Computer Communications 181 (2022) 236–256

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Buffer-loss estimation to address congestion in 6LoWPAN based resource-restricted 'Internet of Healthcare Things' network

Himanshu Verma [*,1], Naveen Chauhan[2], Narottam Chand[3], Lalit Kumar Awasthi[4]

Department of Computer Science & Engineering, National Institute of Technology, Hamirpur 177005, Himachal Pradesh, India

ARTICLE INFO

Keywords:
Buffer-loss
Congestion control
Buffer-overflow
Packet-loss estimation
IoHT congestion
IoT Healthcare

ABSTRACT

The Internet of Healthcare Things (IoHT) consists of a wide variety of resource-restricted, heterogeneous, IoT-enabled, wearable/non-wearable medical equipment (things) that connect over the internet to transform traditional healthcare into a smart, connected, proactive, patient-centric healthcare system. The pivotal functions of the 6LoWPAN protocol stack enable comprehensive integration of such networks from wearable wireless sensor networks (W-WSN) to IoHT, as TCP/IP does not suffice the requirements of IoHT networks. As a result, the congestion in the IoHT network increases with a growing number of devices, resulting in loss of critical medical information due to buffer loss and channel loss, which is unacceptable. In this paper, we explored different applications of patient-centric IoHT architectures to draw a realistic resource-limited topological layout of IoHT for congestion estimation. After critically reviewing existing congestion schemes for 6LoWPANs, we proposed an effective buffer-loss estimation model based on the Queuing Theory to determine the number of packets lost at the node's buffer. The buffer is modeled as an M/M/1/K Markov Chain Queue. The M/M/1/K Queue equilibrium equation is used to establish a relationship between the probabilities of the buffer being empty or completely filled. We derived the expressions for total buffer-loss probability and expected mean packet delay for the resource-constraint IoHT network. Furthermore, to validate the buffer-loss estimation, an analytical model is used to compare buffer-loss probabilities, the number of packets dropped at leaf/intermediate nodes and the number of packets successfully received at the local sink node. The results show a close correlation between both the models on varying values of the number of leaf nodes, buffer size, offered packet load and available channel capacity. Thus, in resource-restrictive IoHT, the proposed model performs better than two related works.

1. Introduction

IPv6 over Low Power Wireless Personal Area Network (6LoWPAN) is an essential technology in the Internet of Things (IoT). A large number of IoT 'Things' are 6LoWPAN enabled motes [1,2]. The defined 6LoWPAN protocol stack helps to comprehensively integrate WSN (Wireless Sensor Network) nodes with IoT motes. Due to this, the application domain of 6LoWPAN becomes wider. These applications can be segregated based on data delivery mechanisms as (i) Event-based; (ii) Query-based; (iii) Continuous; (iv) Hybrid applications. The IoT-enabled healthcare application is a hybrid kind of domain.

In the IoHT application, wearable/non-wearable 6LoWPAN based medical sensing equipment is used to monitor and collect various patient health parameters. The captured data is transmitted towards personal digital devices (smartphone, laptop, tablet) that act as a local sink in the IoHT network. This transmission could be a direct one or through the multi-hop environment. These motes could be tiny in size and have minimal networking resources such as memory, computational capability, bandwidth and so on.

These restrictions of sensing devices could lead to congestion in the network. Congestion happens when more than one node starts sending packets at a higher rate simultaneously and when a node relays two

* Corresponding author.
E-mail addresses: himanshu@nith.ac.in (H. Verma), naveen@nith.ac.in (N. Chauhan), nar@nith.ac.in (N. Chand), lalit@nith.ac.in (L.K. Awasthi).
URLs: https://portfolios.nith.ac.in/index.php?/nith/dr-naveen-chauhan- (N. Chauhan),
https://portfolios.nith.ac.in/uploadresume/1607886196nar_short_cv_23112020.pdf (N. Chand),
https://portfolios.nith.ac.in/index.php?/nith/dr-lalit-kumar-awasthi- (L.K. Awasthi).
[1] Ph.D. Research Scholar.
[2] Associate Professor (Ph.D. Supervisor).
[3] Associate Professor.
[4] Professor.

https://doi.org/10.1016/j.comcom.2021.10.016
Received 14 March 2021; Received in revised form 10 September 2021; Accepted 9 October 2021
Available online 19 October 2021

or more network routes. Due to congestion, packets are being dropped instead of sending them to their destination. These dropped packets are further re-transmitted, increasing network traffic and unnecessarily consuming the scarce networking resources. These packets are lost either at buffer or wireless link. The buffer overflow scenario occurs when there is a mismatch of arrival and departure data rates. That means, either 'slow-sender fast-receiver' or 'fast-sender slow-receiver' or 'slow link' can cause congestion in the network. As we know, IoHT deals with crucial and time-critical data, where delay or loss of such data is not accepted and undesirable. Therefore, the performance of 6LoWPAN networks degrades when congestion happens. Due to that, more packets are being dropped and fewer packets are successfully reaching the local sink. These essential data packets are lost either at the node's buffer or the wireless link.

A proper estimation of these lost packets is required to address congestion in IoHT networks. Traffic control and resource control are two approaches for congestion control, but both are individually not sufficient to control congestion in IoT applications. Therefore, we analyzed popular congestion control algorithms for 6LoWPAN networks and observed that a hybrid methodology benefiting traffic and resource control schemes is necessary to control congestion in the IoHT network. In this work, we considered a resource-restricted IoHT network layout that consists of few leaf nodes, one intermediate node and one local sink to estimate buffer loss. It has been noticed that packet loss due to the node's buffer overflow is far more responsible for congestion than packets dropped at the channel.

Queuing Theory is frequently used to analyze the performance of computer networks [3,4]. We used this concept to estimate the buffer-loss probability of a node. The buffer (at node's MAC layer) is considered as a queue where incoming packets are stored to be processed and further forwarded towards the destination. We modeled the node's MAC buffer as an M/M/1/K queue because the arrival and departure rate of the packet follows Markovian memory-less property (i.e., the present state is unaware of its predecessor). Thus, the size of the buffer represents individual states of the Markov Chain. We calculated the 'probability of packet loss' based on this queuing model due to the unavailability of buffer space at node's buffer and average packet delay.

This M/M/1/K queue-based model was compared with an analytical model to study and analyze the probability of buffer loss at the leaf and intermediate nodes. Other than that, the number of packets lost due to channel-loss and buffer-loss, number of packets successfully received at the local sink, expected packet delay, relation between channel-loss and buffer-loss are also computed in this work.

We observed a close correlation between M/M/1/K queue-based model and the analytical model. At leaf and intermediate node, probability of buffer-loss, the number of packets lost at node's buffer increases when more leaf nodes are involved in the IoHT network and when offered load keeps on increasing. When we increase the leaf nodes' buffer size, fewer packets are lost at the leaf node. However, this scenario is reversed at the intermediate node because more packets are being sent towards the intermediate node from the leaf at a large buffer size. The intermediate node's buffer is not capable of storing all of them. However, the expected mean packet delay rises when the number of the leaf nodes, buffer size and packet arrival rate increases. The performance of evaluating parameters degrades when the available channel capacity shrinks from 250 kbps to 120 kbps. In addition, we also compared the proposed method with two existing scheme presented in [5,6]. The result exhibits that proposed method significantly outperform the existing schemes in resource-restricted IoHT scenario.

The remaining paper is organized as follows: Popular existing congestion control schemes (traffic control, resource control and hybrid) for 6LoWPAN networks are comparatively studied, reviewed and summarized in Section 2. In Section 3, we elaborate on the different types of patient-centric Internet of Healthcare Things architectures. Where we discuss 'InHm-IoHT', 'Ot-IoHT', 'InV-IoHT', 'InAmb-IoHT' and 'InHos-IoHT' patient's remote health monitoring scenarios in detail. Section 4 described the topological aspects of IoHT architecture.

To alleviate congestion in resource-restricted IoHT layout, in Section 5, we presented a Markov chain-based M/M/1/K queue model to estimate packet loss due to the node's buffer overflow at leaf and intermediate node. Here, we defined packet loss probability due to insufficient buffer space and the expected delay a packet can suffer. Furthermore, we introduce an analytical model to estimate congestion in 6LoWPAN based IoHT network in Section 6, where the probability of buffer-loss and channel-loss are calculated. In Section 7, we have validated the presented analytical model with M/M/1/K queue-based buffer-loss model. The overall conclusion of this work is explained in Section 8.

A rigorous review of published research papers on handling congestion in 6LoWPANs is done below.

2. Literature review: Congestion schemes for 6LoWPAN networks

It is suggested to consider three steps to address congestion in 6LoWPAN based IoHT networks. These are:

- Congestion Detection
- Congestion Notification
- Congestion Control

Parameters such as buffer occupancy, channel load, packet service time, packet loss and delay can be used for congestion detection. Congestion notification is either implicit or explicit. Traffic control and Resource Control are two countermeasure strategies for congestion control. Whilst, for the IoHT kind of scenario, a hybrid scheme (combination of traffic and resource control technique) needs to be incorporated to design and develop a congestion control algorithm.

In the traffic control strategy, the sending node reduces the rate of packets injected into the network to a threshold limit. This reduction can be made by the window-based or rate-based method. The traffic rate increased slowly (slow-start phase) in the congestion window-based scheme. When the source node detects congestion, it shrinks the window (mostly half of the threshold). It can be seen as AIMD (additive increase multiplicative decrease) method, where the source expands the congestion window linearly while decreases exponentially. However, bandwidth estimation is used to adjust the packet transmission rate in the rate-based scheme. While reducing the data rate is undesirable for time-critical and event-based IoHT applications where packet carries crucial medical information.

The resource control mechanism is an alternative that counters the drawback of traffic control. In this scheme, the source forwards the data packet to the receiver from other uncongested paths to know about congestion occurrence. It is stated that this method provides a higher packet delivery ratio than the traffic control scheme. Nevertheless, the availability of congested paths is not always promised. Therefore, many proposals combine both the schemes and developed a hybrid method to handle congestion. In this mechanism, one first check the availability of an uncongested path; if present, then apply resource control method, otherwise packet forwarding rate is reduced using traffic control strategy.

Some appropriate research proposals are investigated in the below subsection.

2.1. Congestion handling schemes for 6LoWPAN networks

An analytical model was proposed to estimate the buffer-loss for 6LoWPAN [5]. This model used the concept of queuing theory to analyze the lost packet due to buffer loss. However, the results of the model were closed to the simulation scenario.

In [6], a noncooperative Game Theory-based energy-efficient congestion control (NGECC) mechanism for the 6LoWPAN network was

proposed. The developed scheme utilized a traffic control strategy to determine optimal data transfer rate for leaf nodes (source) using a noncooperative game. In addition, they considered channel occupancy and buffer overflow factors of packet loss to design an energy-efficient payoff function for each leaf node.

Michopoulos et al. [7] presented an algorithm named 'DCCC6' that detected congestion using buffer-occupancy parameter and applied the traffic control method to alleviate congestion. The mode of the operation depended on the duty cycle. The simulation result showed that DCCC6 perform better than CSMA, HCCP [8], AFA [9] and IFRC [10] algorithms. This method is unsuitable for the 6LoWPAN-IoT application because it does not support a hybrid congestion control strategy.

Congestion for simplex and duplex traffic was addressed in [11]. The proposed schemes were 'Griping, Deaf and Fuse' to control congestion in CoAP based 6LoWPAN networks. They implemented a back-pressure method at the sensor's networking layer. Buffer occupancy was used to detect congestion. The traffic control scheme was utilized to mitigates congestion. In Griping, a back-pressure message was periodically sent back to the sender. If the node's buffer was exhausted by these messages, then the source halved the data rate. If the sender had not received any back-pressure message in an interval, it increased the data rate. In Deaf, the rate of sending the ACK (acknowledgment) packet and waiting time for getting an ACK was adjusted when there was not enough space in the receiver's queue. The Fuse used a combined strategy of both schemes. The simulation showed that Fuse was better than the other two schemes.

Al-Kashoash et al. proposed a non-cooperative game theory-based solution named 'GTCCF' [12]. Nash equilibrium concept was used to adjust the packet forwarding rate. To make it IoT compatible, they involved node and application priority in the proposal. As a result, the presented solution outperformed the DCCC6 algorithm [13] in terms of throughput, delay, energy awareness and packet loss.

Influenced by the bird flocking concept, a CoAP/RPL/6LoWPAN based congestion controlling algorithm was presented by Hellaoui et al. [14]. The resource control scheme was used for congestion control and the buffer occupancy parameter was used for congestion detection. In addition, they defined 'Zone of Repulsion' (1-hop distance) & 'Zone of Attraction' (2-hop distance) to find the non-congested path. Simulation results explained that the proposed solution might perform better when congestion was present. However, it is not suggested for IoT applications because it consumes considerably more energy and the packet suffers a much higher delay.

QU-RPL [15,16], an algorithm that used an effective queue utilization mechanism to reduce packet loss when congestion occurs. The load balancing of injected packets was done using the queue utilization (QU) factor. In case of congestion, a node changed its parent, shifted to a less occupied node and considered less hop distance in this switching. The results showed that the proposed algorithm performed better than the existing RPL scheme.

The concept of 'Game theory' was used in [17,18] to mitigate congestion for 6LoWPANs. They also used the shifting parent node strategy to find alternative uncongested routes. The packet flow rate was used as a congestion detection parameter. Game theory was used to decide whether to change parent or not. RPL-OF0 & RPL-ETX(Expected Transmission Count)-OF schemes were used to compare with the presented algorithm in simulation. The result depicted that proposal gave an almost double performance in terms of throughput & number of packets received.

An RPL based multi-path routing named 'CA-RPL' was presented to avoid congestion in [19]. They used the 'DELAY-ROOT' parameter to minimize the delay. Traffic was forwarded through different routes to reduce the load at one path. The result stated that the proposed work reduced delay by 30% and packet loss by 20%.

Lodhi et al. [20] presented 'M-RPL' that supported multi-path routing in case of congestion. Packet delivery ratio was used for congestion detection. Node halved the data rate for the original and selected parent, then transmitted packets to sink from different paths. The simulation showed that the proposal was better than the existing RPL, as it consumed less energy and supported higher throughput.

In [21], Ha et al. introduced 'MLEq' for 6LoWPAN. They used distributed dynamic load balancing concept to develop this work for the multi-gateway 6LoWPAN network. The water flow concept inspired them to find congestion levels. Results of the NS2 simulator showed that it performed better than RPL.

Load balancing was involved in RPL to distribute traffic in 6LoWPAN networks [22]. They used a buffer utilization counter for load distribution adjustment. The presented work was simulated on 1000 nodes and its results outperformed RPL.

Tang et al. in [23] submitted an optimized multi-path RPL to mitigate congestion by reducing packet loss. ETX and packet send to sink were combinedly used in this dynamic adaptive routing method. The result showed that the proposed work decreased the packet loss & end-to-end delay when congestion occurs.

A congestion-aware objective function for RPL (RPL-CA-OF) was presented in [24]. The objective function was able to identify less congested nodes because of incorporated buffer occupancy and ETX parameters. They compared the proposed work with RPL-OF0, RPL-ETX-OF and RPL-Energy-OF. The simulation showed that CA-OF performed 37.4% better than others in terms of packet loss, energy utilization and packet delivery ratio.

Al-Kashoash et al. [25,26] introduced an optimization theory-based hybrid congestion control scheme named 'OHCA' by combining both traffic and resource control strategies. They utilized Gray Relational Analysis (GRA) (i.e., a multi-attribute optimization method), which used buffer occupancy, ETX and queuing delay to detect non-congested parents. Moreover, if the uncongested path was unavailable, an optimization theory and NUM (Network Utility Maximum) based traffic control scheme was used. Finally, they included node and application priorities to support IoT applications. The application sending rate was treated with constrained optimization methodology. The results of the proposal outperformed DCCC6 and QU-RPL.

Existing congestion addressing algorithms are summarized in Table 1. Their pros & cons are discussed in Table 2.

The following section elaborates on different scenarios of patient-centric IoHT.

