IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 4, 2020, accepted June 23, 2020, date of publication June 30, 2020, date of current version July 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3005936

Resilient Service Embedding in IoT Networks

HAIDER QAYS AL-SHAMMARI, (Member, IEEE), AHMED Q. LAWEY, (Associate Member, IEEE), TAISIR E. H. EL-GORASHI, AND JAAFAR M. H. ELMIRGHANI, (Senior Member, IEEE)

School of Electrical and Electronic Engineering, University of Leeds, Leeds LS29JT, U.K.

Corresponding author: Haider Qays Al-Shammari (eng.hqs@gmail.com)

This work was supported in part by the Engineering and Physical Sciences Research Council (EPSRC), in part by INTelligent Energy awaRe NETworks (INTERNET) under Grant EP/H040536/1, in part by SwiTching And tRansmission (STAR) under Grant EP/K016873/1, and in part by Terabit Bidirectional Multi-user Optical Wireless System (TOWS) projects under Grant EP/S016570/1.

ABSTRACT The Internet of Things (IoT) can support a significant number of services including those in smart homes and the automation of industries and public utilities. However, the growth of these deployments has posed a significant challenge especially in terms of how to build such deployments in a highly resilient manner. The IoT devices are prone to unpredicted failures and cyber-attacks, i.e. various types of damage, unreliable wireless connections, limited transmission power, computing ability, and storage space. Thus resilience is essential in IoT networks and in the services they support. In this paper, we introduce a new approach to resilience in IoT service embedding, based on traffic splitting. Our study assesses the power consumption associated with the services embedded and the data delivery time. The results are compared to recent approaches in resilience including redundancy and replication approaches. We constructed an optimization model whose goal is to determine the optimum physical resources to be used to embed the IoT virtual topology, where the latter is derived from a business process (BP). The embedding process makes use of the service-oriented architecture (SOA) paradigm. The physical resources of interest include IoT links and devices. The model made use of mixed integer linear programming (MILP) with an objective function that aimed to minimize both the total power consumption and the traffic latency. The optimization results show that the power consumption is reduced and the data delivery time is reduced in the service embedding approach where the proposed traffic splitting approach is employed resulting in the selection of energy efficient nodes and routes in the IoT network. Our methods resulted in up to 35% power saving compared to current methods and reduced the average traffic latency by up to 37% by selecting energy-efficient nodes and routes in IoT networks and by optimizing traffic flow to minimize latency.

INDEX TERMS Energy efficiency, Internet of Things, mixed integer linear programming, queuing, resilience, smart buildings, service-oriented architecture, virtualization.

I. INTRODUCTION

The Internet of Things (IoT) is an emerging technology that can support different devices connected to the Internet to service ubiquitous and pervasive applications. The IoT facilitates the interaction and communication between smart devices and their services by using the Internet infrastructure. IoT can also enable a range of services/applications offered to smart buildings [1]. In a smart building paradigm, the embedded sensors collect data from certain specific places and sends them to the controller for processing and for making decisions seamlessly and efficiently. The IoT devices carry out actions defined by the IoT services. The combination of a smart building and IoT has been used in several paradigms and research studies [2] and poses several challenges when the reliability of services has to be guaranteed. Some of the key challenges are due to the vulnerabilities of the interconnectivity and the interdependencies of the devices and applications. Physical connectivity and hardware limitations can lead to unexpected system failures caused by the failures in the interconnected networks. In addition to the network connectivity, the large heterogeneity of network access technologies increases the complexity of the network and can cause deployment problems in the communication domain. Political and social acceptance challenges may appear as another type of challenge in the form of privacy

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

and civil rights concerns because of the right to access and use the information in the smart building. Furthermore, economic challenges can constrain the financial budget for the replacement and deployment of new technologies [3].

A. PROBLEM STATEMENT

The majority of IoT devices have wireless connectivity, and thus, survivability and failure tolerance are significant considerations. As the IoT plays a significant role in smart building projects. Traffic resilience of an IoT network is also considered an important factor in the design of smart building projects [4], [5]. IoT devices are probably prone to different types of failures and attacks, i.e. various types of damage, computing and transmission power limitations, radio interference, and storage space limitations. The IoT paradigm consists of a heterogeneous combination of Internet-connected devices. Furthermore, traffic routing in IoT networks mainly depends on the routing protocol for low-power and lossy networks (RPL). RPL has been designed to find a single route between the source and the destination nodes [6]. These motivations mean that resilience is a significant consideration in various engineering, scientific, and social applications [7].

Theoretically, resilience can be defined as the capability of a system to accomplish its operation in an appropriate manner notwithstanding disruptions and to regain its performance after a temporary system failure. In communication systems, adverse disruption is a key consideration, and these systems are expected to operate even under adverse disruptions and to rapidly recover to their full functional services [8].

In general, there are many definitions of 'resilience'. The most common one is that it is the ability to operate and maintain a process with an acceptable service level during various faults or attacks [3]. In [1], the researchers defined network resilience as the ability to have at least one operational backup path within a certain minimum time interval when at least one device on the primary path fails.

Practically, network resilience has no metric value but can be estimated using the time the network takes to resume its normal operation after being subjected to disruption [9]. Traffic resilience can be measured by the time required by the network to resume its normal operation after being subjected to disruption [3], [10]. Consequently, it is complicated to estimate network resilience in terms of the quantitative value of network resilience. Another key aspect is the number of failed nodes or links that the network can endure while maintaining its performance [6]. The direct correlation between the network resilience and performance can be established by observing the time required to recover the service from failure, where the queuing delay is considered as a significant factor in network performance. Besides, a problem related to network resilience is the additional transmission overhead and energy consumption needed to provide and ensure resilience. In our proposed model, we obtain better performance with higher savings in energy consumption due to the selection of routes which also reduces the packet delivery times.

B. CURRENT RESILIENCE APPROACHES

In IoT networks, traffic routing mainly relies on RPL, engineered by IETF in 2009 [11]. The RPL protocol is considered to be the de facto routing protocol for the IoT, because of its fit to the IoT requirements and its contributions to the improvement of the communications with other standards in order to provide a baseline architecture for IoT. RPL was designed to find a single route between the source and the destination nodes. Therefore, network resilience is important in this context. Its goal should be to improve the network's ability to handle faults and restore its operation and does not necessarily mean failure resistance [10]. Resource constraints, energy limitations, the unreliability of wireless links and single-path routing are factors that degrade the IoT network resilience and performance. In order to overcome these factors, many research groups have proposed multi-path solutions for the routing protocol in IoT networks.

Among these traffic routing protocols, a popular resilient technique for link failure recovery is multipath routing. This technique is based on the selection of a set of paths between the source device and the destination device to ensure traffic delivery. This technique has the advantage of high resilience but with varying energy consumption and link capacity.

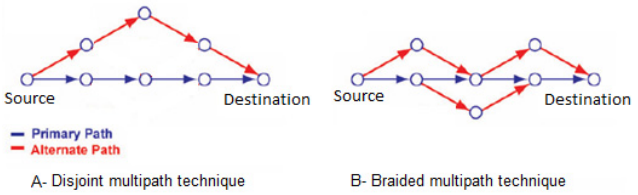


FIGURE 1. Multipath routing techniques.

Multipath routing methods have two main techniques to create their multipath network, as shown in Fig. 1. The first is the disjoint multipath as shown in Fig. 1-A. In this technique, a number of paths with independent nodes/links are created as alternatives to the primary path, and thus, a failure in any or all of the nodes/links on the primary path does not affect any of the alternative paths. The second technique is the braided multipath as shown in Fig. 1-B. In this technique, the alternative paths partially overlay the primary path [12], [13].

Resilient routing protocols in IoT networks [3], [22] are categorized into three types on the basis of the path-finding methodology. The first method is called proactive routing, where all the paths are selected beforehand in the routing table, and the second method is reactive routing, where all the paths are selected on demand and updated in the routing table. The third method is hybrid routing and depends on both of the previous methods [13]. This leads to a probabilistic approach that assumes that the network can tolerate at most n failed nodes where $0 < n < k$, in a k-connected network. The term k-connected network denotes the fact that the network

can preserve its node connectivity after removing no more than k − 1 nodes [14]–[16]. The value of k is an indicator of the network resilience, where a high value of k denotes high network resilience.

C. ORIGINAL CONTRIBUTIONS

In this study, we present a novel resilience technique where traffic is split from the source device to the destination device in two paths, where each path routes 50% of the data traffic and a 'keep-alive' signal is directed on the same paths. When a failure is encountered on one path, the source resends the undelivered data, (which will not exceed 50% of the original data), of the failed path on the second path. Consequently, we save both energy and delivery time. The traffic splitting into two equal values (i.e.50% for each link) gurantees minimum traffic value and arrival rate for each sub-link, consequently, that minimizes the queuing delay. We evaluated the performance and the implications of this technique in terms of the data delivery time and the energy consumption. Our model implemented an optimized service-oriented architecture (SOA). The SOA forms a virtual topology that consists of virtual nodes and links in the form of a business process (BP). The BP encapsulates all the virtual demands represented by processing, sensing and actuating functions and traffic between virtual nodes. Our model maps the virtual topology of each BP to the physical layer of IoT network. An IoT service to be embedded in an IoT network may contain a set of BPs interconnected in a given topology. We built a model to find the optimal set of IoT devices and links to embed BPs as an optimization problem, where the node and route selection is statically determined beforehand by our model with the objective of minimizing both the total power consumption and the traffic latency. This problem was formulated using mixed integer linear programming (MILP). We benefit from our track record in energy efficiency and network virtualization, and track record in IoT service embedding [17]–[19]. In our previous work, [17]–[19], we evaluated the energy efficiency of IoT service embedding with QoS parameters including traffic queuing latency, while in this work, we introduce resilience for the first time to IoT service embedding and evaluate the energy efficiency with the level of resilience considering a range of scenarios. The main contributions of this paper are as follows:

- Modelling the problem of service embedding in IoT networks and evaluating the total power consumption and the queuing delay of service embedding considering a smart building setting.
- Optimizing the selection of IoT nodes and traffic routing to minimize the power consumption and end-to-end delay for different nodes and examining traffic resilient service embedding scenarios.
- Proposing a novel resilience technique based on traffic splitting and evaluating recent resilience techniques such as redundancy and replication in terms of power consumption and end-to-end delay.

