COMPARISON OF SOFTWARE DEFINED NETWORKING WITH TRADITIONAL NETWORKING USING NS2 SIMULATOR

*B. S. E. Zoraida (1), G. Indumathi (2)**

(1) Department of Computer Science, Bharathidasan University, Tiruchirappalli
(2) AVVM Sri Pushpam College, Poondi
India

* Corresponding Author, e-mail: ginduavvmspc@gmail.com

Abstract: The Software Defined Network (SDN) is an emerging concept in network engineering that entails the decoupling of the control plane and data plane. The data plane is executed on discrete nodes, while a centralised control plane is accountable for overseeing network-wide functionalities. In conventional networks, the integrated planes are incorporated into the network suite, and the transmission is determined by the route. In this work, the traditional way of routing using a communication plane is compared with routing using an SDN controller. The present study employs the NS2 simulator to evaluate the quality of service performance under high background traffic conditions. In the event of network congestion, it is imperative to utilize the available bandwidth to its fullest extent in order to increase the rate of bit transmission per second. The results of the traditional network and SDN network based on various parameters like Ambiguous collision, Delay, Jitter, Availability and Latency are compared in this paper. The results show that the SDN network's performance is better with concerning time.

Key words: traditional network, software-defined network, packet transmission, jitter, latency, ambiguous, delayed and quality of service.

1. INTRODUCTION

In contemporary times, routine tasks are reliant on the internet for the purpose of communication, encompassing the exchange of information, concepts, and monetary transactions. The transport layer is responsible for processing data in communication. The fundamental function of the transport layer is to furnish communication services in a direct manner to the application processes that are operational on disparate hosts. The transport layer offers a comprehensive end-to-end resolution for dependable communication. Furthermore, it offers additional functionalities such as dependable data transmission, bandwidth allocation, and latency assurances. The fundamental role of the Transport layer is to receive data from the Session layer and, if necessary, divide it into smaller segments. Furthermore, transmit these fragments to the Network layer and verify the accurate delivery of all fragments at the receiving end. The transmission control protocol (TCP) and user datagram protocol (UDP) are utilised by each of the applications within the application layer to transmit messages. The software system establishes communication through the utilisation of one of two available protocols. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) establish communication with the Internet Protocol (IP) at the Internet layer. TCP detects losses through timer expiration during instances of low traffic or when acknowledgments are not received. In a conventional network, the determination of packet transmission is carried out by routers. The current network architecture, commonly referred to as the traditional network, remains highly intricate. In a conventional network, individual devices possess distinct configurations (control planes) and data (forwarding planes) that are integrated within the device itself [2]. The implementation of Software-Defined Networking (SDN) presents a mechanism that enhances diverse facets of network administration [3]. The fundamental principle of Software Defined Networking (SDN) involves the explicit division of the control and forwarding plane. Software-Defined Networking (SDN) is a network architecture that enables centralised management of numerous network devices, facilitating efficient allocation of resources and connectivity. Software-defined networking (SDN) has the capability to automate network behaviour and optimise device utilisation. Various aspects related to programmability, including network bandwidth optimisation, load balancing, and traffic engineering, have been identified [4]. Prior research has investigated the potential of Software-Defined Networking (SDN) to offer enhanced mechanisms for conventional network management. The execution of configuration tasks has been observed in diverse scenarios such as the Internet of Things [5], cellular SDN [6], and data centre networks [7]. In view of this the contributions of this work are as follows:

- The traditional way of routing using a communication plane is compared with routing using an SDN controller.
- An efficient node management method is carried out between source and destination by exchanging HELLO and ACK control packets.
- The transmission of data from the sensor nodes is facilitated through the utilisation of a packet that encompasses specific control fields.

The rest of this article is ordered as follows - Section 2 mentions a few existing research works, Section 3 shows the preliminaries. Section 4 show the proposed method. Section 5 exhibits the experimental outcomes and discussion, and, finally, Section 5 ends up with conclusion and future work.