3. Patient-centric IoHT architectures

Depending on the application scenarios, the layout of the involved devices (medical sensors, relay nodes, local sink, gateway, root node) in IoHT could be simple or complex. Both wearable and non-wearable devices take account of on-body and off-body sensing of health parameters in these scenarios. Based on applications, these architectures can be classified as:

- In-Home Healthcare (InHm-IoHT)
- Outdoor Healthcare (Ot-IoHT)
- In-Vehicle Healthcare (InV-IoHT)
- In-Ambulance Healthcare (InAmb-IoHT)
- In-Hospital Healthcare (InHos-IoHT)

These healthcare architectures have resource-constraint and resource-sufficient sensing devices. In addition to that, mobility can also be present in such scenarios. The patient's movement introduces mobility in such networks. The overall IoT-healthcare application consists of various 6LoWPAN based IoT enabled, resource-limited/resource-capable, wearable/non-wearable and on-body/off-body medical sensors that capture the patient's vital signs. Besides these vital collecting devices, many other IoT-enabled sensing devices keep track of various medical equipment, staff, resources, labs, pharmacies, wards, ambiance, different sections, units, and hospital buildings. Every smallest unit of the healthcare system that needs to be controlled and systematized automatically without any human intervention should

Table 1
Summary of existing congestion addressing algorithms for 6LoWPAN networks.

Ref.	Congestion Control Method	Congestion Detection Parameter	Performance Evaluating Parameter
[6]	Traffic Control	Channel Occupancy and Buffer Overflow	Packet transmission rate, PDR (packet delivery ratio), throughput, weighted fairness index, energy consumption and delay.
[7]	Traffic Control	Buffer Occupancy	End Delay, Energy Utilization, Jain's fairness index, Goodput
[11]	Traffic Control	Buffer Occupancy	Overhead, Packet dropping rate, Multi-hop delay, Receiving rate, Packet loss probability
[12]	Traffic Control	Traffic intensity	Throughput, packet loss, Delay, Energy utilization, Weighted fairness index
[14]	Resource Control	Buffer Occupancy	Transmission delay, Repeated packets
[15,16]	Resource Control	Buffer Occupancy	Packet delivery, Hop distance, Packet Overhead, Packet delivery ratio, Packet loss
[17,18]	Resource Control	Variance of packet generation	packet service rate, Throughput, Hop count, Rate of packet loss
[19]	Resource Control	Not defines	End delay, Throughput, Packet drop rate
[20]	Resource Control	Packet delivery ratio	End delay, Throughput, Energy Consumption
[21]	Resource Control	Not defines	Jain's fairness index, Overhead of control messages, Throughput
[22]	Resource Control	Not defines	End-to-end delay, Packet delivery ratio
[23]	Resource Control	Not defines	End delay, Receiving rate, Packet loss rate
[24]	Resource Control	Buffer Occupancy	Dropped packets, Packet delivery ratio, Energy consumption, Throughput
[25,26]	Hybrid (combination of traffic and resource control)	Buffer Occupancy, ETX, Traffic Intensity	Packet loss, Delay, Weighted fairness index, Energy utilization, Throughput

Table 2
Analysis of existing 6LoWPAN-congestion control algorithms.

Ref.	Benefits	Drawbacks
[6]	Utilized noncooperative Game Theory to design energy-efficient congestion control scheme; Both channel occupancy and buffer overflow parameters were used in payoff function; For sending data rate tuning, a noncooperative game was developed; Outperform GTCCF, OHCA algorithms	Does not fit for hybrid applications; Neglected benefits of resource control strategy; Limited compatibility in IoT applications
[7]	Have Radio Duty Cycle (RDC) method; Enhance energy utilization and fairness; reduce delay	Not compatible for IoT Applications; No option for uncongested path
[11]	Less overhead; Better receiving rate and less buffer-loss	Incorrect identification of receiver's buffer overflow; Not suitable for IoT applications; Does not check for uncongested routes
[12]	Use non-cooperative game theory; Use Nash equilibrium for forwarding rate adaptation	Does not use non-congested path; Aware of node and application priorities; Outperform in terms of throughput, delay, fairness, energy consumption and packet loss
[14]	Used bird flocking concept to avoid congestion-less redundant traffic; Better forwarding time	Always ON radio consume more energy; Faulty parameter selection; Does not support RDC mechanism
[15,16]	Support traffic load balancing; Improved packet delivery ratio and less packet loss	More overhead; Cannot adjust traffic rate when uncongested path not found.
[17,18]	Used Game theory to search less congested routes; More throughput and less packet loss	More control overhead; Traffic control policies are missing
[19]	Have traffic distribution policies to handle heavy traffic; Reduces packet loss and delays	Does not consider buffer overflow scenario; Traffic rate cannot be adjusted when congestion occurs
[20]	Share sending rate to multiple paths; Enhance throughput, decrease latency and energy utilization	Sender does not reduce forwarding rate in case of congestion; Not suitable for IoT applications
[21]	Use water flowing principle for load balancing and traffic distribution; Make use of available multiple gateways; Better fairness and throughput, Less overhead	No Congestion detection methodology; Does not support traffic rate adjustment; Cannot support hybrid applications
[22]	Traffic load is distributed to multiple parents; Enhanced packet delivery ratio and less end-delay	Congestion detection not supported; When congestion identified, source rate cannot be reduced
[23]	To address congestion, dynamic adaptive path finding scheme was used; Improved receiving rate, lessen packet loss rate and delay	Congestion detection was not incorporated; Traffic control strategies not involved
[24]	Buffer occupancy parameter was used to find less congested routes; More throughput, less packet loss, decrease energy consumption	Sender cannot reduce forwarding rate when congestion occur; Does not support hybrid case
[25,26]	Support Hybrid applications; Traffic and Resource control strategies are combinedly used; Used NUM for traffic control and GRA for resource control; Aware of node and application priorities; Enhance fairness and throughput, alleviate packet loss, energy utilization and end-to-end delay	Simulated with less number of nodes

connect to the IoHT network by utilizing all the benefits of the IoT. These devices access the internet from fixed or wireless networking infrastructure to transmit their captured information to the cloud (root node) and hospital server. The discussion explains the complexity of the 'Internet of Healthcare Things' that keeps on increasing.

For better understanding, the IoHT architectures are segregated into different the point-of-applications explained below.

3.1. InHm-IoHT (In-Home) architecture

As shown in Fig. 1, Sensing, Local sink, gateway, cloud and end-user are the different working units of an in-home intelligent healthcare network. It is an individual patient-centric setup for capturing different health parameters that need to be associated with every patient in an intelligent IoT healthcare system. A large number of such networks are present in connected IoHT systems.

Sensing of vital signs is done using 6LoWPAN-based IoT-enabled medical sensors. These sensing devices are either attached to the body of the patient or present in the near periphery. Instruments like blood pressure monitors, glucose meters, weighing machines, gym equipment, physical exercise equipment and others can also be enabled with IoT capabilities to collect the vitals. All such sensing devices are considered leaf nodes in IoT-healthcare architecture. Non-wearable equipment could be a higher capability device than tiny resource-constraint wearable medical sensors in terms of networking resources such as memory, computation, power and bandwidth, etc. As they are bigger in size, they might have a rechargeable power option and digital electronic capabilities. These resource-sufficient devices can act as an intermediate node (relay node/parent node) for resource constraint sensors connected using a p2p wireless link to provide connectivity to the sensors. The patient's mobility introduces connection and disconnection of these off-body devices that need to be considered when routing data packets.

This 6LoWPAN enabled collective vital sensing unit gets connected with the patient's intelligent personal digital devices (smartphone, tab, PC, laptop) using short-range wireless links (BLE, ZigBee, etc.). Patient's personal digital devices are higher capability devices with sufficient networking resources in terms of bandwidth, computation capability, memory, power resources, etc. These same devices act as a local sink for the sensing devices and host applications to provide local alerts and assistance to the patient. Near-device data processing can also be done using edge computing schemes to prevent redundant data from being forwarded to the cloud or server. Therefore, this Personal digital device layer can be viewed as local data processing and filtration unit for the data coming directly from the sensors. It is an essential layer in architecture. It processes and filters out the absolute or redundant data sent by the sensing unit layer because resource-limited sensors transmit everything they sense periodically without any data processing. The applications hosted in personal smart devices use this processed and filtered data to provide real-time alert notifications and assistance locally to the user.

These high-capability personal devices are intermediate nodes for sensors that relay or forward locally analyzed and processed data towards the cloud. These intermediate devices get either cellular connectivity or Wi-Fi access point (modem/routers) provided by Internet Service providers (ISP). Primarily IEEE 802.11 Wi-Fi links are used by such devices, but wired connectivity is also available as an option for internet connectivity. So, cellular services provide Wi-Fi APs or 4G/LTE/5G-based data connectivity are gateway nodes to access internet connectivity. These gateway devices are connected to ISP using licensed or unlicensed long-range communication interfaces like cellular systems, satellite communication, LoRa, etc. Till this point (internet connection layer), the network setup is considered local. Then, gateway devices connect this local network with the outside world.

This gateway interface lets leaf nodes (IoT-enabled medical sensors and instruments) send captured data to the cloud for storage, complex computing, high-end analysis, and processing of transmitted data. The cloud functions as the global sink or root node. Information processed by various complex cloud services, AI, ML, big data and data analytics, etc., is stored on the cloud for global access. As the cloud is equipped with all the necessary and sufficient networking and computational resources, several complex processing and computing algorithms, including AI, ML and other technologies, execute to convert raw data into the most meaningful information and store it for further use. Critical decision-making is done based on this processed information.

The hospital's server is real-timely synchronized to the cloud with zero loss of information. Multiple connection interfaces provide never-breaking internet connectivity and keep information up-to-date and adequately synchronized between the hospital server and the cloud. Additionally, multiple synchronized and connected redundant servers are installed for the network's robustness and fault tolerance. The bi-directional communication medium is used between the cloud and the hospital server to minimize the delay. Any update or changes made by one device must be reflected on all other devices in no time. The hospital server should be directly connected with all the sections of the hospital system (including reception, pharmacies, labs, wards, critical units and others). Therefore, data updation made anywhere should be reflected on the server and the cloud for real-time processing.

Using high-speed internet connectivity and world wide web (www), stakeholders (such as hospital system, doctors, patients, caretakers, family, medical staff, NGOs, health insurance companies and emergency services) get access to the finally processed information (stored on the cloud) for complex decision-making scenarios and other usages.

The process of sensing the patient's vitals and medical data, which should be analyzed and stored at the cloud and hospital server, should happen in real-time and instantaneous. Even the smallest segment of captured data is time-critical for relevant notification, alert and assistance. The slightest delay can cause disaster in real-time monitoring of the patient. No delay, zero loss of information, highest data rate, no-fault, zero error, fastest transmission, quick complex analysis, never breaking high-speed internet connectivity, etc., are primary requirements of the IoHT network. Lacking anything will lead to a severe complication and can cause the implementation infeasibility of intelligent, connected healthcare.

3.2. Ot-IoHT (Outdoor) architecture

This IoHT application scenario is much resource restricted than In-Home IoHT. As shown in Fig. 2, the remote monitoring of the patient can be primarily done by wearable medical sensors attached to the patient's body. Other off-body medical instruments available in In-Home monitoring do not concern much because the patient is not in their vicinity. Therefore, in this case, we considered that only on-body sensors sensed the patient's vital. As discussed in Section 3.1, these tiny wearable sensors are the most resource-constraint devices as they do not have much computing capability, memory, power source and bandwidth. Moreover, these devices are the leaf nodes in this network. Therefore, we assumed that only on-body medical sensing devices carried by the patient are 6LoWPAN based IoT-enabled devices that form a 6LoWPAN-wireless body sensor network (WBSN).

In the outdoor scenario, we considered the most general case, that patient only carries the smartphone while she/he is outside the home. This smartphone is the only intermediate node serving leaf nodes attached to the patient's body. It is the only device with higher computation capability and other resources; therefore, it acts as a local sink node. It processes data coming from sensors, hosts concerning applications, issues appropriate notifications/alerts and forwards data from sensors to the cloud. 6LoWPAN-WBSN connects itself to the smartphone using the short-range communication interface to get access to the internet. Smartphones are served by the cellular system in the region that provided 5G/4G/LTE cellular data connectivity to the smartphone.

In the outdoor scenario, getting signal connectivity without any disturbance is a challenge and many factors affecting cellular signals

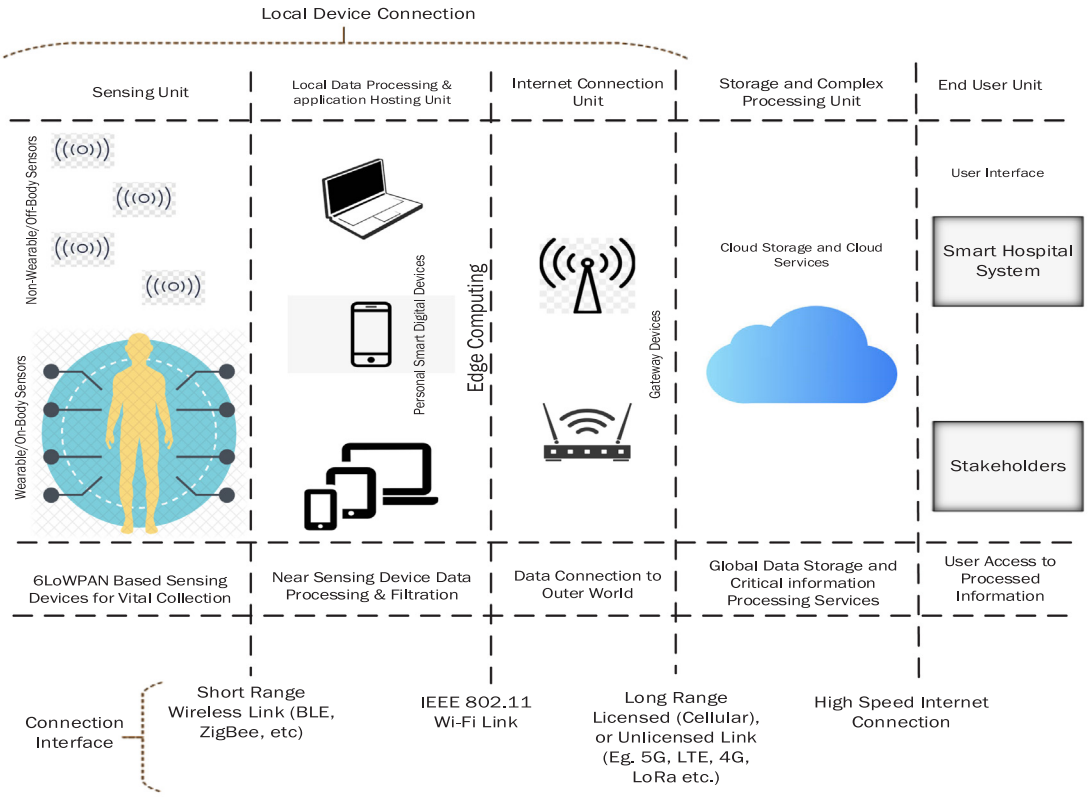


Fig. 1. InHm-IoHT (In-Home) architecture.