The rest of this paper is organized as follows: In Section II, we review the related research. In Section III, we review the resilience techniques in IoT networks. In Section IV, we propose our resilience model, compare it with the recent techniques, and introduce our new technique for the evaluation of the resilience of service embedding. In Section V, we discuss the results obtained. Finally, Section VI concludes this paper.

II. LITERATURE REVIEW

The authors in [1] presented a survey on the modelling, research opportunities and challenges in realizing resilience in IoT in smart cities applications. The survey studied the challenges beyond the complex multi-realm of a multilevel network of the global Internet. The survey also investigated the significant incorporation of the IoT in the context of smart cities and complexity. These challenges are not only in the modelling and structure but are also due to the impact of the heterogeneity of protocols and mechanisms.

The authors in [20] proposed a novel fog security service (FSS). The proposed security mechanism provides identity-based authentication, data integrity, and the non-repudiation of connecting nodes by using a private key generator (PKG). The proposed security mechanism improves the communication security of the end-to-end traffic between the IoT layer and the fog layer. The authors implemented and evaluated their proposed security mechanism in the form of simulation using OPNET. The results displayed performance in terms of the response time for various operations of the proposed security mechanism with different traffic loads. The results showed that the overall response time of FSS was better than that of the legacy method. The proposed work considered the response time as a performance measurement.

The authors in [5] presented a comparative study on the resilience of IoT networks and proposed the most suitable secure mesh routing protocol for IoT-based ambient assisted living (AAL) applications. The proposed architecture, named PASER, was evaluated against denial of service (DoS) attacks. The proposed work introduced position aware secure and efficient route discovery protocol for wireless mesh network (PASER) as routing protocol for sensitive applications. The authors evaluated the performance in terms of the packet delivery ratio, delay and throughput.

The authors in [21] introduced an architecture for data collection and control using blockchain. The proposed architecture considered drone-based applications for sensor data collection. The proposed architecture aimed to reduce potential attacks and data loss by enhancing reliability and accountability, and real-time data collection. They implemented a prototype of the drone system architecture.

The proposed work evaluated the performance in terms of average response time of drone chain with a varying number of drones and with a varying size of data.

The authors in [22] proposed a model for fog computing. The proposed model aimed to improve the QoS for IoT

applications and to support cooperation among fog nodes in each location by serving the largest number of service requests. The proposed model attempted to improve the latency based on an offloading scheme. The proposed model optimized the selection of the fog nodes that share the data processing overload. The proposed model highlighted the benefits of virtualized platforms that provide application services and achieve a sustainable network model.

The authors in [23] proposed an architecture that creates short-term service level agreements (SLAs) dynamically. The proposed architecture maximized user satisfaction and fog profit gains to the cloud subscribers. The proposed architecture built definite workflows for new service requests on the basis of a learning mechanism. The learning mechanism relied on online and offline simulation results. The proposed architecture displayed significant improvements in terms of the service delivery success rate, service quality, reduced power consumption for data centres, and maximized fog service provider profits.

The authors in [24] analysed the communication architecture for IoT platforms and evaluated the effects of the communication on the end-to-end transmission performance. The authors proposed hybrid network infrastructures based on software defined networking (SDN) and redundant non-SDN segments to enhance the communication performance and resilience level of IoT networks. The authors defined an automatic technique that realizes dynamic switching between redundant non-SDN communications. The authors evaluated their proposed architecture in a real network topology through laboratory-scale experiments. The proposed work introduced practical experiments that involve the SDN based architecture to improve the communication performance and evaluated the performance in terms of throughput and Round Trip Time (RRT) of end-to-end communication between the components of the platform.

The authors of [25], [26] developed schemes to enhance the energy efficiency of IoT networks, while the authors of [27] and [28] considered the virtualization of such networks. The authors in [29] considered analytics based big data processing of sensor data. The author in [30] considered big data analytics to enhance actuation efficiency in the network. The authors of [31], [32] discussed greening these big data networks. The authors of [33], [34] evaluated the methodologies that can be used to provide energy efficient clouds to process the IoT data, while the authors in [34], [35] discussed energy efficient content sharing. The energy efficiency of the networks supporting different services was optimized in [36]–[44]. Resilience is a significant parameter for a range of services; hence, in [45], [46], the researchers introduced different methodologies to enhance the resilience level and energy efficiency of their systems. In [47], the researchers considered the use of big data analytics on the basis of the data collected from IoT networks to improve the QoS offered to the users, while in [48], [49], the scholars considered ways to embed functions in the network while maximizing the energy efficiency. The purpose of the above review is to establish a clear idea of the correlation between recent research and our work in this paper and hence identify directions for future studies. In this paper, we presented a a novel resilience technique that enhance the network performance by minimizing data delivery time and reducing cost by minimizing energy consumption compared with recent techniques. We present an optimization model and a range of results for our technique.

III. RESILIENT SERVICE EMBEDDING IN IoT NETWORKS

We developed a model that enhanced the resilience of service embedding in IoT networks (e.g. in a smart building setting). In this paper we, introduce resilience to service embedding for the first time. We studied service embedding in IoT in our work in [17]–[19]. The architecture and the optimization model introduced in this paper structure a network such that it has an acceptable level of fault tolerance and introduce the ability to restore from a node or link failure in the network. The model proposes multilevel resilience, where each probable type of failure (i.e. sensor, controller, or link failure) requires an appropriate level of failure recovery. We evaluated the proposed resilience levels by considering their impact on the end-to-end service delay and energy consumption. The proposed resilience levels are as follows:

A. RESILIENT SERVICE EMBEDDING WITH NODE COEXISTENCE CONSTRAINT

We considered service embedding with a coexistence constraint as the basic level of resilience. This scheme is considered to be the basic solution for a network with a probable temporary failure, i.e. data collision or packet drop.

This resilience scheme is based on a single path between the source and the destination nodes, where the source node ensures the recovery of lost packets by retransmitting them until an acknowledgment is received from the destination node. This scheme has the disadvantages of additional transmission overheads and high network congestion.

B. RESILIENT SERVICE EMBEDDING WITH SENSOR–ACTUATOR NODE REDUNDANCY

To enhance the resilience of IoT networks, we introduced redundant nodes and links for the sensor and actuator nodes. This redundancy scheme enhanced the infrastructure's resilience against service failure or disruptive attacks. We considered the redundant sensing and actuating nodes for accuracy and data fidelity in addition to the resilience concern.

C. RESILIENT SERVICE EMBEDDING WITH ALL-NODE REDUNDANCY

In many services, such as fire protection and security services in public buildings resilience has significant importance. In applications where resilience has high priority over cost of service components, a scheme based on the allocation of redundant components to all nodes enables end-to-end traffic routing with multipath capability.

D. RESILIENT SERVICE EMBEDDING WITH TRAFFIC REDUNDANCY

This scheme is related to traffic resilience and is based on setting up multiple paths between the source and the destination nodes. One of these paths is considered the main or primary path to route the traffic between the nodes, while one or more other paths are considered the alternative or backup paths. These paths are used to recover from a traffic failure of the primary path and are sustained by sending a 'keep-alive' signal continuously over the paths. When a primary path has a failure, the intermediate node sends back the data packet to the source node and sends a failure report to the destination node. As a result, the source and the destination nodes remove the failed path information from the routing table and switch the traffic to an alternative path.

E. RESILIENT SERVICE EMBEDDING WITH TRAFFIC REPLICATION

This scheme fulfils the requirement of resilient traffic by sending multiple replicas of the data over selected multiple paths from the source node to the destination node. This technique has the advantages of a high packet delivery ratio with a low data delivery time, and there is no need for signalling for state maintenance between the source node and the destination node, because even in the case of a partial data packet loss, the destination node can recover the packet from the other copies of the packet. Replication achieves high resilience but at the cost of high energy consumption that arises because of the added traffic and traffic overheads at each node along with the network.

F. RESILIENT SERVICE EMBEDDING WITH TRAFFIC SPLITTING

Here, we propose a technique wherein the traffic is split from the source node to the destination node in two paths, where each path routes 50% of the data traffic and the 'keep-alive' signal is redirected on the same path. When a failure is encountered on one path, the source resends the undelivered data, which does not exceed 50% of the original data, of the failed path on the second path. Consequently, this scheme saves both energy and delivery time. We propose the use of the braided multipath technique in our model. In this technique, the alternative nodes partially overlay the nodes of the primary path to avoid service blockage.

IV. MILP MODEL OF RESILIENT-ENERGY EFFICIENT SERVICE EMBEDDING IN IoT NETWORKS

In this section, we introduce our model developed to embed services in IoT networks in a smart building setting. This model is based on MILP optimization with the objective of minimizing the total power consumption and the traffic mean latency of the service embedding in IoT networks and enhancing the node/traffic resilience level.

