

Heuristic – Driven Disjoint Alternate Path Switching – Based Fault Resilient Multi-Constraints Routing Protocol for SDN-mIoT

Suprith Kumar K. S.*

Dept of ECE, B.M.SCE

E-mail: Suprithkumarks.ece@bmsce.ac.in

ORCID iD: <https://orcid.org/0009-0001-9590-6950>

*Corresponding Author

Eesha D.

Dept of ECE, B.M.SCE

E-mail: eesha.ece@bmsce.ac.in

ORCID iD: <https://orcid.org/0000-0002-5843-7518>

Pooja A. P.

Dept of ECE, B.M.SCE

E-mail: poojaap.ece@bmsce.ac.in

ORCID iD: <https://orcid.org/0009-0005-6191-5452>

Monika Sharma D.

Dept of ECE, B.M.SCE

E-mail: monikas.ece@bmsce.ac.in

ORCID iD: <https://orcid.org/0000-0002-6967-667X>

Received: 09 February, 2024; Revised: 10 May, 2024; Accepted: 12 July, 2024; Published: 08 October, 2024

Abstract: The last few years have witnessed exponential rise in internet-of-things (IoT) systems for communication; yet, ensuring quality-of-service (QoS) and transmission reliability over mobile topology has remained challenge. Despite the fact that the use of software defined networks (SDN) have enabled IoTs to achieve resource efficiency and reliability; it doesn't guarantee optimality of the solution over the network with high dynamism and non-linearity. Moreover, the major at hand SDN-IoT protocols have applied standalone node parameters to perform routing and allied transmission decision that confine its robustness over dynamic network topologies. Interestingly, none of the state-of-art SDN-IoT protocols could address the problem of iterative link-outage and corresponding network discovery cost. Furthermore, even multi-path selection strategies too failed in addressing the problem of joined shortest path selection and allied iterative link-outage due to the common node failure. Considering it as motivation, in this paper a novel and robust Heuristic-Driven Disjoint Alternate Path Switching -based Fault-Resilient Multi-Constraints Routing Protocol for SDN-mIoT system (HDAP-SDNIoT) is proposed. HDAP-SDNIoT exploits multiple dynamic parameters like medium access control information, flooding and congestion probability information. HDAP-SDNIoT exploits aforesaid node parameters to perform node profiling that serves multi-constraints best forwarding path selection. The proposed model retrieves multiple best alternating paths which are fed as input to the Adaptive Genetic Algorithm (AGA) that retains three disjoint best forwarding paths. HDAP-SDNIoT protocol at first avoids any malicious node(s) to become forwarding node, while it provides auto-switching capability to the forwarding node to select a disjoint forwarding alternate path in case of any link-outage in current forwarding path. _Simulation results confirm robustness of the proposed model in terms of high packet delivery rate of 96.5%, low packet loss rate 3.5% and low delay of 211 ms that affirms its suitability towards real-time SDN-mIoT applications.

Index Terms: Software Defined Network, Internet-of-Things, Disjoint Alternate Forwarding Path, Heuristic Optimization, Quality-of-Service.

1. Introduction

The last few years have witnessed exponential rise in wireless transmission technologies serving an array of industries for reliable and decentralized communication purposes. Almost major industries and applications encompassing telecommunication, manufacturing, business communication, healthcare, civic surveillance and administration, etc. wireless communication has become an integral part [1-3]. To cope up with up-surging demands and applications including smart home, smart factory, smart city, e-healthcare, etc. wireless communication technologies have evolved significantly. Internet-of-things (IoT) technology is one of those innovations which targets on contributing low-cost, decentralized communication and control infrastructures for aforesaid applications [3-7]. Architecturally, IoT embodies low-power lossy network (LLNs), sensor technologies and software analytics to collect real-world data, analyses and disseminate data or instructions for varied real-time decisions. In the last few years, IoT communication systems have applied mobility features to serve an array of communication and/or transmission services; however, ensuring reliability over exceedingly high dynamism, topological changes, non-linear traffic patterns and more importantly vulnerable channel condition remains challenge [8]. Though, a few technological innovations such as software defined network (SDN) have played decisive to improve IoT reliability and scalability to cope up aforesaid demands [8]. In the last few years, SDN-based IoT, often called SDN-IoT technology has gained widespread attention due to resource efficient, reliable and quality-of-service (QoS) oriented communication abilities [8, 9]. The different applications including industrial monitoring and control, defense communication, telemedicine, Smart-City, Human Machine Interfaces (HMI), civic surveillance etc. can be benefitted by SDN-IoT technology, provided it guarantees QoS constructs over the dynamic, uncertain and non-linear network conditions [9]. Despite the fact that SDN can help achieving resource efficacy and security over static networks [9,34]; yet, node mobility and allied network's dynamism in mobile-IoT can't be ruled out that consequently can impact overall reliability of the network or system [10]. Ensuring reliability of SDN-IoT over large distributed and dynamic nodes remains challenge and therefore requires addressing network dynamics, security while ensuring time-efficient transmission. Noticeably, as stated earlier in mobility-based IoT the nodes might enter and exit network's radio abruptly and hence can force it to undergo frequent link-outage, retransmission and hence increased delay. The link-outage and resulting data losses can not only impact throughput and QoS but can impose security threat where an attacker node can intrude inside and can repeatedly drop data to impact overall reliability and QoS constructs [34]. It requires SDN-IoT network to have the ability to ensure reliable routing under the different operating characteristics. It can be considered as the key driving force behind this research [10-12].

In sync with real-time application's demand, it is inevitable to ensure successful packet delivery even under varying network conditions due to the node failure or switch failure, node attacks, link failure, link-delay, congestion etc. [9-12]. To address aforesaid challenges, majority of the existing approaches have either focused on improving routing protocols or to detect malicious node detection [13]. However, in reality the malicious node detection models in IoT networks have either applied temporal or sequential network patterns to detect anomaly or have used static threshold conditions to detect and isolate misbehaving nodes. None of these methods guarantees generalizability over dynamic network conditions which is quite frequent and probable in mobile-IoT (i.e., SDN-mIoT) networks [6,11,12]. A number of state-of-arts have applied static threshold conditions such as packet loss rate [15-17] delay as the parameter to detect lossy paths or malicious nodes for further alternate routing path discovery. However, executing alternate routing path discovery (ARPD) iteratively over SDN-mIoT can be exhaustive and can impose significant latency [16,17]. This as a result can limit efficacy of the SDN-mIoT network to serve communication purposes. In the past, a few approaches have applied the concept of fault-resilient routing and multi-path transmission in IoT to serve QoS communication. However, the likelihood of increased signaling and transmission costs can't be ruled out, especially over mobile-IoT (i.e., mIoT). The major existing protocols have suggested to use reactive best forwarding path selection strategy to enable data transmission in case of link-outage or node death; yet, the latency imposed over node discovery and best forwarding path selection can be large enough to impact QoS or network performance [15-18]. Though, a few proactive routing methods are proposed in the past which apply delay and (shortest path) distance information to perform alternate forwarding path selection in mobile networks; however, merely applying these parameters under dynamic network conditions can't guarantee optimality of the alternate path as an inappropriate path selection can cause iterative link-outage and hence can impact overall performance [16-18]. This is because a node within the radio range and fulfilling shortest path criteria doesn't guarantee reliability of the transmission or forwarding under dynamic topology due to its unpredictable trajectory, load or congestion and packet velocity characteristics. It infers that the SDN-mIoT networks require proactive routing strategy with the multiple dynamic parameter-based best forwarding path selection and proactive alternate path selection. Additionally, it requires maintaining no common-nodes in multiple (alternate) path selection as the failure of a common node might directly impact the efficiency of both path and hence their reliability towards QoS communication. In other words, a network with an optimal multi-constraint driven best forwarding path with disjoint link criteria can achieve QoS communication. Here, the use of multiple constraints (say, multiple network parameters) can help improving routing efficacy and fault-resilience, while disjoint alternate forwarding path (DAFP) can provide proactive alternate forwarding path to meet QoS constraints or delay criteria. This as a result can help achieving QoS performance by SDN-mIoT to serve major communication demands.

This paper proposed a novel and robust Disjoint Alternate Forwarding Path assisted Fault-Resilient Multi-Constraints Routing Protocol (HDAP-SDNIoT) for SDN-mIoT networks. As the name indicates, the proposed model at first exploits multiple network parameters including residual energy, congestion information, medium access control (MAC) information and data flooding information to perform routing decision. Considering dynamic network conditions (in mIoT network), we define at hand routing problem and allied alternate forwarding path selection as NP-hard non-convexity problem, and therefore apply adaptive genetic algorithm (AGA) heuristic to learn over the dynamic parameters to perform fault-resilient best forwarding path selection and disjoint alternate forwarding path selection. The AGA-based alternate disjoint path selection method ensures that it retains minimum delay and source-sink distance. Thus, HDAP-SDNIoT protocol intends to achieve time-efficiency as well as reliability of wireless transmission to meet QoS constructs in SDN-mIoT network. Unlike traditional SDN-based IoT protocols [24,2527], where the authors have applied either data plane or control plane information to perform forwarding path selection, we exploited dynamic parameters from both layers to strengthen fault-resilience under varied operating conditions. More specifically, HDAP-SDNIoT protocol applied congestion information, MAC flooding information, throughput to perform node profiling. This information is later applied by the heuristic model to identify a set of disjoint alternate paths for reliable transmission. Here, the node profiling helps detecting and isolating malicious nodes from participating forwarding path(s), and therefore serves as security measure as well. On the other hand, the proposed HDAP-SDNIoT protocol ensures reliability of the transmission without undergoing iterative node discovery and forwarding path selection costs (signaling overheads, energy and latency) during link-outage condition(s). The overall proposed routing protocol achieves secure, fault-resilient and QoS-centric communication environment for SDN-mIoT systems, which can be of paramount significance for varied networking purposes. The proposed HDAP-SDNIoT routing protocol is developed using network simulator tool and corresponding efficacy is examined in terms of the packet delivery rate (PDR), packet loss rate (PLR), delay over the different network conditions (i.e., payload and node velocity). The simulation results confirm robustness of the proposed routing model in terms of high PDR of 96.5%, low PLR (3.5%) and low delay (211 ms), signifying suitability for the different SDN-mIoT communication purposes.