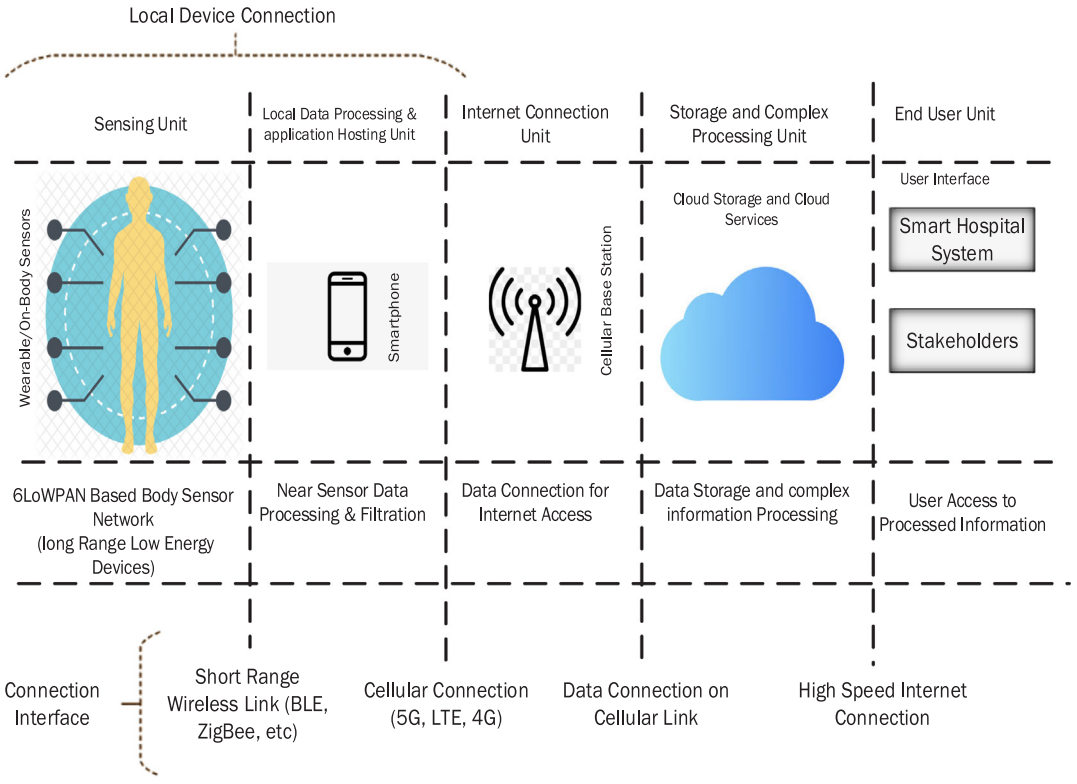


Fig. 2. Ot-IoHT (Outdoor) architecture.

are present. Noise, interference, week signal, low quality of cellular service and so on are common factors that degrade the cellular and data connectivity in the outdoor healthcare network. Therefore, seamless and everlasting data connectivity is essential to serve real-time remote monitoring of outdoor patients. As discussed, the outdoor healthcare network seems to be the most resource-restricted architecture with few

resource-limited sensors (leaf nodes) forming IoT-enabled WBSN connected to the smartphone (local sink) and getting internet connectivity via cellular data services. A combination of IoT-WBSN and smartphone units forms a patient-centric outdoor-IoHT [Ot-IoHT].

Data captured by sensing devices, pre-processed and locally analyzed by smartphones, is transmitted and stored on the cloud. Cloud computing services further perform complex processing and analysis of the data. The final processed and analyzed information is stored and synchronized in real-time with the hospital server. Stakeholders are benefited by using this processed information in various ways. Activities after smartphone layers are discussed in detail in Section 3.1.

The cellular system handles mobility (either low, mid, or high) because mobility occurs when the patient with the smartphone moves. Medicals sensors are affixed to the patient, so no mobility happens there (means that leaf nodes have no mobility). It is assumed that the communication link connecting WBSN and smartphone should remain undetachable. Thus, cellular systems take care of the mobility of smartphones in cellular infrastructure. Altering standard schemes that deal with mobility in a cellular system is out of the scope of our research. Disconnection of data connectivity due to smartphone mobility in the cellular system incurs congestion in the system due to channel loss. We estimate congestion caused by buffer-loss in outdoor healthcare in this paper.

3.3. InV-IoHT (In-Vehicle) architecture

In-Vehicle healthcare monitoring case is almost similar to the OT-IoHT Remote Health Monitoring (RHM). It only differs in terms of the high mobility of the patient as she/he is in the moving vehicle. Fig. 3 exhibits the layout of connected networking components for remote health monitoring when the patient is in transport mode. The connected 6LoWPAN-WBSN and smartphone work as a single unit here (same as in the outdoor case). Sensors affixed on the patient's body collect and transmit the patient's vitals to the smartphone (local sink) using a short-range communication interface, where raw data are locally pre-processed and analyzed. Then patient's smartphone transmits this pre-processed data to the cloud on the go using cellular data connectivity. The significant difference here is that the local collective unit (data sensing and local sink) is under high mobility with the patient. The serving cellular base stations providing cellular services (data and others) frequently change here, which causes recurrent handoff. The cellular system handles handoff strategies (disconnection from one BS and connecting to new BS) to provide uninterrupted data and cellular services. Availability of serving base stations plays a significant role in continuous remote health monitoring in InV-IoHT. The functioning of the rest of the components, elements, and layers of InV-IoHT architecture is the same as in others (explained in Sections 3.1 and 3.2). Here also, channel loss is a significant factor causing congestion.

3.4. InAmb-IoHT (In-Ambulance) architecture

Fig. 4 depicts the layout of different components and layers used in this RHM scenario. This case is applicable when a patient is being carried in the ambulance. The ambulance is equipped with many 6LoWPAN based IoT-enabled medical equipment and sensors that make the ambulance an IoT-enabled emergency vehicle. It also has satellite or cellular communication capabilities to transfer patients' health data and other important information towards the cloud and hospital server. The patient (under RHM) carrying by ambulance is already equipped with IoT-enabled medical sensors connected with the patient's smartphone. If he/she is not the one who is under observation in RHM, then medical staff in the ambulance fixed a wearable IoT-WBSN unit (consisting of different medical sensors) on the patient's body and register that with the patient's smartphone. It means every patient has to be associated with on-body 6LoWPAN-WBSN for remote health monitoring. Therefore, the ambulance carries a patient (under remote monitoring) wearing WBSN registered with the smartphone and many other IoT-enabled medical devices that collect various patient health parameters on the go. Off-body medical devices installed in the ambulance are higher capable and resource-sufficient devices that can pre-process and locally analyze the data sensed by the on-body sensing unit. Both on-body and off-body medical instruments communicate with the cloud using the long-range communication interface (satellite or cellular) pre-installed in the ambulance.

Like other architectures, data stored on the cloud is processed and analyzed using various cloud computing services and complex AI, ML, Bigdata and Data analytic algorithms. The processed data is real-timely synchronized with the hospital server. Stakeholders used processed data stored on the cloud through WWW. Real-time alerts, notifications and decisions are directly communicated to the concerned doctor, patient, family and other caretakers.

High mobility of the ambulance may incur connection and disconnection of communication links that can cause congestion in this network setup. Therefore, both buffer-loss and channel-loss situations need to be sincerely addressed here.

3.5. InHos-IoHT (In-Hospital) architecture

InHos-IoHT is displayed in Fig. 5. It is the most complex architecture that represents the layout of smart IoT-enabled healthcare solutions. A hospital itself is a complex structure consisting of different sections and units serving patients in different ways. Therefore, monitoring the health parameters of every patient admitted or present in the hospital, including various other types of patient data (i.e., reports, locations, physical and personal data, etc.), is a prime concern of this network setup. Patients outside hospital are remotely monitored using architectures explained in Sections 3.1–3.4. Automated management, maintenance/monitoring of enormous medical resources, instruments/equipment (both movable and fixed) is also an important task that needs to be done in this smart hospital system. It also connects and smartly monitors different sections, labs, departments, wards and other important units of a hospital.

Every patient (let say 'n') present in the hospital should be equipped with a wearable 6LoWPAN-IoT enabled WBSN unit registered with his/her smartphone. These 'n' sensing units consist of resource-limited leaf nodes. Besides these, there is an 'x' number of IoT-enabled, 6LoWPAN compatible off-body medical equipment associated with 'n' patients. A patient can be assigned to more than one off-body device. As also discussed in other architecture, these off-body devices are resource-sufficient devices that can serve as an intermediate node between the leaf nodes (on-body resource-constraint sensors) and the local sink node. Near-device data computation can be applied here to pre-analyze the raw data. These devices work as an access point that provides data connectivity to leaf nodes. Other than these, various IoT-capable medical resources such as wheelchairs, stretchers, stethoscopes and others are also considered leaf nodes.

Every BSN unit and off-body medical devices communicate with the associated intermediate node using a short-range communication link. All such devices are wirelessly connected to the pre-existing communication infrastructure of the hospital. This Communication infrastructure is nothing but a network setup of routers, APs, gateways, etc., that establish communication and Internet connectivity hospital-wide. The hospital server and database are directly connected to this network using a wired or wireless link. All the departments and sections (every place) of the hospital connect to the hospital server using this network setup. Hygiene monitoring, alarm, ambiance monitoring, emergency, waste management, disaster response, fire, etc., hospital systems also get connected to the hospital network using this network.

A *Hospital Server* is a very high computational capability system equipped with all the high-end networking resources required to execute very complex algorithms. Furthermore, data storage units (database) is directly connected with the hospital server to store all

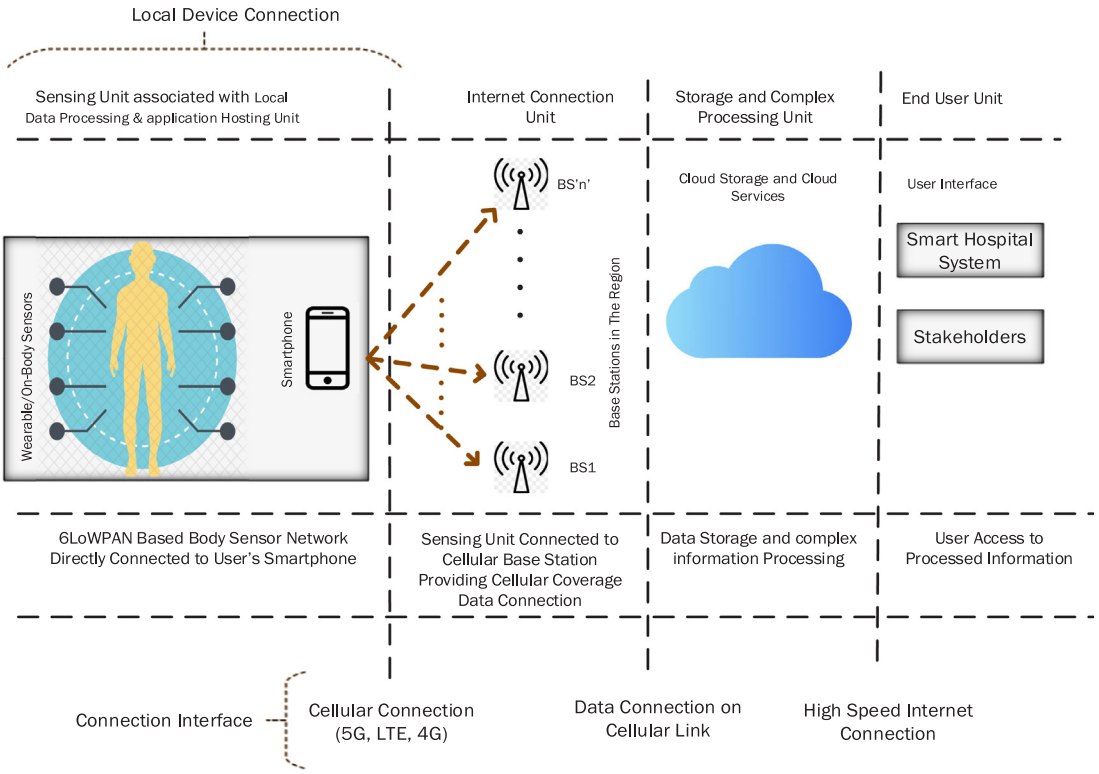


Fig. 3. InV-IoHT (In-Vehicle) architecture.

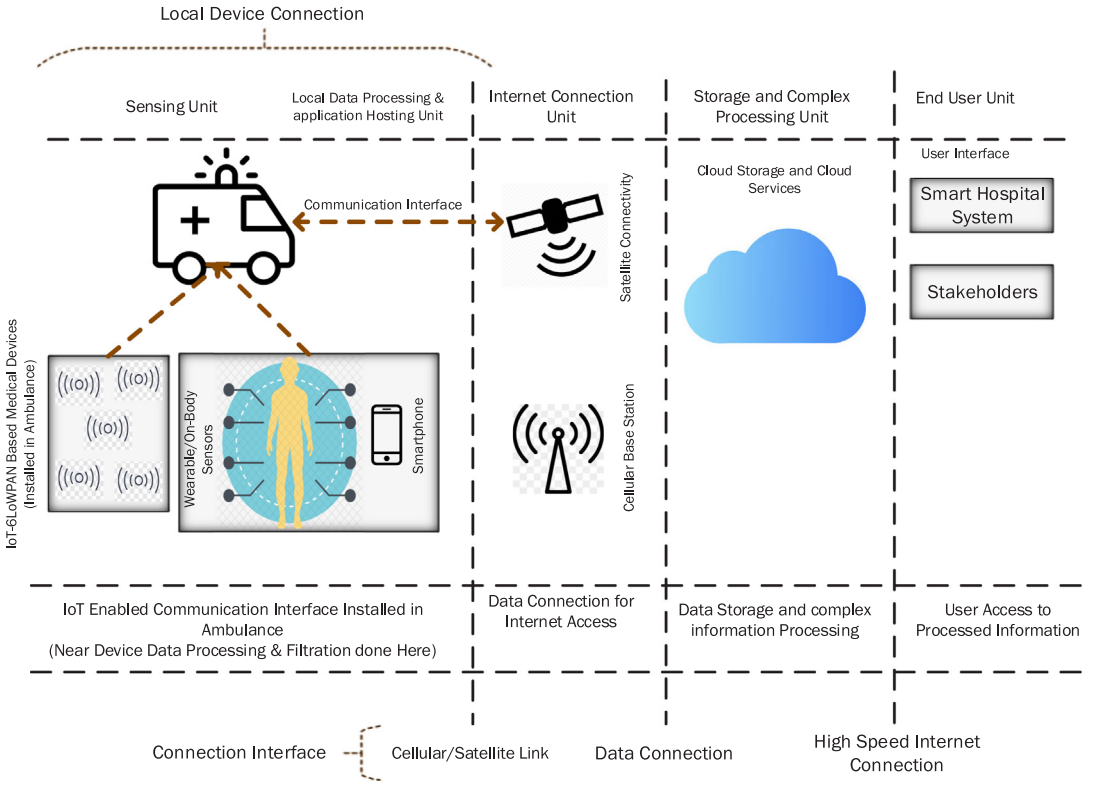


Fig. 4. InAmb-IoHT (In-Ambulance) architecture.

kind of data coming from anywhere in the hospital in real-time. Thus, hospital servers act as a local sink node for the entire hospital, where high-level, complex information processing algorithms utilize technologies like AI, ML. BigData, Data Analytics, etc., to extract all the information from the raw data. This extracted information helps doctors and medical staff with improved decision-making, reduced treatment errors, effective health monitoring of the patient, better & proactive treatment, faster disease diagnosis and so on.

