I.J. Wireless and Microwave Technologies, **2024, 1, 29-42**
Published Online on February 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2024.01.03

A Novel Approach by Integrating Dynamic Network Selection and Security Measures to improve Seamless Connectivity in Ubiquitous Networks

Prasanna Kumar G*
Department of Information Science & engineering, The National Institute of Engineering, Mysuru, 570018, India
E-mail: g3p3k3@gmail.com
ORCID iD: https://orcid.org/0000-0002-8962-8034
*Corresponding Author

Shankaraiah N
Department of Electronics and Communication engineering, Sri Jayachamarajendra College of Engineering, Mysuru, 570006, India
E-mail: shankarsjce@gmail.com
ORCID iD: https://orcid.org/ 0000-0003-2810-3872

Rajashekar M B
Department of computer Science & engineering, GSSS Institute of Engineering & Technology for Women, Mysuru, 570016, India
E-mail: rajucit.mb@gmail.com
ORCID iD: https://orcid.org/0000-0002-5623-2092

Sudeep J
Department of Information Science & engineering, The National Institute of Engineering, Mysuru, 570018, India
E-mail: sudeep@nieit.ac.in
ORCID iD: https://orcid.org/ 0000-0001-7427-4555

Shruthi B S
Department of Information Science & engineering, The National Institute of Engineering, Mysuru, 570018, India
E-mail: shruthinieit@gmail.com
ORCID iD: https://orcid.org/0000-0003-2643-888X

Darshini Y
Department of Information Science & engineering, The National Institute of Engineering, Mysuru, 570018, India
E-mail: darshinigowda09@gmail.com
ORCID iD: https://orcid.org/0009-0008-5769-6092

Manasa K B
Department of Information Science & engineering, The National Institute of Engineering, Mysuru, 570018, India
E-mail: manasakb@nieit.ac.in
ORCID iD: https://orcid.org/0000-0002-5128-1581

Received: 16 August, 2023; Revised: 30 September, 2023; Accepted: 15 October, 2023; Published: 08 February, 2024

Abstract: Researchers have developed an innovative approach to ensure seamless connectivity in ubiquitous networks with limited or irregular network coverage. The proposed method leverages advanced network technologies and protocols to seamlessly establish and maintain network connections across various environments. It integrates multiple wireless communication technologies and dynamic network selection algorithms, overcoming issues like poor reliability, limited scalability, and security problems. Compared to existing solutions, the method exhibits improved connection

handover efficiency, network throughput, and end-to-end delay. Considering user mobility, network availability, and quality of service needs, it makes informed decisions about the most suitable network connections. The proposed method is expected to significantly impact the development of future ubiquitous networking solutions.

Index Terms: Ubiquitous Network, reliability, Handover Efficiency, Throughput, Sidechaining.

1. Introduction

With the increasing need for anytime, anywhere network access, ubiquitous networking has become crucial for various applications and services. Seamless connectivity is a critical component of ubiquitous networking, ensuring transparent and uninterrupted establishment and maintenance of network connections. This feature is particularly vital for applications requiring reliable and nonstop network connectivity, including telemedicine, online gaming, voice communication, video communication, and many more. Because the network environment in ubiquitous networks is so dynamic and diverse, ensuring seamless connectivity can be difficult. Users are continuously moving around and switching between different devices, and network connections' accessibility and quality can change greatly. This creates an extreme need for innovative methods to overcome these challenges and provide seamless connectivity in ubiquitous networks.

Seamless connectivity in ubiquitous networking is provided by considering the user's mobility, network availability, and quality of service requirements to make intelligent decisions about network connections. The assessment outcomes reveal substantial enhancements in the quality of uninterrupted connectivity for users of ubiquitous networks. The implication of this paper is on the development of next-generation ubiquitous networks and the delivery of seamless connectivity is also discussed. It can be done based on the integration of multiple network technologies and protocols, such as Wi-Fi, cellular, and satellite networks. The method can use a combination of network selection algorithms, network handoff mechanisms, and network monitoring techniques to ensure that network connections are established and maintained seamlessly and transparently.

Researchers working to solve this problem face formidable obstacles as an outcome of the sharp rise in demand for continuous connectivity in ubiquitous networks without break. This paper proposes a novel method that aims to provide seamless connectivity in environments with limited or inconsistent network coverage. The proposed work leverages advances in network technologies and protocols to ensure that network connections are established and maintained seamlessly and transparently with reliability, regardless of the user's location or device.

The proposed approach incorporates multiple wireless communication technologies and dynamic network selection algorithms, aimed at mitigating issues related to poor dependability, limited scalability, and security concerns that arise during integration. To enhance seamless and efficient network selection, this approach considers critical elements like user mobility, network accessibility, and quality of service prerequisites. It enables well-informed decisions regarding the optimal network connections to establish and uphold. Based on simulation results, the proposed method outperforms existing solutions in terms of connection stability, network throughput, and end-to-end delay. Extensive testing of the approach across various ubiquitous network scenarios demonstrates considerable enhancements in energy efficiency, throughput, delay reduction, and packet delivery ratio when compared to existing models.

For enhanced network security, the presented study incorporates a sidechaining model, mitigating attack vulnerabilities during inter-node communications. This model ensures robust distributed computing with attributes like immutability and traceability, all the while upholding the network's quality of service. The potential influence of this research on forthcoming ubiquitous networking solutions is considerable, paving the way for seamless connectivity across diverse user environments.

Our paper makes the following significant contributions:

1) Our paper mainly focuses at providing seamless connectivity in ubiquitous network architecture by improving connection stability, network throughput, and end-to-end delay.

2) We perform a network simulation through Network Simulator 2 (NS2), encompassing a thorough assessment of diverse parameters. These parameters encompass end-to-end delay, the Received Signal Strength Indicator (RSSI), movement patterns, and more.

3) Finally, we propose a novel approach to improve the security of network by adopting a sidechain model which focus on delivering imutability, tracebility, high-performance & distributed computing

The outline of this paper is as follows: Section 2 covers the review of literature. Section 3 discusses on the methodology along with experimental design. Section 4 highlights on results and discussion by emphasizing on performance of securities for different kernels in presence of network attacks. At last, the conclusion of this paper is discussed in Section 5.

2. Review of Previous Studies

With advancements in wireless networks, it is crucial to design effective mechanisms for network handoffs. Numerous works have been undertaken on handoffs for similar network scenarios. The 5th Generation(5G) and Beyond 5th Generation(B5G) networks not only support such changes but also offer high-reliability connectivity and massive data exchange. Next-generation networking technologies are a key enabler for 5G, with the Information-Centric Network (ICN) being a promising part of this ecosystem. The ICN is the future network architecture, aims to address issues in the current host-centric model, and natively supports several features like abstraction content naming and transparent in-network content caching, improving network performance, reducing traffic, and lowering latency. The authors in [1] provide a potential roadmap by introducing different next-generation active technologies, including Mobile-Edge Computing (MEC), Software-Defined Networking (SDN), and Network Function Virtualization (NFV), to enable the big picture of 5G. They present a comprehensive review of recent content naming schemes and in-network content caching solutions, classified based on the used technologies and working principles. Finally, research challenges are highlighted, and promising directions for the research community are proposed.

