Taxonomy of NDN based disaster management methodologies.

NDN/CCN switch architecture design. The interest messages are sent to neighboring clients in case a disaster occurs. The experiments show that their proposed scheme

TABLE 2. Comparison between NDN-fragmented network methodologies.

Ref.	No. of NDN Nodes and Interest Packets	Disaster Support	PULL /PUSH Support	Results
Fragment [41]	50 NDN nodes	Exist	PULL	Traffic overhead by 35 times through SIT as compared to legacy methodology. Other factors like minimum hop distance fluctuate in the start but get stable after some interval.
Decentralized [37]	6 data mules with 8Kb each obj. size	Exist	PULL	Memory utilization get steady rather than viewing unusual exponential actions
PUSH Beacon [32]	Total 384 interest chunks with 10MB object size and 27KB content slots	Not-exist	PULL+PUSH	Critical content size in Push VNDN that decreases the overall transfer time.
ETS [35]	Total calls =2923/day Avg. time b/w calls =30 sec	Exist	PULL	At 100 prosecutions, the decryption time by the ABE algorithm is about 0.13 sec, which infers that solo PC is sufficient to knob all disaster alerts at Tokyo Japan.

performs better and gives higher throughput especially when the infrastructure is destroyed [39]. Hasegawa *et al.* [42], proposed an NDN based crisis message system in light of [43] with the attribute-based message encryption technique [42]. The authors proposed an option for existing cellular networks. Furthermore, the system is adaptive to disaster situations [35]. The comparison between NDN-based Fragmented Network methodologies have been summarized in Table. 2.

IV. NDN-BASED COMMUNICATION MODEL FOR FRAGMENTED NETWORKS

As we know that a fragmented network is formed due to the occurrence of different disasters. Our proposed scheme is based on two different modes, i.e., before and after the occurrence of a disaster.

The proposed solution is divided into different parts. In first task, we detect that disaster has occurred and fragments have been formed up. Detection is based on the threshold value of different sensors. In the next step, we switch the normal mode into disaster mode where the actual working of the model has been started. The alert beacon message [32] will be flooded into the entire network. The flowchart is shown in Figure 7.

To test the scheme, we consider a disaster scenario that has occurred due to the fire. We have used the base model of SIT [41]. Simple NDN model is not capable of handling such kind of scenarios where the information is limited and the network is fragmented. In the proposed scheme, we enhance the architecture to make the NDN network resilient.

The model works well in the case of fragmented networks but there are few limitations, for example, this model takes more processing time to detect and switch between

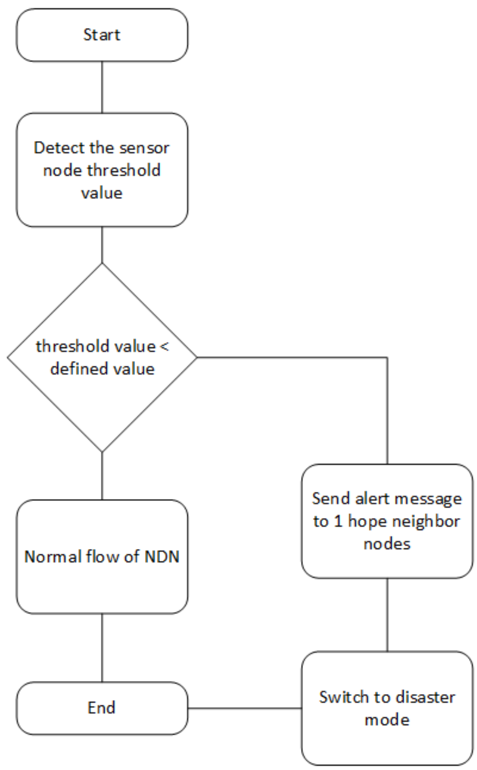


FIGURE 7. Flowchart of the proposed NDN based disaster management scheme.

two modes [41]. In addition, there is no proper mechanism to alert other nodes that now the mode has been changed. Every time when a request comes to the CS, it checks and repeats the whole procedure for that. This affects the overall performance of the model. Our scheme follows the basic model of SIT