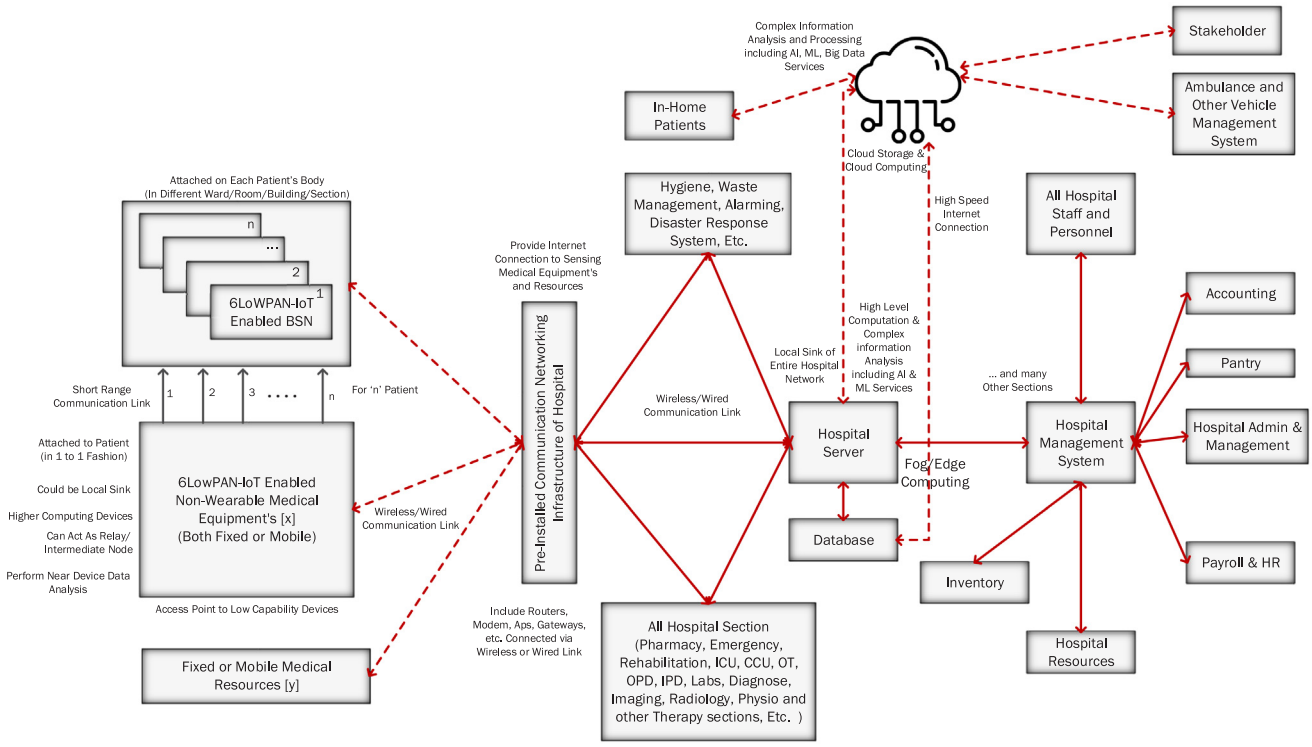


Fig. 5. InHos-IoHT (In-Hospital) architecture.

Edge/fog computing is also applied here for near device information processing. All the functionalities of edge computing are applied to the data coming from every device in the intelligent healthcare system to improvise performance and minimize latency issues. Applying edge computing also reduces the demand of bandwidth required and the cost spent on data processing done in the cloud. Therefore, it is an important layer that needs to be incorporated in IoT-based hospital systems.

The hospital server has a high-speed internet connection and transmits all the data to the cloud (root node) through the edge gateway. Various cloud services are applied to the data coming from the hospital server. Patients under remote observation in different scenarios (mentioned in Sections 3.1–3.4), are connect with hospital server via this cloud layer. The cloud node is the ultimate place where all the information arriving from anywhere is stored, processed and analyzed. The cloud also provides secure global access to the stored medical information to different stakeholders via www for further use.

The hospital management system (HMS) is a time-saving technology that is directly connected to the hospital servers through the hospital's networking infrastructure that manages the different roles of HMS such as inventory, accounting, administration, payroll, hospital resources canteen and many more. It handles and controls data of all the departments (clinical, IPD, OPD, financial, materials, labs, nursing, pharmacy, imaging, rehabilitation, radiology, path-labs). HMS is an intermediate software solution that makes the interaction between the user (hospital employee) and the hospital network possible. It helps hospital members to perform tasks such as: Electronic health records (EHR), enhanced patient care, improved customer services, deploying & managing hospital resources/ staff, accounting & billing of patient's expenditure, administrative & clinical management, automated inventory monitoring & management, smart user-centric pantry, cuts-down operational cost, improved quality and compliance, fewer errors, faster processing & speedy results, data security & recoverability and many others. It is an intelligent platform providing solutions for all sorts of maintenance and managing services efficiently and effectively. It optimizes and digitizes various processes involved in operating a healthcare organization.

3.5.1. In-hospital topology

The in-hospital architectural layout (unveiled in Figs. 6, 7) are different from the IoHT architecture for patient's remote monitoring outside the hospital. It consists of leaf nodes, intermediate nodes, local sink access points, a sink node and a root node. Each patient admitted to the hospital is get associated with the on-body and off-body sensing unit. Other than that, few other IoT-enabled medical instruments are used to monitor or carry the patient. These all three kinds of IoT-enabled, 6LoWPAN-based devices are considered leaf nodes. Some of these devices are equipped with higher networking and computation capabilities. Such devices can be used as intermediate nodes to relay data collected from leaf nodes towards a local sink node.

6LoWPAN based local sink APs are installed in every corner of hospital infrastructure as a part of the hospital's communication network. Every possible leaf node should connect wirelessly to these local sink APs directly or via an intermediate node. These local sinks are also wirelessly connected and form a network of local sink APs. These APs are higher capability devices with sufficient resources to serve multiple leaf nodes without any delay or loss of data packets.

The network of local sinks is a part of the pre-existing communication network. Edge computing devices are also installed in this network to filtrate the data coming from sensing devices that reduce the consumption of networking resources. The hospital communication network is a complex system of interconnected (through wired or wireless link) access points, modems, routers and other networking devices, covering every area & corner (rooms, sections, departments, etc.) of the hospital. This same network provides internet connectivity to each device that is involved in any sort of data communication. Uninterrupted Internet access is required here for real-time data transmission. At another end of this network, a hospital server is connected that provides all the necessary services. The hospital server is the sink node where all the captured data is stored and processed into precise information. It further connects to the cloud (via a high-speed internet link) to avail high-end cloud computing and data processing services. The processed information stored at both devices should be synchronized to each other. Users (stakeholders) can securely access

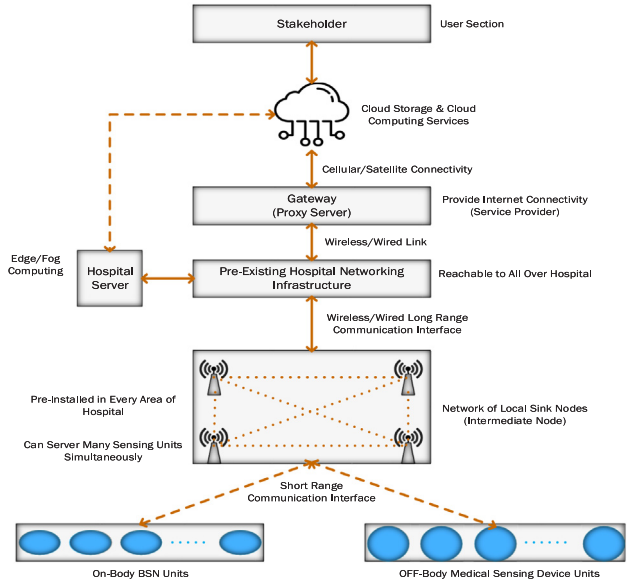


Fig. 6. Generalized topological view of In-hospital IoHT.

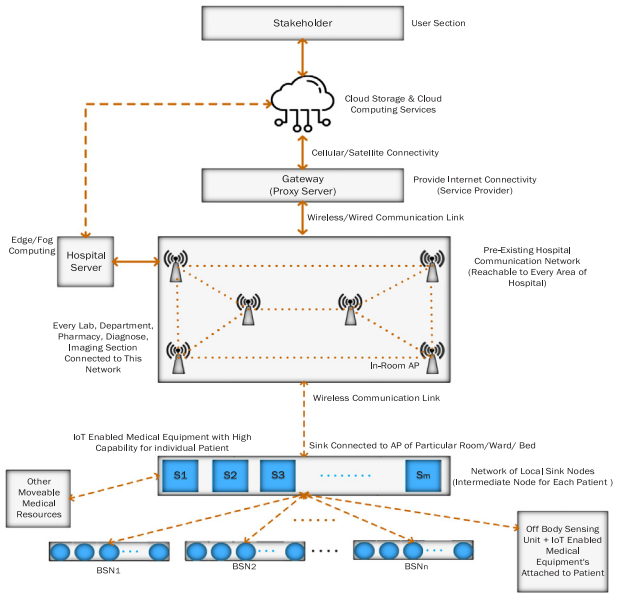


Fig. 7. Detailed topological view of In-hospital IoHT.

information from the cloud through a web-based platform interface.

This detailed discussion of different patient-centric IoHT architecture leads us to shape a generalized topological layout for Remote Health Monitoring in the following section.

4. Topological layout of IoHT for Remote Health Monitoring (RHM)

In this section, we elaborate on the analysis of different IoHT-architectures explained in Section 3. Here, we summarize how different components of IoHT are physically connected to form a topology. As we have already identified in every IoHT architecture, there are different nodes such as leaf nodes, intermediate nodes, local sink and sink (root) nodes.

Leaf nodes are resource-limited sensing devices (could be on-bod/off-body) that have limited computing capability. These nodes capture data from the patient's body and transmit it to the serving intermediate node. It can consume available bandwidth to the fullest as they only communicate forward, i.e., uplink (leaf node to intermediate). Many leaf nodes (>intermediate node) connect to an intermediate node using short-range wireless communication interfaces.

Intermediate nodes are higher computing devices that transmit data coming from leaf nodes to the local sink. Its data rate is half due to bandwidth division in the link receiving data from the leaf node and sending it to the local sink node. IoT-enabled medical instruments may have high computational capabilities. Personal digital devices that are not acting as a local sink can also act as an intermediate node. There could be one or more intermediate nodes, and one such node can serve multiple leaf nodes simultaneously. If there are multiple intermediate nodes, they all must be connected (form a network of intermediate nodes). The intermediate node functions as a gateway to the outer world.

Local sinks are the nodes where the data collected from medical devices is temporarily stored and transmitted to the cloud. Such nodes include devices like smartphones, PC, laptops and other personal digital devices that are not intermediate devices. There could be only one such device in a patient-centric IoHT architecture. The local sink node hosts various applications that interpret data coming from the sensing unit. This device has internet connectivity and provides internet access to leaf nodes.

Near-device data computing concepts (edge/fog computing) can also be applied to reduce data redundancy and filter out unnecessary data. Pre-processing and regional data analysis can also be done at the local sink to provide notifications, suggestions and alerts locally with no delay in response from the cloud. The patient's smartphone is a recommended device to be considered as a local sink. The patient's smartphone can serve as an intermediate node and the local sink node (the most restricted IoHT architecture). The connection setup of the leaf nodes, intermediate and a local sink node forms a local network layout connected through short-range wireless communication technology. Edge computing gateway (or services) are applied at local sink nodes that remove unnecessary data to be transmitted and stored at the root node (cloud) to save bandwidth, memory and other resources.

The local sink node uses licensed or unlicensed long-range communication technology such as cellular, satellite, and Wi-Fi. This internet connectivity lets the local sink node pass on the data captured from the leaf node to the sink node (the cloud). The cloud (global sink) node owns complex computation capabilities required to process and analyze the data and store it for further use. From this node, global access to processed information is securely provided to its users.

We consider two scenarios of the IoHT architectural layout and explained them in the following subsections.

4.1. Generalized RHM IoHT layout

Fig. 8 displays a generalized topological setup of different nodes and elements in an IoHT network. Architecture such as In-Home healthcare, In-Ambulance, In-hospital (explained in Sections 3.1, 3.4 and 3.5) normally follows this layout. As displayed, leaf nodes (on-body and off-body medical sensing equipment) connect to the intermediate node using wireless short-range p2p links. One intermediate node or a set of connected intermediate nodes (devices having high computational capabilities) serves these leaf nodes by transmitting their data to the local sink device. Suppose the same amount of bandwidth is allocated to leaf and intermediate nodes (our consideration). In that case, the data rate of the intermediate node is half of the leaf node because the intermediate node simultaneously communicates with the leaf node and local sink node. If the link capacity is not sufficient, then the leaf node can experience a buffer overflow situation that causes congestion at the leaf node. A proper estimation of buffer-overflow needs to be done by considering all the factors affecting packet loss at buffer to reduce the chances of congestion at a leaf node.

Each intermediate node serves a few leaf nodes that may cause faster occupancy of a buffer queue. Furthermore, it can lead to packet

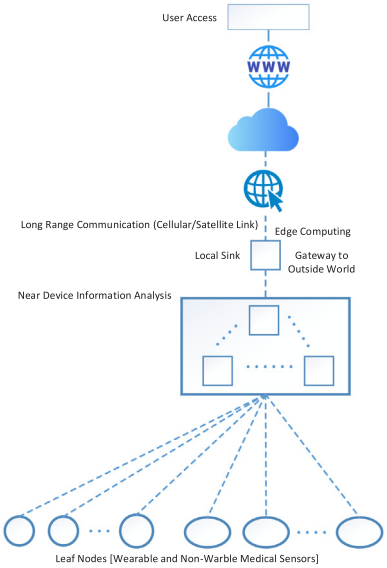


Fig. 8. Generalized topological layout of Outside-IoHT.

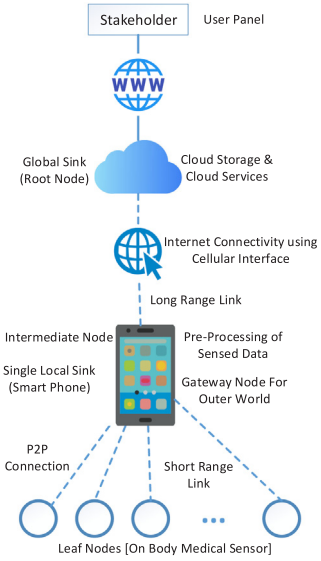


Fig. 9. Resource-restricted topological layout Outside-IoHT.

loss at the buffer of the intermediate node if the incoming and outgoing rate of packets mismatches. This situation can start congestion at the intermediate node. Therefore, handling congestion at an intermediate node that occurs when packet drops due to the unavailability of buffer space is essential.

Packet loss and delayed delivery of a packet due to any reason are undesirable in the IoHT network. It disturbs the real-time transmission of data from the leaf node to the sink node. The local sink node is a higher computation device with all the required resources to pre-process the raw data. It hosts applications that medically assist a patient based on locally captured data. The short-range wireless link connects the intermediate node and the local sink. An edge computing device (or gateway) can also be added separately after the local sink if required.

The local sink (or edge gateway) is connected to the cloud (root node) via high-speed internet connectivity. Here, complex processing and analysis of received data are done to convert it into the most appropriate information. The root node is further connected to the hospital server to provide patient's captured information locally to the hospital for various usage. Finally, users and other stakeholders access processed information from the cloud through web-based platforms.

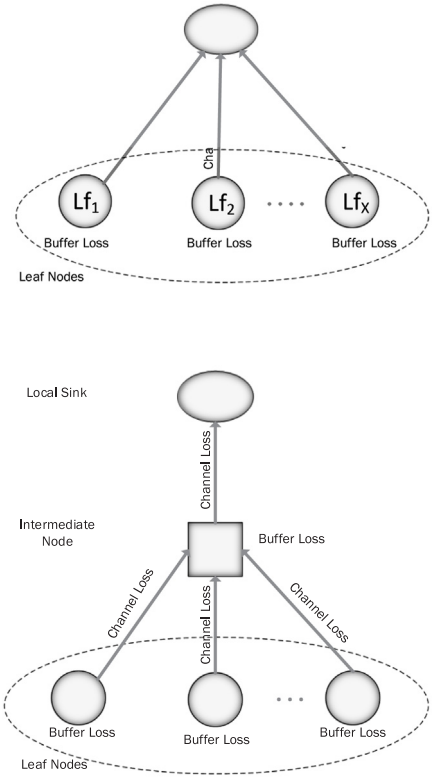
4.2. Resource-restricted RHM IoHT layout

Ot-IoHT and InV-IoHT are laid out in this type of topological setup shown in Fig. 9. However, this interconnected setup can differ from the general IoHT layout (explained in Section 4.1) at two points:

- First, at the leaf node layer, there are only on-body (wearable) medical sensing devices. Whereas, in general architecture, both on-body and off-body medical sensing devices are present. It means the number of leaf nodes is less in resource-restricted IoHT architecture.
- Second, utmost one intermediate node, one local sink device (patient's smartphone) is directly connected to the Wearable-WBSN. Thus, smartphones alone do the functioning of the intermediate node and the local sink node.