Most Named Data Networking (NDN)-based frameworks focus on enabling users in a censoring network to access data available outside the network but do not consider how data producers in a censoring network can make their data available to users outside of the network. This challenge is particularly difficult, as NDN communication paths are symmetric, and producers must sign the data they generate and identify their certificates. In a previous study [2], the authors introduced Harpocrates, a framework built on the NDN architecture, designed to enable anonymous data publication in the presence of censorship. Harpocrates offers a solution for content producers operating within censoring networks, allowing them to share data with users outside these networks while maintaining their anonymity from the censoring authorities. Through extensive evaluation, the effectiveness of Harpocrates in achieving anonymous data publication under various censoring conditions was demonstrated, showcasing its ability to detect and adapt to different forms of censorship.

Fog computing is an advanced technique that aims to improve the Quality of Service (QoS) and reduce latency I the network and energy consumption for Internet-of-Things (IoT) devices. In a prior study [3], researchers introduce a resource allocation strategy prioritizing QoS. This scheme aims to reduce overhead within the fog computing network, encompassing task processing delay and energy consumption. Moreover, it ensures the fulfillment of varied QoS demands for distinct types of IoT devices. The proposed scheme jointly considers the association between Fog Nodes (FNs) and IoT devices, transmission, and computing resource allocation to optimize the offloading decisions while minimizing the network overhead. To achieve this, an analytic hierarchy process-based evaluation framework is first established to find the preference of QoS parameters and the priority of different types of IoT tasks. Then, a Resource Block (RB) allocation algorithm is introduced to allocate RBs to IoT devices based on their priority, satisfaction degree, and quality of RBs. Additionally, a QoS-aware bilateral matching game is introduced to optimize the association between FNs and IoT devices. Finally, the offloading decisions are based on the previous steps to minimize the network overhead to improve the RB utilization and reduce the network overhead.

In a recent study [4], a novel approach was introduced to address the challenge of jointly optimizing bandwidth resource allocation and task offloading scheduling in a 5G network with multiple edge servers within an edge cloud. The proposed strategy aims to improve task computation efficiency by dynamically managing network resources in real-time. The approach consists of two consecutive phases that work together to achieve the desired optimization. Extensive simulations were conducted to evaluate the efficiency of the proposed algorithm, and the results indicate significant improvements in task offloading utility and enhanced utilization of network symbol resources. A novel Delay-aware Content Caching (DCC) algorithm is proposed for the Internet of Vehicles (IoV)[5]. The algorithm comprises three key components: vehicle associations, content caching, and precaching decisions optimization. To optimize vehicle associations, a delay-aware vehicle associations (DVAs) algorithm is proposed at the beginning. The optimization of content caching decisions in two network scenarios is conducted depending on the vehicle associations results, taking into consideration the existance of handover vehicles. To evaluate the performance of the DCC algorithm, simulations are carried out in a realistic scenario of Shanghai with traffic flow that varies over time. The obtained results validate the efficiency of the proposed algorithm.

Assessing the Quality of Experience (QoE) of a satellite constellation can be a difficult task due to the diverse needs of users and the limited resources available. To address this challenge, [6] put forward a satellite constellation design approach that takes QoE into account, to improve user satisfaction through the inclusion of QoE factors.

The diversity of user demands and satellite resource poses a great challenge in evaluating the QoE of the satellite constellation. In their study [6], the authors present a satellite constellation design scheme that prioritizes QoE factors in order to improve user satisfaction. The scheme aims to construct a satellite constellation that is specifically optimized for enhancing QoE.

In their study [7], the researchers perform an extensive examination of the most recent methods suggested for reducing communication overhead between control and data planes. They also aim to improve the scalability of the OpenFlow-SDN framework within the context of a logically centralized distributed SDN control plane architecture. The survey mainly focuses on four issues, including logically centralized visibility, link-state discovery, flow rules

placement, and controllers' load balancing. In addition to this, a discussion is done on each issue, and presented an updated and detailed study of existing solutions and limitations in enhancing the OpenFlow-SDN scalability and performance. The authors also outline the potential challenges that need to be addressed further in obtaining adaptive and scalable OpenFlow-SDN flow control.

This algorithm in [8] introduces an energy-efficient clustering and hierarchical routing algorithm named energy-efficient scalable routing algorithm (EESRA). The objective of the algorithm is to extend the network lifespan despite an increase in network size. The proposed algorithm employs a hierarchical three-layer structure to minimize the load on cluster heads and introduce randomness in their selection process. Additionally, the algorithm utilizes multi-hop transmissions for intra-cluster communication, effectively implementing a hybrid Medium Access Control (MAC) protocol for Wireless Sensor Networks (WSNs). Comparative analysis against other WSN routing protocols demonstrates that the algorithm, referred to as EESRA, achieves superior network performance, particularly in relation to changes in network size. Simulation results highlight EESRA's advantages over benchmarked protocols, specifically in terms of load balancing and energy efficiency, particularly in large-scale WSN deployments.

3. Methodology/Experimental Design

Researchers in [9] focused on Mobile Wireless Networks (MWNs) composed of nodes exhibiting diverse movement patterns. Analyzing these patterns for accurate movement prediction is crucial for facilitating smooth handoffs. The presence of differing node-to-node communication interfaces escalates the intricacy within heterogeneous MWNs compared to their homogeneous counterparts. This intricacy manifests across various aspects like assessing node metrics, appraising node-to-node link levels, accommodating network fluctuations, and more. Consequently, this contributes to the intricacies of handoff decision-making, ultimately leading to compromised network performance and affecting the quality of communication service.

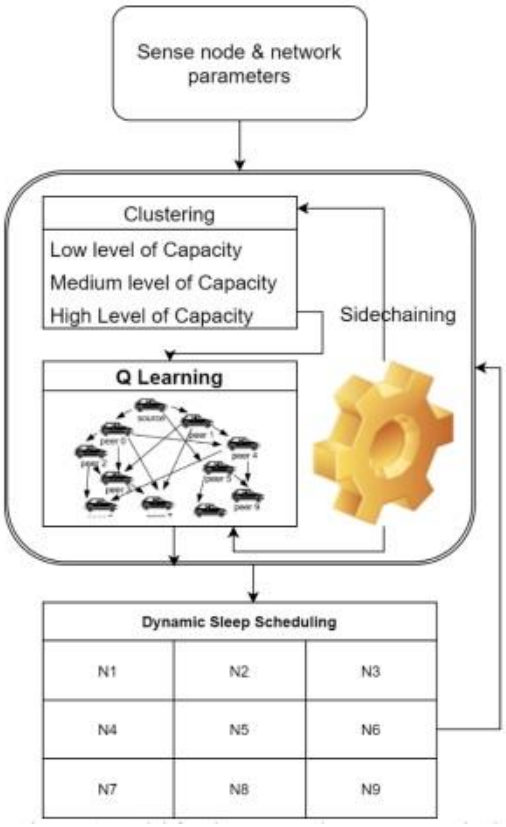

Fig.1. Model for the proposed NLADSS method

The Node-Level Augmentation & Dynamic Sleep Scheduling (NLADSS) concept is introduced by the researchers in [10]. To address the challenges posed by highly dynamic environments, they propose efficient handover models that take into account multiple network-level parameters such as trust levels, capacity, QoS, and more, as elaborated in the preceding section. Additionally, these algorithms assess various node-level metrics like end-to-end delay, RSSI, movement pattern, and others to appropriately associate nodes with relevant networks. However, these methods face limitations when dealing with high-speed environments, potentially leading to QoS degradation. Furthermore, most of these models overlook node-level enhancements, constraining their effectiveness in real-world scenarios. Refer to Fig.1. for a visualization of handoff decision-making models involving dynamic sleep scheduling, sidechaining, Q-learning,