A. MODEL DEFINITIONS

The model in this section is based on our previous work in [19]. We reproduce that model here for completeness and to help the flow, but add the new features needed to achieve resilience. These include for example the new primary and secondary variables $R1_{cdef}^{TR}$ and $R2_{cdef}^{TR}$; I_{cdef}^{R1} and I_{cdef}^{R2}; R_{ef}^{TRFL1} and R_{ef}^{TRFL2}. The new features also include the new equations (2), (4), (18) – (30), (35) and (36). Before introducing the model, we define the following sets, parameters, and variables:

1) SETS

B	Set of business processes (BPs) in the virtual layer
V	Set of virtual nodes in each BP
VN_{ia}	Set of neighbors of each virtual node in each BP ($i \in B, a \in V$)
P	Set of IoT nodes in the physical layer
PN_c	Set of neighbors of IoT nodes ($c \in P$)
F	Set of functions supported by IoT nodes
Z	Set of zones in the IoT physical layer
λ	Set of arrival rates
W_j	Set of mean latency per arrival rate (j $\in \lambda$) in ms per packet

2) PARAMETERS

V_{ian}^{FUNC}	$V_{ian}^{FUNC} = 1$ If virtual node a in BP i requires the function n, $V_{ian}^{FUNC} = 0$ otherwise
V_{iaz}^{ZONE}	$V_{iaz}^{ZONE} = 1$ If virtual node a in BP i requires zone z, $V_{iaz}^{ZONE} = 0$ otherwise
V_{ia}^{MCU}	Processing requirement of the virtual node a in BP i in MHz
V_{ia}^{RAM}	Memory requirement of the virtual node a in BP i in kB
V_{iab}^{TRFIC}	Traffic demand between the virtual node pair (a, b) in BPi in kb/s
P_{cn}^{FUNC}	$P_{cn}^{FUNC} = 1$ If IoT node c can provide the function n, $P_{cn}^{FUNC} = 0$ otherwise.
P_{cz}^{ZONE}	$P_{cz}^{ZONE} = 1$ If the IoT node c is located in zone z, $P_{cz}^{ZONE} = 0$ otherwise.
P_{c}^{MCU}	Processing capability of the IoT node c in MHz.
P_{c}^{RAM}	Memory capability of the IoT node c in kB.
P_{ef}^{DIST}	Distance between the neighboring IoT nodes pair (e, f) in meters.
P_{c}^{IDLECP}	Idle processor power in each IoT node c in mW.
P_{c}^{MAXCP}	Maximum processor power consumption in each IoT node c in mW.
P_{c}^{IDLETP}	Idle network power consumption in each IoT node c in mW.
E_{ef}^{PBT}	Energy per bit for each IoT link (e, f) in mW/kbps.
M	Large number ($=10^8$).
P_{e}^{CAPT}	Link capacity for each IoT node (e) in kbps.
F_{ef}^{TR}	Transmit amplifier factor for each IoT link (e, f) in mW/kbps/m^2.

3) VARIABLES

I_{iac}^{NE}	I_{iac}^{NE} is node embedding indicator, $I_{iac}^{NE} = 1$ If virtual node a in BP i has been embedded in IoT node c, $I_{iac}^{NE} = 0$ otherwise.
I_{iacn}^{F}	I_{iacn}^{F} is function embedding indicator, $I_{iacn}^{F} = 1$ if IoT node c has the function n required by virtual node a in BP i, $I_{iacn}^{F} = 0$ otherwise.
I_{iacz}^{Z}	I_{iacz}^{Z} is zone embedding indicator, $I_{iacz}^{Z} = 1$ if IoT node c is located in zone z required by virtual node a in BP i, $I_{iacz}^{Z} = 0$ otherwise.
I_{iabcd}^{LE}	I_{iabcd}^{LE} is link embedding indicator, $I_{iabcd}^{LE} = 1$ if the neighboring virtual nodes (a, b) in BP i have been embedded in IoT nodes (c, d), $I_{iabcd}^{LE} = 0$ otherwise.
X_{iabcd}^{XOR}	Dummy binary variable
R_{cd}^{TRFP}	Embedded traffic demand between IoT nodes (c, d) in kbps.
$R1_{cdef}^{TR}$	Primary path between IoT nodes (c, d) traversing the neighboring IoT nodes (e, f) in kbps.
$R2_{cdef}^{TR}$	Secondary path between IoT nodes (c, d) traversing the neighboring IoT nodes (e, f) in kbps.
I_{cdef}^{R1}	Primary path indicator, $I_{cdef}^{R1} = 1$ If the traffic demand between IoT nodes (c, d) traverses neighboring IoT nodes (e, f), $I_{cdef}^{R1} = 0$ otherwise.
I_{cdef}^{R2}	Secondary path indicator, $I_{cdef}^{R2} = 1$ If the traffic demand between IoT nodes (c, d) traverses neighboring IoT nodes (e, f), $I_{cdef}^{R2} = 0$ otherwise.
R_{ef}^{TRFL1}	Traffic in first alternative path between neighboring IoT nodes (e, f) in kbps.
R_{ef}^{TRFL2}	Traffic in second alternative path between neighboring IoT nodes (e, f) in kbps.
R_{f}^{TRFN}	Arrival rate of IoT nodes (f) in kbps.
LI_{fj}^{Lmbda}	Lambda indicator for each IoT node (f) with corresponding arrival rate (j) then $LI_{fj}^{\text{Lmbda}} = 1$, otherwise 0.
W_{f}^{NODE}	Traffic mean latency for each node (f) in ms.
I_{c}^{PM}	$I_{c}^{PM} = 1$ if the processing module indicator of IoT node c is powered on, $P_{c}^{PM} = 0$ otherwise.
I_{c}^{TM}	$I_{c}^{TM} = 1$ if the network module indicator of IoT node c is powered on, $I_{c}^{TM} = 0$ otherwise.
TPP	Total processing power consumption in the IoT network in mW.
TNP	Total network power consumption in the IoT network in mW.
TL	Total traffic mean latency in the primary path in ms.

B. MODEL OBJECTIVE FUNCTION

The proposed model minimizes the power consumption and the queuing latency in an IoT network by using the following objective function:

$$\textbf{Objective} : \textbf{minimize } \boldsymbol{\alpha}.\boldsymbol{TL} + \boldsymbol{\beta}.\boldsymbol{TPP} + \boldsymbol{\gamma}.\boldsymbol{TNP} \tag{1}$$

where the first term represents the IoT network total latency, the second term represents the total processing power consumption and the last term represents the total network power consumption; and α, β, and γ are the weight values thus used for magnitude and units. The model selects the traffic value for each link in the network that preserves low power consumption and low mean traffic latency at the given values of the arrival rate. To enhance the optimality of the power saving and latency minimization, we used the weight values given in our former work ($\alpha = 30$/ms, $\beta = 1$/mW, and $\gamma = 1$/mW) [19].

Here, the total traffic latency for the IoT nodes can be calculated as follows:

$$TL = \sum_{f \in P} W_{f}^{NODE} \tag{2}$$

where W_{f}^{NODE} represents the average waiting time of the packets waiting to be processed for each IoT node in milliseconds according to the queuing waiting time.

TPP is the total processing power and can be calculated as follows:

$$TPP = \sum_{c \in P} I_{c}^{PM} \cdot P_{c}^{IDLECP} + \sum_{c \in P} \sum_{i \in B} \sum_{a \in V} I_{iac}^{NE} \cdot P_{c}^{MAXCP} \cdot \frac{V_{ia}^{MCU}}{P_{c}^{MCU}} \tag{3}$$

where I_{c}^{PM} is a binary variable used as processing indicator in IoT node c, P_{c}^{IDLECP} is a parameter that presents the idle processing power value of IoT node c in milliwatts, I_{iac}^{NE} is a binary variable embedding indicator of virtual node a in BP i embedded in IoT node c, P_{c}^{MAXCP} is a parameter that represents the maximum CPU power consumption value for each IoT node c in milliwatts, V_{ia}^{MCU} is a parameter that specifies the processing demand of virtual node a in BP in megahertz, and P_{c}^{MCU} is a parameter that specifies the processing capability of the IoT node c in megahertz.

Here, the network power consumption in the IoT network can be expressed as follows:

$$\begin{aligned} TNP = & \sum_{e \in P} I_{e}^{TM} \cdot P_{e}^{IDLETP} \\ & + 2 \cdot \sum_{e \in PN} \sum_{f \in PB_e} R_{ef}^{TRFL1} \cdot E_{ef}^{PBT} \\ & + 2 \cdot \sum_{e \in PN} \sum_{f \in PB_e} R_{ef}^{TRFL2} \cdot E_{ef}^{PBT} \\ & + \sum_{e \in PN} \sum_{f \in PB_e} R_{ef}^{TRFL1} \cdot (P_{ef}^{DIST})^2 \cdot F_{ef}^{TR} \\ & + \sum_{e \in PN} \sum_{f \in PB_e} R_{ef}^{TRFL2} \cdot (P_{ef}^{DIST})^2 \cdot F_{ef}^{TR} \end{aligned} \tag{4}$$

where I_{e}^{TM} is a binary variable that indicates an active network module in IoT node e, P_{e}^{IDLETP} is the idle network

power consumption parameter of IoT node e, R_{ef}^{TRFL1} and R_{ef}^{TRFL2} indicate the primary and alternative paths,' traffic between neighboring IoT nodes (e, f) in kilobits per second, E_{ef}^{PBT} represents the energy per bit of each IoT link (e, f) in milliwatts per kilobit per second, P_{ef}^{DIST} denotes the distance between the neighboring IoT nodes pair (e, f) in meters, and F_{ef}^{TR} represents the transmit amplifier factor [50] for each IoT link (e, f) in milliwatts per kilobit per second per metre square.