The other sections of this paper are divided as follows. Section II discusses the related work, which is followed by problem formulation in Section III. Section IV presents research questions, while the overall proposed method and its implementation are given in Section V. The simulation results and allied inferences were discussed in Section VI. References used in this manuscript are given at the end of the manuscript.

2. Related Works

This section discusses some of the key literatures pertaining to the SDN-based IoT networks. To be noted, in majority of the state-of-arts SDN solutions were mere focused on network monitoring and resource control; however, very less efforts have been made towards reliable routing decisions in IoT [15]. Since, this research emphasizes on designing a robust routing protocol for SDN-based mIoT networks, a snippet of the recent efforts made in SDN-based IoT field are discussed in this section.

As stated earlier, the majority of the state-of-art SDN architectures were developed for resource monitoring and assignment as well as security tasks [15,34]. Recently, a few efforts such as [15-18] made effort on QoS-oriented routing decisions. More specifically, the authors performed traffic aware QoS routing in SDN-based IoT systems. They applied link-delay or path delay along with the packet loss information to perform best forwarding path selection. However, failed to address major challenges related to the mobility-based IoTs such as congestion probability, dynamic MAC behavior etc. Some other approaches such as [19-23] applied standalone or single QoS parameter (say, QoS metric) to perform best forwarding routing decision. Though, in [17], the authors made effort to amalgamate delay, packet loss and resource availability information together to perform QoS-oriented routing. Yet, while performing routing decision the authors [17,18] failed in addressing the mobility scenario and allied network outage due to topological and link-disruption. Despite their proposed multi-constraints routing decision, the avoidance of mobility and resulting (due to link outage) network discovery and retransmission cost can limit their efficacy to become real-time SDN-IoT solution. Though, the researches like [24] suggests that the use of UDP can make delay-sensitive transmission; yet, the likelihood of packet loss, especially over low rate UDP and when the data passes through the same shared network can't be ruled out. It confines their suitability towards real-time IoT communication. Moreover, IoT being resource constrained network can undergo exhaustive conditions due to these approaches or routing mechanism [17-24]. Though, the authors [17,18] proposed a simplified architecture based on SWAY for communication in heterogeneous nodes based IoT; yet, its reliability becomes questionable over real-time network conditions. It indicates the need of a more robust and QoS-oriented controller to have more effective routing decision and reliability centric transmission control. As multi-constraints routing (in SDN-IoT), the authors [17] applied tuple information along with the path delay and packet loss [27] to perform best forwarding decision. Here, customized weights were assigned to each parameter to perform best forwarding path selection. Undeniably, this approach can serve more reliable routing; yet, lacks the consideration of common-element or shared component-based path formation, where any possible common node failure can collapse entire network and its QoS performance. The authors [17,25,35] applied four different node parameters which was later processed for optimization, considering it as NP-hard convexity problem, so as to achieve QoS efficacy. Here, the heuristic model applied merely performed shortest path estimation to enable time-efficient routing. For the

shorted path routing, they applied Yen's K-shortest path method [26]. Yet, common-node problem and allied proactive disjoint routing path selection issues could not be addressed. In recent research, the author [17,18] compared the efficacy of the SWAY model with the other state-of-art approaches such as shortest path delay, minimum occupied rule capacity methods. The depth performance characterization revealed that the use of SWAY model can achieve superior performance over the state-of-arts (i.e., shortest delay path selection and minimum occupied rule capacity models). However, it doesn't apply any specific QoS parameter having direct impact on delay, jitter etc., which is common in varied contemporary IoT applications. Though, a few other approaches such as [27-32] have focused on energy optimization; yet, requires addressing aforesaid QoS metrics as well to cope up real-time IoT demands. Realizing the real-world fact that the performance of entire SDN-based IoT relies on the (SDN) controller and therefore in case of any controller failure entire network might collapse, developing a robust routing controller is inevitable [15]. Ensuring network reliability can be inevitable especially over the large autonomously and heterogenous IoT ecosystems. It can not only improve network QoS efficacy but reliability as well where it can identify the malicious entity within milliseconds and can enable routing without undergoing QoS losses. The authors [35] applied link-quality as parameter to perform routing decision in SDN-based IoT systems; yet, being driven by standalone network metric, it doesn't guarantee reliability of network and allied transmission, especially over the dynamic topologies. The above inferences indicate that the use of multi-constraints criteria [33,36,37] in conjunction with disjoint path formulation can improve routing as well as transmission reliability over heterogenous and mobile IoT networks. It can be considered as the key driving force(s) behind this research.

3. Problem Formulation

A number of existing approaches towards fault-tolerant SDN-IoT have mainly focused on risk identification and shortest path-based routing decision to avoid delay (primarily caused due to network discovery cost). However, such approaches could employ merely one or two parameters such as cost factor, energy, link quality etc. On the contrary in mobile topology based SDNs there can be exceedingly high dynamism and hence the classical reactive mechanisms can't yield expected performance. To cope up with aforesaid exceedingly high network dynamism, proactive decision ability is inevitable which can be accomplished well with multiple network parameter sensitive decision and routing concept. Moreover, an SDN controller can have better efficacy if it is armored with multiple-network parameters-based risk identification. It can not only help in identifying the malicious node but can also improve frequent link-outage which can make SDN-IoT more robust and reliable. Noticeably, a few literatures indicate that in the contemporary SDN-IoT, the malicious nodes or the intruder behaves or mimics the normal node and allied traffic to intrude inside the network and cause losses. In such case, unlike single parameter-based decisions the exploitation of the multiple behavioral parameters can be of vital significance towards risk identification and assessment. In this reference, in this work at first node profiling is performed for each node connected or deployed in the network. Here, the intent is to achieve dual purposes, first to identify the malicious node and isolate it from the forwarding path selection and second to perform optimal forwarding path selection by considering best nodes with suitable network or node characteristics (say, node features). Unlike state-of-arts [17,18,27,35,37], where authors applied only link-failure or other standalone node information to perform risk assessment, HDAP-SDNIoTprotocol considers multiple node parameters and allied QOS metrics including both statistical features (link-loss or link-availability, topology information) as well behavioral features (MAC information and flooding nature) for node-profiling and subsequent best forwarding path selection. It can improve overall transmission reliability. For the aforesaid multi-constraints criteria, the moving window averaging concept has been applied which helps identifying a set of paths for forwarding decision to meet QoS demands. The proposed multi-constraints forwarding path selection model is designed to serve proactive routing purpose, where it identifies multiple forwarding paths so that in case of link-outage a transmitter can use alternate path for delay-resilient transmission without undergoing iterative node and/or network discovery cost (i.e., delay, signaling overheads). Undeniably, the use of aforesaid multi-constraints criteria improves reliability of routing; however, the presence of common node in multi shortest path can't be ruled out. In the work of Malik et al. (2019), once identifying link-failure in SDN, authors employed Dijkstra shortest path algorithm for the forwarding path selection. However, such approaches can be delay-prone and even might undergo frequent link-outage due to Common Component Failure (CCF), often called shared component failure (SCF). Merely, employing Dijkstra-based or Euclidean distance-based shortest path for the forwarding (alternate) link formation can't provide fault-resilient communication as due to sudden change in topology such approaches might fail and thus giving rise to the frequent network failure. On the other hand, being under exceedingly high network dynamism such approaches might be limited to cope up with the SDN-IoT demands. Moreover, developing a disjoint forwarding path selection under dynamic network condition seems to be a NP-hard problem, which can be solved only by means of certain heuristic method or nature-driven optimization algorithms. This work proposed a heuristic-based disjoint alternate forwarding path (DAFP) which exploits the different node's parameters and identifies a set of disjoint forwarding path. More specifically, the genetic algorithm (GA) is applied to exploit aforesaid node parameters and initially selected forwarding paths to identify the disjoint forwarding paths. In this manner, the proposed model guarantees that no common node participates multiple paths and hence avoids iterative link failure due to the probable common node failure scenarios. In this manner, the proposed DAFP mechanism retains dual-disjoint forwarding paths. In case a node identifies any link failure, it switches to the alternate disjoint path,

without undergoing any network discovery phase and thus avoids delay and allied communication cost. This approach not only intends enables fault-resilient routing but also suppresses the likelihood of retransmission, delay and allied signaling and memory cost. The overall proposed SDN-mIoT routing protocol was designed and simulated by using Network Simulator-2 software, where it exhibited superior efficiency in terms of high packet delivery rate, low packet loss rate and low delay over the different network conditions (i.e., network density, velocity and payload conditions) affirming its robustness and suitability towards real-time SDN-mIoT communication. Though, the use of GA heuristic helped identifying disjoint shortest forwarding paths; however, at the cost of high (here, 200 generations) computations that in real-time can be time-consuming. In future, other lightweight heuristic can be designed and applied to improve time-efficiency and hence scalability of the protocol for larger network applications.

4. Research Questions

In sync with the overall research intends and allied methodological paradigms, in this work a few research questions are defined. These research questions are:

RQ1: Can the use of multi-constraints dynamic network parameters including MAC information, flooding, network dynamism and congestion probability driven node profiling be effective towards fault-resilient best forwarding routing protocol for SDN-mIoT systems?

RQ2: Can the use of heuristic driven disjoint alternate forwarding path selection (DAFP) method be effective towards QoS-centric routing in SDN-mIoT systems?

RQ3: Can the strategic amalgamation of aforesaid dynamic node profiling based proactive routing (RQ1) and heuristic-driven DAFP model (RQ2) be effective towards QoS oriented SDN-mIoT communication?

RQ4: Heuristic-Driven Disjoint Alternate Path Switching -based Fault-Resilient Multi-Constraints Routing Protocol be effective towards delay-resilient and reliable communication in SDN-mIoT communication?

Thus, the overall research intends to achieve answers for these key research questions that consequently can contribute a robust routing protocol for SDN-mIoT systems.

5. System Model

This section discusses the proposed Heuristic-Driven Disjoint Alternate Path Switching -based Fault-Resilient Multi-Constraints Routing Protocol for SDN-mIoT. As discussed earlier, the overall proposed method encompasses two phases. These are:

1. *Dynamic Node Profiling and Fault-resilient forwarding Node/Path selection, and Heuristic-based disjoint alternate path selection.*

The detailed discussion of the overall proposed routing protocol is given in the subsequent sections.