and clustering. Detailed descriptions of each block are provided in subsequent subsections, aiding readers and network designers in implementing them for their specific network setups.

To address these limitations, the researchers introduce an innovative approach known as the Connectivity as a Service (CaaS) model in their work [15]. This model employs node-level augmentation and dynamic sleep scheduling techniques to achieve efficient handoffs within heterogeneous wireless networks. Additionally, the study presents a novel sidechain model that focuses on bolstering security by mitigating the potential for attacks during inter-node communications. The primary goal of this sidechain model is to establish resilient distributed computing with exceptional performance, all the while ensuring immutability and traceability. Importantly, these enhancements are achieved without compromising the QoS provided by the network.

The formula to calculate Node-Level Augmentation(NLA) should capture the evaluation of node-level metrics and their integration into the network selection algorithm.

$$NLA = f(D_e, RSSI, MP, ...) \tag{1}$$

Where, NLA represents the process of node-level augmentation. NLA refers to the inclusion and evaluation of specific metrics and characteristics of individual network nodes to enhance network performance and decision-making.

NLA represents the augmented information or enhanced attributes associated with each network node. It captures the additional knowledge or metrics obtained through the node-level augmentation process. The function denoted as f() represents the specific function or algorithm employed to amalgamate and process the given input variables. End-to-end Delay (De) gauges the time elapsed for data to traverse from its source node to the intended destination node, encapsulating all delays encountered throughout its route. This metric effectively encapsulates the latency or delay encountered by the network node during communication processes. The RSSI serves as a quantifiable measure of the potency or intensity of the signal received at a designated node. It furnishes insights into signal quality and facilitates the evaluation of the node's proximity to neighboring or source nodes. Movement Pattern (MP) characterizes the distinctive pattern or manner in which a node traverses within the network. This pattern can encompass variables such as speed, direction, acceleration, or even alterations in location. The movement pattern significantly influences aspects like network connectivity, decisions regarding handoffs, and the overall performance of the network.

By considering these parameters, among potentially others, the node-level augmentation process aims to enrich the information available for each node. This augmented information can then be utilized in network selection algorithms, handoff decisions, and other decision-making processes to improve network efficiency, reliability, and quality of service.

The algorithm to calculate Node_Level_Augmentation := $f(D_e, RSSI, MP, ...)$

1. *Input: End-to-end Delay, RSSI, Movement Pattern, ...*
2. *Initialize NLA as an empty set.*
3. *For each network node:*
   - *Calculate the augmented attributes or metrics based on the provided inputs.*
   - *Incorporate additional relevant information, such as node-specific characteristics, network conditions, or contextual factors.*
   - *Perform any necessary computations, transformations, or feature engineering steps.*
4. *Store the augmented attributes in NLA set, associating them with the corresponding network nodes.*
5. *Output: NLA containing the enhanced information for each network node.*

The specific details of the algorithm, such as the computations and transformations performed in Step 3, would depend on the research objectives, the nature of the network, and the desired enhancements. The algorithm can be customized and extended to include additional steps or processes as needed for the node-level augmentation.

To assess the QoS performance of your proposed method, a formula is designed, that quantifies the overall QoS metric based on different parameters as shown in (2). This formula capture the weighted combination of relevant QoS parameters.

$$QoS = w1 * D + w2 * T + w3 * J + ... \tag{2}$$

where, QoS embodies an evaluation of the comprehensive effectiveness and dependability of a network or system. This assessment formula harmonizes a spectrum of quality metrics, encompassing Delay (D), Throughput (T), Jitter (J), and conceivably additional relevant factors. This amalgamated approach yields an aggregated QoS appraisal. Delay represents the temporal interval essential for data packets to navigate from their origin to a designated terminus. This metric's significance lies in its impact on the swiftness and punctuality of network communications. Diminished delay values generally correspond to heightened operational efficiency. Throughput gauges the data volume that a network can proficiently convey over a specific span. This measurement exemplifies the network's capacity and adeptness in handling data flow. Augmented throughput values correlate with superior network efficiency. Jitter characterizes the

diversity in packet delivery delays. It quantifies the irregularity or fluctuation in the timing of packet arrivals. Reduced jitter values delineate a network that demonstrates enhanced steadiness and an augmented level of predictability. *w1, w2, w3, etc.* represent weighting factors assigned to each quality metric, indicating their relative importance or priority in determining the overall QoS. The values of these weights can be adjusted based on specific requirements or preferences.By multiplying each quality metric by its corresponding weight and summing them together, the formula calculates a composite QoS score. The weights (w1, w2, w3, etc.) allow customization of the formula based on the specific needs and priorities of the network or system being evaluated. For example, if low delay is critical, a higher weight can be assigned to the Delay term in the formula.

The resulting QoS value provides a single numerical representation of the overall quality and performance of the network, considering multiple factors simultaneously. It enables researchers or network administrators to compare and evaluate different systems or configurations based on their QoS scores and make informed decisions for optimization and improvement.

3.1. Working of Sidechain

Sidechains, as detailed in [16], introduce inventive frameworks that facilitate the secure utilization of tokens and digital assets from one blockchain within a distinct blockchain. This process enables the subsequent return of these assets to the original blockchain as required. The introduction of such mechanisms holds considerable promise in bolstering the functionalities of established blockchain systems. A sidechain is essentially an independent blockchain network, which establishes a connection to another blockchain termed the parent blockchain or mainnet. This connection is established through a two-way peg mechanism, as visually depicted in Fig.2.