2. RELATED WORKS

The perspective of SDN is founded on the segregation of the data plane and the control plane [8]. In their publication, Rahman et al. (2018) proposed an energy-efficient and secure framework for Blockchain-enabled software-defined IoT in intelligent networks. The authors proposed a layered architecture to ensure secure network communication for the deployment of a distributed and efficient Blockchain-based SDN-IoT framework [9]. Almohaimeed and Asaduzzaman (2019) proposed a novel framework that integrates edge computing with software-defined networking (SDN) to enhance the processing of large-scale data. Their approach demonstrated superior performance in this regard. The creation of high pressure on the central controller by SDN has resulted in an issue that impacts the overall network output. This issue manifests as longer latency when the data size increases. The researchers employed a novel SDN Edge Controlling model through the integration of edge computing technologies [10]. Assume SDN-IoT networks in [11], where IoT devices operate via the Zigbee protocol. For IoT observation services, a minimum end-to-end delay (MaMED) routing method is proposed; this scheme doesn't need to know the input traffic beforehand. The "DistB-SDCloud" architecture for improved cloud security for smart IIoT applications is introduced in [12]. The suggested architecture offers safety anonymity, confidentiality, and integrity while being adaptable and scalable by using a distributed Block Chain (BC) technique Utilise the features of Blockchain in [13] to verify users in a Software-Defined Network based Internet of Things (SDN-IoT) network. Centralised administration of the expanding IoT devices is provided by the SDN. Blockchain is an appropriate technology for the system since it provides a decentralised, tamper-proof way to store and share authentication data. For each gadget connection application, a virtual token is created using a smart contract. To address these issues, [14] present an Industrial IoT (IIoT) architecture for software-defined networking that integrates blockchain technology and is energy-efficient. In order to achieve effective energy use and cluster-head selection for IIoT applications, we provide a framework for implementing decentralised blockchain combined with SDN. Additionally, the distributed ledger powered by blockchain assures data consistency across the SDN controller network and keeps track of the controller's mandated nodes. In [15], the authors evaluated the security risks, challenges, efficacy, and viability of IoT-based applications before identifying blockchain as a feasible solution. Additionally, In [16] looked at the main components and functions of the blockchain-based smart home for IoT for privacy and security considerations. They used a local, private blockchain that provides safe access management for IoT devices and preserves a time-ordered transaction record for each level of the smart house. In [17], a method for defining RESTful Application Programming Interfaces (APIs) is shown that enables mobile edge apps to keep track of subscriber spending caps regardless of the type of measurement used, such as monetary, volume, time, etc., as well as to manage sponsored connection. Investigate a few communication factors when using the digital spice to access remote resources in [18]. The objective is to examine potential losses in sustaining communication performance, which is based on the organisation of two types of experiments – programme monitoring and simulation – and preliminary mathematical formalisation.

3. PRELIMINARIES

3.1. Traditional Network

In traditional Networking, control and data planes are tightly coupled and coexist on Networking Element (NE). One control plane per data plane. Management plane mainly exists off-network over one or more management hosts. Legacy networking nodes include both control and data plane functions Control plane function is predominantly implemented using the software. The data plane function is predominantly implemented using hardware. The management plane function is split between the node and management host(s).

3.2. Software-Defined Networking

Software-defined networking (SDN) is a network architecture that involves the physical segregation of the network control plane from the data plane. A solitary control plane governs numerous physical or software entities within the forwarding plane. Multiple control planes can manage a single switch. The SDN controller configures forwarding tables based on FCP functions and management policies.

SDN controllers operate in the following three modes:

- *Default mode* – layer two learning Switch; no controller needed
- *Non-Default mode*
  - Proactive Controller – flow entries created on the connection
  - Reactive Controller – flow entries created on packet arrival

3.3. Node Management

In WSN, various nodes communicate by exchanging HELLO and ACK control packets. Each sensor node discovers its one-hop neighbour. The Hello packets' fields are as follows shown in Figure 1 - i) Source Id; ii) Source Position; iii) Sink Distance.

Source ID	Source Position	Sink Distance

Figure 1. Hello Packet

Each node sends an ACK packet containing the following fields in response to the Hello packet as shown in Figure 2 – i) Neighbour Id; ii) Neighbour Position; iii) Sink Distance; iv) Node Energy.