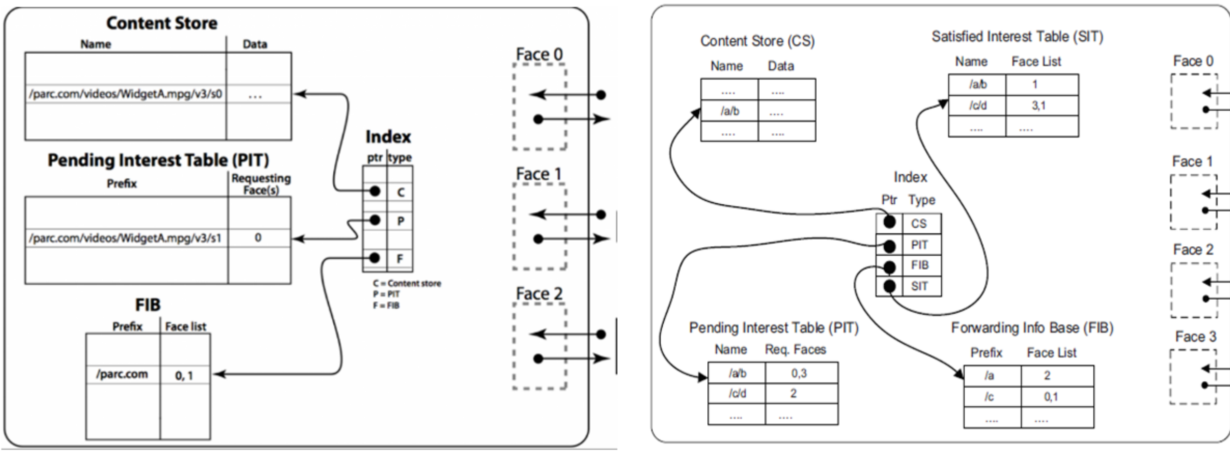


FIGURE 8. Basic NDN and SIT model (Adapted from [41]).

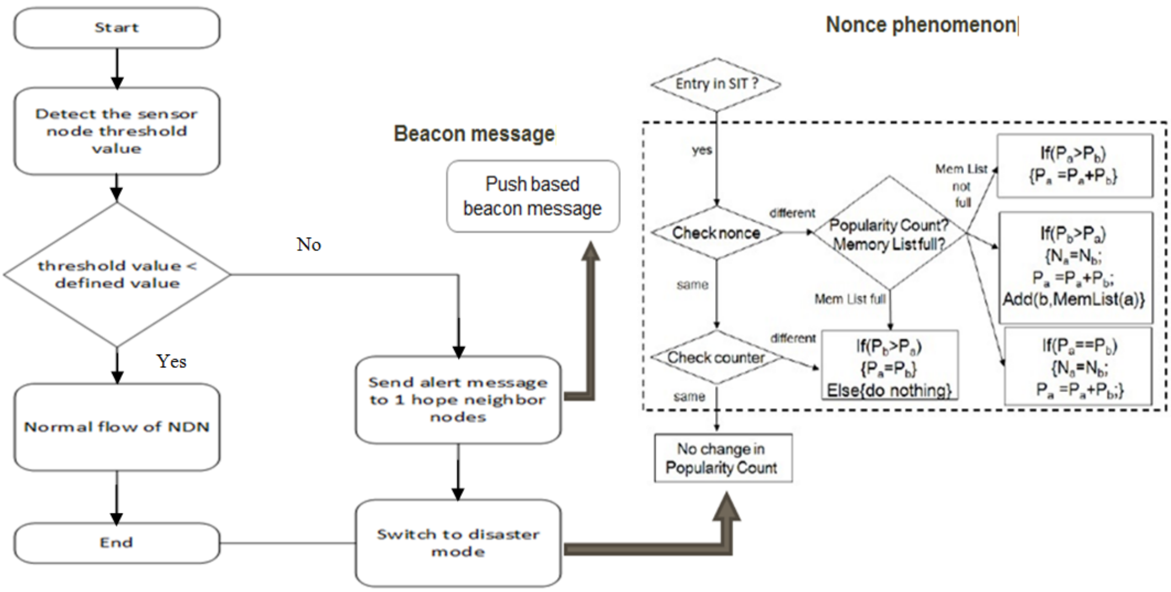


FIGURE 9. The basic flow of proposed scheme along with beacon [32] and nonce [37].

along with different techniques [41]. In Figure 8, the basic model of NDN and SIT has been shown, which describes the disaster management system.

A. EARLY DETECTION AND ALERT MESSAGE

In the literature review section, we have discussed the working of a simple NDN model. The SIT is designed to fulfill the requirements of the basic fragmented network. The working of SIT is divided into the following steps:

1) When packet request comes on the face of CS model, it checks the availability of information, if found, sends it back.
2) If not found in the CS, it checks in the PIT. If found then sends it back.
3) If not found in the PIT, it checks in the FIB table. If found, the request is sent to the respected router and then information is sent back on arrival.
4) If not found in the CS, PIT, and FIB, it checks the information in the SIT table. If the information is found, this means that now the network has been fragmented because this shows that previously the information was part of that network and now due to some reasons this node is not a part of other networks.

The SIT works like cache storage. Though, we are briefly working on the storage parameter in this research work, our scheme utilizes memory efficiently because routers and gateway nodes have limited storage capacity. We have used the sensor value because we are assuming that it is built-in in a router. When the threshold values increase from the pre-defined values, it automatically changes the mode to the disaster mode [41].