A. *Dynamic Node Profiling and Fault-resilient forwarding Node/Path selection*

In real-time IoT-based networks, especially the one designed with mobility can undergo network dynamism and hence frequent link-outage, data loss, retransmission and hence delay. Noticeably, aforesaid network issues can be because of the topological changes as well as intrusion. For instance, a mobile node going away from a transmitting node can undergo loss of link (i.e., when the inter-node distance d_{ij} is higher than the ratio range of the node (say, R_i) (i.e., $d_{ij} > R_i$). Though, it can also take place due to the physical damage of the node or due to the low (say, below threshold) residual energy (also called, node death). Noticeably, similar to the aforesaid network events, even an intruder node can cause delay (due to the denial or service attack), packet loss (due to eavesdropping or replay attack), redundant transmission (due to replay attack), etc. In fact, distinguishing aforesaid attack-driven losses and radio range outage (say, link failure) caused losses remains challenge for a network controller. In addition, almost major at hand network controllers make use of single network parameter such as delay, energy or packet loss to perform routing decision. In this case, a protocol applying packet delivery rate (PDR) as parameter classifies and annotate any node having PDR less than a threshold as malicious and avoids including it for further routing decision. However, this exclusion criteria don't affirm that the specific node was malicious as due to abrupt link-outage it could have undergone data loss and hence low PDR. In the same manner, ignoring a node for its low PDR and assuming that it can be due to the link-outage probability in mobile-IoT can be disastrous, as it doesn't guarantee that the node is not malicious or intruder. Such dilemma can make SDN-IoT vulnerable of network intrusion and hence can question reliability. To alleviate such issues, exploiting multiple node parameters can be of utmost significance, where the network controller can make use of the different node parameters including link-quality, PDR, MAC information, data flooding, residual energy etc. Noticeably, the use of these multiple parameters altogether can enable multi-constraints driven best forwarding node (and path) selection. This approach can not only improve routing reliability but can also isolate possible malicious node. Considering it as motivation, in the paper proactive network management strategy was considered in which the node parameters including MAC information, PDR, network dynamism, congestion probability. The proposed model estimates these parameters dynamically. More specifically, the aforesaid network parameters were

measured iteratively at the interval of 10 ms and based on these parameters' node profiling was done. Noticeably, the proposed multi-constraint node profiling signifies the estimation of the different node parameters dynamically and dynamically assign score to each node that puts foundation for the further forwarding path selection. Once obtaining the target node parameters, moving average method was applied to identify the set of suitable node parameters for further forwarding path selection. Before discussing the proposed multi-constraints best forward path selection method, a brief of the network parameters considered for node profiling and subsequent best forwarding path selection is given as follows:

— *IEEE 802.15.11/IEEE 802.15.4 MAC Information*

As stated earlier, a few state-of-art SDN driven network controllers have applied delay and network congestion parameters to perform routing and allied link-outage recovery scheduling. Noticeably, such routing strategies strongly hypothesizes that the varying and non-linear MAC information indicate the presence of malicious node, link-vulnerability and even network failure. Though, there can be varied such conditions where despite active status, a node might undergo dynamic or non-linear behavior signifying vulnerability in QoS-centric routing. In reference to the QoS-centric communication, in multi-constraint routing decision the assessment of MAC information can help segmenting vulnerable node so as to guarantee fault-resilient routing. In the proposed method, MAC information is obtained for each participating node. As MAC information, we measured key parameters including congestion probability and transmission efficacy (the probability quotient). Here, in real-world network the PDR and PLR performance is somewhere related to the congestion probability, where higher congestion on a node might result packet loss and hence retransmission probability and delay. Therefore, unlike using PDR performance as parameter, we use congestion probability as parameter to assess whether a node can ensure reliable transmission to achieve QoS performance. To achieve it, the proposed routing protocol (say, network controller) initiates or multicasts HELLO message and receives acknowledgement (ACK) as unicast signal. In this manner, it receives ACK message as unicast response from all neighboring nodes that subsequently enables measurement of the different node parameters including the following:

— *Congestion Probability*

— *Transmission efficacy (probability Quotient), and Traffic Dynamism.*

A brief of these node parameters is given as follows:

a. *Congestion Probability*

Congestion probability is one of the most used and decisive node parameters obtained from the MAC layer to assess suitability of the specific node towards best forwarding path selection. In mobile-IoT (mIoT) network, where due to the dynamic network topology a node might undergo frequent load conditions and hence there can be scenario where the cumulative resource demand or load on a node might go beyond its maximum buffer capacity. The moment when a node undergoes load (demand) more than its buffer capacity, it is stated to be congested that eventually result into random packet drop and hence imposes significant retransmission cost. In real-time transmission scenario, the cumulative congestion on a participating node i can be because of abrupt and iterative transmission effort by the neighboring nodes, especially when the cumulative buffer demands or resource demand by the transmitting neighboring node turns out to be higher than the maximum buffer capacity (of the i – th node). To ensure a reliable transmission protocol and QoS assurance, retaining only those nodes with low or almost no congestion probability as forwarding node can be of great significance. In this reference, our proposed routing protocol proposes a cumulative congestion probability estimation model. In this method, the proposed SDN-mIoT network controller measured congestion probability at each participating node.

To be noted, unlike traditional network deployment where the authors hypothesize to have single or standalone buffer for each node, we propose to deploy dual-buffer strategy. We assume that almost major at hand IoT applications perform both real-time transmissions (i.e., instant sensing and control) as well as data logs (i.e., data aggregation towards future analytics services). For instance, IoT deployed in smart factory setup can provide real-time sensing data such as surveillance data, gas sensor, fire sensor, pressure sensor, etc. to the controllers for timely monitoring and control. On the contrary, the same network or sensor node might aggregate information for future analytics such as fault probability assessment, device-level performance examination etc. Interestingly, both types of these data traffic used to have distinct priority and therefore assigning separate buffer for each type of traffic (i.e., real-time traffic and non-real-time traffic) can be of great significance. It can not only ensure optimal resource management, but can reduce congestion probability towards RTD traffic to support QoS assurance in SDN-mIoT network. In this reference, our proposed SDN-mIoT network controller make use of current buffer availability (CBAI) to perform congestion probability estimation. More specifically, we apply equation (1) and (2) to measure cumulative congestion probability (CCP) at a node, for further node-profiling and allied routing decision.

$$CCP_i = \frac{CCD_{RTD} + CCD_{NRT}}{CCD_{RTD_Max} + CCD_{NRT_Max}} \quad (1)$$

$$CCD_{FN} = \sum_{i=1}^N CCP_i \quad (2)$$

In above equations, the parameters CCD_{RTD} and CCD_{NRT} represents the current buffer available towards RTD traffic and NRT traffic, correspondingly. On the contrary, the components CCD_{RTD_Max} and CCD_{NRT_Max} represents the maximum buffer capacity of the deployed RTD and NRT buffers, respectively. The right-hand side parameter, CCP_i states the cumulative congestion at certain node i . In this work, the proposed CCP_i information was measured iteratively at the interval of 10 ms. Here, the higher value of CCP_i indicates vulnerability and hence the proposed SDN-mIoT network controller avoids such nodes to become the candidate forwarding node.

b. Transmission efficacy (probability Quotient)

In this work, the target node (profile) parameters are measured frequently over a definite interval and thus, assesses node information between the interval of t_1 and t_2 . Thus, estimating transmission characteristics (i.e., transmitted packets and the received packets), we measured transmission efficacy of each participating or connected node. We applied equation (3) to measure transmission efficacy.

$$Tr_{Eff} = \frac{\xi_{Rx}(t_{i-1}, t_i)}{\xi_{Exp}(t_{i-1}, t_i)} \quad (3)$$

In (3), the parameter ξ_{Rx} states the total received packet, while ξ_{Exp} signifies the total expected or transmitted data over the transmission period of (t_{i-1}, t_i) second(s).

c. Traffic Dynamism

As discussed earlier, SDN-mIoT networks might undergo frequent (network) dynamism including topological changes, congestion, link-outage as well as payload changes. Because of such network dynamism the sensor node might undergo abrupt packet drops and even high-flooding. The likelihood of abrupt transmission or the burst-over the dynamic network conditions (or transmission) can't be ruled out. Though, the role of any intruder or malicious node in such burst transmission can also incite researcher's attention. In this case, assessing traffic dynamism of a node can help segmenting a malicious node(s) or vulnerable node(s) that consequently can achieve fault-resilient forwarding path estimation and hence routing decision. This as a result can improve overall transmission reliability and hence QoS assurance. In this work, the proposed network controller hypothesizes that a node having high flooding or non-linearity should be avoided from using as a forwarding node. In this reference, we measured queue length (at the IEEE 802.11 MAC layer) as a parameter to assess respective traffic non-linearity.

Consider that i be the connected node and l_j be the queue length for the assessment period (t_{i-1}, t_i) for the j -th path. Then, over the queue-length of L , we estimated the average traffic load at the node i as per (4).

$$Traffic_{load_i} = \frac{1}{L} \sum_{j=1}^N l_j \quad (4)$$

Let, l_{max} be the maximum tolerable extent of the queue length at a node, then the overall traffic density at a node connecting possible source-to-destination path is given as per (5).

$$Traffic_{loadDensity_i} = \frac{Traffic_{load_i}}{l_{max}} \quad (5)$$

Thus, with reference to the above stated traffic density information, we examined the likelihood of successful transmission S_{prob_i} at the node i , is estimated as per the equation (6).

$$S_{prob_i} = [1 - Traffic_{loadDensity_i}] \quad (6)$$

Since, the probability of successful data transmission is related to the packet delivery, low value of S_{prob_i} and hence resulting retransmission imposes latency, redundant transmission and hence resource consumption. It eventually can impact overall QoS performance. In reference to this fact, we applied only those nodes having low queue length and high transmission probability to become the forwarding node in SDN-mIoT systems.