Neighbour ID	Neighbour Position	Sink Distance	Node Energy

Figure 2. ACK Packet

3.4. Packet Transmission

When in wireless sensor networks, when a sensor node receives data as a result of an event or a packet from a neighbouring node, it employs multi-hop communication to relay the data to the sink node. In order to achieve this objective, every sensor node consults its routing table and transmits the data packet to the prospective subsequent node towards the sink node. The temporal limit for completion of a task may be designated by the user or approximated by the originating node of the event region. The transmission of data from the sensor nodes is facilitated through the utilisation of a packet that encompasses specific control fields, namely: i) Source Id; ii) Sink Id; iii) Deadline.

Upon receipt of the aforementioned packet, the sensor node proceeds to select the subsequent node for packet forwarding, utilising the following set of criteria:

- It is imperative that the subsequent node in the network topology be positioned at a shorter distance from the intended endpoint compared to the present node.
- The velocity at which the data packet propagates through the chosen link must satisfy the requisite propagation speed of that particular link.

The determination of the required propagation speed is contingent upon the estimated deadline. Permit the adjacency of node nj to nodeni, where i is less than j. The representation of the distance between nodes ni and nj is denoted by $d(ni, nj)$ in academic discourse. The necessary velocity for end-to-end propagation of data, denoted as V_{req}, is determined by the quotient of the change in distance between the source node, S, and the sink node, T, with respect to the estimated deadline, t_{set}. Given that the propagation speed (v_{prov}) on the aforementioned link is greater than or equal to the required propagation speed (v_{req}), and the specified node is located at a shorter distance from the sink node in comparison to the current node. In situations of this nature, the allocated node will be selected to operate as a forwarding node. Propagation speeds, both required and provided, are computed at each intermediate node situated between the source and the link.

The data's estimated deadline, T_l is updated in each intermediate node as $tl = tl - link\ delay$. As shown, the required speed is recalculated.

$$v_{req} = \frac{(ni,T)}{(tl - link\ latency)} \tag{1}$$

In this case, ni is an intermediate node on a path between the source and the destination and the sink When $I = 0$. The source node S is ni. Similarly, the propagation speed on each selected. The link is calculated as shown in Eq. (2).

$$v_{prov} = \frac{d(ni,T) - d(ni+1,T)}{Ii+1} \tag{2}$$

Suppose the provided speed, v_{prov}, is greater than or equal to the required speed, v_{prov}, and the forwarding node is closer to the destination than the current node. In that case, it will be selected as a forwarding node.

4. PROPOSED WORK

In conventional network architectures, network devices are typically comprised of two distinct components: a control plane and a forwarding plane. Consequently, the configuration of each network device is executed in command line interface. The expansion of network devices, advancements in network device performance, efficient network problem resolution, and provisioning of new services can pose challenges for a conventional network. SDN arises through the establishment of a network framework that involves the segregation of the control and forwarding planes. The management of the control plane is facilitated through a programmable centralised controller, which enables the configuration of policies for individual devices such as routers, switches, and firewalls. The transmission of data entails a shift from a network architecture featuring a dispersed control plane to one characterised by a consolidated control plane.

4.1. Various Parameters to compare Current architecture and SDN with Simulation Environment:

The transport layer exclusively facilitates the transmission of packets. The User Datagram Protocol (UDP) is employed for providing connectionless service and ensuring the final delivery of transmissions.

- Ambiguous-When multiple packets are transmitted from different path in the network through internet that time ambiguity occur in a node. When particular node will be the intermediate node for more than one path at the same time.
- Availability-When multiple packets are transmitted through the internet. Subsequently, every packet is transmitted to its intended endpoint via the most optimal pathway. The term "availability" refers to the proportion of time, over a designated period, in which a server, cloud service, or other machine is operational and capable of being utilised.
- Jitter-Jitter refers to the temporal fluctuations in the latency of network transmissions, quantifying the degree of variability in ping.
- Delayed-Within the context of computer networking, a packet refers to a diminutive portion of a more extensive communication. Information transmitted through computer networks, such as the Internet, is fragmented into multiple packets.
- Latency-The phenomenon of communication delays over a network is commonly referred to as network latency. Within the realm of networking, latency can be conceptualised as the duration required for a data packet to traverse various network components, subsequently arriving at its intended endpoint, and undergoing decoding.