In addition, we have used the push-based beacon [32] alert message to alert other nodes in the network. The benefit of this message is that other nodes will change their mode so

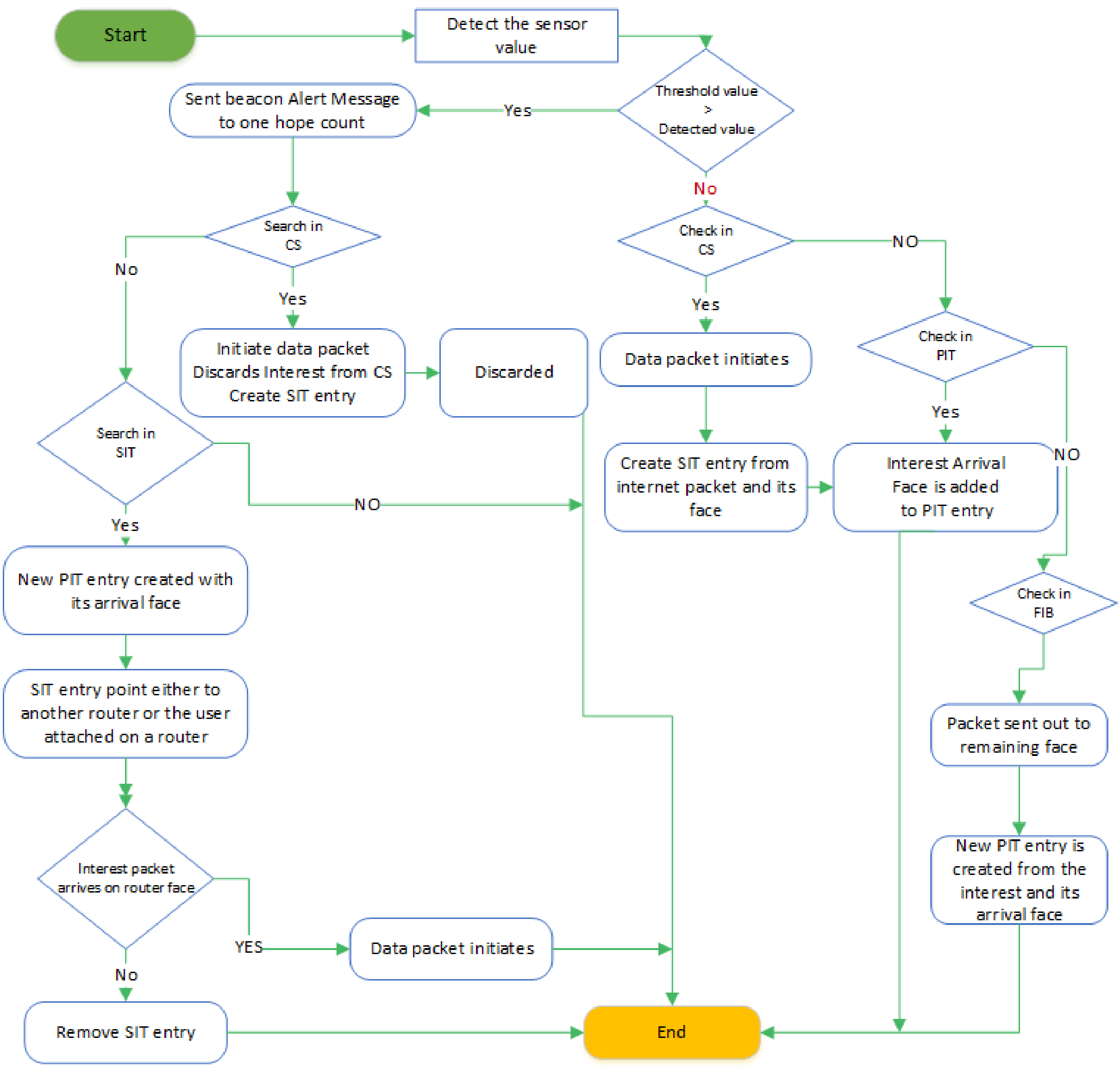


FIGURE 10. **Detail flow control of the proposed NDN-IoT scheme.**

that they do not have to repeat the whole process of finding information in the PIT and FIB.

We have followed the Nonce [37] policy so that the SIT stores the value in an efficient manner as we know that routers have limited storage capacity. Figure 9 shows the basic policy of Nonce [37] along with the special alert message [32].

B. WORKING OF THE PROPOSED SOLUTION

We have used the same concept of SIT along with Special Alert Message (SAM) [32] and proposed a slight change in the given architecture. The SAM is generated from a producer node when the threshold limit of fire sensor is exceeded to its predefined threshold limit, i.e., 50 degrees Celsius. This indicates that now the network is fragmented and the producer will respond to a fixed sequence number. In our scenario, '0' represents the fire disaster state. When consumer nodes get this sequence number in the CS and PIT, it broadcasts the SAM interest packet to its nearly placed consumer nodes. The SAM is forwarded through a multi-hop transmission forwarding technique so that all subscriber nodes receive the packets. On the other hand, '1' represents normal flow, which means that the communication among nodes follows a generic NDN architecture. We have also used the Nonce policy whenever an entry is placed in the SIT [37]. The detailed flow control diagram of the proposed scheme is shown in Figure 10.