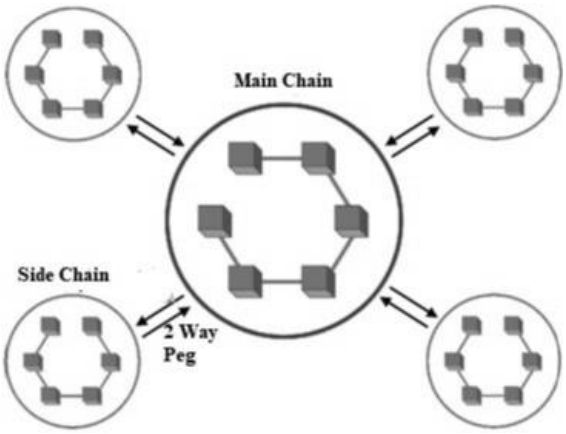

Fig.2. Working of sidechain

These secondary blockchains [17] operate with their individual consensus protocols. These protocols serve to enhance privacy and security within a blockchain network, thereby diminishing the additional trust needed to sustain the network's operations. An essential characteristic of sidechains is their capability to enable seamless asset exchange between the mainnet and the secondary blockchain. This means that digital assets such as tokens can be securely transferred between blockchains, enabling projects to expand their ecosystem in a decentralized manner. In practice, a user on the Bitcoin mainnet must send bitcoin to an output address, which could be a hard wallet, a hot wallet, or a sidechain. After a transaction is verified, a notification of the finalized transaction is disseminated throughout Bitcoin's network.

3.1.1 Federations

A federation[18] is a collection of entities that serve as an intermediary between a parent blockchain and one of its sidechains. The main responsibility of this group is to regulate when the tokens used by a user are locked up and released. The creators of the sidechain have the authority to select the members of the federation, but this structure can pose a potential issue since it adds another layer of complexity between the parent chain and the sidechain. The presence of a federation can create additional coordination and governance challenges, and can also potentially introduce points of failure or security vulnerabilities. Despite these challenges, however, a federation can also offer benefits such as increased flexibility, interoperability, and scalability to blockchain systems[19].

3.1.2 Security

Individuals bear the responsibility of safeguarding their respective Sidechains. Inadequate security measures could render a Sidechain vulnerable to potential attacks. Given the independent nature of each Sidechain, any repercussions stemming from a security breach will remain confined to the specific chain in question. The overarching parent chain

remains unaffected by such incidents. Equally, if the parent chain is compromised, it may still be operational, but the peg will lose a significant portion of its value. Sidechains require specific miners, who can be obtained through "fused mining," which involves the simultaneous mining of two separate cryptocurrencies based on the same algorithm[20].

If you are discussing the security aspect of the sidechain model, you can introduce a formula that represents the security level or risk assessment. This formula should consider various factors, such as the probability of attacks and the effectiveness of security measures. For example:

$$SC_{Security} = h\left(P_{Attacks}, E_{Security\_Measures}, ...\right) \quad (3)$$

where, $SC_{Security}$ represents the level of security provided by a sidechain in a blockchain network. The formula combines various factors related to security to assess the overall security level of the sidechain. $P_{Attacks}$ represents the likelihood or chance of security breaches or malicious attacks occurring on the sidechain. It takes into account factors such as the vulnerability of the network, the sophistication of potential attackers, and the presence of security vulnerabilities. A lower probability of attacks implies a more secure environment. $E_{Security\_Measures}$ refers to the capability of the security measures implemented in the sidechain to mitigate or prevent attacks. The evaluation encompasses the efficacy and dependability of the established security measures, encompassing encryption, authentication protocols, access controls, and surveillance systems. Enhanced efficacy ratings signify robust security provisions. The symbol "h" embodies the function that unites attack probability, security measure effectiveness, and conceivably other elements to ascertain the comprehensive security level of the sidechain. The precise structure of the function "h" may fluctuate in accordance with the contextual specifics and the particular prerequisites of the sidechain..

The formula enables the assessment and quantification of the security level provided by the sidechain. By applying the function h to the relevant factors, it produces a single numerical value that represents the overall security of the sidechain. This value allows for comparison and evaluation of different sidechains in terms of their security capabilities.

Employing DSS, Q-learning, and capacity-based grouping has yielded enhancements in the QoS during handoffs. QoS evaluation involves scrutinizing parameters like end-to-end delay [21], energy consumption [22], throughput [23], jitter [24], and handoff efficiency [25]. Furthermore, the integration of sidechaining reinforces the model's resilience against diverse attacks, encompassing Masquerading, Sybil, and DDoS. Consequently, this section undertakes a comparative analysis of QoS performance between the proposed approach and preceding research [11, 12, 13], spanning both attack and non-attack scenarios. To ensure consistency in the evaluation, all configurations were tested under the same network simulation settings as specified in Table 1 below.

Table 1. Network and node configurations

Parameter	Configured value
MAC Version	802.16
Propagation Model	Two Ray Ground
Routing Protocol	DSDV
Antenna Model	Omnidirectional
Interface queue (IFQ) type	Drop Tail & Priority Queue
Network dimensions	0.4 km x 0.4 km
Number of vehicles	50 to 1000
Vehicle power consumption during transmission	4mW
Vehicle power consumption during sleep mode	0.002mW
Vehicle power consumption during idle mode	2mW
Delay required for this transition	0.01 s
Vehicle power consumption during data reception	2mW
Residual energy for each vehicle (initially)	2000 mW
Vehicle power required during transition from sleep to wakeup mode	0.1mW

In the simulation, the No. of handoffs and communication requests was systematically increased from 20 to 200 using the specified configuration. Stochastic modeling was used and nodes were randomly selected for routing. The likelihood of Masquerading, Sybil, and DDoS attacks altered from 1% to 20%. The QoS parameters were assessed before and after the attacks and matched against previous studies [11, 12, 13].

It was found that the suggested model was able to restore these parameters to their original values even after an attack, demonstrating its resilience to such attacks. Section 4.1 outlines the assessment of the proposed approach's performance in the face of different attack types. This presentation aims to validate the research and contribute to the comprehensive evaluation of the NLADSS model within a spectrum of network conditions.

4. Results and Discussion

The outcomes are derived via the establishment of a wireless network through simulation conducted using NS2. In accordance with established standards [26], the configurations underwent rigorous testing within the network simulation conditions detailed in the preceding Table 1. The assessment encompasses prevalent attack variants, including the Sybil attack, masquerading attack, and DDoS attack scenarios.

4.1. Security performance of different kernels in presence of network attacks

The NLADSS model stands out for its exceptional QoS performance, outperforming established models ([11, 12, 13]) in diverse attack scenarios due to its incorporation of a sidechaining model. The evaluation of QoS involved a systematic approach: varying the Number of Attacker nodes (NA) from 1% to 20% and meticulously analyzing the resulting QoS values. To ensure a comprehensive assessment, the NLADSS model was deployed across each scenario, allowing for the calculation of average QoS parameters. This meticulous process facilitated a nuanced estimation of the NLADSS model's performance, enabling a direct, substantive comparison against existing models. Within Table 2, the tabulated end-to-end delay (D) values for different protocols during a Masquerading attack offer a clear demonstration of the NLADSS model's effectiveness. This detailed evaluation strategy illuminates the model's robustness and its ability to maintain good QoS standards even during various attacks.