C. MODEL CONSTRAINTS

The proposed model performs the embedding operation in two parts as follows:

1) EMBEDDING OF VIRTUAL NODES

$$\sum_{c\in P} I_{iac}^{NE} = 1 \quad \forall i \in B,\ \forall a \in V \tag{5}$$

$$\sum_{a\in V} I_{iac}^{NE} \leq 1 \quad \forall i \in B,\ \forall c \in P \tag{6}$$

Constraint (5) ensures that each virtual node in a BP is embedded in a single IoT node only. Constraint (6) states that each IoT node is not allowed to host more than one virtual node in each BP. This is considered the coexistence constraint and is not used in all the scenarios, such as controller node virtualization.

$$\sum_{i\in B}\sum_{a\in V} I_{iac}^{NE} \geq I_{c}^{PM} \quad \forall c \in P \tag{7}$$

$$\sum_{i\in B}\sum_{a\in V} I_{iac}^{NE} \leq I_{c}^{PM} \cdot M \quad \forall c \in P \tag{8}$$

Constraints (7) and (8) add a processing module in IoT node c if this node is chosen for embedding at least one virtual node a in BP i or more, where M is a sufficiently large unitless number to ensure that $P_c^{PMI} = 1$ when $\sum_{i\in B}\sum_{a\in V} P_{iac}^{NE}$ is greater than zero.

$$\sum_{i\in B}\sum_{a\in V} V_{ia}^{MCU} \cdot I_{iac}^{NE} \leq P_{c}^{MCU} \quad \forall \mathrm{c} \in \mathrm{P} \tag{9}$$

$$\sum_{i\in B}\sum_{a\in L} V_{ia}^{RAM} \cdot I_{iac}^{NE} \leq P_{c}^{RAM} \quad \forall \mathrm{c} \in \mathrm{P} \tag{10}$$

Constraints (9) and (10) represent the MCU and the memory capacity constraints, respectively. They ensure that the embedded MCU and memory workloads in an IoT node do not exceed the processor and memory capacities, respectively.

$$I_{iac}^{NE} \cdot V_{ian}^{FUNC} = I_{iacn}^{F} \tag{11}$$

$$P_{cn}^{FUNC} \geq I_{iacn}^{F} \quad \forall i \in B,\ \forall a \in L,\ \forall c \in P,\ \forall n \in F \tag{12}$$

Constraints (11) and (12) ensure that the required function of each virtual node in a BP is provided by its hosting IoT node by creating a binary indicator I_{iacn}^{F}, where $I_{iacn}^{F} = 1$ if the virtual node a in BP i is requesting function n and that function n is available in IoT node c.

$$I_{iac}^{NE} \cdot V_{iaz}^{ZONE} = I_{iacz}^{Z} \tag{13}$$

$$P_{cz}^{ZONE} \geq I_{iacz}^{Z} \quad \forall i \in B,\ \forall a \in V,\ \forall c \in P,\ \forall z \in Z \tag{14}$$

Constraints (13) and (14) ensure that the required zone of each virtual node in BP is matched by the zone of the hosting IoT node by creating a binary indicator I_{iacz}^{Z}, where $I_{iacz}^{Z} = 1$ if the virtual node a in BP i is requesting to be embedded in zone z which is the same zone where IoT node c is located.

2) EMBEDDING OF VIRTUAL LINKS

$$I_{iac}^{NE} + I_{ibd}^{NE} = X_{iabcd}^{LE} + 2 \cdot I_{iabcd}^{LE} \quad \forall i \in B,\ \forall a \in V,\ \forall b \in VN_{ia} : a \neq b,\ \forall c, d \in P : c \neq d \tag{15}$$

Constraint (15) ensures that neighboring virtual nodes a and b of i in B are also connected in embedding IoT nodes c and d. We achieved this by introducing a binary variable I_{iabcd}^{LE}, which is only equal to 1 if I_{iac}^{NE} and I_{ibd}^{NE} are exclusively equal to 1; otherwise, it is zero, when X_{iabcd}^{LE} is a neglected variable.

$$\sum_{i\in B}\sum_{a\in L}\sum_{b\in LNB_{ia}} I_{iabcd}^{LE} \cdot V_{iab}^{TRFIC} = R_{cd}^{TRFP} \quad c, d \in P : c \neq d \tag{16}$$

Constraint (16) generates the path's traffic matrix resulting from embedding virtual nodes a and b into IoT nodes c and d. Here, I_{iabcd}^{LE} is the binary indicator of the traffic between the embedding nodes and V_{iab}^{TRFIC} is the parameter of the traffic demand between the virtual nodes.

a: RETRANSMISSION- AND REPLICATION-BASED SCHEMES

In these schemes, the proposed model finds two energy-efficient routes for the traffic between the embedded nodes, namely the primary and the alternative routes.

$$\sum_{f\in PN_e} R_{cdef}^{TR1} - \sum_{f\in PN_e} R_{cdfe}^{TR1} \begin{cases} R_{cd}^{TRFP} & if\ e = c \\ -R_{cd}^{TRFP} & if\ e = d \\ 0 & otherwise \end{cases} \quad \forall c, d, e \in P : c \neq d\ and\ e \neq f \tag{17}$$

Constraint (17) represents the flow conservation constraint for the traffic flows in the IoT network. The constraint states the IoT node is either a source, a relay, or a destination node according to the traffic flowing into or out of the node.

$$\sum_{c\in P}\sum_{d\in P} R_{cdef}^{TR1} = R_{ef}^{TRFL1} \quad \forall e \in P,\ \forall f \in PN_e \tag{18}$$

Constraint (18) generates a link's traffic matrix between the neighboring IoT nodes e and f by summing the total traffic between all of the source and the destination nodes.

$$R_{cdef}^{TR1} \geq I_{cdef}^{R1} \tag{19}$$

$$R_{cdef}^{TR1} \leq I_{cdef}^{R1} \cdot M \quad \forall c, d, e \in PN,\ \forall f \in PB_e : c \neq d,\ e \neq \mathrm{f} \tag{20}$$

Constraints (19) and (20) build the primary path indicator between embedding IoT nodes c and d through neighboring IoT nodes e and f, where $I^{R1}_{cdef} = 1$ if there is a traffic path between IoT nodes c and d that passes through neighboring IoT nodes e and f, where M is a sufficiently large unitless number to ensure that $R^{R1}_{cdef} = 1$ when R^{ROUTE1}_{cdef} is greater than zero.

$$\sum_{f \in PB_e} I^{R1}_{cdef} \leq 1 \quad \forall c, d, e \in PN : c \neq d \text{ and } e \neq f \quad (21)$$

Constraint (21) ensures that traffic splitting is prevented for each path between embedding IoT nodes c and d, such that the maximum number of physical links between neighboring IoT nodes e and f is one.

$$\sum_{f \in PN_e} R^{TR2}_{cdef} - \sum_{f \in PN_e} R^{TR2}_{cdfe} \begin{cases} R^{TRFP}_{cd} & \text{if } e = c \\ -R^{TRFP}_{cd} & \text{if } e = d \\ 0 & \text{otherwise} \end{cases}$$
$$\forall c, d, e \in PN : c \neq d \text{ and } e \neq f \quad (22)$$

Constraint (22) represents the flow conservation constraint for the alternative path's traffic flows in the IoT network.

$$\sum_{c \in P} \sum_{d \in P} R^{TR2}_{cdef} = R^{TRFL2}_{ef} \quad \forall e \in PN, \ \forall f \in PB_e \quad (23)$$

Constraint (23) generates the alternative link's traffic matrix between neighboring IoT nodes e and f.

$$R^{TR2}_{cdef} \geq I^{R2}_{cdef} \quad (24)$$
$$R^{TR2}_{cdef} \leq I^{R2}_{cdef} \cdot M \quad \forall c, d, e \in PN, \ \forall f \in PB_e : c \neq d, e \neq \text{f} \quad (25)$$

Constraints (24) and (25) build the alternative path between embedding IoT nodes c and d through neighboring IoT nodes e and f, where $R^{R2}_{cdef} = 1$ if there is a traffic path between IoT nodes c and d that passes through neighboring IoT nodes e and f, where M is a sufficiently large unitless number to ensure that $I^{R2}_{cdef} = 1$ when R^{TR2}_{cdef} is greater than zero.

$$\sum_{f \in PB_e} R^{R2}_{cdef} \leq 1 \quad \forall c, d, e \in PN : c \neq d \text{ and } e \neq f \quad (26)$$

Constraint (26) ensures that traffic splitting is prevented for each path between embedding IoT nodes c and d, such that the maximum number of physical links between neighboring IoT nodes e and f is one.

$$I^{R1}_{cdef} + I^{R2}_{cdef} \leq 1 \quad \forall c, d, e \in PN, \ \forall f \in PB_e : c \neq d, e \neq \text{f} \quad (27)$$

Constraint (27) ensures the creation of two distinct paths between embedding IoT nodes c and d such that each path uses different physical links between neighboring IoT nodes e and f.

$$\sum_{c \in PN} \sum_{d \in PN} \sum_{f \in PB_e} I^{R1}_{cdef} + I^{R2}_{cdef} \geq I^{TM}_{e} \quad (28)$$
$$\sum_{c \in PN} \sum_{d \in PN} \sum_{f \in PB_e} R^{R1}_{cdef} + R^{R2}_{cdef} \leq I^{TM}_{e} \cdot M$$
$$e \in PN : c \neq d \text{ and } e \neq f \quad (29)$$