C. LIMITATION OF THE PROPOSED SCHEME

There are some limitations in this research that are to be addressed. Firstly, the scheme takes more initialization time to check the sensor value. Secondly, the model utilizes extra bit to store sequence value, and lastly, the scheme utilizes more processing time in normal mode as compared to the SIT due to the comparison of sensor value and threshold value [41].

V. PROOF OF CONCEPT EXPERIMENT

For the fragmentation of network, we used fire disaster scenario in a Metropolitan Area Network (MAN). To design the scenario, we take a group of small buildings. We call it as smart colony (SC). The model architecture of the scenario is illustrated in Figure 11.

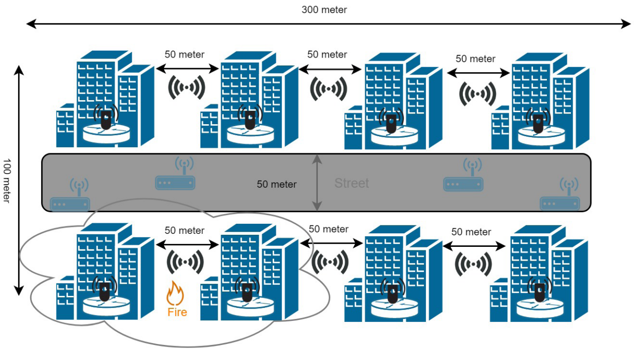


FIGURE 11. Detailed architecture of the proposed scenario.

For the simulation and experiment purposes, we have considered that there are many sensors in a particular building; one of these sensors is the fire sensor, as shown in Figure 11. We consider one building as one cluster. There is only one producer sensor in the building and rest of the sensors act as consumer nodes. Every node is configured with the IEEE 802.15.4 Zig-Bee protocol, which is operated in a normal mode and fragmented mode as described in the proposed scheme. Data packets are requested by consumer nodes from the producers in the normal mode, while an alert is automatically generated from the producer to the consumer nodes when the fire sensor exceeds the threshold limit. This mode is presented as fragment mode. In the fragment mode, crucial data is being transferred from one building to another using a multi-hop wireless communication scheme. Each simulation has run for 500 seconds and the final results have obtained by taking an average of twenty runs. The distribution of nodes in a single cluster (building) is defined in Figure 11.

In a cluster, we placed NDN nodes using the random function. The area covered by clusters is 100 × 300 meters. In each cluster, we have 200 NDN nodes covering the area of 25 × 25 meters, parallel to the street in the proposed scenario, as shown in Figure 2. Every node is using IEEE 802.11 protocol (Wi-Fi). A cluster signifies the buildings and all of these clusters are a part of a society separated by a distance of 50 meters. Each building has all the common attributes, i.e., static nodes, mobile nodes, and hybrid nodes. We used the random-direction model for nodes' mobility. The operating system used for this purpose is Ubuntu 16.04 LTS. The detail description of the experimental setup is defined in Table 3.

VI. RESULTS AND DISCUSSION

For the better understanding of results, we divided our solution into different parts. Initially, we apply the technique

TABLE 3. Experiment details along with different parameters.

Matrix	Detail
Propagation Loss Model	Nakagami Propagation Loss Model
Propagation Delay Model	Constant Speed Propagation Delay Model
Wireless Connectivity	WiFi, ZIG-BEE
Mobility Model	Random-Direction
CS Dimension	1000 messages
Nodes in each cluster (offices)	200
Number of nodes (Smart buildings)	8 Each scattered in the area of 25 x 25
frequency/sec on single messages	8-10 /s
The total covered area in meters	100 x 300
Caching adoption	LCE
Cache replacement algorithm	LRU
Total simulation in unit time	500 sec
Geographical networking	MAN

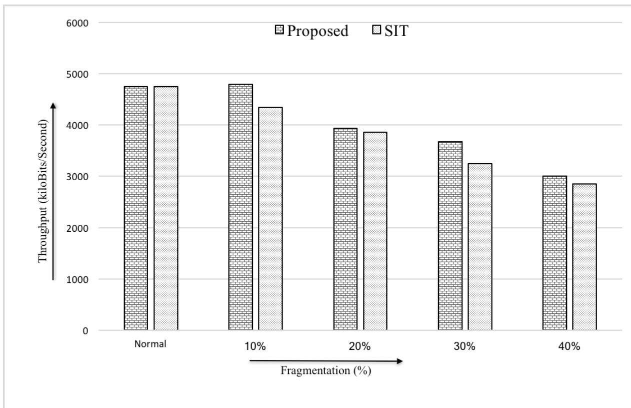


FIGURE 12. Throughput comparison of the proposed methodology with the SIT.

in normal mode, where we say that the entire node structure is connected and no fragments are formed. Secondly, we increased the fragment size, which means that the proposed technique and the SIT are applied on the larger and smaller sizes of nodes [41]. This is achieved through random function. If the random factor is increased, a larger number of nodes will appear disconnected in the simulation results. We run the simulations according to the experimental details. We take 20 simulations to calculate each parameter for better results.