4.2. Model Enhancements for Stability and Security

The NLADSS model integrates several key methodologies to ensure stability, security, and optimized performance within vehicular network environments. Notably, the model employs specific techniques across various domains:

4.2.1. Weight Initialization Schemes

Initial weights play a crucial role in neural network convergence. The NLADSS model adopts the Xavier/Glorot initialization scheme [27], strategically initializing weights to maintain gradient scale uniformity across layers and enhance training efficiency, thereby avoiding issues related to vanishing or exploding gradients.

4.2.2. Regularization Techniques

To curb overfitting and enhance generalization, regularization techniques are pivotal. In this context, the NLADSS model utilizes L2 regularization [28] in its neural network layers. This regularization approach penalizes large weights, fostering better model generalization and stability in the face of varying network conditions.

4.2.3. Optimization Algorithms

Efficient training of the NLADSS model relies on optimized optimization algorithms. Employing the Adam optimizer [29], the model dynamically adjusts learning rates for each parameter, expediting convergence and mitigating the risk of getting trapped in local minima during training.

4.2.4. Constraints for Stability and Security

Ensuring stability and security in the NLADSS model involves specific constraints embedded within the model architecture. Weight clipping constraints are imposed [30], restricting weight values within defined bounds during training, thus preventing undesirable weight magnitudes that might destabilize the model. Additionally, encryption-based techniques [31] are incorporated to secure sensitive data transmission within the vehicular network, augmenting the model's resilience against potential security breaches.

Table 2. Average end-to-end delay for different models (Masquerading Attack)

Type of Attack Masq.				
NA (%)	D (ms) [11]	D (ms) [12]	D (ms) [13]	D (ms) Proposed
1	0.66	0.77	0.73	0.63
2	0.72	0.84	0.79	0.69
3	0.78	0.89	0.83	0.73
4	0.81	0.92	0.87	0.76
5	0.85	0.98	0.92	0.81
6	0.91	1.05	1.01	0.87
7	0.98	1.20	1.19	0.99
8	1.17	1.52	1.51	1.24
9	1.36	1.74	1.72	1.41
10	1.57	1.97	1.90	1.59
11	1.79	2.11	2.02	1.74
12	1.98	2.27	2.15	1.88
13	2.04	2.36	2.24	1.95
14	2.11	2.45	2.34	2.02
15	2.20	2.59	2.49	2.13
16	2.30	2.73	2.62	2.25
17	2.62	3.11	2.97	2.55
18	2.98	3.47	3.31	2.86
19	3.26	3.85	3.65	3.16
20	3.67	4.19	3.95	3.47

The integration of the proposed NLADSS model leads to a notable 5% reduction in end-to-end delay within the context of a Masquerading attack. Comparable delay outcomes are achieved across various Sybil attacker scenarios, as evidenced by the data presented in Table 3,

Table 3. Average end-to-end delay for different models (Sybil Attack)

Type of Attack Sybil				
NA (%)	D (ms) [11]	D (ms) [12]	D (ms) [13]	D (ms) Proposed
1	0.76	0.88	0.84	0.73
2	0.83	0.96	0.91	0.79
3	0.90	1.02	0.96	0.85
4	0.94	1.07	1.00	0.88
5	0.98	1.13	1.06	0.93
6	1.04	1.21	1.16	1.00
7	1.13	1.38	1.37	1.14
8	1.34	1.75	1.74	1.42
9	1.57	2.01	1.96	1.62
10	1.81	2.27	2.19	1.84
11	2.04	2.44	2.33	2.01
12	2.27	2.61	2.47	2.16
13	2.35	2.71	2.57	2.24
14	2.43	2.81	2.68	2.33
15	2.54	2.97	2.85	2.45
16	2.63	3.14	3.02	2.58
17	3.02	3.58	3.42	2.94
18	3.43	3.98	3.80	3.30
19	3.74	4.43	4.20	3.63
20	4.23	4.81	4.54	3.99

Incorporating the proposed NLADSS model resulted in a 6% reduction in delay. This delay is further estimated for DDoS attack and can be observed from Table 4 as follows,

Table 4. Average end-to-end delay for different models (DDoS Attack)

Type of Attack DDoS				
NA (%)	D (ms) [11]	D (ms) [12]	D (ms) [13]	D (ms) Proposed
1	0.65	0.75	0.71	0.62
2	0.70	0.82	0.77	0.67
3	0.77	0.87	0.81	0.72
4	0.79	0.90	0.85	0.75
5	0.83	0.96	0.90	0.79
6	0.89	1.03	0.99	0.85
7	0.96	1.17	1.16	0.97
8	1.14	1.49	1.49	1.21
9	1.33	1.71	1.70	1.38
10	1.53	1.93	1.86	1.56
11	1.73	2.07	1.98	1.69
12	1.93	2.22	2.10	1.83
13	1.99	2.30	2.19	1.90
14	2.06	2.39	2.29	1.98
15	2.15	2.53	2.42	1.99
16	2.25	2.67	2.56	2.20
17	2.56	3.04	2.90	2.50
18	2.91	3.39	3.23	2.80
19	3.18	3.76	3.56	3.09
20	3.59	4.09	3.86	3.40

Table 5. Average energy consumption for different methods (Masquerading attack)

Type of Attack Masq.				
NA (%)	E (mJ) [11]	E (mJ) [12]	E (mJ) [13]	E (mJ) Proposed
1	1.69	2.12	2.03	1.55
2	2.12	2.40	2.26	1.80
3	2.20	2.51	2.37	1.88
4	2.33	2.66	2.50	1.99
5	2.47	2.83	2.65	2.11
6	2.62	2.97	2.78	2.23
7	2.72	3.09	2.89	2.32
8	2.83	3.21	3.01	2.41
9	2.87	3.27	3.07	2.45
10	2.94	3.34	3.14	2.50
11	3.01	3.43	3.23	3.55
12	3.07	3.52	3.33	2.63
13	3.17	3.67	3.44	2.74
14	3.27	3.79	3.57	2.82
15	3.46	3.89	3.65	2.91
16	3.56	4.01	3.71	3.00
17	3.65	4.01	3.67	3.01
18	3.56	3.85	3.36	2.86
19	3.37	2.98	2.83	2.44
20	3.24	3.26	3.32	2.01

The data demonstrates an appreciable 8% reduction in delay attributed to the integration of the proposed NLADSS model. This delay reduction is attributed to the utilization of the sidechain model, which contributes to the detection of even the most minimal attack probabilities within the network. Analogous findings are noted in terms of energy performance, as exemplified by the Masquerading attack data in Table 5,

The results indicate a substantial 28% reduction in energy consumption attributed to the integration of the proposed NLADSS model. This pronounced reduction is a direct outcome of the model's implementation. Comparable energy performance enhancements are witnessed in the context of Sybil attacks, as corroborated by the data presented in Table 6,

Table 6. Average energy consumption for different methods (Sybil attack)