Fig. 10 illustrate interconnection of different nodes involved in local patient-centric IoHT. The connectivity and functionalities of the other elements are the same as described in the generalized layout (Section 4.1).

We considered the layouts exhibited in Fig. 10 to model Buffer loss for 6LoWPAN-based, resource-restricted IoHT network in the following section.



(b) with an intermediate node

Fig. 10. Local Interconnection of Nodes in Resource-Constraint IoHT.

5. Modeling buffer loss for resource-restricted ioht

Congestion in IoHT can substantially degrade the overall quality of service (QoS) and impact the energy efficiency of the network. Furthermore, it significantly increases the packet loss and delays while reducing the throughput of the system. In 6LoWPAN based networks, there are two points when congestion can happen: (i) Node, (ii) Link. The Node-level congestion triggers buffer overflow, while congestion at the link is caused by interference and leads to contention and

collisions. Therefore, a hop-by-hop strategy is recommended to control the congestion in the wireless 6LoWPAN network. Furthermore, congesting notification and recovery of losses should be implemented locally at each intermediate node to handle the congestion occurrence immediately.

The reason for congestion in this 6LoWPAN based IoHT network are:

- Multiple leaf nodes simultaneously transmit packets at a higher data rate.
- More than one network route is relayed by a node (case of the intermediate node).

These events can trigger a buffer overflow and collision of packets at wireless link [27]. The buffer overflow intervenes when the incoming and outgoing rates of the packets have a significant variation (mismatch). Therefore, when a fast-source node rapidly sends packets to a slow receiver, its MAC layer buffer fills very frequently, and it further cannot handle all the incoming packets. Due to that, many packets are lost at the receiver's buffer. Moreover, the source node will retransmitted these lost packets because the receiver could not process all incoming packets.

A good estimation of buffer loss would minimize the packet loss. *Queuing Theory* is an essential concept that is frequently used to study, analyze and measure the performance of computer networks. Queuing analysis is a particular case of Markov chains that deal with the node's buffer. Therefore, we used Queuing theory to design a buffer-loss estimation model.

Based on the queuing theory, we have drawn a model for buffer overflow estimation in the subsections below.

5.1. Queuing model for buffer overflow estimation

A node's buffer (at MAC layer) can be visualized as a waiting line, i.e., a queue of packets arrived from the upper layer with an expected (average) arrival rate of λ packets/second. These arrivals of packets follow the 'Poisson distribution' over time because:

- The number of arrivals in non-overlapping time intervals are statically independent.
- The packet arrival events are independent and the average packet arrival rate is constant.
- Only one arrival can happen in the shortest time interval (δ) and no two arrival events can co-occur.
- Due to the memory-less property of the Markov chain, The arrival property is independent of the past.

The arrived packets are further transmitted by the node's radio with an average μ packet/second departing rate that is 'Exponentially distributed' over time. The reason for exponential distributed departure rate is:

- The packet arrival following Poisson distribution has exponentially distributed departure that constitutes an independent identically distributed (iid) process.
- The time in the state (service time) follows exponential distribution due to memory-less property.
- Transition to ith state from $i-1$th or $i+1$th state cannot be differentiated as it does not store any such information.
- Initially, if a queue is empty, it is guaranteed by the fact that Poisson-distributed arrival has exponential-distributed interval time.
- Even if the queue is not empty, the time in each state must also be exponentially distributed.
- It states that the service time must be exponentially distributed with value $\frac{1}{\mu}$.

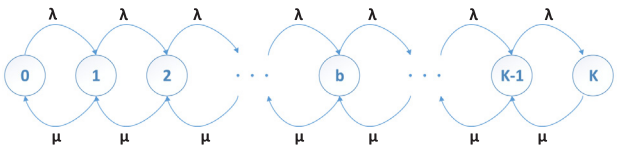


Fig. 11. Markov chain of buffer.

As we know, there is only one buffer and one radio transmitter in nodes (6LoWPAN devices involved in IoHT). Therefore, if the buffer size is 'K', it forms a finite queue of M/M/1/K type of the queuing theory, a particular case of the Markov chain. Generally, for infinite queues, $\frac{\lambda}{\mu} < 1$ condition should hold. However, in this case, $\frac{\lambda}{\mu} > 1$ then some (at least 1) packet could not be transmitted ever. Nevertheless, in the case of M/M/1/K finite queue, we certainly do not worry much about condition $\frac{\lambda}{\mu} < 1$ being true. Because if $\frac{\lambda}{\mu} > 1$ is the case, then some packets dropped and could not get the entry in the queue. If $\lambda < \mu$, then a queue is required due to the inter-arrival of packets. Again, λ, μ are expected mean (average) values over a long period. These are not actual values. Force balking is happened when a packet comes after the buffer is full. The packets present in the buffer queue are served in FIFO (first-in-first-out) fashion. Markov chain (State diagram) for this M/M/1/K queue (Node's Buffer) is exhibited in Fig. 11.

(a) ***Equilibrium Equation:***
Due to the memory-less property of the 'Markovian queue', any previous state does not consider defining the present state. At steady state (having K states), probabilities of having 0, 1, 2, ..., K packets in the buffer is represented as $p_0, p_1, p_2, \ldots, p_b, .., p_K(p_{pkt-drop})$. During a minimal time interval δ, only one event occurs, i.e., either the arrival of one packet or the departure of a packet.
Thus, the load balancing equation is described as:

$$\begin{aligned} p_k(T+\delta) = {} & [p_{k-1}(T) \times (1 - arrival \ \& \ no - service)] \\ & + [p_{k+1}(T) \times (No - arrival \ \& \ 1 - service)] \\ & + [p_k(T) \times (No - arrival \ \& \ No - service)] \end{aligned} \tag{1}$$

Where, 1 arrival = $\lambda\delta$; 1 service = $\mu\delta$; No Arrival = $(1-\lambda\delta)$; No Service = $(1-\mu\delta)$; After putting these values in Eq. (1).

$$\begin{aligned} p_k(T+\delta) = {} & [p_{k-1}(T) \times \lambda\delta(1-\mu\delta)] + [p_{k+1}(T) \times \mu\delta(1-\lambda\delta)] \\ & + [p_k(T) \times (1-\lambda\delta)(1-\mu\delta)] \end{aligned}$$

On simplifying and leaving 2nd (and higher) order terms.

$$p_k(T+\delta) = [p_{k-1}(T) \times \lambda\delta] + [p_{k+1}(T) \times \mu\delta] + [p_k(T) \times (1-\lambda\delta-\mu\delta)]$$

$$\frac{p_k(T+\delta) - p_k(T)}{\delta} = [p_{k-1}(T) \times \lambda + p_{k+1}(T) \times \mu - p_k(T) \times (\lambda+\mu)]$$

At steady state, the change of $p_k(T)$ to the interval λ becomes zero because probabilities do not depend on time.

$$0 = [p_{k-1}(T) \times \lambda + p_{k+1}(T) \times \mu - p_k(T) \times (\lambda+\mu)]$$

Then, the equilibrium equation is formulated as:

$$(\lambda)p_{k-1} + (\mu)p_{k+1} = (\lambda+\mu)p_k \tag{2}$$

(b) ***Finding Relation between Probabilities:***
Two consecutive probabilities form a relation here. It can be drawn as:

$$\begin{aligned} p_0(T+\delta) = {} & [p_1(T) \times (No - arrival \& 1 - service)] + \\ & [p_0(T) \times (No - arrival \& No - service)] \end{aligned}$$

After putting associated values:

$$p_0(T+\delta) = [p_1(T) \times (1-\lambda\delta) \times \mu\delta] + [p_0(T) \times \ (1-\lambda\delta) \times (1-\mu\delta)]$$

Because there is no packet in the system, therefore, no service can be done. Hence, $(1-\mu\delta) = 1$. Replacing it in the above equation and leaving the higher-order terms.

$$p_0(T+\delta) = [p_1(T)\times\mu\delta] + [p_0(T)\times(1-\lambda\delta)]$$
$$\frac{[p_0(T+\delta)-p_0(T)]}{\delta} = [p_1(T)\times\mu] - [p_0(T)\times\lambda]$$

As we already mentioned, The rate of change w.r.t δ (at steady state) is zero.

$$\frac{[p_0(T+\delta)-p_0(T)]}{\delta} = 0$$

Finally, the relationship between consecutive probabilities is:

$$\mu p_1 = \lambda p_0 \tag{3}$$

That defines,

$$p_1 = (\frac{\lambda}{\mu})\times p_0$$

At k=1, Eq. (2) results:

$$\mu p_2 = \lambda p_1$$
$$p_2 = (\frac{\lambda}{\mu})p_1 = (\frac{\lambda}{\mu})^2 p_0$$

Consider that, $\frac{\lambda}{\mu} = \rho$, that denotes the traffic intensity (service utilization). In general, for a stable system, the relation 'ρ<1' must be true (especially for infinite queue). If it is not, then at least one packet could not be served ever. However, it is recommended to have the 'ρ<1' condition true for finite queue cases but not worry too much about this. If the condition does not hold in the finite queue, the packet cannot enter the buffer and drop due to *Force Balking*.

In general, the above equation is represented as:

$$p_k = (\frac{\lambda}{\mu})p_{k-1}$$
$$p_k = \rho p_{k-1} \tag{4}$$

That is further deduced as:

$$p_k = (\frac{\lambda}{\mu})^k p_0$$
$$p_k = \rho^k p_0 \tag{5}$$

Eq. (4) is said as a *Load Balancing Equation*.

5.2. Modeling node's buffer as M/M/1/K queue

In M/M/1/K queuing model, first 'M' represents the expected (average) packet arrival rate ('λ') that follows the 'Poisson distribution.' Then, the second 'M' shows the packet's average service/departure rate ('μ') following an 'Exponential distribution.' Finally, the '1' define that the system has a single server and the finite buffer size is denoted by 'K.'

(a) ***Finding probability of empty*** ('p_0') & ***full*** ('p_K') ***buffer:*** Using the normalization condition (i.e. the sum of all individual state probabilities is 1):

$$p_0 + p_1 + p_2 + \cdots . + p_{K-1} + p_K = 1$$

Where, $p_0, p_1, p_2, \ldots, p_{K-1}, p_K$ are probabilities when there are 0, 1, 2, …, up to K packets are in the buffer.

$$p_0 + \rho p_0 + \rho p_1 + \cdots . + \rho p_{K-1} = 1$$
$$p_0 + \rho p_0 + \rho^2 p_0 + \cdots . + \rho^K p_0 = 1$$
$$p_0[1 + \rho + \rho^2 + \cdots + \rho^K] = 1$$

The series in the square bracket represents a finite geometric progression series that starts from 1 and have K+1 terms.

Therefore, it can be written as:

$$p_0\left[\frac{(1-\rho^{K+1})}{(1-\rho)}\right] = 1$$

– ***Probability of empty buffer*** is:

$$p_0 = \left[\frac{(1-\rho)}{(1-\rho^{K+1})}\right] \tag{6}$$

The probability of a filled buffer (denoted by p_K) is also the probability of packet drop or loss. It can be derived using Eq. (5) and relation $p_K = \rho^K p_0$ as:

– ***Probability of full buffer (prob. packet drop)***

$$p_{pkt-drop} = p_K = \rho^K\left[\frac{(1-\rho)}{(1-\rho^{K+1})}\right] \tag{7}$$

(b) ***Performance evaluation parameters:***

Following are the different performance evaluating parameters:

– ***Average number of packets in the system***

It can also known as 'system occupation' and computed as:

$$E[K] = \sum_{k=0}^{K} k p_k = \sum_{k=0}^{K} k\rho^k p_0 \tag{8}$$

After substituting values, it is deduced as:

$$E[K] = \frac{\rho[1 + K\rho^{K+1} - (K+1)\rho^K]}{(1-\rho)(1-\rho^{K+1})}$$

After simplifying,

$$E[K] = \left(\frac{\rho}{1-\rho}\right) - \left(\frac{(K+1)\rho^{K+1}}{(1-\rho^{K+1})}\right) \tag{9}$$

The first part of Eq. (9) indicates occupancy of the infinite queue and the second part describes queue occupancy lost due to finite buffer. As observed, the second part of the above equation tends to zero when $\rho < 1$. when $\rho = 1$ then $E[K] = \frac{K}{2}$.

However, due to finite queue (buffer), there could be a situation of Force Balking. It means when there are K packets in the buffer already. Then, the new arriving packet balks. Due to the finiteness of the buffer, not every arriving packet joins the buffer queue. Because of this, the actual packet arrival rate λ changes to $\lambda_{effective}$, and it is calculated as:

The packets that are actually in the buffer have probability as $(1-p_K)$. Therefore,

$$\lambda_{effective} = \lambda(1-p_K) \tag{10}$$

– ***Average number of packets in the buffer***

It is denoted by $E[K_q]$ and calculated as:

$$E[K_q] = \sum_{k=0}^{K}(k-1)p_k = E[K] - \frac{\lambda_{effective}}{\mu} \tag{11}$$

– ***Average number of packets in the processing***

$$E[K_p] = (1-p_0) \tag{12}$$

And, by utilizing $\frac{\lambda}{\mu} = \frac{(1-p_0)}{(1-p_K)}$ equality. It can also be derived as:

$$E[K_p] = \rho(1-p_k)$$

Eqs. (9), (11), and (12) holds a relation as:

$$E[K] = E[K_q] + E[K_p] \tag{13}$$

– ***Expected packet delays***

Using Little's Law [28], average delays can be defined as:

$$E[D] = \frac{E[K]}{\lambda_{effective}}$$
$$E[D_q] = \frac{E[K_q]}{\lambda_{effective}} \tag{14}$$
$$E[D_p] = \frac{E[K_p]}{\lambda_{effective}} = \frac{(1-p_0)}{\lambda_{effective}}$$

Where E[D] is an average delay of a packet in the system, $E[D_q]$ is the average delay of a packet in the buffer queue, and $E[D_p]$ is the average delay of a packet in processing.

– ***The relation between delays*** is defined as:

$$E[D] = E[D_q] + E[D_p]$$

– ***Probability of buffer-loss*** is computed as:

$$P_{Buffer-Loss} = (Prob.\ Full\ Buffer\ at\ leaf) + \frac{(Prob.\ Full\ Buffer\ at\ intermediate\ node)}{X}$$

After substitution, The equation is:

$$P_{Buffer-Loss} = (P_K)^{Leaf} + \frac{(P_K)^{Int}}{X} \tag{15}$$

– ***The number of packets lost at the leaf node's buffer due to buffer overflow*** is calculated as:

$$(P_K)^{Leaf} \times \lambda \tag{16}$$

– Similarly, $(P_K)^{Int} \times \lambda$ gives the number of packets lost at the intermediate node's buffer.

– The total dropped packets due to buffer loss are the sum of packets dropped at each leaf and the intermediate node.

– ***The overall number of packets lost due to buffer-loss*** is computed as

$$P_{Buffer-Loss} \times \lambda \tag{17}$$

– ***The total packet received at local sink node*** is calculated as:

$$\lambda \times (1 - P_{Buffer-Loss}) \times (1 - P_{Channel-Loss}) \tag{18}$$

– The portion belonging to the intermediate node is discarded if it is not involved in the topology.

– ***Throughput***

$$Thr = \mu(1 - p_0) \tag{19}$$

6. Analytical Model for Congestion in 6LoWPAN-IoHT Network

Here, an analytical model is presented to evaluates the performance of the 6LoWPAN network in a congestion scenario. *Expected number of packet lost due to buffer-loss* and *average packet received at local sink node* are used as performance measures. The buffer of sensor nodes is a queue, where packets arrive to be processed and dispatched. A variation of *Number of sensor nodes (leaf)*, *buffer size*, and *number of arriving packets (load)* is used to examine the performance of this resource-constraint 6LoWPAN-IoHT network.