Now, once estimating above discussed node parameters, node profiling was done and a set of forwarding nodes was obtained for each source-destination node pair. The proposed routing protocol applied three different parameters (2), (3) and (6) to perform forwarding node selection for a definite source-destination pair. More specifically, we applied equation (7) to perform node profiling and hence a set of best forwarding paths was obtained.

$$Node_Profile_{BFN} = f[(\min_{i \in N} CCD_{FN}), (\max_{i \in N} S_{prob_i}), (\max_{i \in N} Tr_{Eff})] \quad (7)$$

Thus, applying above derived equation (7), a set of forwarding nodes was obtained, which were subsequently applied to derive three different forwarding paths. Noticeably, in the proposed model though a single path is applied to perform data transmission; however, in case of link-outage it executes and assigns alternate path available to complete

transmission. In this manner, it ensures transmission without undergoing iterative network discovery and allied costs (signaling cost, delay and redundant transmission).

B. Heuristic-Based Disjoint Alternate Path Selection

Though, the use of our proposed node profiling and adaptive forwarding path can enable reliable routing decision; however, the likelihood of the forwarding paths with multiple common nodes can't be ruled out. The failure of a common node amongst the multiple forwarding paths can cause iterative link-outage and hence transmission failure. This problem can be severe over mobile-IoT networks and hence it is vital to define and use disjoint alternate forwarding path (DAFP) can be of paramount significance. The use of DAFP can improve transmission reliability and hence QoS assurance of SDN-mIoT networks. An illustration of the multiple recovery (forwarding) path is depicted in Fig.1.

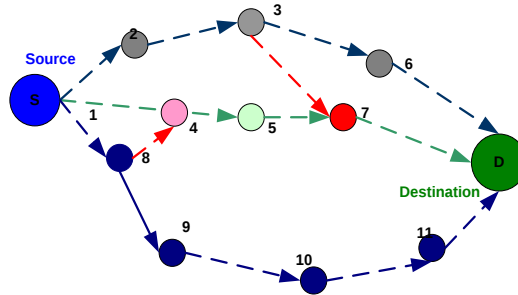


Fig. 1 An illustration of disjoint alternate forwarding path (DAFP) selection method

Consider that the proposed multi-constraints node profiling model identifies a set of N nodes as the best forwarding node (here, $N = \{N_1, N_2, N_3, N_4, N_5, N_6, N_7, N_8, N_9, N_{10}, N_{11}\}$ in Fig. 1). In Fig. 1, the node N_1 and N_7 are deployed as the source and the destination node, respectively. Thus, consider that there be multiple forwarding (recovery) paths, given as (8).

$$\begin{aligned}
 P_1 &= \{N_1 \rightarrow N_4 \rightarrow N_5 \rightarrow N_7\} \\
 P_2 &= \{N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_6 \rightarrow N_7\} \\
 P_3 &= \{N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_5 \rightarrow N_7\} \\
 P_4 &= \{N_1 \rightarrow N_8 \rightarrow N_4 \rightarrow N_5 \rightarrow N_7\} \\
 P_5 &= \{N_1 \rightarrow N_8 \rightarrow N_9 \rightarrow N_{10} \rightarrow N_{11} \rightarrow N_7\}
 \end{aligned} \tag{8}$$

With the identified best forwarding nodes (7), different best forwarding paths including P_1, P_2, P_3, P_4 and P_5 can be derived; however, only P_1, P_4 and P_3 can be selected as forwarding path considering the shortest path (distance) information. Though, the use of the shortest path information can give rise to the three different paths P_1, P_4 and P_3 ; however, these paths might undergo complete transmission failure in case node N_5 undergoes any failure or node death. The failure of this specific common node (N_5) can result collapse of all derived forwarding paths (i.e., P_1, P_4 and P_3). Consider that the forwarding path P_1 undergoes link-outage or failure, the SDN-mIoT controller, which is assumed to select either P_3 or P_4 as alternate forwarding path. Unfortunately, doing so can even cause subsequent failure due to the common node N_5 failure. It clearly indicates that an optimal routing protocol targeting QoS-oriented routing requires considering alternate forwarding path only with the disjoint nodes. Avoiding a common node in multiple forwarding paths can ensure successful transmission through recovery paths without worrying any possible common node.

In conjunction with the best forwarding node selection criteria (7), the proposed model executes proactive routing strategy where it identifies multiple DAFPs to meet reliable transmission and QoS. The proposed routing protocol exploits the different cross-layer information (7) the different DAFPs were obtained for reliable transmission. However, identifying a set of DAFPs while fulfilling aforesaid best forwarding node criteria (7) and disjoint path selection goal remains an NP-hard problem. To solve this problem, in this paper adaptive Genetic Algorithm (AGA) is applied to retrieve a set of DAFPs that achieves an optimal set of disjoint recovery path by applying identified best forwarding nodes without applying any common node across the forwarding paths (7).

To perform DAFPs estimation, the proposed AGA heuristic model at first identifies the source node, destination node and corresponding best forwarding node by using equation (7). To ensure reliability of the DAFP selection, our proposed AGA model applies link-connectivity information amongst the nodes (7). To achieve it, the proposed model initially executes the 1st order approximation which helps identifying the path unavailability. The proposed model performed Monte Carlo simulation to help dynamic topology estimation which is then updated to node table. This simulation also performed probabilistic network deployment. The network was deployed as per the Bayesian network model over the deployed SDN-mIoT networks. The simulation provides the network information including link connectivity and link-unavailability which was later applied to identify the optimal DAFPs to perform routing and optima transmission.

a. Link Connectivity Estimation

In the targeted SDN-mIoT network, the link connectivity signifies the likelihood that minimum one forwarding path can be active between the deployed source-destination pair. In this reference, a node n_i remains connected to the transmission failure recovery path, especially when the node n_0 remains active, provided that minimum one path exists between the source-destination pair. Here, the proposed model hypothesizes that each connected node possessing two disjoint forwarding paths, with no connected (common) element. Consider that for a node, the forwarding path be $\mathcal{P}_0, \dots, \mathcal{P}_{K-1}$, where $\overline{\mathcal{P}_k}$ signifies the node connectivity with $\mathcal{P}_k$. Then the proposed estimates the connected path as per the equation (9).

$$C(s_0) = A(s_0)A(\bigcup_{k=0}^{K-1} \overline{\mathcal{P}_k})A(C) \quad (9)$$

In (9), the component $A(\bigcup_{k=0}^{K-1} \overline{\mathcal{P}_k})$ signifies the possible forwarding paths fulfilling expected failure recovery purpose. Despite being active the connectedness of the node n_i might suffer network failure, and therefore link-loss results $\overline{\mathcal{P}_k}$ path failure which can take place due to device hardware damage, node death, etc. Hypothesizing that the deployed node and allied link condition as autonomous, the proposed model estimates related link-availability by using equation (10).

$$A(\bigcup_{k=0}^{K-1} \overline{\mathcal{P}_k}) = 1 - \prod_{k=0}^{K-1} U_r(\overline{\mathcal{P}_k}) \quad (10)$$

Consider that the deployed SDN-mIoT network contains $\{n_{k,0}, \dots, n_k, n_k\}$ nodes, and their respective forwarding path k be $\{e_{k,1,2}, \dots, n_k, f_{k-1}, f_k\}$. Then, the allied link-availability or connectivity is measured as per (11).

$$U_r(\overline{\mathcal{P}_k}) = 1 - A_r(\overline{\mathcal{P}_k}) = 1 - \prod_{i=1}^{f_{k-1}} A_n(n_{k,i}) \prod_{j=0}^{f_{k-1}} A_e(e_{k,j,j+1}) \quad (11)$$

Thus, for a transmitter node n_i , we applied equations (9-11) to measure link-connectivity by using equation (12).

$$C(s_0) = A(n_i)A(C) \times \left(1 - \prod_{k=0}^{K-1} \left(1 - \prod_{i=1}^{f_{k-1}} A_n(n_{k,i}) \prod_{j=0}^{f_{k-1}} A_e(e_{k,j,j+1})\right)\right) \quad (12)$$

We applied equation (12) to estimate link-connectivity for each best forwarding node, as derived through equation (7). To identify the disjoint paths with no common element (say, node), we hypothesize that the disjoint path can be achieved by decoupling the need of common or connected shared node from the connected forwarding path. Consider that M_0 and M_1 are the two forwarding paths, then using aforesaid derivations, their link-connectivity can be derived as (13).

$$C(n_i) = \prod_{j \in \Phi_n}^f A_n(n_j) \prod_{k \in \Phi_e}^{f-1} A_e(e_{k,k+1}) \times \left(1 - \left(1 - \prod_{i \in \Phi_{n,0}} A_n(n_{0,i}) \prod_{j \in \Phi_{e,0}} A_e(e_{0,j,j+1})\right) \times \left(1 - \prod_{i \in \Phi_{n,1}} A_n(n_{1,i}) \prod_{j \in \Phi_{e,1}} A_e(e_{1,j,j+1})\right)\right) \quad (13)$$

In the derived link-connectivity model (14), the parameters Φ_n and Φ_e be the shared nodes. In the same manner, the set of disjoint nodes over the i -th path is obtained as $\Phi_{n,i}$ and $\Phi_{e,i}$. In this manner, using the 1st order approximation, the connectivity loss is measured as (14).

$$L(n) = 1 - C(n_i) \quad (14)$$

$$L(n_i) \approx \sum_{j \in n}^f U_n(n_j) + \sum_{k \in \Phi_e}^{f-1} U_e(e_{k,k+1}) +$$

$$\left(\sum_{i \in \Phi_{n,0}} U_n(n_{0,i}) + \sum_{j \in \Phi_{e,0}} U_e(e_{0,j,j+1})\right) \times \left(\sum_{i \in \Phi_{n,1}} U_n(n_{1,i}) + \sum_{j \in \Phi_{e,1}} U_e(e_{1,j,j+1})\right) \quad (15)$$

Now, with (15), the probability that the disjoint path doesn't affect successful retransmission is measured as (16).

$$L(n_i) \approx \sum_{j \in \Phi_n}^f U_n(n_j) + \sum_{k \in \Phi_e}^{f-1} U_e(e_{k,k+1}) \quad (16)$$