Type of Attack Sybil				
NA (%)	E (mJ) [11]	E (mJ) [12]	E (mJ) [13]	E (mJ) Proposed
1	1.95	2.44	2.34	1.78
2	2.44	2.76	2.59	2.07
3	2.53	2.89	2.72	2.17
4	2.68	3.06	2.88	2.29
5	2.83	3.26	3.06	2.43
6	3.02	3.42	3.20	2.56
7	3.14	3.55	3.33	2.66
8	3.26	3.69	3.46	2.76
9	3.31	3.77	3.54	2.82
10	3.39	3.84	3.61	2.88
11	3.46	3.94	3.71	2.95
12	3.52	4.05	3.83	3.03
13	3.64	4.18	3.97	3.14
14	3.76	4.37	4.11	3.25
15	3.89	4.48	4.18	3.35
16	4.09	4.60	4.27	3.45
17	4.20	4.61	4.23	3.47
18	4.10	4.43	3.86	3.29
19	3.88	3.43	3.26	2.80
20	4.08	3.74	3.81	2.61

The data illustrates a significant 24% decrease in energy consumption attributed to the integration of the proposed NLADSS model. This pronounced energy efficiency improvement is a direct result of the model's implementation. The assessment of energy consumption extends to scenarios involving DDoS attacks, as evidenced by the data presented in Table 7,

Table 7. Average energy consumption for different methods (DDoS attack)

Type Of Attack DDoS				
NA (%)	E (mJ) [11]	E (mJ) [12]	E (mJ) [13]	E (mJ) Proposed
1	1.65	2.07	1.99	1.51
2	2.07	2.35	2.20	1.76
3	2.15	2.47	2.32	1.84
4	2.28	2.60	2.46	1.95
5	2.41	2.76	2.59	2.06
6	2.56	2.91	2.72	2.18
7	2.66	3.02	2.83	2.26
8	2.77	3.14	2.94	2.35
9	2.83	3.21	2.99	2.40
10	2.88	3.27	3.07	2.45
11	2.94	3.35	3.17	2.52
12	3.00	3.45	3.26	2.57
13	3.10	3.52	3.31	2.64
14	3.20	3.71	3.48	2.76
15	3.34	3.81	3.51	2.83
16	3.47	3.92	3.63	2.93
17	3.57	3.92	3.59	2.94
18	3.48	3.76	3.28	2.79
19	3.30	2.91	2.77	2.39
20	3.47	3.18	3.25	2.23

The data showcases a notable 28% reduction in energy consumption attributed to the integration of the proposed NLADSS model. This energy efficiency enhancement can be attributed to the utilization of clustering and sidechaining techniques, which contribute to the design of low-power networks. A parallel pattern of observations is evident in terms of throughput performance, where this performance is averaged across all attacks. This comprehensive throughput performance is readily available in Table 8,

Table 8. Average throughput performance for different models (averaged between Masquerading, Sybil and DDoS attacks)

Avg. of Masq. Sybil DDoS				
NA (%)	T (kbps) [11]	T (kbps) [12]	T (kbps) [13]	T (kbps) Proposed
1	232.2	259.6	241.2	272.6
2	235.1	261.8	243.1	275.2
3	236.2	263.4	244.7	276.8
4	238.0	265.8	246.9	279.2
5	240.4	268.2	249.2	281.8
6	242.4	270.5	251.3	284.2
7	244.5	272.8	253.4	286.6
8	246.5	275.0	255.4	288.9
9	247.4	276.1	256.4	289.8
10	248.5	277.3	257.5	291.3
11	249.5	278.4	258.2	292.5
12	250.6	279.5	259.6	293.7
13	251.6	280.4	258.8	294.8
14	252.6	281.8	261.7	296.1
15	253.5	283.1	262.7	297.2
16	254.6	284.1	263.8	298.4
17	256.7	286.3	265.9	300.8
18	258.7	288.6	266.3	302.6
19	260.8	283.9	227.8	287.3
20	262.8	286.2	229.1	293.0

The data distinctly reveals a noteworthy 15% enhancement in throughput stemming from the integration of the proposed NLADSS model. This throughput improvement is a direct outcome of incorporating high-speed sidechaining and clustering procedures, which collectively reduce overheads and facilitate low-latency operations. Corresponding trends are evident in the context of handoff efficiency (Eff.) performance. This performance is averaged across the spectrum of Masquerading, Sybil, and DDoS attacks, as evidenced in the data presented in Table 9,

Table 9. The handover efficiency performance is averaged across various models, encompassing Masquerading, Sybil, and DDoS attacks.

Avg. Of Masq. Sybil DDoS				
NA (%)	Eff. (%) [11]	Eff. (%) [12]	Eff. (%) [13]	Eff. (%) Proposed
1	75.0	70.1	76.9	87.7
2	76.4	70.8	77.8	88.4
3	76.7	71.2	78.1	88.9
4	77.0	71.8	78.7	89.7
5	78.0	72.5	79.6	90.6
6	78.6	73.1	80.2	91.3
7	79.3	73.7	80.9	92.1
8	79.9	74.3	81.6	92.9
9	80.3	74.5	81.9	93.4
10	80.6	74.9	82.2	93.6
11	80.9	75.2	82.5	93.9
12	81.2	75.5	82.9	94.4
13	81.6	75.7	83.2	94.7
14	82.0	76.1	83.5	95.1
15	82.3	76.3	83.8	95.4
16	82.6	76.7	84.2	95.9
17	83.3	77.3	85.0	96.7
18	83.9	78.0	85.6	97.4
19	84.6	78.6	86.3	98.2
20	85.3	79.2	86.9	99.0

It is evident that the inclusion of the proposed NLADSS model results in a notable 15% enhancement in handoff efficiency. This improvement can be attributed to the integration of DSS and Q-Learning mechanisms, which mitigate request drops to a minimum and optimize efficiency. The observed outcomes affirm the superiority of the proposed model in terms of handoff efficiency and overall QoS performance, irrespective of attack presence. This broad applicability renders the proposed model suitable for diverse vehicular network scenarios.

5. Conclusion

The integration of weight initialization schemes, regularization techniques, optimization algorithms, and specific constraints within the NLADSS model demonstrates its robustness, adaptability, and superior performance in vehicular network environments. These enhancements not only ensure model stability and security but also significantly elevate the model's overall efficiency, making it an exemplary solution for addressing security challenges in dynamic network scenarios. The functionality of Q-Learning hinges on a reward mechanism, which aids in selecting the most optimal node partner for any given node. This synergy with dynamic sleep scheduling and hierarchical clustering contributes to

an overall enhancement in handover performance. However, this performance is susceptible to security vulnerabilities stemming from the use of dynamic partner nodes. To fortify the overall security posture, this study introduces a novel machine learning sidechaining model. The culmination of these models equips the foundational system model with the capacity to reduce end-to-end delay by 8% to 15%, contingent on network configuration. Additionally, energy consumption drops by over 14% when compared against [7, 12, 18], thereby signifying an extended network lifespan. Furthermore, this model surpasses existing methodologies in terms of throughput and overall handoff efficiency, primarily attributable to the amalgamation of DSS, Q-Learning, and dynamic clustering strategies. The model's applicability extends to lowering the likelihood of network attacks through the inclusion of sidechain-based data storage and communication capabilities. The model's performance can be enhanced further by exploring novel blockchain consensus models characterized by lower complexity. Moreover, fine-tuning the machine learning process through hyperparameter tuning holds the potential to further refine its efficacy.