5. PERFORMANCE EVALUATION

The protocol under consideration was subjected to simulation using the community Simulator ns-2.35. The deployment of nodes occurs within a 600x400 square metre flat grid region, where various knots simulate the protocol, 50, 75, 100, 125, and 150. The simulation time is further increased to 100 seconds, 200 seconds, 300 seconds, 400 seconds, and 500's. IEEE802.11 MAC protocol. Total number of paths considered is 10. The experiment is used in this work. The entire set of selected simulation parameters is summarized in Table 1 and figure 3 below.

Table 1. Simulation Environment

No of Nodes	50,75,100,125,150,200
Simulation Time	100s,200s,300s,400s,500s
Node Placement	Flat Grid
Area	600 x 400
MAC Protocol	802.11
Propagation Model	Two ray ground
Transmission Range	250 m
Traffic Type	CBR

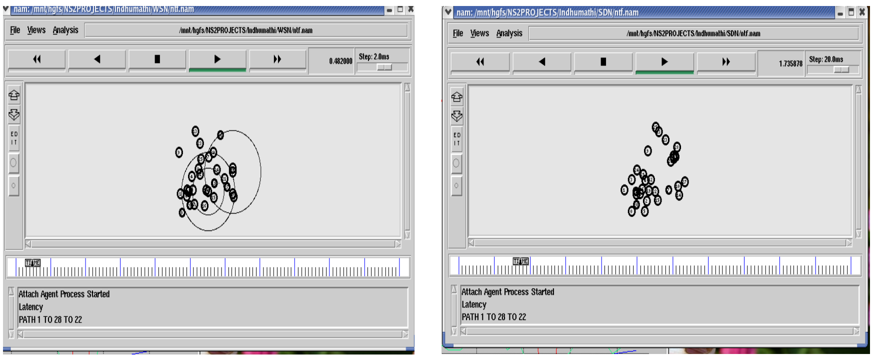


Figure 3. Simulation scenario

5.1. Simulation Results

The key performance metrics valuated in the experiment are (i) Ambiguous, (ii) Availability, (iii) Jitter, (iv) Delayed and (v) Latency. A group of forecasting algorithms are known as exponential smoothing methods. To predict future values, they make use of weighted averages of earlier observations. The goal is to give the most recent values in the series more weight. As a result, the significance of these values decreases exponentially with increasing age of the observations.

Ambiguous. Twenty-nine nodes are created in Virtual memory. Packets are transmitted in 3 paths with an energy of 40 secs. The packets are transmitted from the sink to the agent. Setting time as 0.5 secs. When the sec is 0.4, an ambiguous collision occurs at 28 nodes. In the sink, bw1 stores the number of bytes, bw2 stores the total number of packets and bw3 stores the last packet time. The values of bw1, bw2 and bw3 are represented as a1, a2 and a3 in a graphical representation. The ambiguous collision starts at 0.4 sec and ends at 20 secs through UDP protocol. The X axis denotes the number of nodes/packets, and the Y axis denotes the Delay. While comparing these networks (SDN & WSN). In Packet transmission, the packets are travelled from three paths (i.e.) 1-28-22, 6-28-11 & 12-28-13. That time in node 28, an ambiguous collision occurred in UDP. Using the NS-2 simulator, it was compared with WSN & SDN.