RPL (IPv6 Routing Protocol for Low-power, Lossy networks) build the topology in 6LoWPAN networks [29]. Fig. 10 illustrates the interconnection of leaf, intermediate and local sink nodes. Topological architectures displayed in Fig. 10(a), 10(b) are considered to estimate buffer loss. Let us say that there is 'X' leaf nodes that transmit sensed data towards the local sink device either directly (shown in Fig. 10(a)) or via an intermediate node (displayed in Fig. 10(b)). One local sink and one intermediate node (if available) are used in topology.

The following sections elaborate on the presented analytical model.

6.1. System model

We assumed that each node in this 6LoWPAN-based IoHT network has a buffer of 'K' size. Each node in the network shares the wireless channel capacity of 'R' bits/second. The intermediate node has half of the channel capacity in comparison to the leaf node's channel capacity. Because transmitter (radio) of leaf node only send packets while intermediate node transmits and receive packet simultaneously. That means, sending rate of the leaf node is double the intermediate node's sending rate. It is also supposed that nodes work on the contention-based IEEE 802.15.4 MAC protocol and use unslotted CSMA/CA for access control.

Leaf node's application layer captures data and forwards it to its MAC layer with an average arrival rate λ. These packets are stored at the Leaf's MAC buffer for processing and transmitting to intermediate or local sink nodes. At Leaf, packets may get dropped with probability $p^{Leaf}_{Buffer-Loss}$ due to insufficient (limited) buffer space. Leaf's MAC protocol forward packets stored at buffer with average departure rate of μ_{Leaf}. At the wireless link, packets may be lost due to link collision with probability $p_{channel-Loss}$. Packets from leaf nodes are arrived at intermediate node (if present) with an **average arrival rate** λ^{Int}_j that is computed as:

$$\lambda^{Int}_x = (1 - p^x_{channel-Loss})\mu^{Leaf}_x \tag{20}$$

Where, $x = 1, 2, 3, \ldots,$ X denotes the number of available leaf nodes.

Leaf's departure rate is figured out as:

$$\mu_{Leaf} = (1 - p^{Leaf}_{Buffer-Loss}) \times \lambda \tag{21}$$

The total expected packets arrival rate is calculated as:

$$\lambda^{Int}_{Total} = \sum_{j=1}^{X} \lambda^{Int}_j \tag{22}$$

The intermediate node stores the incoming packet in its buffer, where packets are dropped with probability $p^{Int}_{Buffer-Loss}$ due to buffer overflow. Stored packet at intermediate's buffer is further forwarded to local sink with an average departure rate μ_{Int}.

6.2. Estimating buffer-loss probability

This modeling is influenced by M/M/1/K queue, where the average packet arrival rate λ follows Poisson distribution, and packet departures to be Exponentially distributed with mean departure rate μ. The expected service time of each packet is $\frac{1}{\mu}$. State transition would take time interval δ that is computed as $\delta = \frac{1}{R}$. Where 'R' is channel capacity in bps. If channel capacity is given in bits, then it can be converted in bits per second (bps) using $R = \frac{Channel\ Capacity\ (in\ bits)}{Packet\ Length}$.

(a) ***At leaf node:***

Probability of packet arrival and packet departure is computed as:

$$p^{Leaf}_{Arrival} = \frac{\lambda}{R}$$
$$p^{Leaf}_{Departure} = \frac{\mu^{Leaf}_{Max}}{R} \tag{23}$$

As mentioned above, the leaf shares double channel capacity as compared to the intermediate node.

– **The maximum departure rate of the leaf node** is estimated as:

$$\mu^{Leaf}_{Max} = \frac{2R}{2X + 1}$$

– Therefore, the expected number of packets dropped in time δ at each leaf's buffer is derived as:

$$E\left[N^{\delta}_{Leaf}\right] = (p_K)^{Leaf} \times p^{Leaf}_{Arrival} \times (1 - p^{Leaf}_{Departure}) \tag{24}$$

– Thus, **the expected number of packets dropped per second at leaf node** is computed as:

$$E\left[N_{Leaf}\right] = (p_K)^{Leaf} \times p^{Leaf}_{Arrival} \times (1 - p^{Leaf}_{Departure}) \times R \tag{25}$$

– Thereby, **the leaf node's probability of packet loss due to buffer overflow** is given by:

$$p^{Leaf}_{Buffer-Loss} = \frac{E[N_{Leaf}]}{\lambda} \tag{26}$$

(b) ***At Intermediate Node:***
The probability of packet arrival and packet departure is computed as:

$$p^{Int}_{Arrival} = \frac{\lambda^{Int}_{Total}}{R}$$
$$p^{Int}_{Departure} = \frac{\mu^{Int}_{Max}}{R} \quad (27)$$

– ***Intermediate node's maximum departure rate*** is estimated as:

$$\mu^{Int}_{Max} = \frac{R}{2X+1} \quad (28)$$

– Therefore, the expected number of packets dropped in time δ at the buffer of the intermediate node is figure out as:

$$E\left[N^{\delta}_{Int}\right] = (p_K)^{Int} \times p^{Int}_{Arrival} \times (1 - p^{Int}_{Departure})$$

– Thus, ***the expected number of packets dropped per second at intermediate node*** is computed as:

$$E\left[N_{Int}\right] = (p_K)^{Int} \times p^{Int}_{Arrival} \times (1 - p^{Int}_{Departure}) \times R \quad (29)$$

– Thereby, ***the intermediate node's probability of packet loss due to buffer overflow*** is calculated as:

$$p^{Int}_{Buffer-Loss} = \frac{E[N_{Int}]}{\lambda^{Int}_{Total}} \quad (30)$$

(c) ***Total mean number of the lost packet at buffer*** in the network is:

$$E\left[N_{Buffer-Loss}\right] = X \times E\left[N_{Leaf}\right] + E\left[N_{Int}\right] \quad (31)$$

And, if no intermediate node is involved, Then:

$$E\left[N_{Buffer-Loss}\right] = X \times E\left[N_{Leaf}\right] \quad (32)$$

(d) ***Total buffer-loss probability*** in the network is:

$$p_{Buffer-loss} = \frac{E\left[N_{Buffer-Loss}\right]}{X \times \lambda} \quad (33)$$

(e) After substitution, ***Total buffer-loss probability*** is formulated as:

$$p_{Buffer-loss} = \frac{[X\,(P_K)^{Leaf}\,\lambda(R - \mu^{Leaf}_{Max})] + [(P_K)^{Int}\,\lambda^{Int}_{Total}(R - \mu^{Int}_{Max})]}{X\;\lambda\;R} \quad (34)$$

(f) ***Expected number of the received packet at local sink 'LS'*** When one intermediate node involved in between leaf nodes and local sink, is computed as:

$$E\left[N^{LS}\right] = \left(1 - p^{Int}_{Channel-loss}\right)\left(1 - p^{Int}_{Buffer-loss}\right)\lambda^{Int}_{Total} \quad (35)$$

(g) ***Expected number of the received packet at local sink 'LS'*** When no intermediate node involved, is figure out as:

$$E\left[N^{LS}_{no-Int}\right] = \lambda\left(1 - p^{Leaf}_{Buffer-Loss} - p^{Leaf}_{Channel-Loss}\right) \quad (36)$$

6.3. Probability of packet loss at wireless link

As published by Di Marco et al. [30], the two reasons behind the loss of a packet at the wireless link are:

– Channel Access failure
– Maximum limit of packet re-transmission

In *Channel Access process*, when a node wants to send the packet, it first senses that the channel is idle or not. If the channel is free, then it starts transmitting the packets. However, if the channel is busy (transmitting other packets/ACKs), it waits for a backoff period and then senses the channel again. The backoff period depend of two-parameter: (i) *Number of backoffs (NB)* and (ii) *backoff exponent (BE)*. 'NB' and 'BE' are increased in each try of channel access. NB range between $0\,to\,2^{BE} - 1$. Backoff Period $= 20\,symbol \times 16\mu sec/symbol$ [31]. The packet is dropped when 'BE' surpass '*mac-max-CSMA-backoff*' parameter.

In the second case, the node waits for an acknowledgment (ACK) after transmitting a packet. The same packet is retransmitted again if the node does not receive the packet's ACK. It happens due to ACK timeout expires or if the ACK packet gets collided. Before retransmitting a packet the *retransmitting count* is incremented. The packet is dropped if *retransmitting count* reaches *mac-max-frame-retries*.

Let us say, if *maximum number of backoff* is 'u', and *maximum number of re-transmission* is 'v'. Therefore, the packet is lost at a node if it does not get idle channel within $(u+1)$ backoffs. The packet also gets dropped if $(v+1)$ consecutive collision occurs while re-transmitting the same packet.

– Therefore, ***the Channel loss probability*** of a node is calculated as:

$$p^{x}_{Channel-Loss} = p^{x}_{Channel-Access-Failure} + p^{x}_{Max-Retransmit} \quad (37)$$

– ***Probability of channel access failure and probability of maximum re-transmission for unslotted IEEE 802.15.4*** is modeled in [30] as:

$$p^{x}_{Channel-Access-Failure} = \frac{(p^{x}_{channel-busy})^{u+1}\left(1 - \left(p^{x}_{collide}\left(1 - (p^{x}_{channel-busy})^{u+1}\right)\right)^{v+1}\right)}{1 - p^{x}_{collide}\left(1 - (p^{x}_{channel-busy})^{u+1}\right)} \quad (38)$$

$$p^{x}_{Max-Retransmit} = \left(p^{x}_{collide}\left(1 - (p^{x}_{channel-busy})^{u+1}\right)\right)^{v+1}$$

Where, for a node 'x', the probability of channel being busy $\left(p^{x}_{channel-busy}\right)$ and probability that a packet get collided $\left(p^{x}_{collide}\right)$ can be calculated as elaborated by [30].

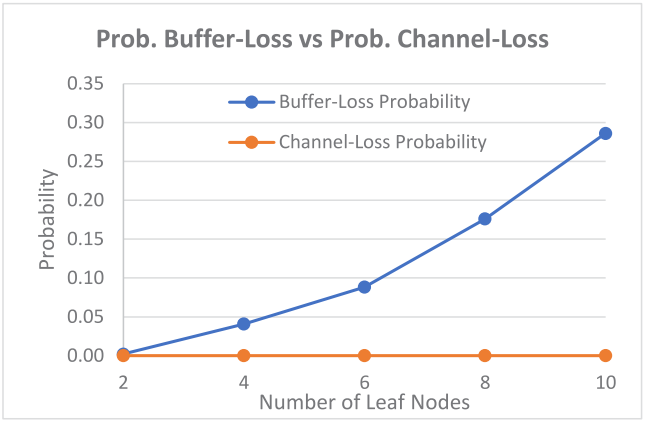


Fig. 12. Probability of buffer-loss vs probability of channel-loss (at Buffer=10 & Load=32).

7. Results & discussions

We consider, *Maximum number of backoff = Maximum number of re-transmission of a packet* = 3, and *Probability of channel is busy = Probability a packet gets collided* = 10%.

Table 3 shows the parametric values used in graphical results. Case 1 has different *number of leaf node*, while *buffer size* and *number of packets arriving per second (load)* is fixed. In case 2, different *buffer size* taken into consideration while *number of leaf nodes* and *number of*

Table 3
Parameter table.

Parameter	Channel capacity = 250 kbps			Channel capacity = 120 kbps		
	Case-1	Case-2	Case-3	Case-1	Case-2	Case-3
Number of leaf Node	2,4,6,8,10	5	6	2,4,6,8,10	5	6
Buffer Size (in packets)	10	5,10,15,20	10	10	5,10,15,20	10
Avg. Number of Packet Arriving (per sec)	32	32	1,2,4,8,16,32,64	32	32	1,2,4,8,16,32,64

packets arriving per second is constant. And, in case 3, *number of leaf nodes* and *buffer size* remains unchanged, but offered load is different.

The graphical relation between channel-loss and buffer-loss probabilities exhibit in Fig. 12. It shows that the probability of buffer-loss rises rapidly when the number of leaf nodes increases while channel-loss probability remains almost constant. It states that the buffer-loss is a more significant cause than channel-loss, which can trigger congestion in the 6LoWPAN network (mentioned in Fig. 10). The average packet drops due to channel loss are far lower than packet dropped due to buffer loss. Thus, it certifies the statement that buffer-loss is a significant factor of congestion in 6LoWPANs. A similar tendency is followed in other cases also because the probability of channel loss is independent of buffer size and offered load.

When we observe results in Figs. 13–18, we found a close relation between results obtained from M/M/1/K queuing theory and results of the analytical model. Fig. 13 display the pattern of packet dropping probability due to buffer overflow in all three cases. As shown in Fig. 13(a) when leaf nodes increase while keeping packet load and buffer size unchanged, the probability of packet dropping due to buffer-loss also increases. In Fig. 13(b) reveals that the buffer-loss probability slightly decreases when buffer size increases. This probability gets worse after a point when the packet arriving rate grows exponentially. In all three cases, the packet dropping probability worsens with a drop in channel capacity. The buffer-loss probability at the intermediate node (shown in Fig. 14) follows a similar trend as-it-is at the leaf node. Case 1, 2, 3 reflect in Fig. 14(a), 14(b), 14(c).

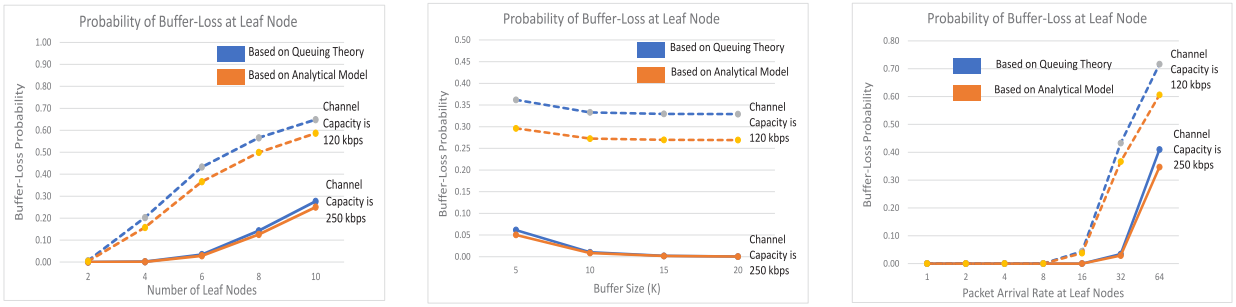
Figs. 15, 16 shows the average number of packets lost per second due to insufficient buffer space at leaf and intermediate node. Fig. 15(a) representing Case-1 depicts that when the number of leaf nodes increases, the number of dropped packets increases with it because when the number of leaf nodes increases, the part of channel capacity shared among leaf nodes reduces. We have seen that when channel capacity reduces, the probability of buffer-loss increases (as observed in Fig. 14(a)). The impact of increasing buffer size is reflected in Fig. 15(b), which states that fewer packets are being dropped if buffer size grows. Packet dropping rate escalates when there is an increment in the average packet arrival rate (offered load), as observed in Fig. 15(c). Fig. 16(a) displays case-1 where the average number of packets lost per sec is higher when channel capacity is also high (250 kbps). When channel capacity is 120 kbps, more packets are being dropped at the leaf node itself. Therefore, fewer packets are forwarded to the intermediate node. While at channel capacity 250 kbps, more packets are being sent to the intermediate node. Thus, more packets are lost at the intermediate node when the leaf increases. While comparing Figs. 15(b) and 16(b), we notice that at the intermediate node, more packet is lost even when buffer size increases. It is because when the buffer expands, the probability of buffer loss decreases at the leaf. Thus more packets are being forwarded towards the intermediate node. Fig. 16(c) depicts case-3 at intermediate node. Due to the same reason (mentioned above), The lesser number of packets are lost at 120 kbps channel capacity compared to the 250 kbps channel capacity. At 120 kbps channel capacity, more packets are dropped at the leaf node due to increase buffer-loss probability.