References

[1] Serhane, Oussama, Khadidja Yahyaoui, Boubakr Nour, and Hassine Moungla. "A survey of ICN content naming and in-network caching in 5G and beyond networks." IEEE Internet of Things Journal 8, no. 6 (2020): 4081-4104.

[2] Al Azad, Md Washik, Reza Tourani, Abderrahmen Mtibaa, and Spyridon Mastorakis. "Harpocrates: Anonymous data publication in named data networking." In Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies, pp. 79-90. 2022.

[3] Huang, Xiaoge, Yifan Cui, Qianbin Chen, and Jie Zhang. "Joint task offloading and QoS-aware resource allocation in fog-enabled Internet-of-Things networks." IEEE Internet of Things Journal 7, no. 8 (2020): 7194-7206.

[4] Zeng, Luyuan, Wushao Wen, and Chongwu Dong. "QoS-aware Task Offloading with NOMA-based Resource Allocation for Mobile Edge Computing." In WCNC, pp. 1242-1247. 2022.

[5] Sarkar, Indranil, Mainak Adhikari, Neeraj Kumar, and Sanjay Kumar. "A collaborative computational offloading strategy for latency-sensitive applications in fog networks." IEEE Internet of Things Journal 9, no. 6 (2021): 4565-4572.

[6] Dai, Cui-Qin, Mingjian Zhang, Chong Li, Jian Zhao, and Qianbin Chen. "QoE-aware intelligent satellite constellation design in satellite internet of things." IEEE Internet of Things Journal 8, no. 6 (2020): 4855-4867.

[7] Alsaeedi, Mohammed, Mohd Murtadha Mohamad, and Anas A. Al-Roubaiey. "Toward adaptive and scalable OpenFlow-SDN flow control: A survey." IEEE Access 7 (2019): 107346-107379.

[8] Elsmany, Eyman Fathelrhman Ahmed, Mohd Adib Omar, Tat-Chee Wan, and Altahir Abdalla Altahir. "EESRA: Energy efficient scalable routing algorithm for wireless sensor networks." IEEE Access 7 (2019): 96974-96983.

[9] Wang, Tianyu, Shaowei Wang, and Zhi-Hua Zhou. "Machine learning for 5G and beyond: From model-based to data-driven mobile wireless networks." China Communications 16, no. 1 (2019): 165-175.

[10] Gurumallu, Prasanna Kumar and Shankaraiah. "NLADSS: Design of Connectivity as a Service (CaaS) Model using Node-Level Augmentation & Dynamic Sleep Scheduling for Heterogeneous Wireless Network Handoffs." International Journal of Intelligent Engineering and Systems 15, no. 5 (2022): 273-283.

[11] Jadey, Sudeep, et al. "Introduction to Cyber Security." Methods, Implementation, and Application of Cyber Security Intelligence and Analytics, edited by Jena Om Prakash, et al., IGI Global, 2022, pp. 1-24. https://doi.org/10.4018/978-1-6684-3991-3.ch001.

[12] Wu, Yuansheng, Guanqun Zhao, Dadong Ni, and Junyi Du. "Dynamic handoff policy for RAN slicing by exploiting deep reinforcement learning." EURASIP Journal on Wireless Communications and Networking 2021, no. 1 (2021): 1-17.

[13] Sun, Jiani, Zhihong Qian, Xin Wang, and Xue Wang. "Es-dqn-based vertical handoff algorithm for heterogeneous wireless networks." IEEE Wireless Communications Letters 9, no. 8 (2020): 1327-1330.

[14] Wang, Weijia, and Lei Hu. "A secure and efficient handover authentication protocol for wireless networks." Sensors 14, no. 7 (2014): 11379-11394.

[15] Wang, Shumin, Honggui Deng, Rujing Xiong, Gang Liu, Yang Liu, and Hongmei Liu. "A multi-objective model-based vertical handoff algorithm for heterogeneous wireless networks." EURASIP Journal on Wireless Communications and Networking 2021, no. 1 (2021): 1-18.

[16] Yang, Yizhou, Zitong Liu, Guanxin Zhang, Xisha Zhang, and Deqing Zhang. "The effects of side chains on the charge mobilities and functionalities of semiconducting conjugated polymers beyond solubilities." Advanced Materials 31, no. 46 (2019): 1903104.

[17] Singh, Amritraj, Kelly Click, Reza M. Parizi, Qi Zhang, Ali Dehghantanha, and Kim-Kwang Raymond Choo. "Sidechain technologies in blockchain networks: An examination and state-of-the-art review." Journal of Network and Computer Applications 149 (2020): 102471.

[18] Doyle, Joseph, Muhammed Golec, and Sukhpal Singh Gill. "Blockchainbus: A lightweight framework for secure virtual machine migration in cloud federations using blockchain." Security and Privacy 5, no. 2 (2022): e197.

[19] Bouras, Mohammed Amine, Boming Xia, Adnan Omer Abuassba, Huansheng Ning, and Qinghua Lu. "IoT-CCAC: a blockchain-based consortium capability access control approach for IoT." PeerJ Computer Science 7 (2021): e455.

[20] Li, Taotao, Mingsheng Wang, Zhihong Deng, and Dongdong Liu. "Sepow: Secure and efficient proof of work sidechains." In Algorithms and Architectures for Parallel Processing: 21st International Conference, ICA3PP 2021, Virtual Event, December 3–5, 2021, Proceedings, Part III, pp. 376-396. Cham: Springer International Publishing, 2022.

[21] Letaief, Khaled B., Wei Chen, Yuanming Shi, Jun Zhang, and Ying-Jun Angela Zhang. "The roadmap to 6G: AI empowered wireless networks." IEEE communications magazine 57, no. 8 (2019): 84-90.

[22] Nurgaliyev, Madiyar, Ahmet Saymbetov, Yevhen Yashchyshyn, Nurzhigit Kuttybay, and Didar Tukymbekov. "Prediction of energy consumption for LoRa based wireless sensors network." Wireless Networks 26 (2020): 3507-3520.

[23] Ahmed, Shakil, Mostafa Zaman Chowdhury, and Yeong Min Jang. "Energy-efficient UAV-to-user scheduling to maximize throughput in wireless networks." IEEE Access 8 (2020): 21215-21225.