It clearly affirms that a DAFP can be achieved without applying any common node. In this manner, our proposed AGA heuristic model applied link-availability for each deployed node as the cost function to identify and select DAFPs.

b. AGA-based Link-Availability Sensitive DAFP Optimization

The GA algorithm is a heuristic method that follows Darwin's principal of natural selection and selects a solution having the highest fitness value. In other words, it estimates a solution with the highest fitness value (here, link availability). In function, it identifies an optimal or sub-optimal solution from the available multiple candidate solutions (say, possible DAFP paths). In function, AGA algorithm performs three key processes; first, population initialization, crossover and mutation and optimal solution estimation. Here, the initial population initialization signifies the deployment of n -random solutions (i.e., DAFPs), while crossover states the process to generate other candidate solution over the subsequent generation so that a superior candidate solution can be achieved. On the contrary, mutation helps dropping the insignificant or inferior candidate solution so that the search space could be optimized to achieve more computationally efficient solution. In the proposed research, the initial population size was defined as 10, while crossover and mutation probability were fixed at 0.6 and 0.4. Though, to alleviate any probability of local minima and convergence due to exceedingly high search space problem, adaptive GA method was designed, where the crossover and mutation probability values were optimized as per the equation (17). In the proposed AGA heuristic model, we updated crossover probability P_c and mutation probability P_m dynamically by using equation (17) and (18).

$$(P_c)_{k+1} = (P_c)_k - \frac{C_1 * N_{SSF}}{7} \quad (17)$$

$$(P_m)_{k+1} = (P_m)_k - \frac{C_2 * N_{SSF}}{7} \quad (18)$$

Here, $(P_c)_{k+1}$ and $(P_m)_{k+1}$ represents the updated crossover and mutation probability, while the current probability values be $(P_c)_k$ and $(P_m)_k$, respectively. In this work, we assigned coefficient parameters C_1 and C_2 as 0.1 and 0.01, correspondingly. The parameter N_{SSF} defines the total solutions (here, DAFPs) having similar fitness value. Thus, executing the proposed AGA heuristic model and applying link-availability (16) as cost function or fitness function, we performed optimization that yielded a set of optimal DAFPs guaranteeing no connected component or shared nodes exists in the different forwarding paths.

In HDAP-SDNiOT, AGA is executed over all possible set of candidate paths and thus an optimal set of DAFPs were obtained for further routing task. Once obtaining the DAFP forwarding paths over k iterations, the paths for a source-destination pair N_k having poor link availability (i.e., cost function) are pruned. Though, for sake of easy implementation we applied link connectivity loss (i.e., 1-link availability or 1-link connectivity) as the objective function $c(\mathcal{P})$ (19) to measure fitness for each candidate DAFP path $\mathcal{P}$.

$$\mathcal{P}^* = \arg \min_R c(\mathcal{P}) \quad (19)$$

Let, $\bar{\mathcal{P}}$ states the forwarding path for the node having zero connectivity loss. In this case, a path R can be connected to the transmitter (source-destination pair) n_f , and hence for any forwarding path $M_i \in N_k$, $L(\bar{\mathcal{P}}, M_i)$ the connectivity-loss with respect to n_i , the mean connectivity loss is measured as (20).

$$\tilde{L}(\mathcal{P}) = \frac{1}{S_c} \sum_{i=1}^{S_c} L(\bar{\mathcal{P}}, M_i) \quad (20)$$

Here, the function (20) was further redefined as (21), where $E(\mathcal{P})$ was estimated on the basis of the mean loss imposed per link across the paths (i.e., dual disjoint paths).

$$c(\mathcal{P}) = \tilde{L}(\mathcal{P}) + E(\mathcal{P}) \quad (21)$$

Where, $E(\mathcal{P})$ is measured using equation (23).

$$E(\mathcal{P}) = \frac{1}{N_c} \sum_{i=1}^{N_c} E(\mathcal{P}, M_i) \quad (22)$$

Where,

$$E(\bar{\mathcal{P}}, M_i) = \frac{\tilde{L}(M_i)}{\lambda} d(s_{\mathcal{P}}, s_f) \quad (23)$$

To further tune performance, AGA model applied topological information as well for DAFP selection. In other words, we applied both link-connectivity loss and hop-counts are the cost function parameters or objective function. To measure distance between the nodes, graph theory method was applied, in which network graph signifies a graph matrix A possessing the nodes a_{ij} with the active or connected status (say, $a_{ij} = 1$). Noticeably, here, $a_{ij} = 1$ states that the source i and destination node j are connected and active. In this manner, it retrieves a matrix $B(k)$, given as (24).

$$B(k) = \mathbb{A}^k \quad (24)$$

In (24), $B(k)$ embodies $b_{ij}(k)$ which is same as the total paths connecting the source node j to the destination node j , maintaining the hops lower than k . To measure inter-node distance $d(i, j)$ the shortest path estimation model (25) was applied.

$$d(i, j) = \min_{b_{ij}(k) > 0} \{k\} \quad (25)$$

In this manner, applying the derived objective functions (16) and (25), the optimal set of DAFPs was obtained. More specifically, the proposed model identified three DAFPs for each transmission (i.e., between the source i and destination j) with no common node. Thus, applying this method, the proposed routing model identifies the set of DAFPs for each pair of source-destination and updates to the node able of N_k , which is updated proactively at the interval of 10 ms. In other words, for a source-destination pair ij , it estimates three disjoint DAFPs $DAFP_{ij}^1$, $DAFP_{ij}^2$ and $DAFP_{ij}^3$.

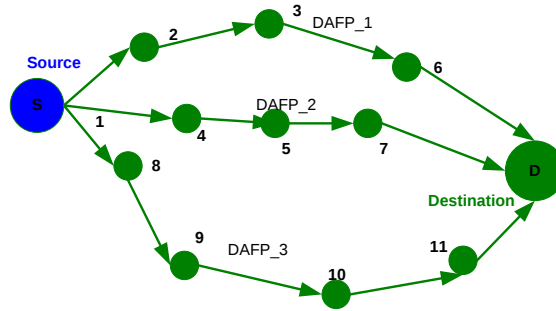


Fig. 2. Optimized DAFP

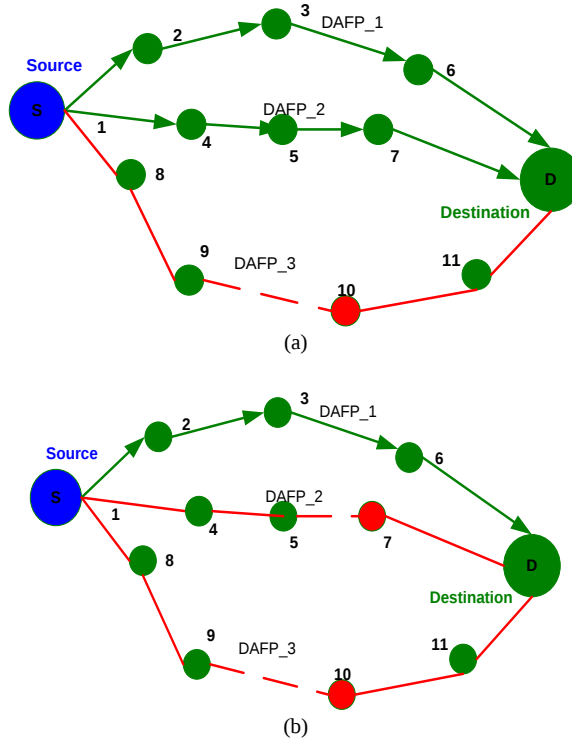


Fig. 3. (a) Transmission when $DAFP_{ij}^3$ fails, (b), when $DAFP_{ij}^3$ and $DAFP_{ij}^2$ fail

As depicted in Fig. 2 and Fig. 3, once identifying $DAFP_{ij}^1$, $DAFP_{ij}^2$, and $DAFP_{ij}^3$ paths for the source-destination pair ij , the proposed model executes transmission with the path having the highest fitness value (say, $DAFP_{ij}^3$). During the course of transmission, in case the path $DAFP_{ij}^3$ fails or undergoes link-outage, the proposed SDN-mIoT protocol switches to the alternate path $DAFP_{ij}^2$ (Fig. 3 (a)) without undergoing or performing node discovery or allied best forwarding path selection cost. Similarly, in case $DAFP_{ij}^2$ too undergoes link-loss or failure, the proposed protocol

executes $DAFP_{ij}^1$, as depicted in Fig. 2 (b). Thus, the proposed routing protocol performs network self-configuration even under link-outage probability and thus avoids any iterative network discovery or link-formation cost. It not only improves transmission reliability, latency but also suppresses unwanted redundant transmission. The proposed network's self-configuring model applies logical AND function to select or switch recovery alternate path, in case it undergoes link-failure or path loss. Thus, applying the proposed routing protocol the proposed SDN-mIoT network performs reliable and QoS-centric communication. The detailed discussion of the simulation results is given in the subsequent section.

6. Results and Discussion

The high-pace rising mobility driven wireless networks have broadened the horizon for the different communication systems and allied applications to serve real-time communication and allied decision-making demands. With aforesaid rising demands, the related challenges too are on rise including QoS, security etc. To achieve it, wireless technologies have witnessed significant innovation and evolution. Amongst such innovations IoT technologies have gained widespread attention to serve the major industries with scalability, reliability and swift communication potential. Despite robustness and rising significances, increasing node densities (to cope up scalability), network complexities and resulting QoS challenges have alarmed academia-industries to achieve more efficient solutions. Noticeably, achieving an optimal communication ability over aforesaid IoT networks, ensuring reliability of the transmission, resource control and allocation, optimal routing etc. seem to be decisive and therefore in this regards a number of efforts have been made, including SDN controllers that improves scalability of IoT efficiently. This is the matter of fact that SDN-IoT technologies can achieve superior performance over state-of-art WSN or IoT systems (as standalone network solution); however, guaranteeing QoS over mobility driven IoTs remains a challenge. The dynamic mobility, link-vulnerability, and allied frequent network discovery and path planning (say, routing) cost can limit its efficacy and real-time significance. Noticeably, the majority of the state of art methods have applied reactive or proactive routing approaches with single node parameters to perform routing decision that itself makes routing vulnerable, as a real-time SDN-IoT network might undergo frequent changes in link, packet loss, buffer availability and congestion etc. In this case applying maximum possible node information can be more effective to perform best forwarding node and subsequent best forwarding path selection. Additionally, even though someone performs multiple parameters (say, multi-constraints) driven best forwarding path selection strategy, any link-loss problem over dynamic topology might force network controller to undergo iterative network discovery (post link outage) and therefore can impose delay, redundant transmission as well as power exhaustion due to iterative redundant (re)transmission. To alleviate it, multi-path or multiple alternate path planning strategy seems to be more viable approach. In the past though, numerous efforts have been made by applying multi-path transmission strategies; however, almost all state-of-arts have applied either distance-based routing or residual energy. These state-of-art don't bother on the use of common elements or nodes to constitute forwarding path. Unfortunately, the failure of any of the deployed or considered common nodes might force entire network to collapse. This as a result can impact overall performance and QoS performance.