For topology displayed in Fig. 10(a), when there is no intermediate node present in the topology, the leaf nodes directly send data packets to the local sink device. Fig. 17 represents the average number of packets received by the local sink in this topology. A drop in received packets is noticed in Fig. 17(a) when the leaf node surges. It happens because more number packets are dropped at leaf when the number of leaf increases (as shown in Fig. 15(a)). Fig. 17(b) shows that with increased buffer size, more packets are received at the local sink from leaf nodes. It is because a better number of packets are received at a higher channel capacity. However, it drops when the packet arrival rate keeps on increasing, as observed in Fig. 17(c). For the layout shown in Fig. 10(b), the average number of packets received at the local sink is exhibited in Fig. 18. It describes that number of packet received at local sink decrease when leaf node expands (depicted in Fig. 18(a)) because the chance of dropping a packet at leaf and intermediate node increases. Case-2 scenario for received packet represented in Fig. 18(b). Fig. 18(c) depicts that the average number of the received packet at the local sink increases when the offered load rises. However, it instantly dropped after a certain limit of packet arrival rate (i.e., 16 packets/sec for channel capacity 120 kbps and 32 packets/sec for channel capacity 250 kbps).

Expected delay (in seconds) for a packet at leaf node is illustrated in Fig. 19. It is observed that the mean delay for a packet increases with more number of leaf nodes, shown in Fig. 19(a). The reason is that when the number of leaf nodes increases, a packet will spend more time in the buffer before it get serviced. The delay gets worse if the channel capacity decreases. The same trend is followed in case-2 & case-3 displayed in Fig. 19(b), 19(c) respectively. Fig. 20 presents all three cases of mean delay (in seconds) spent by a packet at the intermediate node. It is noticed that the average delay at the intermediate node is far greater than the delay at the leaf node. It is due to that traffic intensity (ρ) is much higher at the intermediate node than the leaf node. In most instances, the ratio of arriving(λ) & departing(μ) packet rate is greater than 1, while it is expected to be less than 1. Due to this reason, a packet will spend more time at the intermediate node's buffer. This delay drastically increases when channel capacity gets down. Fig. 20(a), 20(b), 20(c) exhibits the three cases respectively.

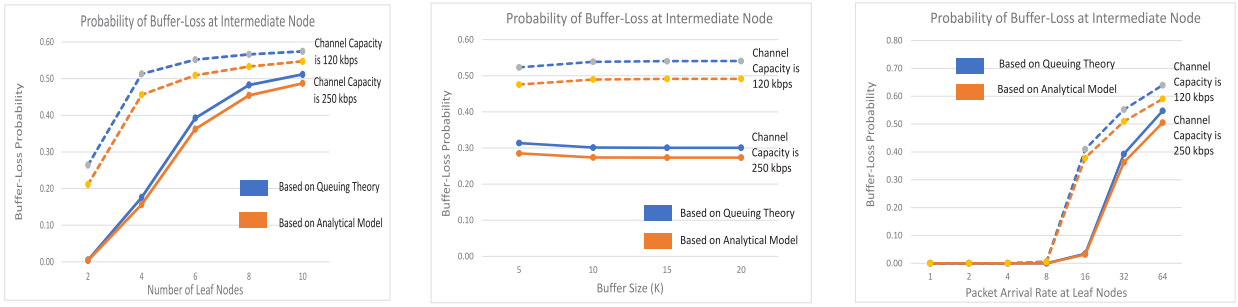
In Figs. 21–24, we performed comparative performance analysis in terms of buffer loss probability and packet loss (per sec) between our proposed method and two relevant existing schemes introduced in Ref. [5,6]. The analysis is done for all three cases concerning 250 kbps and 120 kbps channel capacity. Fig. 21 depicts the comparison of buffer loss probabilities of all the schemes at 250 kbps channel capacity in different cases. As observed, the buffer loss probability is almost equivalent in all the schemes. However, this paper's proposed scheme outperforms the other two when an increased number of leaf nodes are available, a large buffer is present and a higher packet arrival rate. As shown in Fig. 22, the performance of our proposed method significantly improved with limited buffer size and lesser channel capacity as the proposed scheme is aware of the resource-restricted environment. At 120 kbps channel capacity, our method accomplishes better results even when there are many leaf nodes in the network and a high packet arrival rate.

The total number of packets lost per second in the resource-restricted IoHT network (exhibited in Fig. 23, 24) follows equivalent correlation with its buffer loss probabilities. The proposed scheme drops the lesser number of packets in comparison to other schemes in all three cases (when channel capacity is 250 kbps). As illustrated in Fig. 24, the packet loss of our proposed method is significantly lower than the other two mechanisms with the smallest buffer size and lesser channel capacity (i.e., 120 kbps). The comparative results show that the proposed model estimating buffer loss in resource-restricted IoHt network substantially outperforms the methods suggested by [5,6] in terms of packet loss at node's buffer.



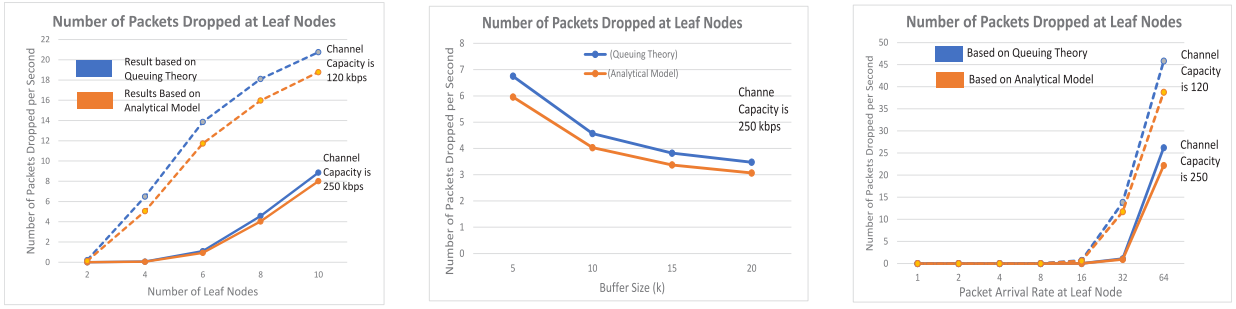
(a) Case 1:at buffer=10 & Load=32 (b) Case 2:at Leafs=5 & Load=32 (c) Case 3:at Leafs=6 & Buffer=10

Fig. 13. Packet loss probability (per second) due to buffer overflow at the leaf node.



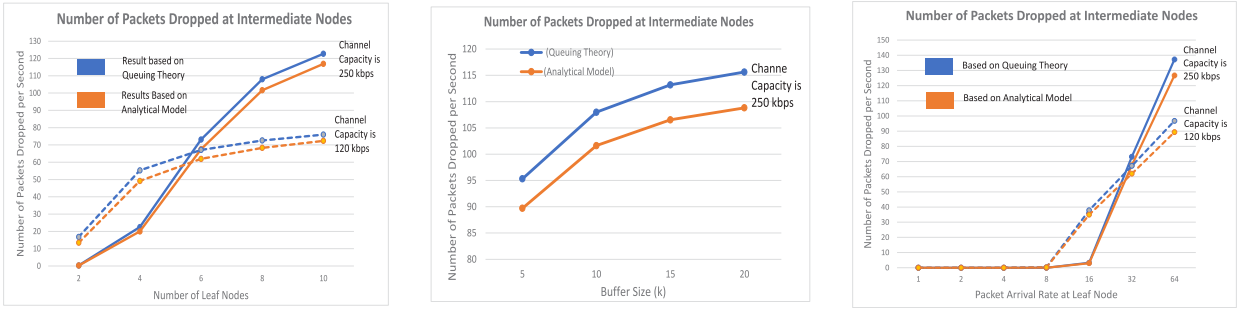
(a) Case1: at buffer=10 & Load=32 (b) Case 2: at Leafs=5 & Load=32 (c) Case 3: at Leafs=6 & Buffer=10

Fig. 14. Probability of packet-loss (per second) due to buffer overflow at the intermediate node.



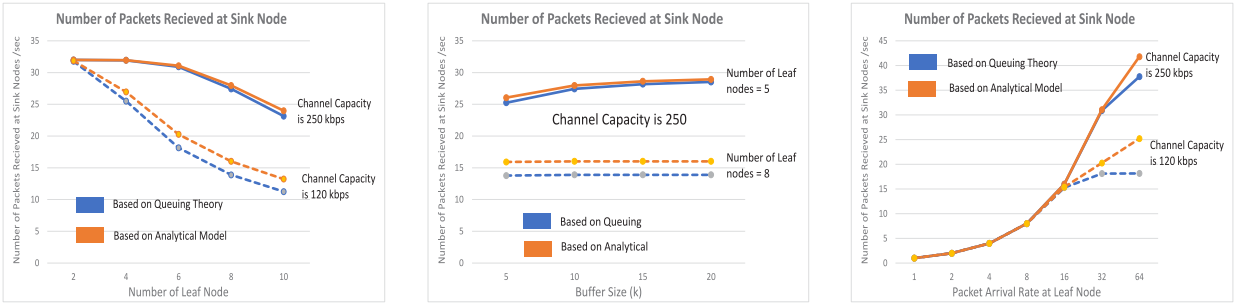
(a) Case 1: at buffer=10 & Load=32 (b) Case 2:at Leafs=8 & Load=32 (c) Case 3:at Leafs=6 & Buffer=10

Fig. 15. Average number of packet dropped (per second) at the leaf node.



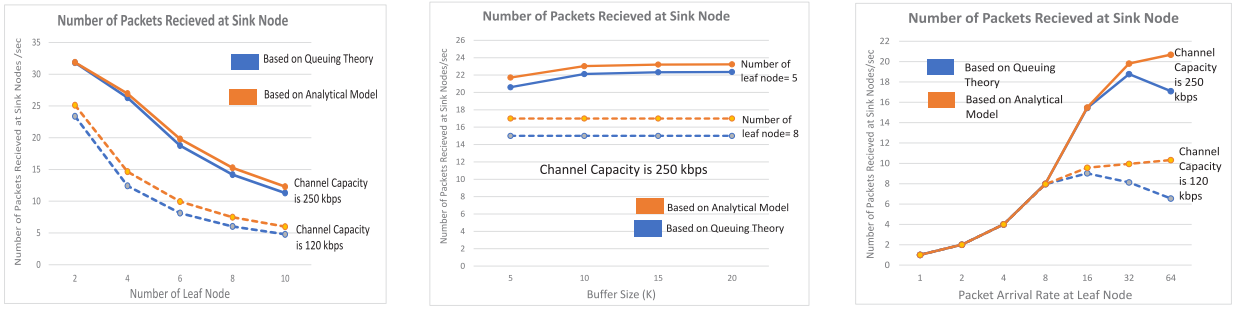
(a) Case 1:at buffer=10 & Load=32 (b) Case 2:at Leafs=8 & Load=32 (c) Case 3:at Leafs=6 & Buffer=10

Fig. 16. Average number of packet dropped (per second) at the intermediate node.



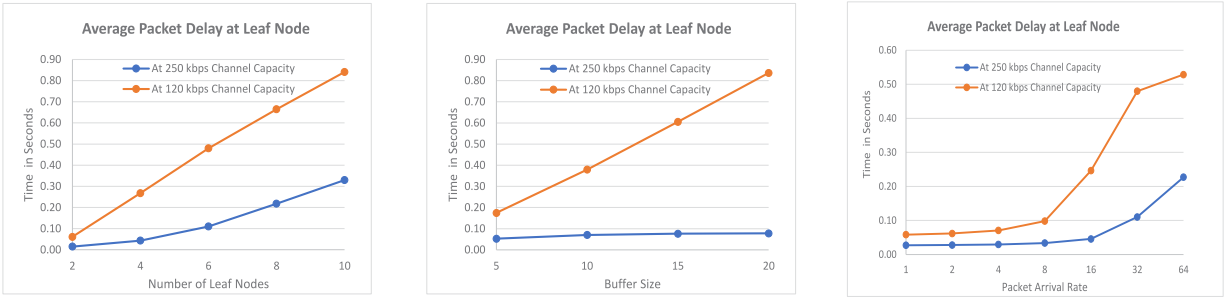
(a) Case 1:at buffer=10 & Load=32 (b) Case 2:at Leafs=5,8 & Load=32 (c) Case 3:at Leafs=6 & Buffer=10

Fig. 17. Average number of packet received (per second) at the local sink node (when no intermediate node involved).



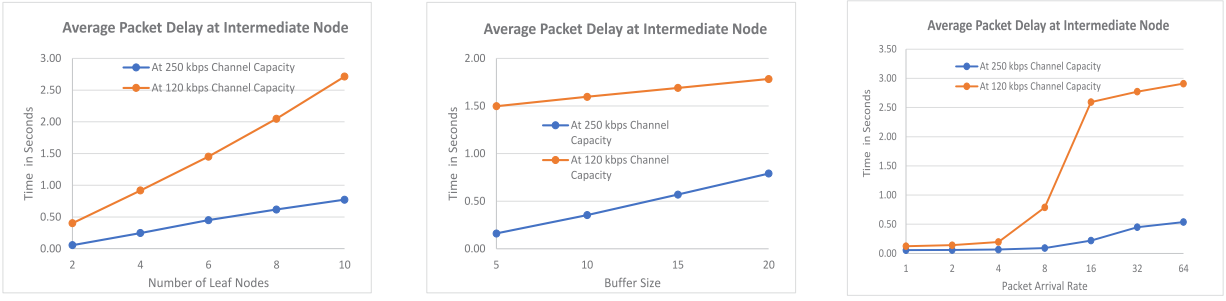
(a) Case 1:at buffer=10 & Load=32 (b) Case 2:at Leafs=5,8 & Load=32 (c) Case 3:at Leafs=6 & Buffer=10

Fig. 18. Average number of packet received (per second) at the local sink node (when a intermediate node is present).



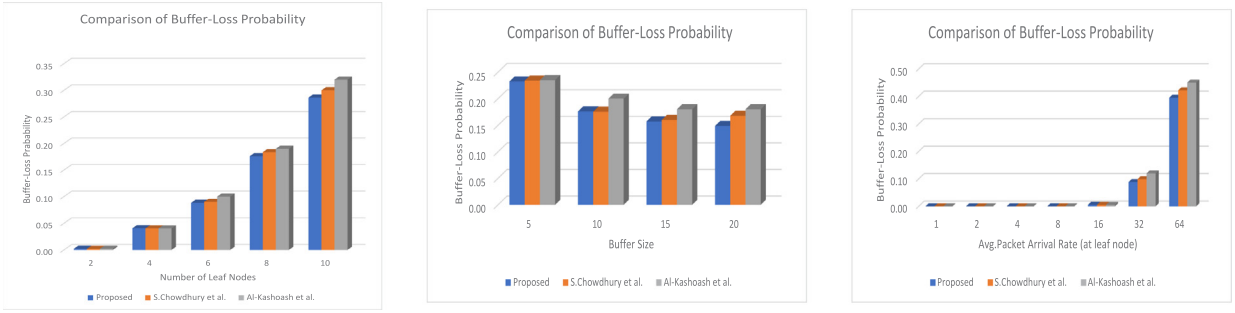
(a) Case 1:at buffer=10 & Load=32 (b) Case 2:at Leafs=5 & Load=32 (c) Case 3:at Leafs=6 & Buffer=10

Fig. 19. Expected (mean) packet delay (in second) at the leaf node.



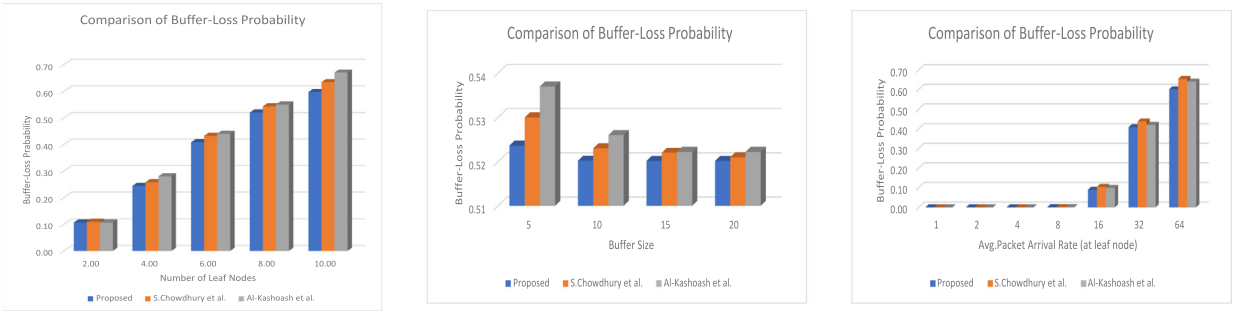
(a) Case 1:at buffer=10 & Load=32 (b) Case 2:at Leafs=5 & Load=32 (c) Case 3:at Leafs=6 & Buffer=10

Fig. 20. Expected (mean) packet delay (in seconds) at the intermediate node.