We have compared the proposed scheme with the existing SIT scheme. We have taken different scenarios, where the fragment size is increased variations in the result are investigated. In the metric of latency, the proposed scheme takes more time than the SIT in initialization and sensing the values from the fire sensors, but comparatively, it takes lesser time while switching the mode from normal to the disaster mode [41].

Figure 12 shows the throughput comparison of the proposed solution with the SIT [41]. In normal mode, both techniques have the same throughput because no particular work of sensors is being carried at this point since no fragments are formed up (see Figure 12). When the fragments are formed, the proposed model outperforms the SIT and provides better throughput.

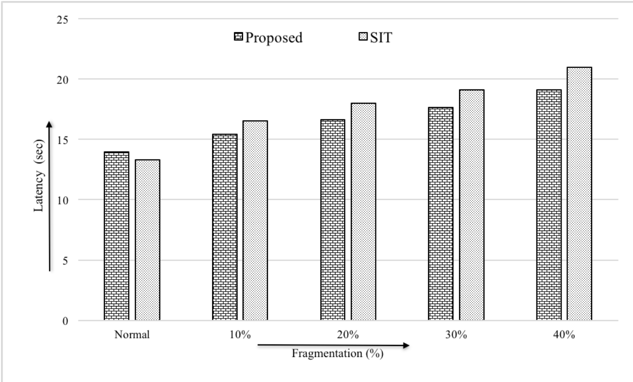


FIGURE 13. Simulation results for the network.

The slight increase in the latency with the normal mode is because of the initialization of devices and switching of the mode. However, during the occurrence of a disaster, results of the proposed scheme are better than the SIT. As the fragment size increases, the latency of in the proposed scheme is lower. The comparison of latency with the SIT is made in Figure 13.

VII. CONCLUSION

In this research, we have proposed a hybrid NDN-IoT based model where network connectivity is either lost or limited due to a disaster scenario. We have used the SIT along with Beacon and Nonce mechanisms provided by NDN to improve the network efficiency in terms of throughput and latency . We defined the early detection mechanism using Beacon alert message for the detection of a disaster. This improved the overall processing time. We have enabled Nonce for better memory utilization and throughput. Working in the scenario of fragments, we simulated the proposed scheme and compared results with those of the SIT for the following parameters: latency and throughput. It is worth to mention that the proposed system outperformed in both metrics. We believe that this research can also be extended for different scenarios such as smart homes, smart transportation, smart buildings, and especially in smart underwater sensor networks where the information is no longer reachable. For the future work, we can improve the following parameters:

1) Network scalability: we can enhance the number of nodes and space in the network
2) Memory: We briefly investigated memory consumption, but as we know that sensors and smart devices have limited memory space, we need improvement in the memory utilization.
3) Model complexity: Smart devices and sensors are less energy efficient. If we have complex node architecture, it will definitely take more power to handle the complexity, therefore, it is still needed to work in the complexity aspect.
4) Architecture modification: We still need a recovery mechanism in case of fragment occurrences.
5) Loop detection: We can also improve the loop detection mechanism with the help of custom built technique.
6) SIT entry: We need an algorithm to reduce the architecture complexity and improve the entry of packet interests in the SIT.