Constraints (28) and (29) build a network module indicator of IoT node e if this IoT node is chosen for the send/receive traffic for at least one link or more, where M is a sufficiently large unitless number to ensure that $I^{TM}_{e} = 1$ when $\sum_{c \in PN} \sum_{d \in PN} \sum_{f \in PB_e} I^{R1}_{cdef} + I^{R2}_{cdef}$ is greater than zero.

$$\sum_{e \in PN_f} R^{TRFL1}_{ef} + R^{TRFL2}_{ef} = R^{TRFN}_{f} \quad \forall f \in P : e \neq \text{f} \quad (30)$$

Constraint (30) estimates the arrival traffic for each IoT node.

$$\sum_{f \in P} R^{TRFN}_{f} \leq CAPACITY \quad (31)$$

Constraint (31) states that the total traffic flow of the IoT node f should not exceed the node capacity.

$$\sum_{j \in J} LI^{LMBDA}_{fj} \cdot j = R^{TRFN}_{f} \quad \forall f \in P \quad (32)$$

Constraint (32) determines the arrival rate for each IoT node.

$$\sum_{j \in J} LI^{LMBDA}_{fj} \leq 1 \quad \forall f \in P \quad (33)$$

Constraint (33) ensures that each IoT node has only one arrival rate indicator.

$$\sum_{j \in J} W^{LIMDA}_{j} \cdot LI^{LMBDA}_{fj} = W^{NODE}_{f} \quad \forall f \in P \quad (34)$$

Constraint (34) estimates the traffic delay for each IoT node f on the basis of the product of the lambda indicator and the corresponding latency for this lambda j.

In this section, we propose a traffic splitting-based resilience scheme through the multipath routing concept to reduce the arrival rates through the intermediate nodes; doing so will consequently minimize the delivery time in addition to enhancing the resilience of the IoT network.

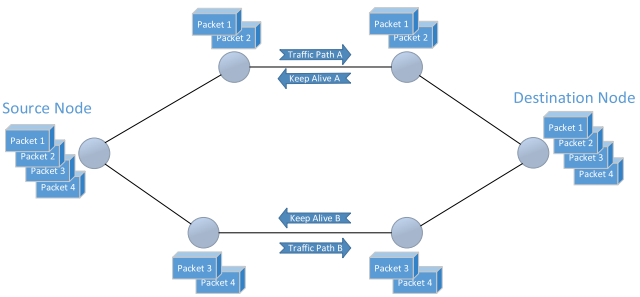


FIGURE 2. Traffic splitting scheme.

The proposed model splits the traffic between the source node and the destination node and routes it on two paths (A and B), as shown in Fig. 2. The source node sends one half of the traffic through path A and the other half through path B to the destination node, and the source node receives a 'keep-alive' signal continuously from both paths (A and B). Once a failure occurs on one path, the source no longer receives an acknowledgement from this path and therefore switches the traffic to another path. The traffic splitting into two equal

values (i.e. 50% for each link) guarantees minimum traffic value and arrival rate for each sub-link, consequently, that minimizes the queuing delay.

Let us suppose that the source node has 100 packets to send to the destination node. The source node selects two paths and sends 50 packets on each path to the destination node. In a probabilistic scenario in which one link has failed, the source node will resend only 50 packets or less rather than resending all of the 100 packets as in the case of retransmission.

In this scheme, the proposed model finds the two best routes in terms of energy efficiency for the traffic between the embedded nodes, namely the primary and the secondary routes. The main difference between this splitting scheme and the former schemes is the flow conservation constraints in (17) and (22).

$$\sum_{f \in PN_e} P_{cdef}^{ROUTE1} - \sum_{f \in PN_e} P_{cdfe}^{ROUTE1} \begin{cases} 0.5 \cdot P_{cd}^{TRFP} & if\ e = c \\ -0.5 \cdot P_{cd}^{TRFP} & if\ e = d \\ 0 & otherwise \end{cases}$$
$$\forall c, d, e \in PN : c \neq d \text{ and } e \neq f \quad (35)$$

$$\sum_{f \in PN_e} P_{cdef}^{ROUTE2} - \sum_{f \in PN_e} P_{cdfe}^{ROUTE2} \begin{cases} 0.5 \cdot P_{cd}^{TRFP} & if\ e = c \\ -0.5 \cdot P_{cd}^{TRFP} & if\ e = d \\ 0 & otherwise \end{cases}$$
$$\forall c, d, e \in PN : c \neq d \text{ and } e \neq f \quad (36)$$

Constraints (35) and (36) represent the flow conservation constraints for the primary and secondary paths for the traffic splitting scheme.

V. RESULTS AND DISCUSSION

Our proposed model has introduced resilience to service embedding by adding alternate/redundant nodes, links and paths. This provides higher network resilience, however, can have implications on the power consumption and latency. In traditional resilience approaches, little attention has been given to the potential increase in power consumption and latency and ways in which they can be minimized. This is the focus of our current work; network resilience and the power consumption and latency are directly correlated. In this work, our focus is on embedding and routing techniques that can reduce the impact of the added resilience on power consumption and latency.

To evaluate the performance of our proposed resilience and service embedding approaches, we considered a smart building paradigm (i.e. enterprise or university campus) where the physical layer is composed of 30 IoT nodes connected by 89 bidirectional wireless links. We considered this number of IoT nodes and links to cover all the facilities of the university's buildings across the campus in an area of 500 m × 500 m, considering a maximum link distance of less than 100 m between the neighboring nodes. These IoT nodes

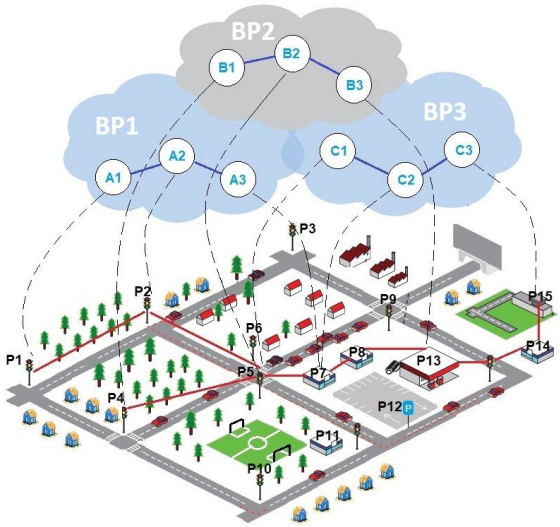


FIGURE 3. Service embedding layers in IoT networks.

were distributed randomly in buildings across the campus, as shown in Fig. 3.

A similar setting was considered in our former work in [17]–[19]. We investigate the service embedding with sequential arriving, one at a time up to 5 BPs. Each BP is composed of three sequential virtual nodes. Each virtual node requests a specific function (sensor, controller and actuator), to be embedded in a given zone. The traffic demands of each virtual link have been specified from 50 to 200 packets per second with consideration of 1 kb packet payload, that presents 20-80% of the physical links capacity.

We evaluated the power consumption and the mean traffic latency resulting from resilient service embedding across distinct zones with the coexistence constraint. The model considered the objective function discussed in Section IV–B for energy efficient–low latency service embedding. Tables 1 and 2 list the model input parameters [51]. A comprehensive description of the setup and the processors used in each IoT node can be found in our previous work in [19].

TABLE 1. MILP model input parameters.

Parameter Description	Value and Unit
Energy per bit	50 nJ/bit
Maximum traffic capacity of node	250 kb/s
Packet size	128 byte
Maximum link distance	100 m
Transmitter amplifier power coefficient	255 pJ/bit. m^2
Scale factor with large value (M)	1000000

The classic probabilistic failure and resilience model is based on k-connected nodes with the assumption that the network has the ability to recover from failures in the case of a link or node failure. This assumption has considered that all the nodes and links have the same level of reliability,

TABLE 2. Processing modules power specifications and power consumption in active mode.

MCU Type	MCU CLK	Idle Power	Max. Power
MSP430F1	8 MHz	1 mW	8 mW
MSP430FR5	16 MHz	1 mW	14 mW
MSP430FR6	16 MHz	1 mW	20 mW
MSP430F5	25 MHz	1 mW	14 mW
MSP432P4	48 MHz	1 mW	16 mW

availability and QoS. We used our model to evaluate two resilience schemes:

A. ENERGY EFFICIENT–LOW LATENCY NODE-RESILIENT SERVICE EMBEDDING

For the node-resilient scheme, we run three resilience levels with the objective of minimizing the total power consumption and the mean traffic latency:

- Coexistence constraint node resilience (CCNR)
- Partial redundancy node resilience (PRNR)
- Full redundancy node resilience (FRNR)

The results in Fig. 4 show the total power consumption of CCNR, PRNR, and FRNR. These results were compared to those obtained in the energy-latency-resilience unaware (ELRU) scenario. The results demonstrated that the CCNR scenario had an average power saving of 35% compared with the ELRU scenario. While the higher level of power consumption in the PRNR scenario had an average power saving of 10% compared with ELRU.

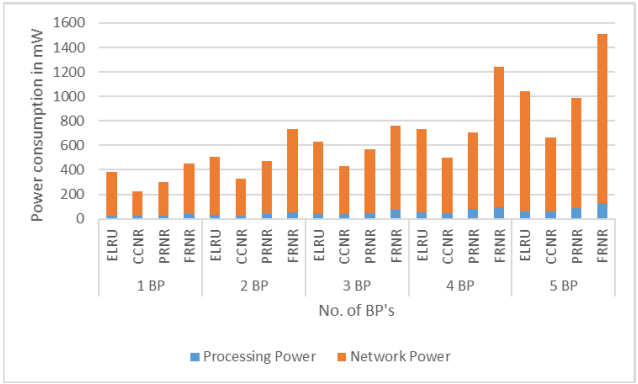


FIGURE 4. Power consumption of energy efficient–low latency node-resilient service embedding.