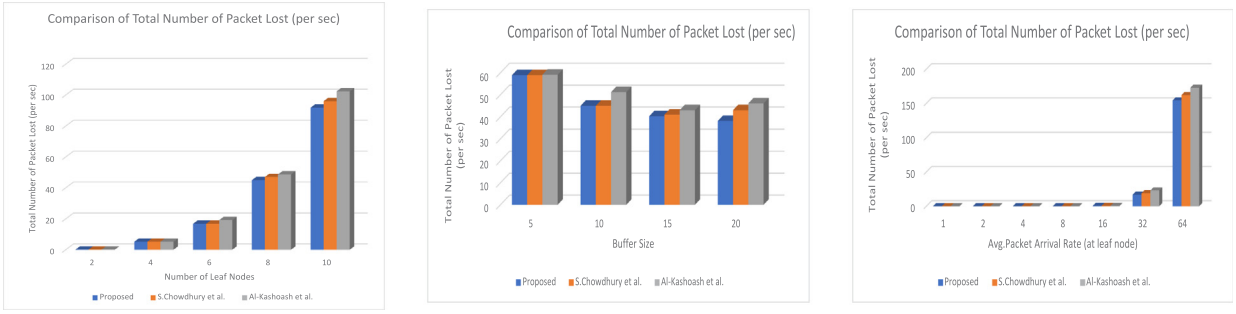
(a) Case 1:at buffer=10 & Load=32 (b) Case 2:at Leafs=5 & Load=32 (c) Case 3:at Leafs=6 & Buffer=10

Fig. 21. Comparison of Buffer-loss Probabilities (at 250 kbps channel capacity).



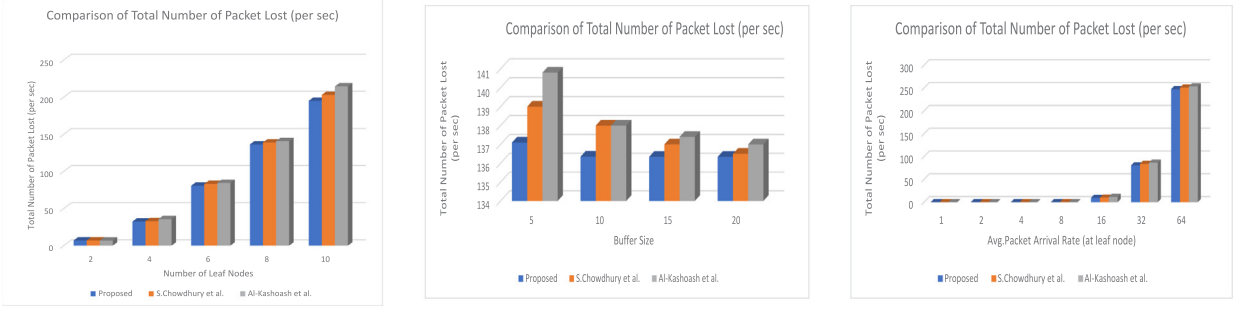
(a) Case 1:at buffer=10 & Load=32 (b) Case 2:at Leafs=5 & Load=32 (c) Case 3:at Leafs=6 & Buffer=10

Fig. 22. Comparison of buffer-loss probabilities (at 120 kbps channel capacity).



(a) Case 1:at buffer=10 & Load=32 (b) Case 2:at Leafs=5 & Load=32 (c) Case 3:at Leafs=6 & Buffer=10

Fig. 23. Comparison of total number of packet lost (per second) due to Buffer-Overflow (at 250 kbps channel capacity).



(a) Case 1:at buffer=10 & Load=32 (b) Case 2:at Leafs=5 & Load=32 (c) Case 3:at Leafs=6 & Buffer=10

Fig. 24. Comparison of total number of packet lost (per sec) due to Buffer-Overflow (at 120 kbps channel capacity).

8. Conclusion

This paper proposed an estimating model to address congestion by calculating the expected number of packets lost due to buffer overflow in 6LoWPAN-based, resource-restricted IoHT. An average number of packets successfully reaching the local sink node is also estimated in this work. After reviewing existing congestion control schemes for 6LoWPAN networks, the IoHT architectures for remote health monitoring are identified for different application purposes. Topological layouts for these architectures are highlighted along with their networking aspects and further used for modeling buffer loss.

To estimate packet loss due to the node's buffer insufficiency, we proposed a model based on the M/M/1/K queue concept for resource-constraint IoHT. After establishing a relation between empty and filled buffer probabilities, we derived packet drop probabilities for leaf and intermediate nodes. Furthermore, an analytical model is used to validate the estimation of the lost packets, their loss probabilities, average number of packets received at the local sink and average packet delay. It is observed that the buffer-loss is a significant factor of packet loss (at node's buffer) because the buffer-loss probability rises drastically while channel-loss probability remains approximately constant. Therefore, it is essential to estimate buffer loss to address congestion in 6LoWPAN-based IoHT networks. Hence, we considered three different cases of leaf nodes, buffer size and packet arriving rate, at 120 kbps and 250 kbps (i.e., maximum and expected) channel capacity to observe its impact on packet loss. The computed results exhibited a closed correlation and were included with theoretical validation. Furthermore, as observed in comparative results, the proposed model substantially outperformed two existing methods when applied in a resource-restricted, 6LoWPAN-based IoHT network. Based on these results, we will try to design and develop a congestion control scheme for resource-restricted IoHT networks in the future.

CRediT authorship contribution statement

Himanshu Verma: Conceptualization, Formal analysis, Investigation, Methodology, Resources, Writing – original draft, Writing – review & editing, Visualization, Validation. **Naveen Chauhan:** Supervision, Conceptualization, Formal analysis, Investigation, Visualization, Validation. **Narottam Chand:** Supervision, Investigation, Visualization, Validation. **Lalit Kumar Awasthi:** Supervision, Visualization, Validation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] H.A. Al-Kashoash, A.H. Kemp, Comparison of 6LoWPAN and LPWAN for the Internet of Things, Aust. J. Electr. Electron. Eng. 13 (4) (2016) 268–274.

[2] M. Raza, N. Aslam, H. Le-Minh, S. Hussain, Y. Cao, N.M. Khan, A critical analysis of research potential, challenges, and future directives in industrial wireless sensor networks, IEEE Commun. Surv. Tutor. 20 (1) (2018) 39–95, http://dx.doi.org/10.1109/COMST.2017.2759725.

[3] F. Gebali, Analysis of Computer Networks, second ed., Springer Publishing Company, Incorporated, 2015.

[4] A. Strielkina, D. Uzun, V. Kharchenko, Modelling of healthcare IoT using the queueing theory, in: 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 2, 2017, pp. 849–852. http://dx.doi.org/10.1109/IDAACS.2017.8095207.

[5] H.A. Al-Kashoash, F. Hassen, H. Kharrufa, A.H. Kemp, Analytical modelling of congestion for 6LoWPAN networks, ICT Express 4 (4) (2018) 209–215, http://dx.doi.org/10.1016/j.icte.2017.11.001.

[6] S. Chowdhury, A. Benslimane, C. Giri, Noncooperative gaming for energy-efficient congestion control in 6LoWPAN, IEEE Internet Things J. 7 (6) (2020) 4777–4788, http://dx.doi.org/10.1109/JIOT.2020.2969272.

[7] V. Michopoulos, L. Guan, G. Oikonomou, I. Phillips, DCCC6: Duty cycle-aware congestion control for 6LoWPAN networks, in: 2012 IEEE International Conference on Pervasive Computing and Communications Workshops, IEEE, 2012, pp. 278–283.

[8] J.-P. Sheu, W.-K. Hu, Hybrid congestion control protocol in wireless sensor networks, in: VTC Spring 2008-IEEE Vehicular Technology Conference, IEEE, 2008, pp. 213–217.

[9] S. Chen, Z. Zhang, Localized algorithm for aggregate fairness in wireless sensor networks, in: Proceedings of the 12th Annual International Conference on Mobile Computing and Networking, 2006, pp. 274–285.

[10] S. Rangwala, R. Gummadi, R. Govindan, K. Psounis, Interference-aware fair rate control in wireless sensor networks, ACM SIGCOMM Comput. Commun. Rev. 36 (4) (2006) 63–74.

[11] A.P. Castellani, M. Rossi, M. Zorzi, Back pressure congestion control for CoAP/6LoWPAN networks, Ad Hoc Netw. 18 (2014) 71–84.

[12] H.A. Al-Kashoash, M. Hafeez, A.H. Kemp, Congestion control for 6LoWPAN networks: A game theoretic framework, IEEE Internet Things J. 4 (3) (2017) 760–771.

[13] V. Michopoulos, L. Guan, G. Oikonomou, I. Phillips, DCCC6: Duty Cycle-aware congestion control for 6LoWPAN networks, in: 2012 IEEE International Conference on Pervasive Computing and Communications Workshops, 2012, pp. 278–283. http://dx.doi.org/10.1109/PerComW.2012.6197495.

[14] H. Hellaoui, M. Koudil, Bird flocking congestion control for CoAP/RPL/6LoWPAN networks, in: Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems, 2015, pp. 25–30.

[15] H.-S. Kim, J. Paek, S. Bahk, QU-RPL: Queue utilization based RPL for load balancing in large scale industrial applications, in: 2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), IEEE, 2015, pp. 265–273.

[16] H.-S. Kim, H. Kim, J. Paek, S. Bahk, Load balancing under heavy traffic in RPL routing protocol for low power and lossy networks, IEEE Trans. Mob. Comput. 16 (4) (2016) 964–979.

[17] J.-P. Sheu, C.-X. Hsu, C. Ma, A game theory based congestion control protocol for wireless personal area networks, in: 2015 IEEE 39th Annual Computer Software and Applications Conference, vol. 2, IEEE, 2015, pp. 659–664.

[18] C. Ma, J.-P. Sheu, C.-X. Hsu, A game theory based congestion control protocol for wireless personal area networks, J. Sens. (2016).

[19] W. Tang, X. Ma, J. Huang, J. Wei, Toward improved RPL: A congestion avoidance multipath routing protocol with time factor for wireless sensor networks, J. Sens. (2016).

[20] M.A. Lodhi, A. Rehman, M.M. Khan, F.B. Hussain, Multiple path RPL for low power lossy networks, in: 2015 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob), IEEE, 2015, pp. 279–284.

[21] M. Ha, K. Kwon, D. Kim, P.-Y. Kong, Dynamic and distributed load balancing scheme in multi-gateway based 6LoWPAN, in: 2014 IEEE International Conference on Internet of Things (IThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), IEEE, 2014, pp. 87–94.

[22] X. Liu, J. Guo, G. Bhatti, P. Orlik, K. Parsons, Load balanced routing for low power and lossy networks, in: 2013 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, 2013, pp. 2238–2243.

[23] W. Tang, Z. Wei, Z. Zhang, B. Zhang, Analysis and optimization strategy of multipath RPL based on the COOJA simulator, Int. J. Comput. Sci. Issues (IJCSI) 11 (5) (2014) 27.

[24] H.A. Al-Kashoash, Y. Al-Nidawi, A.H. Kemp, Congestion-aware RPL for 6L0WPAN networks, in: 2016 Wireless Telecommunications Symposium (WTS), IEEE, 2016, pp. 1–6.

[25] H.A. Al-Kashoash, H.M. Amer, L. Mihaylova, A.H. Kemp, Optimization-based hybrid congestion alleviation for 6LoWPAN networks, IEEE Internet Things J. 4 (6) (2017) 2070–2081.

[26] H. Al-Kashoash, Optimization-based hybrid congestion alleviation, in: Congestion Control for 6LoWPAN Wireless Sensor Networks: Toward the Internet of Things, Springer, 2020, pp. 135–156.

[27] A. Ghaffari, Congestion control mechanisms in wireless sensor networks: A survey, J. Netw. Comput. Appl. 52 (2015) 101–115, http://dx.doi.org/10.1016/j.jnca.2015.03.002.

[28] J.D. Little, S.C. Graves, Little's Law, Springer US, Boston, MA, 2008, pp. 81–100, http://dx.doi.org/10.1007/978-0-387-73699-0_5.

[29] T. Winter, P. Thubert, A. Brandt, J.W. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.-P. Vasseur, R.K. Alexander, et al., RPL: IPv6 routing protocol for low-power and lossy networks, Rfc 6550 (2012) 1–157.

[30] P. Di Marco, P. Park, C. Fischione, K.H. Johansson, Analytical modeling of multi-hop IEEE 802.15. 4 networks, IEEE Trans. Veh. Technol. 61 (7) (2012) 3191–3208.

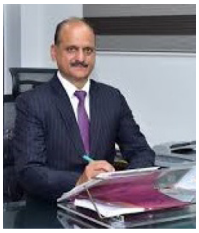
[31] Approved IEEE draft amendment to IEEE standard for information technology-telecommunications and information exchange between systems-Part 15.4:Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANS): Amendment to Add Alternate Phy (Amendment of IEEE Std 802.15.4), IEEE Approved Std P802.15.4a/D7, Jan 2007.

Himanshu Verma is currently pursuing a Ph.D. degree in Computer Science and Engineering from National Institute of Technology Hamirpur, HP, India. His primary research interests are the Internet of Things, IoT-Healthcare, Wearable-WSN and Adhoc Network. He published a few research papers in the relevant research areas. Previously, He served as an Assistant Professor and was a mentor of the Digital Logic Design course in the AKTU MOOCs program. He was also a reviewer in some of IEEE conferences.

Naveen Chauhan is an Associate Professor at Department of Computer Science and Engineering, NIT Hamirpur. He received his Ph.D. (Computer Science & Engineering) from NIT Hamirpur in 2012. His research interest includes Mobile Wireless Networks with particular emphasis on the Internet of Things and its Security Aspects. He has made excellent research contributions and published many research articles in SCI and Scopus indexed journals. In addition, he is a reviewer in various national and international reputed journals and guides many Ph.D. students in these areas.

Narottam Chand Late Dr. Narottam Chand was an Associate Professor at Department of Computer Science and Engineering, NIT Hamirpur. He received his Ph.D. degree from IIT Roorkee in Computer Science and Engineering. Previously, he received M.Tech degree from IIT Delhi and B.Tech degrees from NIT Hamirpur in Computer Science and Engineering. His research areas of interest were mobile computing, mobile ad hoc networks, wireless sensor networks and IoT. He had published more than 150 research papers in International/National journals & conferences, guided many Ph.D. scholars in these areas. He was a fellow of the Institution of Engineers (India), senior member of IEEE and ACM, ISTE, CSI, International Association of Engineers and Internet Society.

He was a leading researcher and finest human being who lost his life due to the Covid-19 pandemic in May'2021. This research paper is a tribute to Late Dr. Narottam Chand Sir and his excellent contributions to this work.



Lalit Kumar Awasthi received his Ph.D. degree from the Indian Institute of Technology Roorkee in Computer Science and Engineering. He is working as Director, Dr. B. R. Ambedkar National Institute of Technology Jalandhar, India and National Institute of Technology Hamirpur, HP, India. Before this, he was the Director/Principal of Government Engineering College, Pragati Nagar, Shimla. He has also served as Professor and Head of Department of Computer Science and Engineering, National Institute of Technology Hamirpur. His research interests are distributed fault-tolerant computing, mobile computing, wireless sensor networks, mobile ad hoc networks. He has published more than 150 research papers in various National/International journals and conferences and guided many Ph.D. scholars in these areas.