REFERENCES

[1] 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.*, to be published.
[2] S. M. Muzammal *et al.*, “Counter measuring conceivable security threats on smart healthcare devices,” *IEEE Access*, vol. 6, pp. 20722–20733, 2018.
[3] H. A. Khattak, M. Ruta, and E. E. Di Sciascio, “CoAP-based healthcare sensor networks: A survey,” in *Proc. 11th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, Jan. 2014, pp. 499–503.
[4] J. Liu, X. Li, X. Chen, Y. Zhen, and L. Zeng, “Applications of Internet of Things on smart grid in China,” in *Proc. 13th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2011, pp. 13–17.
[5] J. Veijalainen, D. Kozlov, and Y. Ali, “Security and privacy threats in IoT architectures,” in *Proc. 7th Int. Conf. Body Area Netw.*, 2012, pp. 256–262.
[6] J. Iqbal *et al.*, “A generic Internet of Things architecture for controlling electrical energy consumption in smart homes,” *Sustain. Cities Soc.*, vol. 43, pp. 443–450, Nov. 2018.
[7] S. Arshad, M. A. Azam, S. H. Ahmed, and J. Loo, “Towards information-centric networking (ICN) naming for Internet of Things (IoT): The case of smart campus,” in *Proc. Int. Conf. Future Netw. Distrib. Syst. (ICFNDS)*, 2017, Art. no. 41.
[8] G. Piro, I. Cianci, L. A. Grieco, G. Boggia, and P. Camarda, “Information centric services in smart cities,” *J. Syst. Softw.*, vol. 88, pp. 169–188, Feb. 2014.
[9] H. A. Khattak, R. Hussain, and Z. Ameer, “Internet of vehicles: Integrated services over vehicular ad hoc networks,” in *Proc. Int. Conf. Smart Cities, Infrastruct., Technol. Appl.* Cham, Switzerland: Springer, 2017, pp. 61–73.
[10] B. Yildirim, J. F. Lawrence, and R. M. Armitano, “Detecting earthquakes through a network of geographically distributed sensors,” U.S. Patent 2017 0 184 740 A1, Jun. 29, 2017.
[11] S.-Y. Kim, S. Robitzsch, D. Trossen, M. Reed, M. Al-Naday, and J. Riihijärvi, “Realizing IP-based services over an information-centric networking transport network,” in *Proc. Conf. 3rd ACM Conf. Inf.-Centric Netw. (ACM-ICN)*, 2016, pp. 215–216.
[12] M. Amadeo *et al.*, “Information-centric networking for the Internet of Things: Challenges and opportunities,” *IEEE Netw.*, vol. 30, no. 2, pp. 92–100, Mar./Apr. 2016.
[13] G. C. Polyzos and N. Fotiou, “Building a reliable Internet of Things using information-centric networking,” *J. Reliable Intell. Environ.*, vol. 1, no. 1, pp. 47–58, Jul. 2015.
[14] M. Amadeo, A. Molinaro, S. Y. Paratore, A. Altomare, A. Giordano, and C. Mastroianni, “A cloud of things framework for smart home services based on information centric networking,” in *Proc. IEEE 14th Int. Conf. Netw., Sens. Control*, May 2017, pp. 245–250.
[15] C. Fang, H. Yao, Z. Wang, W. Wu, X. Jin, and F. R. Yu, “A survey of mobile information-centric networking: Research issues and challenges,” *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2353–2371, 3rd Quart., 2018.
[16] O. A. Khan *et al.*, “NDN based communication for fragmented network: The case of smart metropolitan (MAN),” in *Proc. 24th Int. Conf. Autom. Comput. (ICAC)*, Sep. 2018, pp. 1–6.
[17] K. Ashton, “That ’Internet of Things’ thing,” *RFID J.*, vol. 22, no. 7, pp. 97–114, 2009.
[18] D. E. Culler, “The once and future Internet of everything,” *GetMobile: Mobile Comput. Commun.*, vol. 20, no. 3, pp. 5–11, Jul. 2016.
[19] M. Hussain *et al.*, “Towards ontology-based multilingual URL filtering: A big data problem,” *J. Supercomput.*, vol. 74, pp. 5003–5021, Oct. 2018.

[20] A. Modarresi and J. P. G. Sterbenz, "Multilevel IoT model for smart cities resilience," in *Proc. 12th Int. Conf. Future Internet Technol. (CFI)*, 2017, Art. no. 7.

[21] N. Kshetri, "The evolution of the Internet of Things industry and market in China: An interplay of institutions, demands and supply," *Telecommun. Policy*, vol. 41, no. 1, pp. 49–67, 2017.

[22] A. Siddiqa *et al.*, "Social Internet of vehicles: Complexity, adaptivity, issues and beyonds," *IEEE Access*, vol. 6, pp. 62089–62106, 2018.

[23] B. Balaji *et al.* (2017). "Modeling actuation constraints for IoT applications." [Online]. Available: https://arxiv.org/abs/1701.01894

[24] "IoT standards & protocols guide | 2018 comparisons on network, wireless comms, security, industrial," *Postscapes*. Accessed: Nov. 26, 2018. [Online]. Available: https://www.postscapes.com/internet-of-things-protocols/

[25] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, and M. Wählisch, "Information centric networking in the IoT: Experiments with NDN in the wild," in *Proc. 1st ACM Conf. Inf.-Centric Netw.*, 2014, pp. 77–86.

[26] M. S. Akbar, K. A. Khaliq, R. N. B. Rais, and A. Qayyum, "Information-centric networks: Categorizations, challenges, and classifications," in *Proc. 23rd Wireless Opt. Commun. Conf.*, May 2014, pp. 1–5.

[27] S. H. Bouk, S. H. Ahmed, D. Kim, K.-J. Park, Y. Eun, and J. Lloret, "LAPEL: Hop limit based adaptive PIT entry lifetime for vehicular named data networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 5546–5557, Jul. 2018.

[28] S. H. Ahmed, S. H. Bouk, M. A. Yaqub, D. Kim, H. Song, and J. Lloret, "CODIE: Controlled data and interest evaluation in vehicular named data networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 6, pp. 3954–3963, Jun. 2016.

[29] W. Shang, Q. Ding, A. Marianantoni, J. Burke, and L. Zhang, "Securing building management systems using named data networking," *IEEE Netw.*, vol. 28, no. 3, pp. 50–56, May/Jun. 2014.