The FRNR had higher power consumption than the other scenarios, and the average power consumption was 40% higher than that in the ELRU scenario.

The increase in the power consumption in each scenario is attributed to the embedding of the redundant nodes and the traffic among these nodes, but the node resilience level was improved and the IoT network had the ability to maintain service provisioning even with a failure in one node.

B. ENERGY EFFICIENT–LOW LATENCY TRAFFIC-RESILIENT SERVICE EMBEDDING

For the traffic-resilient scheme, we run three resilience levels with the objective of minimizing the total power consumption and the traffic mean latency:

- Redundancy-based traffic resilience (RDTR)
- Replication-based traffic resilience (RPTR)
- Splitting-based traffic resilience (STR)

The results presented in Fig. 5 display the power consumption of the traffic-resilient service embedding for the RDTR, RPTR, and STR scenarios in the packet delivery case without a failure. These results show that RDTR has the lowest power consumption with an average power saving of 47% and 4% compared with the RPTR and STR scenarios, respectively. Furthermore, note that in some cases (i.e. 3 BP's embedding), the STR has lower power consumption than RDTR. This is attributed to its ability to find energy-efficient routes for part of the traffic, i.e. 50%. of the total traffic. In general, the model, with splitting, has an additional ability to find a route for part of the traffic through an energy efficient path, while without spitting, it may not be possible to find an energy efficient path that can absorb the entire traffic demand.

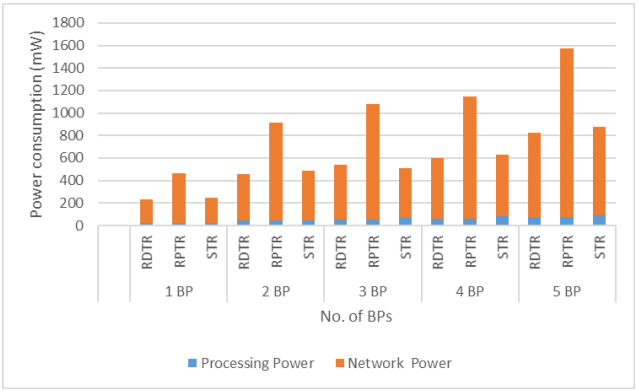


FIGURE 5. Power consumption of traffic-resilient service embedding scenarios without failure.

The results presented in Fig. 6 show the power consumption of the traffic-resilient service embedding for the RDTR, RPTR, and STR scenarios in the packet delivery case with one link failure. These results reveal that RDTR has the same power consumption as RPTR because of the data retransmission through the secondary path. The results also reveal that the STR has an average power saving of 25% compared with the RDTR scenario.

These results show that the proposed technique in the STR scenario has higher power consumption by 4%, but 25% power savings in the case of one link failure.

The results presented in Fig. 7 show the mean network traffic latency of the service embedding without failure scenarios. These results demonstrate that the STR reduces the

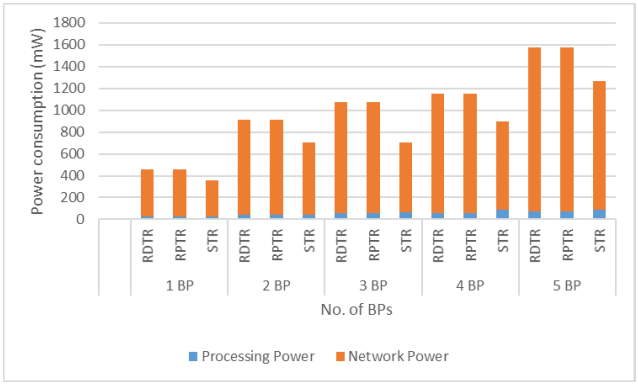


FIGURE 6. Power consumption of traffic-resilient service embedding scenarios with failure.

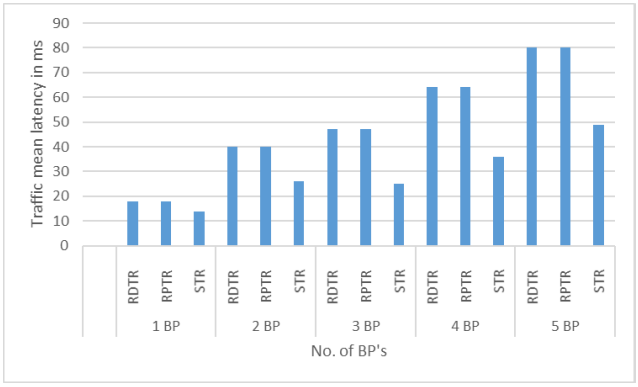


FIGURE 7. Traffic mean latency of traffic-resilient service embedding scenarios without failure.

average mean traffic latency by 37% for the set of parameters used, compared with the RDTR and RPTR scenarios. The mean traffic latency minimization in STR is attributed to the traffic splitting and hence, the reduction in the arrival rate of the individual nodes. The traffic splitting technique offered better performance in terms of the end-to-end delay.

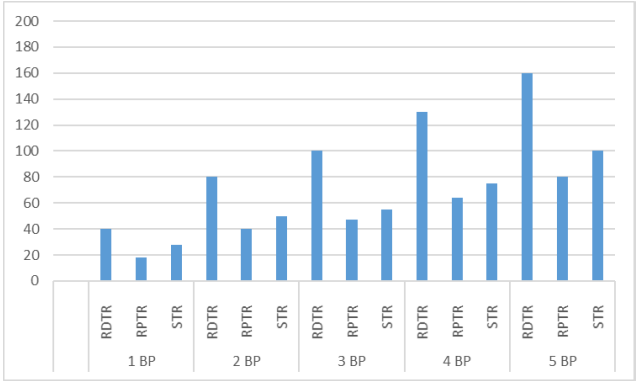


FIGURE 8. Traffic mean latency of traffic-resilient service embedding scenarios with failure.

The results presented in Fig. 8 show the mean network traffic latency of the service embedding with failure scenarios. These results demonstrate that the STR reduces the average mean traffic latency by 39% for the set of parameters used, compared with the RDTR scenario. The mean traffic latency minimization in STR is attributed to the traffic splitting and hence, the reduction in the arrival rate of the individual nodes. The RPTR has a lower average mean traffic latency by 21% and 51% compared with the STR and RDTR scenarios. The mean traffic latency minimization in RPTR is attributed to the parallel transmission of packets in two paths, consequently, the destination node can recover the packets from the other copies of the packet. While the RDTR scenario resulted in higher average mean traffic latency due to re-transmitting the packets through the alternative path.

The packet delivery ratio (PDR) reflects the network performance level, where better network performance results in a high packet delivery ratio. The packet delivery ratio is inversely proportional to the network size in IoT networks, because the routing performance is better in a low-node-density networks.

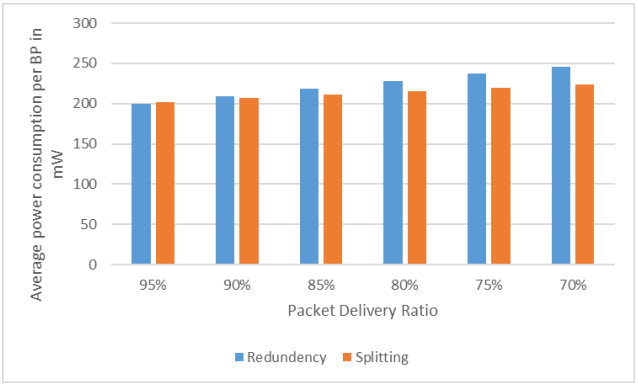


FIGURE 9. Power consumption of traffic-resilient service embedding scenarios for different PDR scenarios.

The results shown in Fig. 9 present a comparison of the total power consumption in the RDTR and STR scenarios for different PDR values [52]. These results demonstrate that the RDTR is an energy-efficient technique for high-performance networks (i.e. PDR $>$ 95%). However, the STR scenario produces higher power savings with lower PDR. The STR scenario exhibited power savings of 10% compared with RDTR when PDR $=$ 70%. These results help in comparing the RDTR and the STR without the RPTR, where the RPTR has the highest power consumption in all the cases.

VI. CONCLUSIONS

The rapid growth of the IoT has escalated the vulnerabilities of IoT for its physical infrastructure. The majority of the IoT physical devices are easily prone to failure and can be easily tampered with through attacks. Therefore, resilience is a critical consideration. We proposed a new resilience technique for IoT networks, while reducing the power consumption, average packet delivery time, and network overheads. We evaluated the proposed technique in the context of recent resilience techniques. We developed an

MILP model to optimize the selection of IoT nodes and routes in the IoT network that meet the demands of the BP's virtual nodes and links, with the goal of enhancing the resilience level and minimizing the IoT network's total power consumption and mean traffic latency through different scenarios with the same objectives.

The first set of results demonstrated the node resilience schemes. The results displayed the total power consumption of CCNR, PRNR, and FRNR and compared the results with those observed in the classic ELRU scenario. These results revealed that the CCNR and PRNR scenarios had an average power saving of 35% and 10%, respectively, compared with the ELRU scenario, while the FRNR had higher power consumption with 40% higher average power consumption than that in the ELRU scenario.