In reference to the aforesaid research inferences, in this research a novel and robust Heuristic-Driven Disjoint Alternate Path Switching -based Fault-Resilient Multi-Constraints Routing Protocol is developed for SDN-mIoT (HDAP-SDNIoT). In sync with aforesaid research goal, the proposed model at first performs multi-constraints node profiling followed by alternate path selection. Subsequently, it applied AGA heuristic model to achieve a set of disjoint alternate forwarding path (DAFP) selection. The proposed DAFP model applied in such manner that the paths with the maximum link availability with no shared component(s) were considered as the best forwarding path. More specifically, the proposed HDAP-SDNIoT protocol was designed for SDN-mIoT network, encompassing mobile as well as statically deployed nodes. In this work, the simulation was done with the different network conditions, including node density (i.e., nodes deployed per unit area) and the velocity of the moving nodes (m/s). Once deploying the nodes, the proposed HDAP-SDNIoT protocol at first performed node profiling. To achieve it, SDN controller multicasts HELLO beacon message and receives unicast ACK response from each connected node. Exploiting the acknowledgement signal from each node, it estimates the different cross-layer parameters including IEEE 802.11 (mobile nodes) and IEEE 802.15.5 (static nodes) parameters such as congestion probability, flooding information, traffic dynamism and transmission efficacy (i.e., probability quotient). Once estimating these node parameters, node profiling was done. Applying moving weighted average method with the network coefficient of 0.3 (congestion probability), 0.3 (MAC information) and 0.4 (network topology) the best forwarding nodes were decided. Mathematically, we applied (26) to identify the set of best forwarding nodes.

$$Node_Profile_{BFN} = 0.3 * CCD_{FN} + 0.3 * S_{prob_i} + 0.4 * Tr_{Eff} \quad (26)$$

Noticeably, the aforesaid node profiling was done and updated after each 10 ms interval so as to ensure reliable proactive routing decision and allied QoS centric transmission. Once identifying the set of best forwarding nodes, the proposed HDAP-SDNIoT protocol identifies three different forwarding paths. These forwarding paths along with the allied node information are fed as input to the AGA heuristic to identify the set of disjoint forwarding path to perform further transmission. Unlike traditional GA-based network optimization or routing decision, our proposed HDAP-

SDNIoT protocol applies Adaptive GA concept that makes use of dynamic crossover and mutation probability. This as a result ensures minimum search space (i.e., the candidate disjoint paths) and hence achieves optimal routing decision (say, DAFP) without undergoing any possible local minima and convergence problem. Though, the initial crossover and mutation probability parameters were assigned as 0.6 and 0.4, along with 100 number of generations; however, the proposed AGA model retrieves solution in early iterations only. It ensures time-efficiency of the proposed model. To assess efficacy of the proposed routing protocol, C++ scripts were developed and simulation was done on Network Simulator 2 tool. We simulated the proposed model on Ubuntu 14 operating system armored with 8 GB RAM and Intel-i5 processor, functional at 3.2 GHz frequency machine. The parameters considered for simulation are given in Table I.

Table 1. Simulation Parameters

Parameter	Specification
Number of Nodes	50, 100, 150, 200 and 250
Network Region	1000 × 1000 m
Payload (kB)	250, 500, 750, 1000, 1500, 2000, 2500, 3000
Physical	IEEE 802.11 PHY
MAC	IEEE 802.15.4/ IEEE 802.11
Protocol	HDAP-SDNIoT (assigned on top of native MAC to cope up backward compatibility)
Link-layer	CSMA
Radio Range	200 meters
Packet deadline time	10 ms.
Traffic	CBR
Topology	Random Movement
Simulation Period	600 seconds
Node Speed	5 m/s, 10 m/s and 25 m/s.
Transmitter Power	130 mW
Message Type	Unicast, Multicast
Simulation Tool	NS2

To assess efficacy of the proposed HDAP-SDNIoT routing protocol, we simulated it with the different network conditions including payload conditions and node velocity. This is because, in mIoT networks the nodes can be even in mobile state thus impacting overall routing and transmission reliability. In the targeted SDN-mIoT network the nodes can be in mobile states as well and can be moving with the different speed. Moreover, the heterogeneity of nodes can cause the diversity of data packets and its sizes, and therefore it becomes more important for HDAP-SDNIoT to ensure QoS delivery over these different network conditions (i.e., payload, node density and speed). We simulated the proposed model with the different payloads and speed. The simulated results and allied inferences are given as follows:

In this work, we simulated the proposed model with the traffic load of 250 packets, 500 packets, 1000 packets, 2000 and 2500 packets, and corresponding performance outputs were plotted in terms of packet delivery rate (PDR), packet loss rate (PLR) and energy consumption. Noticeably, each packet of data carried 512 bytes of information. Similarly, we executed the proposed HDAP-SDNIoT protocol for the different mobility pattern or speeds, and corresponding efficacy was examined. This is the matter of fact that SDN-based IoT is a recent technical innovation and hence not much efforts have been done towards routing optimization. Most of the SDN-based IoT solutions have focused on resource access and management, and very few efforts are made towards routing optimization. In reference to this fact, we identified a close reference contributing SDN-IoT protocol or routing solution. To compare relative efficacy of the proposed routing protocol, we compared it with the traffic-aware QoS routing protocol in software-defined IoT (SWAY). More specifically, we simulated the work of Saha et al. [17,18] in which the authors applied link-delay and packet loss information to perform best routing path. However, the authors failed in avoiding looping problem or the common nodes while planning routing or constituting the forwarding paths. Despite this, since the authors tried to use multiple node parameters like us to perform best forwarding path selection to meet QoS demands, we compared our proposed HDAP-SDNIoT protocol with them. For relevant performance characterization we implemented SWAY protocol as well and simulated with reference to the different node conditions (i.e., packet load and velocity). The relative performance outcomes are given as follows:

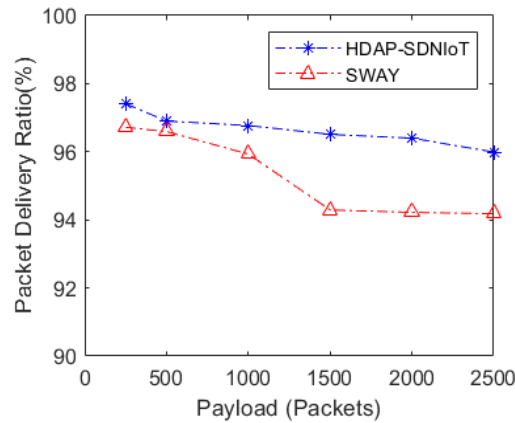


Fig. 4. PDR performance over varying payload (packets)

Fig. 4 presents the PDR performance by the proposed HDAP-SDNiOT protocol and the existing SWAY routing model. Observing the results, it can easily be found that proposed routing model outperforms the state-of-art SWAY routing approach even over high payload condition. The average performance indicates that the proposed HDAP-SDNiOT protocol exhibits average PDR of 95.32% with the highest PDR of almost 97.4%. The proposed model suffers PLR of almost 4.6%. On the contrary, the average PDR by the existing SWAY routing model was measured as 94.11%, while PLR observed was 5.89%. The performance quantification over varying payload indicates that the proposed HDAP-SDNiOT protocol performs superior over the state-of-art. To be noted, though SWAY model applied link-delay and packet loss information to perform adaptive routing decision; however, it failed in addressing numerous other issues including congestion probability which might be frequent over increasing payload. Typically, rising payload over mobility results into congestion. Though, our proposed HDAP-SDNiOT protocol possesses congestion adaptive routing decision, it achieved superior PDR. On the contrary, SWAY model lacked addressing congestion adaptive routing and hence underwent higher packet loss. This result is well justified in reference to the Fig. 4 and Fig.5. In mobility-driven IoT systems, the node density too can be varying over time. In other words, in mobility-based IoT systems can have the different node density based on the topological locations, applications etc. In this reference, we simulated our proposed HDAP-SDNiOT protocol with the different node densities and the results were obtained. The relative performance of the proposed HDAP-SDNiOT protocol and the existing SWAY model over the different node densities is depicted in Fig. 6 and Fig. 7.

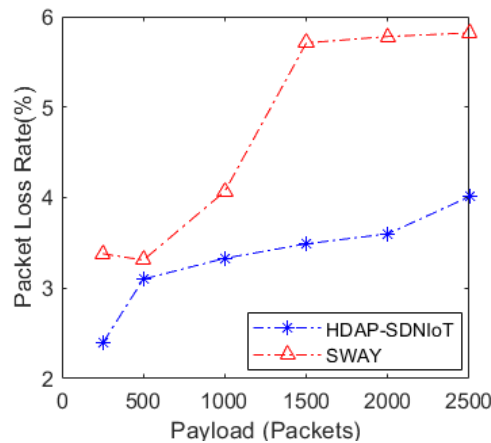


Fig. 5. PLR performance over varying payload (packets)

As depicted in Fig. 6, our proposed HDAP-SDNiOT protocol exhibits higher PDR than the state-of-art SWAY model. The depth assessment reveals that the proposed HDAP-SDNiOT protocol shows average PDR (%) of 96.55%, while it undergoes PLR of almost 3.4%. On the contrary, the existing SWAY model exhibits 96.12% PDR, while the same undergoes PLR of 3.9%. In this manner, the overall research and allied inference indicates that the proposed HDAP-SDNiOT protocol outperforms existing SWAY model. Though, the difference between the PDR performance by the both protocols over the different densities are not much different, yet signifies its efficacy towards QoS performance.