[30] M. Amadeo, C. Campolo, A. Iera, and A. Molinaro, "Information centric networking in IoT scenarios: The case of a smart home," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2015, pp. 648–653.

[31] L. Zhang *et al.*, "Named data networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, 2014.

[32] M. F. Majeed, S. H. Ahmed, and M. N. Dailey, "Enabling push-based critical data forwarding in vehicular named data networks," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 873–876, Apr. 2017.

[33] E. Monticelli, B. M. Schubert, M. Arumaithurai, X. Fu, and K. K. Ramakrishnan, "An information centric approach for communications in disaster situations," in *Proc. IEEE 20th Int. Workshop Local Metrop. Area Netw. (LANMAN)*, May 2014, pp. 1–6.

[34] Y. Shibata, N. Uchida, and N. Shiratori, "A resilient network and information management system for large scale disaster," in *Proc. 30th Int. Conf. Adv. Inf. Netw. Appl. Workshop*, Mar. 2016, pp. 655–660.

[35] H. Yao, Z. Yang, H. Jiang, and L. Ma, "A scheme of ad-hoc-based D2D communication in cellular networks," *Adhoc Sensor Wireless Netw.*, vol. 32, pp. 115–130, May 2016.

[36] M. A. Yaqub, S. H. Ahmed, S. H. Bouk, and D. Kim, "Interest forwarding in vehicular information centric networks: A survey," in *Proc. 31st Annu. ACM Symp. Appl. Comput. (SAC)*, 2016, pp. 724–729.

[37] J. Seedorf, D. Kutscher, and B. S. Gill, "Decentralised interest counter aggregation for ICN in disaster scenarios," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2016, pp. 1–6.

[38] L.-H. Zhang and L. Tang, "DTN earliest-delivery routing algorithm based on routing reliability," in *Proc. IEEE 14th Int. Conf. Commun. Technol.*, Nov. 2012, pp. 449–453.

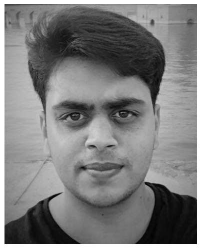
[39] I. Psaras, L. Saino, M. Arumaithurai, K. K. Ramakrishnan, and G. Pavlou, "Name-based replication priorities in disaster cases," in *Proc. IEEE INFOCOM*, Apr./May 2014, pp. 434–439.

[40] S. Jabbar, M. Khan, B. N. Silva, and K. Han, "A REST-based industrial Web of things' framework for smart warehousing," *J. Supercomput.*, vol. 74, no. 9, pp. 4419–4433, 2018.

[41] V. Sourlas, L. Tassiulas, I. Psaras, and G. Pavlou, "Information resilience through user-assisted caching in disruptive content-centric networks," in *Proc. IFIP Netw. Conf. (IFIP Netw.)*, May 2015, pp. 1–9.

[42] T. Hasegawa, Y. Tara, K. Ryu, and Y. Koizumi, "Emergency message delivery mechanism in NDN networks," in *Proc. Conf. 3rd ACM Conf. Inf.-Centric Netw. (ACM-ICN)*, 2016, pp. 199–200.

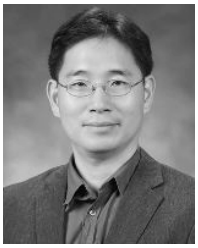
[43] J. Chen, M. Arumaithurai, L. Jiao, X. Fu, and K. K. Ramakrishnan, "COPSS: An efficient content oriented publish/subscribe system," in *Proc. ACM/IEEE 7th Symp. Archit. Netw. Commun. Syst.*, Oct. 2011, pp. 99–110.



OMAIR AHMAD KHAN received the B.Sc. and M.Sc. degrees in computer science from COMSATS University Islamabad, Pakistan, in 2014 and 2016, respectively, and the master's degree in computer science. His M.S. dissertation topic is based on the named data networking-based communication and its applications in smart cities. His current research interests include content-centric networking and named data networking, smart cities, and machine learning.

MUNAM ALI SHAH received the B.Sc. and M.Sc. degrees from the University of Peshawar, Pakistan, in 2001 and 2003, respectively, both in computer science, the M.S. degree in security technologies and applications from the University of Surrey, U.K., in 2010, and the Ph.D. degree from the University of Bedfordshire, U.K., in 2013. Since 2004, he has been with the Department of Computer Science, COMSATS University Islamabad, Pakistan. He has authored over 150 research articles published in international conferences and journals. His research interests include MAC protocol design, QoS and security issues in wireless communication systems, and IoT system design. He received the Best Paper Award from the International Conference on Automation and Computing in 2012.