[24] Tardioli, Danilo, Ramviyas Parasuraman, and Petter Ögren. "Pound: A multi-master ROS node for reducing delay and jitter in wireless multi-robot networks." Robotics and Autonomous Systems 111 (2019): 73-87.
[25] Wang, Shumin, Honggui Deng, Rujing Xiong, Gang Liu, Yang Liu, and Hongmei Liu. "A multi-objective model-based vertical handoff algorithm for heterogeneous wireless networks." EURASIP Journal on Wireless Communications and Networking 2021, no. 1 (2021): 1-18.
[26] Mouaffak, Abdelhak El, and Abdelbaki El Belrhiti El Alaoui. "Considering the environment's characteristics in wireless networks simulations: case of the simulator NS2 and the WSN." International Journal of Information and Communication Technology 14, no. 4 (2019): 427-438.
[27] Glorot, Xavier, and Yoshua Bengio. "Understanding the difficulty of training deep feedforward neural networks." In Proceedings of the thirteenth international conference on artificial intelligence and statistics, pp. 249-256. JMLR Workshop and Conference Proceedings, 2010.
[28] Cortes, Corinna, Mehryar Mohri, and Afshin Rostamizadeh. "L2 regularization for learning kernels." arXiv preprint arXiv:1205.2653 (2012).
[29] Zhang, Zijun. "Improved adam optimizer for deep neural networks." In 2018 IEEE/ACM 26th international symposium on quality of service (IWQoS), pp. 1-2. Ieee, 2018.
[30] Gulrajani, Ishaan, Faruk Ahmed, Martin Arjovsky, Vincent Dumoulin, and Aaron C. Courville. "Improved training of wasserstein gans." Advances in neural information processing systems 30 (2017).
[31] Chaudhry, Shikha. "An encryption-based secure framework for data transmission in IoT." In 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), pp. 743-747. IEEE, 2018.

Authors' Profiles

Dr. Prasanna Kumar G. is an Assistant Professor in the Department of Information Science and Engineering at The National Institute of Engineering, Mysuru. He holds a B.E. in Computer Science and Engineering from Coorg Institute of Technology under Visvesvaraya Technological University. Subsequently, he pursued an M.Tech in Networking and Internet Engineering from SJCE, Mysuru, also under Visvesvaraya Technological University. Passionate about cutting-edge technologies, Dr. Prasanna Kumar earned his Ph.D. in the area of Ubiquitous Networks from SJCE, Mysuru, further cementing his expertise in this field. Throughout his academic journey, he has developed a keen interest in research areas such as Ubiquitous Networks, Sensor Networks, Internet of Things, Machine Learning, and Blockchain. Beyond his primary research interests, Dr. Prasanna Kumar actively explores and contributes to other areas of study. These include Artificial Intelligence and Data Analytics, Wireless Communication and Mobile Networks, Cloud Computing and Edge Computing, Network Security and Privacy, Cyber-Physical Systems, Smart Cities and Sustainable Technologies. With a diverse research portfolio, Dr. Prasanna Kumar continuously seeks to expand his knowledge and contribute to advancements in various technological domains. His dedication to fostering knowledge and empowering students has made him an inspiring figure within the academic community. As an esteemed faculty member, he continues to make significant contributions to research while nurturing the next generation of aspiring engineers and researchers.

Dr. Shankaraiah N received his B.E. degree in Electronics and Communication Engineering from Mysore University, Mysore, India, in 1994, M.Tech. Degree in Digital Electronics and Communication Systems from Mysore University in 1997.He completed Ph.D. under the guidance of Prof. P.Venkataram, Dept. of ECE, IISc., Bangalore. He has Investigated a transaction based QoS, Resource management schemes for mobile communications environment. He has more than 20 years of teaching experience in Engineering. He has published more than 20 papers in national and international journals and conferences. He is a reviewer and chair for many conferences. His research interest includes bandwidth management, Quality of Service (QoS) management, topology management, and Energy management. He is a student member of IEEE and life member of India Society for Technical Education (LMISTE). He is presently working as Professor and Head, in the Department of E&C at Sri Jayachamarajendra College of Engineering, Mysuru, Karnataka, India.

Dr. Rajashekar M B is currently working as Associate Professor in the Department of Computer Science & Engineering at GSSS Institute of Engineering & Technology for Women, Mysore. He obtained Bachelor Degree in Computer Science & Engineering from Coorg Institute of Technology, Ponnampet, Karnataka State, India in 2008. M. Tech from National Institute of Engineering, Mysore, Karnataka State, India. Ph D from VTU, Belagavi in 2023.He has 15 years of teaching experience. currently he published 5 international papers.
ORCID iD: https://orcid.org/0000-0002-5623-2092

Prof. Sudeep J received his Bachelor of Engineering in Information Science and Engineering from Coorg Institute of Technology, Ponnampet, affiliated to Visvesvaraya Technological University, Belgaum, Karnataka, and obtained his Master's Degree in the area of Software Engineering from Sri Jayachamarajendra College of Engineering, Mysore, autonomous under Visvesvaraya Technological University, Belgaum, Karnataka. His research interests include Internet of Things, Cyber Security and Blockchain technologies. He has published research papers in various international conferences and journals. At present he is working as Assistant Professor in the Department of Information science and Engineering at NIE Institute of Technology, Mysuru, Karnataka, India.

Prof. Shruthi B S received her Bachelor of Engineering in Information Science and Engineering from Bahubali college of Engineering, Shravanabelagola, affiliated to Visvesvaraya Technological University, Belgaum, Karnataka, and obtained her Master's Degree in the area of Computer Network Engineering from The National Institute of Engineering, Mysore, autonomous under Visvesvaraya Technological University, Belgaum, Karnataka. Her research interests include Data security, Computer Network, Cloud computing and Machine Learning. At present she is working as Assistant Professor in the Department of Information science and Engineering at NIE Institute of Technology, NIE(North), Mysuru, Karnataka, India.

Prof. Darshini Y G received her Bachelor of Engineering in Computer Science and Engineering from BGS Institute of Technology, BGS Nagara, Bellur Cross, affiliated to Visvesvaraya Technological University, Belgaum, Karnataka, and obtained her Master's Degree in the area of Information Technology from The National Institute of Engineering, Mysore, autonomous under Visvesvaraya Technological University, Belgaum, Karnataka. Her research interests include Wireless Sensor Networks, Internet of Things, Artificial Intelligence and Machine Learning. At present she is working as Assistant Professor in the Department of Information science and Engineering at The National Institute of Engineering(North), Mysuru, Karnataka, India.

Prof. Manasa K B received her Bachelor of Engineering in Information Science and Engineering from GSSS Institute of Engineering & Technology for Women, Mysuru, affiliated to Visvesvaraya Technological University, Belgaum, Karnataka, and obtained her Master's Degree in the area of Computer Science and Engineering from Sri Siddartha Institute of Technology, Deemed University, Tumakuru, Karnataka. Her research interests include Data security, Computer Network, Cloud computing and Machine Learning. At present she is working as Assistant Professor in the Department of Information science and Engineering at The National Institute of Engineering (North), Mysuru, Karnataka, India.

How to cite this paper: Prasanna Kumar G, Shankaraiah N, Rajashekar M B, Sudeep J, Shruthi B S, Darshini Y, Manasa K B, "A Novel Approach by Integrating Dynamic Network Selection and Security Measures to improve Seamless Connectivity in Ubiquitous Networks", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.14, No.1, pp. 29-42, 2024. DOI:10.5815/ijwmt.2024.01.03