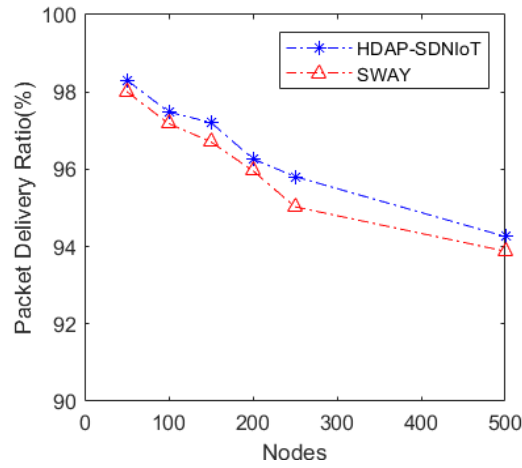


Fig. 6. PDR performance over varying node density

HDAP-SDNiOT protocol being mobility driven IoT systems can frequently undergo the scenario where the different nodes might undergo varying speed (m/s). Noticeably, the change in speed and trajectory can have decisive impact on QoS performance. The results obtained over the different speed (mobility pattern) is depicted in Fig. 8 and Fig. 9.

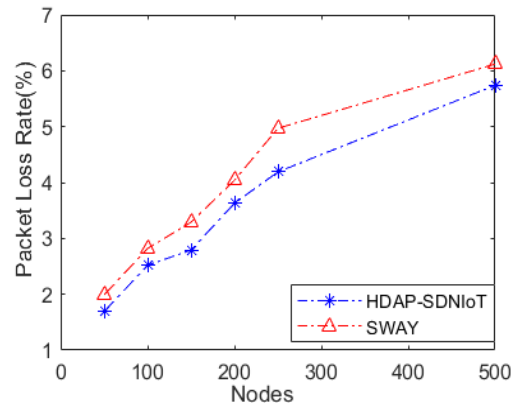


Fig. 7. PLR performance over varying node density

The simulation results infer that the proposed HDAP-SDNiOT protocol exhibits average PDR of 97.23%, while the state-of-art method (i.e., SWAY) exhibits PDR of 96.56%. Similarly, the PLR performance by HDAP-SDNiOT protocol and existing SWAY model was obtained as 2.8% and 3.5%, correspondingly. The depth performance inferred that the proposed HDAP-SDNiOT outperforms existing methods.

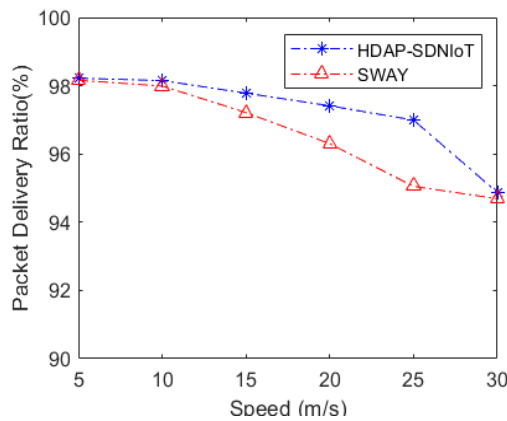


Fig. 8. PDR performance over varying node speed

Considering delay performance, we simulated the proposed model (i.e., HDAP-SDNiOT protocol) as well as SWAY protocol and obtained delay performance. We simulated the developed models over the different network conditions and their average latency was obtained. The simulated results are given in Fig. 10. As depicted in Fig. 10, the

average delay observed by SWAY model was 198 *ms*. On the contrary, our proposed HDAP-SDNIoT protocol exhibits the delay of 211 *ms*. To be noted, our proposed HDAP-SDNIoT protocol applies AGA heuristic to perform DAFP estimation and routing for more reliable transmission. Undeniably, the use of heuristic algorithm increases computation and hence allied time. Because of this the proposed HDAP-SDNIoT protocol can have higher latency. Though, SWAY model which doesn't use any heuristic algorithm shows computation time of 198 *ms*.

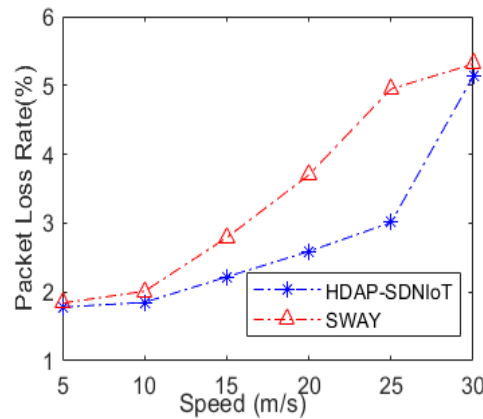


Fig. 9. PLR performance over varying node speed

To be noted, unlike proposed HDAP-SDNIoT protocol, SWAY model applies link-delay and data loss information; yet, undergoes the delay of 198 seconds. Despite higher end algorithm with superior routing abilities, the proposed model consumes 211 *ms* and consumes merely 13 more *ms*; yet, performs superior PDR performance and thus achieves higher reliability or QoS performance.

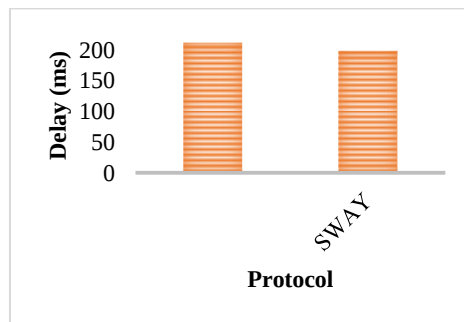


Fig. 10. Delay performance

Thus, observing overall performance it can be stated that the proposed HDAP-SDNIoT protocol performs superior over the state-of-arts SWAY routing protocol for SDN-based IoT systems. The overall research conclusion and allied inferences are given in the subsequent section.

7. Conclusion

In recent years SDN-based IoT networks have gained widespread attention globally to serve varied communications tasks including smart home, smart city, smart factory, civic monitoring and control, e-healthcare, business and defence communications. Despite the fact that the use of both control plane as well as data plane information strengthens SDNs to improve transmission reliability, the network dynamism imposed over mobile-IoT networks puts question over the reliability and QoS assurance of SDN-mIoT networks. In sync with aforesaid cross-layer information usage towards reliable routing decision, a robust routing approach was designed by applying dynamic node information from the different layers, including congestion and flooding information from the MAC layer, residual energy from PHY, and link information from network layer. In this paper, at first node profiling was done for each node connected in the network, which achieved dual purposes, first the malicious node identification and isolation from the forwarding path selection and second the (profile-adaptive) optimal forwarding path selection. It improved transmission reliability. Applying multi-constraints criteria with the moving window averaging concept a set of forwarding paths were obtained. The proposed multi-constraints forwarding path selection model served proactive routing, where it identified multiple forwarding paths so that in case of link-outage a transmitter can use alternate path for delay-resilient transmission without undergoing iterative node and/or network discovery costs. Though, multi-constraints criteria improved routing reliability; however, the presence of common node in multi shortest path couldn't be ruled out. To address this problem, HDAP-SDNIoT designed AGA-based disjoint alternate forwarding path (DAFP) selection model

by which exploited different node's parameters to identify a set of disjoint forwarding path(s) for further transmission decision. Thus, the proposed model guaranteed that no common node participates multiple paths and hence avoided iterative link failure due to the probable common node failure scenarios. The proposed DAFP mechanism retained dual-disjoint forwarding paths and whenever a node undergoes any link-outage, it switches to the alternate disjoint path automatically, without undergoing network discovery phase and thus avoided delay and allied communication cost. It not only enabled fault-resilient routing but also suppressed the likelihood of retransmission, delay and allied signalling and memory cost. The overall proposed SDN-mIoT routing protocol was designed and simulated by using Network Simulator-2 software, where it exhibited superior efficiency in terms of high packet delivery rate 96.5%, low packet loss rate 3.5% and low delay (211 ms) affirming its robustness and suitability towards real-time SDN-mIoT communication. Though, the use of AGA heuristic helped identifying disjoint shortest forwarding paths; however, at the cost of high (here, 200 generations) computations that in real-time can be time-consuming. To be noted, unlike traditional heuristic-based routing methods where the authors have applied fixed number of generation and hence the likelihood of local minima and convergence can't be ruled out, this research contributed Adaptive GA where the crossover and mutation probability varies dynamically (say, updated dynamically). This ability strengthens the proposed HDAP-SDN-mIoT protocol to alleviate any likelihood of local minima and convergence, thereby achieving a reliable and time-efficient routing solution. In future, other lightweight heuristic can be designed and applied to improve time-efficiency and hence scalability of the protocol for larger network applications.

In reference to the overall proposed routing approach and allied simulation results, this research finds the answers of the research questions (RQ1- RQ4 in Section IV) in affirmation. In other words, this research concludes with the following inferences:

- *The use of multi-constraints dynamic network parameters including MAC information, flooding, network dynamism and congestion probability driven node profiling be effective towards fault-resilient best forwarding routing protocol for SDN-mIoT systems (RQ1).*
- *The use of heuristic driven disjoint alternate forwarding path selection (DAFP) method be effective towards QoS-centric routing in SDN-mIoT systems (RQ2).*
- *The strategic amalgamation of aforesaid dynamic node profiling based proactive routing (RQ1) and heuristic-driven DAFP model (RQ2) be effective towards QoS oriented SDN-mIoT communication (RQ3).*
- *AGA Heuristic-Driven Disjoint Alternate Path Switching -based Fault-Resilient Multi-Constraints Routing Protocol be effective towards delay-resilient and reliable communication in SDN-mIoT communication (RQ4).*

In future, the authors can assess relative efficacy of the other lightweight heuristic models such as firefly algorithm to perform DAFP estimation. This is the matter of fact that the use of dual-buffer strategy for each node has helped addressing resource allocation problem and allied management in IoT; yet, in future the focus can also be made on resource allocation strategies to serve or accommodate large IoT devices operating concurrently.