IKRAM UD DIN (S'15–SM'18) received the M.Sc. degree in computer science and the M.S. degree in computer networking from the Department of Computer Science, University of Peshawar, Pakistan, in 2006 and 2011, respectively, and the Ph.D. degree in computer science from the School of Computing, Universiti Utara Malaysia (UUM). He was a member of the InterNetWorks Research Laboratory, UUM, from 2014 to 2016. He has 10 years of teaching and research experience in different universities/organizations. His current research interests include resource management and traffic control in wired and wireless networks, cloud computing, traffic measurement and analysis for monitoring the quality of service, mobility and cache management in information-centric networking, privacy-preserving information lookup systems for information-centric architectures, and access control mechanisms for distributed content storage. He is a member of the IEEE Communications Society. He also served as the IEEE UUM Student Branch Professional Chair.



BYUNG-SEO KIM (M'02–SM'17) received the B.S. degree in electrical engineering from Inha University, Incheon, South Korea, in 1998, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Florida in 2001 and 2004, respectively. His Ph.D. study was supervised by Dr. Y. Fang. From 1997 to 1999, he worked for Motorola Korea Ltd., Paju, South Korea, as a Computer Integrated Manufacturing Engineer in Advanced Technology Research and Development. From 2005 to 2007, he worked for Motorola Inc., Schaumburg Illinois, as a Senior Software Engineer in Networks and Enterprises. The focuses of his research in Motorola Inc., were designing protocol and network architecture of wireless broadband mission-critical communications. From 2012 to 2014, he was the Chairman of the Department of Software and Communications Engineering, Hongik University, South Korea, where he is currently a Professor. His work has appeared in around 174 publications and 25 patents. His research interests include the design and development of efficient wireless/wired networks, including link-adaptable/cross-layer-based protocols, multi-protocol structures, wireless CCNs/NDNs, mobile edge computing, physical layer design for broadband PLC, and resource allocation algorithms for wireless networks. He served as the General Chair for the General Chair of 3rd IWWCN 2017, and a TPC member for the IEEE VTC 2014-Spring and the EAI FUTURE2016, and ICGHIT 2016 and 2019 conferences. He served as the Guest Editor for special issues of the *International Journal of Distributed Sensor Networks* (SAGE), the IEEE ACCESS, *MDPI Sensors*, and the *Journal of the Institute of Electrics and Information Engineers*. He also served as a member of the Sejong-City Construction Review Committee and the Ansan-City Design Advisory Board. He is an Associate Editor of the IEEE ACCESS.

HASAN ALI KHATTAK received the Ph.D. degree in electrical and computer engineering from the Politecnico di Bari, Bari, Italy, in 2015, the master's degree in information engineering from the Politecnico di Torino, Torino, Italy, in 2011, and the B.CS. degree in computer science from the University of Peshawar, Peshawar, Pakistan, in 2006. Since 2016, he has been an Assistant Professor of computer science. His current research interests focus on distributed system, Web of Things, Vehicular Ad Hoc Networks, and data and social engineering for smart cities. He is involved in a number of funded research projects in Internet of Things, semantic web, and fog computing while exploring Ontologies, Web Technologies using Contiki OS, NS 2/3, and Omnet++ frameworks.

JOEL J. P. C. RODRIGUES (S'01–M'06–SM'06) is currently a Professor and a Senior Researcher at the National Institute of Telecommunications (Inatel), Brazil, and also a Senior Researcher at the Instituto de Telecomunicações, Portugal. He is the Leader of the Internet of Things Research Group, CNPq, and the NetGNA Research Group, the Director of Conference Development–IEEE ComSoc Board of Governors, the IEEE Distinguished Lecturer, the Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the President of the Scientific Council at ParkUrbis–Covilhã Science and Technology Park, the Past-Chair of the IEEE ComSoc Technical Committee on eHealth, the Past-Chair of the IEEE ComSoc Technical Committee on Communications Software, a Steering Committee Member of the IEEE Life Sciences Technical Community and the Publications Co-Chair, and a Member Representative of the IEEE Communications Society on the IEEE Biometrics Council. He is the Editor-in-Chief of two international journals and has been the General Chair and the TPC Chair of many international conferences, including the IEEE ICC, the IEEE GLOBECOM, the IEEE HEALTHCOM, and the IEEE LatinCom. He has authored or co-authored over 650 papers in refereed international journals and conferences, three books, and two patents. He received several Outstanding Leadership and Outstanding Service Awards.

HALEEM FARMAN received the M.S. degree from International Islamic University, Islamabad, Pakistan, in 2008, and the Ph.D. degree in computer science from the Department of Computer Science, University of Peshawar, Pakistan, in 2018. He is currently a Lecturer with the Department of Computer Science, Islamia College Peshawar, Pakistan. He has published several papers in reputed journals and conferences. His fields of interests include wireless sensor networks, Internet of Things and Smart Cities, Big Data, and quality of service issues in wireless networks.

BILAL JAN received the M.S. and Ph.D. degrees from the Department of Control and Computer Engineering, Politecnico di Torino, Italy, in 2010 and 2015, respectively. He has published several papers in reputed journals and conferences. He is currently an Assistant Professor with the Department of Computer Science, FATA University, FR Kohat, Pakistan. His research interests include wireless sensor networks, IoT, deep learning, and high-performance computing.