The second set of results demonstrated the traffic resilience schemes. The results displayed the total power consumption and the mean traffic latency of the proposed technique in which the STR scenario produced higher power savings with lower PDR. The STR scenario exhibited a power saving of 10% compared with the RDTR scheme when PDR was equal to 70%. The results also revealed that the STR reduced the average mean traffic latency by 37% compared with the RDTR and RPTR scenarios. The mean traffic latency minimization in STR was attributed to traffic splitting, which reduced the traffic arrival rate at the nodes. The traffic splitting technique also exhibited better performance in terms of the end-to-end delay.

The proposed scheme showed that it was possible to save energy, reduce the end-to-end data delivery time latency, and enhance the resilience level concurrently by optimizing the node and link selection in the IoT network. In future work, we will assess our approach with further QoS consideration, i.e. the availability and reliability of nodes and links.

ACKNOWLEDGMENT

The author Haider Qays Al-Shammari would like to thank the Higher Committee for Education Development (HCED) for funding his scholarship. All data are provided in full in the results section of this paper.

REFERENCES

[1] J. P. G. Sterbenz, "Smart city and IoT resilience, survivability, and disruption tolerance: Challenges, modelling, and a survey of research opportunities," in *Proc. 9th Int. Workshop Resilient Netw. Design Modeling (RNDM)*, Sep. 2017, pp. 1–6.

[2] A. Cenedese, A. Zanella, L. Vangelista, and M. Zorzi, "Padova smart city: An urban Internet of Things experimentation," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2014, pp. 1–6.

[3] Y. Wang, "System resilience quantification for probabilistic design of Internet-of-Things architecture," in *Proc. ASME Int. Design Eng. Tech. Conf. Comput. Inf. Eng. Conf.* New York, NY, USA: American Society of Mechanical Engineers, 2016, pp. 1–11.

[4] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Netw.*, vol. 32, pp. 17–31, Sep. 2015.

[5] S. Alanazi, J. Al-Muhtadi, A. Derhab, K. Saleem, A. N. AlRomi, H. S. Alholaibah, and J. J. P. C. Rodrigues, "On resilience of wireless mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications," in *Proc. 17th Int. Conf. E-Health Netw., Appl. Services (HealthCom)*, Oct. 2015, pp. 205–210.

[6] K. A. Foster, "A case study approachto understanding regional resilience," Inst. Urban Regional Develop., Univ. California, Oakland, CA, USA, Working Paper Series 2007-08, 2007.

[7] K. A. Delic, "On resilience of IoT systems: The Internet of Things (ubiquity symposium)," *Ubiquity*, vol. 2016, pp. 1–7, Feb. 2016.

[8] F. Xing and W. Wang, "Analyzing resilience to node misbehaviors in wireless multi-hop networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2007, pp. 3489–3494.

[9] S. M. A. Oteafy and H. S. Hassanein, "Resilient IoT architectures over dynamic sensor networks with adaptive components," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 474–483, Apr. 2017.

[10] Y. Tsado, D. Lund, and K. Gamage, "Resilient wireless communication networking for smart grid BAN," in *Proc. IEEE Int. Energy Conf. (ENERGYCON)*, May 2014, pp. 846–851.

[11] C. Kiraly, T. Istomin, O. Iova, and G. P. Picco, "D-RPL: Overcoming memory limitations in RPL point-to-multipoint routing," in *Proc. IEEE 40th Conf. Local Comput. Netw. (LCN)*, Oct. 2015, pp. 157–160.

[12] F. Al-Turjman, "QoS—Aware data delivery framework for safety-inspired multimedia in integrated vehicular-IoT," *Comput. Commun.*, vol. 121, pp. 33–43, May 2018.

[13] H. Alwan and A. Agarwal, "A survey on fault tolerant routing techniques in wireless sensor networks," in *Proc. 3rd Int. Conf. Sensor Technol. Appl.*, Jun. 2009, pp. 366–371.

[14] X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, and C. Gill, "Integrated coverage and connectivity configuration in wireless sensor networks," in *Proc. 1st Int. Conf. Embedded Netw. Sensor Syst. (SenSys)*, 2003, pp. 28–39.

[15] F. Dai and J. Wu, "On constructing k-connected k-dominating set in wireless ad hoc and sensor networks," *J. Parallel Distrib. Comput.*, vol. 66, no. 7, pp. 947–958, Jul. 2006.

[16] V. Vasilev, G. Iliev, V. Poulkov, and A. Mihovska, "Optimization of wireless node discovery in an IoT network," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2015, pp. 1–5.

[17] H. Q. Al-Shammari, A. Lawey, T. El-Gorashi, and J. M. H. Elmirghani, "Energy efficient service embedding in IoT networks," in *Proc. 27th Wireless Opt. Commun. Conf. (WOCC)*, Apr. 2018, pp. 1–5.

[18] H. Q. Al-Shammari, A. Lawey, T. El-Gorashi, and J. M. H. Elmirghani, "Energy efficient service embedding in IoT over PON," in *Proc. 21st Int. Conf. Transparent Opt. Netw. (ICTON)*, Angers, France, Jul. 2019, pp. 1–5.

[19] H. Q. Al-Shammari, A. Q. Lawey, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "Service embedding in IoT networks," *IEEE Access*, vol. 8, pp. 2948–2962, 2020.

[20] N. Abbas, M. Asim, N. Tariq, T. Baker, and S. Abbas, "A mechanism for securing IoT-enabled applications at the fog layer," *J. Sens. Actuator Netw.*, vol. 8, no. 1, p. 16, Feb. 2019.

[21] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in IoT using blockchain," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2017, pp. 261–266.

[22] M. Al-Khafajiy, T. Baker, H. Al-Libawy, A. Waraich, C. Chalmers, and O. Alfandi, "Fog computing framework for Internet of Things applications," in *Proc. 11th Int. Conf. Develop. eSystems Eng. (DeSE)*, Sep. 2018, pp. 71–77.

[23] I. Al Ridhawi, Y. Kotb, M. Aloqaily, Y. Jararweh, and T. Baker, "A profitable and energy-efficient cooperative fog solution for IoT services," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3578–3586, May 2020.

[24] H. Sándor, B. Genge, and G. Sebestyén-Pál, "Resilience in the Internet of Things: The software defined networking approach," in *Proc. IEEE Int. Conf. Intell. Comput. Commun. Process. (ICCP)*, Sep. 2015, pp. 545–552.

[25] H. M. M. Ali, T. E. H. El-Gorashi, A. Q. Lawey, and J. M. H. Elmirghani, "Future energy efficient data centers with disaggregated servers," *J. Lightw. Technol.*, vol. 35, no. 24, pp. 5361–5380, Dec. 15, 2017.

[26] J. M. H. Elmirghani, T. Klein, K. Hinton, L. Nonde, A. Q. Lawey, T. E. H. El-Gorashi, M. O. I. Musa, and X. Dong, "GreenTouch GreenMeter core network energy-efficiency improvement measures and optimization," *J. Opt. Commun. Netw.*, vol. 10, no. 2, pp. A250–A269, 2018.

[27] M. O. I. Musa, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "Bounds on GreenTouch GreenMeter network energy efficiency," *J. Lightw. Technol.*, vol. 36, no. 23, pp. 5395–5405, Dec. 1, 2018.

[28] B. G. Bathula and J. M. H. Elmirghani, "Energy efficient optical burst switched (OBS) networks," in *Proc. IEEE Globecom Workshops*, Nov. 2009, pp. 1–6.

[29] A. M. Al-Salim, T. E. H. El-Gorashi, A. Q. Lawey, and J. M. H. Elmirghani, "Greening big data networks: Velocity impact," *IET Optoelectron.*, vol. 12, no. 3, pp. 126–135, Jun. 2018.

[30] S. Igder, S. Bhattacharya, and J. M. H. Elmirghani, "Energy efficient fog servers for Internet of Things information piece delivery (IoTIPD) in a smart city vehicular environment," in *Proc. 10th Int. Conf. Next Gener. Mobile Appl., Secur. Technol. (NGMAST)*, Aug. 2016, pp. 99–104.

[31] A. M. Al-Salim, A. Q. Lawey, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "Energy efficient big data networks: Impact of volume and variety," *IEEE Trans. Netw. Service Manage.*, vol. 15, no. 1, pp. 458–474, Mar. 2018.

[32] M. S. Hadi, A. Q. Lawey, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "Big data analytics for wireless and wired network design: A survey," *Comput. Netw.*, vol. 132, pp. 180–199, Feb. 2018.

[33] A. Q. Lawey, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "Renewable energy in distributed energy efficient content delivery clouds," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 128–134.

[34] J. M. H. Elmirghani, L. Nonde, A. Q. Lawey, T. E. H. El-Gorashi, M. O. I. Musa, X. Dong, K. Hinton, and T. Klein, "Energy efficiency measures for future core networks," in *Proc. Opt. Fiber Commun. Conf., Opt. Soc. Amer.*, 2017, p. 4.

[35] B. G. Bathula, M. Alresheedi, and J. M. Elmirghani, "Energy efficient architectures for optical networks," in *Proc. London Commun. Symp.*, 2009, pp. 1–3.

[36] A. Q. Lawey, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "BitTorrent content distribution in optical networks," *J. Lightw. Technol.*, vol. 32, no. 21, pp. 3607–3623, Nov. 1, 2014.

[37] N. I. Osman, T. El-Gorashi, L. Krug, and J. M. H. Elmirghani, "Energy-efficient future high-definition TV," *J. Lightw. Technol.*, vol. 32, no. 13, pp. 2364–2381, Jul. 1, 2014.

[38] S. H. Mohamed, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "Energy efficiency of server-centric PON data center architecture for fog computing," in *Proc. 20th Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2018, pp. 1–4.