References

- [1] J. Guerrero-Ibanez, S. Zeadally, J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies," *IEEE Wireless Communications*, vol. 22, no. 6, pp. 122–128, Dec. 2015.
- [2] Oxford Dictionary, "Definition of Internet of Things in English," 2018. [Online]. Available: [https://en.oxforddictionaries.com/definition/internet of things](https://en.oxforddictionaries.com/definition/internet%20of%20things)
- [3] Cambridge Dictionary, "The Internet of Things definition," 2018. [Online]. Available: <https://dictionary.cambridge.org/us/dictionary/english/internet-of-things>
- [4] Gartner IT Glossary, "The Internet of Things defined," 2018. [Online]. Available: <https://www.gartner.com/it-glossary/internet-of-things/>
- [5] Luigi Atzori, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey". In: *Computer networks* 54.15 (2010), pp. 2787–2805.
- [6] Lili Yang, Shuang-Hua Yang, and Linda Plotnick. "How the internet of things technology enhances emergency response operations". In: *Technological Forecasting and Social Change* 80.9 (2013), pp. 1854–1867.
- [7] J. Pan, R. Jain, S. Paul, T. Vu, A. Saifullah, and M. Sha, "An Internet of Things Framework for Smart Energy in Buildings: Designs, Prototype, and Experiments," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 527–537, Dec. 2015.
- [8] Rahman, A., Chakraborty, C., Anwar, A., Karim, M., Islam, M., Kundu, D., Rahman, Z., Band, S.S., et al.: Sdn-iot empowered intelligent framework for industry 4.0 applications during covid19 pandemic. *Clust. Comput.* (2021). <https://doi.org/10.1007/s10586-021-03367-4>
- [9] M. M. Raikar, S. M. Meena and M. M. Mulla, "Software Defined Internet of Things using lightweight protocol" *Third International Conference on Computing and Network Communications (CoCoNet, 19, Procedia Computer Science* 171 (2020) 1409–1418.
- [10] K. Sood, S. Yu and Y. Xiang, "Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review," in *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 453–463, Aug. 2016.
- [11] Slavica Tomovic, Kenji Yoshigoe, Ivo Maljevic, and Igor Radusinovic. 2017. Software-Defined Fog Network Architecture for IoT. *Wirel. Pers. Commun.* 92, 1 (January 2017), 181–196.

- [12] S. Al-Rubaye, E. Kadhum, Q. Ni and A. Anpalagan, "Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency," in IEEE Internet of Things Journal.
- [13] Lin, Ying-Dar et al. "SAMF: An SDN-Based Framework for Access Point Management in Large-scale Wi-Fi Networks." *Journal of Communications Software and Systems*, Vol. 13 No. 4, 2017. <https://doi.org/10.24138/jcomss.v13i4.398>
- [14] B. O. Kahjogh and G. Bernstein, "Energy and latency optimization in software defined wireless networks," 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, 2017, pp. 714-719. doi: 10.1109/ICUFN.2017.7993884
- [15] M. Al Ja'afreh, H. Adhami, A. E. Alchalabi, M. Hoda, and A. E. Saddik, "Toward integrating software defined networks with the Internet of Things: a review", *Cluster Computing*, Springer, 2022, Vol. 25, pp. 1619–1636
- [16] Fancy, C., Pushpalatha, M.: Traffic-aware adaptive server load balancing for software defined networks. *Int. J. Electr. Comput. Eng.* (2088-8708) 11(3), 2211–2218 (2021)
- [17] Saha, N., Bera, S., Misra, S.: Sway: Traffic-aware QoS routing in software-defined iot. *IEEE Trans. Emerg. Top. Comput.* 9, 390–401 (2018a)
- [18] Saha, N., Misra, S., Bera, S.: Qos-aware adaptive flow-rule aggregation in software-defined iot. In: 2018 IEEE global communications conference (GLOBECOM), IEEE, pp 206–212 (2018b).
- [19] Qin, Z., Denker, G., Giannelli, C., Bellavista, P., Venkatasubramanian, N.: A software defined networking architecture for the internet-of-things. In: 2014 IEEE network operations and management symposium (NOMS), IEEE, pp 1–9 (2014)
- [20] Munˆoz, R., Vilalta, R., Yoshikane, N., Casellas, R., Martı´nez, R., Tsuritani, T., Morita, I.: Iot-aware multi-layer transport sdn and cloud architecture for traffic congestion avoidance through dynamic distribution of iot analytics. In: 2017 European conference on optical communication (ECOC), IEEE, pp 1–3 (2017)
- [21] Gupta, H., Nath, S.B., Chakraborty, S., Ghosh, S.K.: Sdfog: A software defined computing architecture for qos aware service orchestration over edge devices. Preprint at arXiv:160901190 (2016)
- [22] Llopis, J.M., Pieczerek, J., Janaszka, T.: Minimizing latency of critical traffic through sdn. In: 2016 IEEE international conference on networking, architecture and storage (NAS), IEEE, pp 1–6 (2016)
- [23] Tomovic, S., Yoshigoe, K., Maljevic, I., Radusinovic, I.: Software-defined fog network architecture for iot. *Wirel. Pers. Commun.* 92(1), 181–196 (2017)
- [24] Sawashima, H.: Characteristics of udp packet loss: effect of tcp traffic. *proc of INET'97*. (1997)
- [25] Misra, S., Saha, N.: Detour: dynamic task offloading in softwaredefined fog for iot applications. *IEEE J. Sel. Areas Commun.* 37(5), 1159–1166 (2019)
- [26] Yen, J.Y.: Finding the k shortest loopless paths in a network. *Manage. Sci.* 17(11), 712–716 (1971)
- [27] Bera, S., Misra, S., Saha, N.: Traffic-aware dynamic controller assignment in sdn. *IEEE Trans. Commun.* 68(7), 4375–4382 (2020)
- [28] Bizanis, N., Kuipers, F.A.: Sdn and virtualization solutions for the internet of things: a survey. *IEEE Access* 4, 5591–5606 (2016)
- [29] Mao, B., Tang, F., Fadlullah, Z.M., Kato, N., Akashi, O., Inoue, T., Mizutani, K.: A novel non-supervised deep-learning-based network traffic control method for software defined wireless networks. *IEEE Wirel. Commun.* 25(4), 74–81 (2018)
- [30] Das, S., Sahni, S.: Network topology optimization for data aggregation. In: 2014 14th IEEE/ACM international symposium on cluster, cloud and grid computing, pp. 493–501. IEEE, Piscataway (2014)
- [31] Docker (2021) Docker. <https://www.docker.com/>. Accessed 1 Nov 2023.
- [32] Kubernetes (2021) Kubernetes. <https://kubernetes.io/>. Accessed 1 Nov 2023.
- [33] Sood, Keshav, Yu, Shui, Xiang, Yong and Peng, Sancheng 2016, Control layer resource management in SDN-IoT networks using multiobjective constraint, in ICIEA 2016: IEEE, Piscataway, N.J., pp. 71-76.
- [34] A. A. Hayajneh, M. Z. A. Bhuiyan and I. McAndrew, "Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN)", *MDPI, Computers* 2020, 9, 8; doi:10.3390/computers9010008.
- [35] A. Samanta, S. Bera, and S. Misra, "Link-Quality-Aware Resource Allocation with Load Balance in Wireless Body Area Networks," *IEEE Systems Journal*, 2015, DOI: 10.1109/JSYST.2015.2458586.
- [36] H. Sandor, B. Genge, and G. Sebestyen-Pal, "Resilience in the Internet of Things: The Software Defined Networking approach," in *Proc. of the IEEE Intl. Conf. on Intelligent Computer Communication and Processing (ICCP)*, Cluj-Napoca, Sept. 2015, pp. 545–552.
- [37] Y. Jararweh, M. Al-Ayyoub, A. Darabseh, E. Benkhelifa, M. Vouk, and A. Rindos, "SDIoT: a software defined based internet of things framework," *Journal of Ambient Intelligence and Humanized Computing*, vol. 6, no. 4, pp. 453–461, Aug. 2015.

Authors' Profiles



Mr. Suprith Kumar K. S. , Assistant Professor, ECE dept, B.M.S. College of Engineering, Bangalore. He has done his master's in digital communication from BMSCE and currently pursuing his Ph.D. He has worked as a Reliability Verification Engineer in Intel Corporation and project engineer in LTTS and has a 4 years of industry experience and 3 years of teaching experience. He has handled various courses for UG Level. His areas of interest are Communication Systems, Networking and Signals & Systems. He is a lifetime member of IETE and IEI and member of IEEE.



Eesha. D. is currently working as Assistant Professor in the department of Electronics and Communication Engineering, BMSCE from past 4 years and he has handled various course for UG program. He has completed M-Tech from BMSCE in Digital Communication. He has worked as a Signal Integrity Engineer in Intel Technology India Pvt Ltd. on advanced design and simulation software. He was also a part of Intel funded IISC project working reduction of simulation time and memory requirement for Package/Board interconnects using intelligent segmentation. He has keen interests in Signal processing, Communication, Networking and Antenna Design.



Pooja A. P. is currently working as Assistant Professor in the department of Electronics and Communication Engineering, BMSCE from the past five years. She has overall teaching experience of 10 years She has handled various course for UG program. She has completed M-Tech from Malnad College of Engineering in Information and Communication Systems. She has published research papers on reputed journals in image processing domain. Her area of interest includes Wireless Communication, Networking, Signal Processing, Machine Learning.



Monika Sharma D. is currently working as an Assistant Professor in the department of Electronics and Communication Engineering at B.M.S College of Engineering, Bangalore. She has Completed her BE in Electronics and Communication Engineering and M-Tech in VLSI Design and Embedded Systems. She is having 10 years of teaching experience and her research areas of interest includes Signal Processing, Embedded Systems, low power VLSI and Digital VLSI Design.

How to cite this paper: Suprith Kumar K. S., Eesha D., Pooja A. P., Monika Sharma D., "Heuristic – Driven Disjoint Alternate Path Switching – Based Fault Resilient Multi- Constraints Routing Protocol for SDN-mIoT", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.14, No.5, pp. 12-30, 2024. DOI:10.5815/ijwmt.2024.05.02