[39] M. Musa, T. Elgorashi, and J. Elmirghani, "Bounds for energy-efficient survivable IP over WDM networks with network coding," *J. Opt. Commun.*, vol. 10, no. 5, pp. 471–481, 2018.

[40] X. Dong, T. El-Gorashi, and J. M. H. Elmirghani, "Green IP over WDM networks with data centers," *J. Lightw. Technol.*, vol. 29, no. 12, pp. 1861–1880, Jun. 15, 2011.

[41] N. I. Osman, T. El-Gorashi, and J. M. H. Elmirghani, "The impact of content popularity distribution on energy efficient caching," in *Proc. 15th Int. Conf. Transparent Opt. Netw. (ICTON)*, Jun. 2013, pp. 1–6.

[42] X. Dong, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "On the energy efficiency of physical topology design for IP over WDM networks," *J. Lightw. Technol.*, vol. 30, no. 11, pp. 1694–1705, Jun. 15, 2012.

[43] M. Musa, T. Elgorashi, and J. Elmirghani, "Energy efficient survivable IP-over-WDM networks with network coding," *J. Opt. Commun.*, vol. 9, no. 3, pp. 207–217, 2017.

[44] T. E. H. El-Gorashi, X. Dong, and J. M. H. Elmirghani, "Green optical orthogonal frequency-division multiplexing networks," *IET Optoelectron.*, vol. 8, no. 3, pp. 137–148, Jun. 2014.

[45] X. Dong, T. El-Gorashi, and J. M. H. Elmirghani, "IP over WDM networks employing renewable energy sources," *J. Lightw. Technol.*, vol. 29, no. 1, pp. 3–14, Jan. 1, 2011.

[46] A. N. Al-Quzweeni, A. Q. Lawey, T. E. H. Elgorashi, and J. M. H. Elmirghani, "Optimized energy aware 5G network function virtualization," *IEEE Access*, vol. 7, pp. 44939–44958, 2019.

[47] M. S. Hadi, A. Q. Lawey, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "Patient-centric cellular networks optimization using big data analytics," *IEEE Access*, vol. 7, pp. 49279–49296, 2019.

[48] L. Nonde, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "Energy efficient virtual network embedding for cloud networks," *J. Lightw. Technol.*, vol. 33, no. 9, pp. 1828–1849, May 1, 2015.

[49] L. Nonde, T. E. H. Elgorashi, and J. M. H. Elmirgahni, "Virtual network embedding employing renewable energy sources," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

[50] J. Huang, Y. Meng, X. Gong, Y. Liu, and Q. Duan, "A novel deployment scheme for green Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 2, pp. 196–205, Apr. 2014.

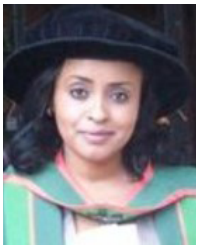
[51] Z. T. Al-Azez, A. Q. Lawey, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "Energy efficient IoT virtualization framework with peer to peer networking and processing," *IEEE Access*, vol. 7, pp. 50697–50709, 2019.

[52] H. Lamaazi, N. Benamar, and A. J. Jara, "RPL-based networks in static and mobile environment: A performance assessment analysis," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 30, no. 3, pp. 320–333, Jul. 2018.

HAIDER QAYS AL-SHAMMARI (Member, IEEE) received the B.Sc. and M.Sc. degrees in computer engineering from Al-Nahrain University, Baghdad, Iraq, in 2002 and 2006, respectively, and the Ph.D. degree in electronic and electrical engineering from the University of Leeds, U.K., in 2019. From 2006 to 2008, he worked as a Billing Engineer in telecommunication with ZTE Corporation, Iraq. From 2008 to 2011, he was a Data Communication Engineer in telecommunication with Huawei Technologies, Iraq. From 2011 to 2014, he was a Transmission Manager with NEC partner, Iraq. He was a Project Manager with Huawei technologies, in 2014. His current research interests include energy efficiency in the IoT networks and service virtualization.

AHMED Q. LAWEY (Associate Member, IEEE) received the B.S. (Hons.) and M.Sc. (Hons.) degrees in computer engineering from the University of Al-Nahrain, Iraq, in 2002 and 2005, respectively, and the Ph.D. degree in communication networks from the University of Leeds, U.K., in 2015.

From 2005 to 2010, he was a Core Network Engineer with ZTE Corporation for Telecommunication, Iraq. He is currently a Lecturer of communication networks with the School of Electronic and Electrical Engineer, University of Leeds. His current research interests include energy efficiency in optical and wireless networks, big data, cloud computing, and the Internet of Things.



TAISIR E. H. EL-GORASHI received the B.S. degree (Hons.) in electrical and electronic engineering from the University of Khartoum, Khartoum, Sudan, in 2004, the M.Sc. degree (Hons.) in photonic and communication systems from the University of Wales, Swansea, U.K., in 2005, and the Ph.D. degree in optical networking from the University of Leeds, Leeds, U.K., in 2010. From 2010 to 2014, she held a Postdoctoral Research position with the University of Leeds, where she focused on the energy efficiency of optical networks investigating the use of renewable energy in core networks, green IP over WDM networks with datacenters, energy efficient physical topology design, energy efficiency of content distribution networks, distributed cloud computing, network virtualization, and big data. She was a BT Research Fellow, in 2012, where she developed energy efficient hybrid wireless-optical broadband access networks and explored the dynamics of TV viewing behavior and program popularity. The energy efficiency techniques developed during her postdoctoral research contributed three out of the eight carefully chosen core network energy efficiency improvement measures recommended by the GreenTouch consortium for every operator network worldwide. She is currently a Lecturer of optical networks with the School of Electrical and Electronic Engineering, University of Leeds. Her work led to several invited talks at GreenTouch, Bell Labs, Optical Network Design and Modelling Conference, Optical Fiber Communications Conference, International Conference on Computer Communications, and EU Future Internet Assembly and collaboration with Alcatel Lucent and Huawei.

JAAFAR M. H. ELMIRGHANI (Senior Member, IEEE) received the B.Sc. degree (Hons.) in electrical engineering from the University of Khartoum, in 1989, the Ph.D. degree in the synchronization of optical systems and optical receiver design from the University of Huddersfield, U.K., in 1994, and the D.Sc. degree in communication systems and networks from the University of Leeds, U.K., in 2014.

From 2000 to 2007, he was a Chair in optical communications with the University of Wales Swansea, where he founded, developed, and directed the Institute of Advanced Telecommunications and the Technium Digital (TD), a Technology Incubator/Spin-off Hub. He joined Leeds, in 2007. He is currently the Director of the School of Electronic and Electrical Engineering, Institute of Communication and Power Networks, University of Leeds, U.K. He has provided outstanding leadership in a number of large research projects at the IAT and TD. He has coauthored *Photonic switching Technology: Systems and Networks* (Wiley). He has published over 450 articles. His research interests include optical systems and networks.

Dr. Elmirghani is a Fellow of IET and the Institute of Physics. He was a member of the Royal Society International Joint Projects Panel and the Engineering and Physical Sciences Research Council (EPSRC) College. He received all four prizes in the department for academic distinction, the IEEE Communications Society Hal Sobol Award, the IEEE Comsoc Chapter Achievement Award for excellence in chapter activities (both in international competition, in 2005), the University of Wales Swansea Outstanding Research Achievement Award, in 2006, the IEEE Communications Society Signal Processing and Communication Electronics Outstanding Service Award, in 2009, the Best Paper Award at IEEE ICC'2013, the IEEE Comsoc Transmission Access and Optical Systems Outstanding Service Award, in 2015, in recognition of Leadership and Contributions to the Area of Green Communications, the GreenTouch 1000x Award, in 2015, for pioneering research contributions to the field of energy efficiency in telecommunications, the IET 2016 Premium Award for best paper in IET Optoelectronics, and shared the 2016 Edison Award in the Collective Disruption Category with a team of six from GreenTouch for their joint work on the GreenMeter. He has been awarded in excess of £22 million in grants to date from EPSRC, the EU and industry and has held prestigious fellowships funded by the Royal Society and by BT. He was the Chairman of the IEEE Comsoc Transmission Access and Optical Systems Technical Committee and the IEEE Comsoc Signal Processing and Communications Electronics Technical Committee. He was a Founding Chair of the Advanced Signal Processing for Communication Symposium which started at the IEEE GLOBECOM'99, where he has continued since at every ICC and GLOBECOM, the first IEEE ICC/GLOBECOM Optical Symposium at GLOBECOM'00, the Future Photonic Network Technologies, Architectures and Protocols Symposium, where he chaired this Symposium, which continues to date under different names, and the first Green Track at ICC/GLOBECOM at GLOBECOM 2011. He is the Chair of the IEEE Green ICT initiative within the IEEE Technical Activities Board (TAB) Future Directions Committee (FDC), a pan IEEE Societies initiative responsible for Green ICT activities across IEEE, since 2012. From 1995 to 2016, he was on the technical program committee of 34 IEEE ICC/GLOBECOM conferences, including 15 times as a Symposium Chair. He has given over 55 invited and keynote talks over the past eight years. He was the Co-Chair of the GreenTouch Wired, Core and Access Networks Working Group, an Adviser of the Commonwealth Scholarship Commission. He was an Editor of the IEEE Communications Surveys and Tutorials, the IEEE Journal on Selected Areas in Communications series on Green Communications and Networking, and the *IEEE Communications Magazine*. He is currently an Editor of *IET Optoelectronics* and the *Journal of Optical Communications*. From 2013 to 2016, he was an IEEE Comsoc Distinguished Lecturer. He is also a Chartered Engineer.