WSN SDN

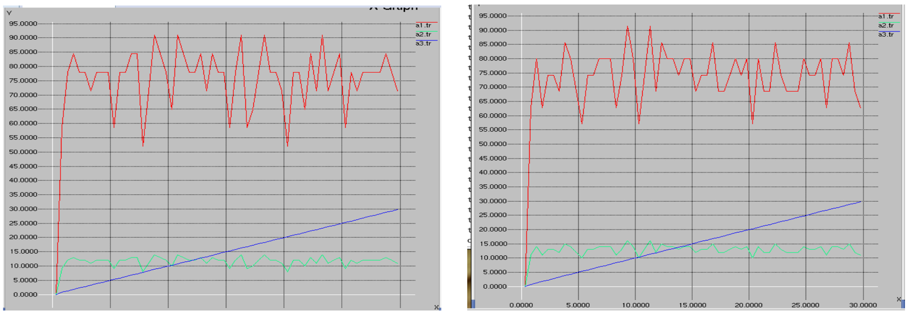
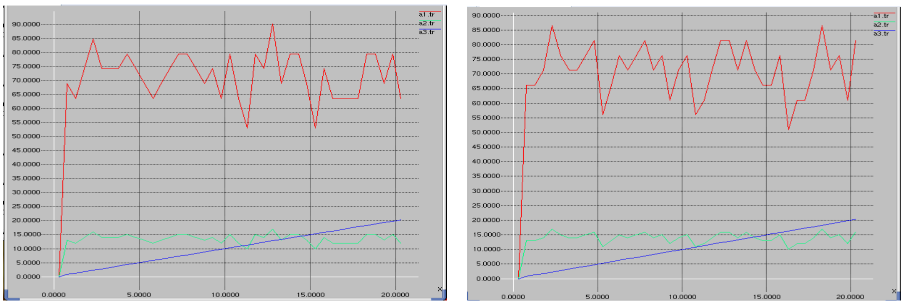


Figure 4. Analysis of ambiguous

Availability. In the simulation environment, three sinks are created as f1, f2 and f3 then the packets are transmitted from paths 2 to 22. The node is not reachable during the communication of packets. The idle time is 12ms. Then it chooses the alternate path of eight instead of 22 to complete the communication. At 5.0 sec, it transmits the packets in an alternate path through the UDP protocol as an agent from the sink node in the NS-2 simulator. The horizontal axis represents the quantity of nodes or packets, while the vertical axis represents the delay. While comparing these networks (SDN & WSN).

WSN SDN



Jitter. The agent starts the tracing at 0.3 secs from path 18-6-19. At 5.5-sec, node 6 has low power. It reroutes the path 6-2-22-19 to complete the packet transmission.

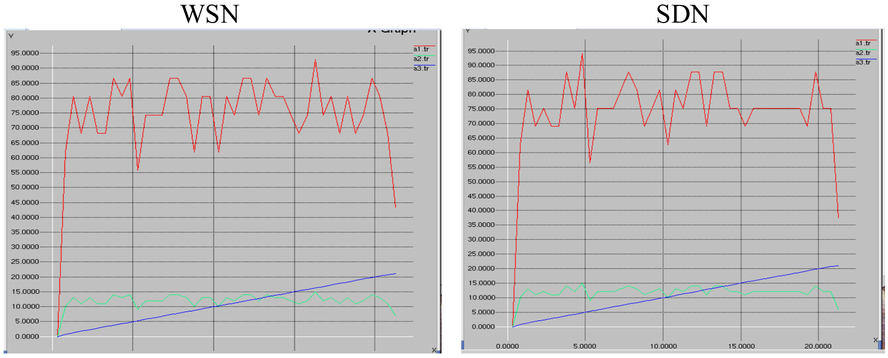


Figure 6. Analysis of jitter

Delayed. In NS 2 simulator, the trace files are started and stored in the tf file. The packets are processed from sink to agent as UDP protocol. At 0.3 sec, the agent starts the process through path 26-27-8. It waits for 12ms. At 5.2 sec, it sends a message as "Waiting for Acknowledgement. “At 5.4 sec, it sends the report. It sends the Delayed Acknowledgement at 10.5 secs. The horizontal axis represents the quantity of nodes or packets, while the vertical axis represents the delay. When comparing SDN and WSN networks, it can be observed that. The percentage of SDN increases from 65% to a peak level of 85%.The Wireless Sensor Network (WSN) experiences an increase from 80% to 93%.When the network size consists of 30 nodes, the delay incurred by a Wireless Sensor Network (WSN) is greater than the delay incurred by a Software-Defined Network (SDN).The presented figure illustrates that as the network size increases, the delay caused by SDN decreases. The findings indicate that the employment of SDN, as opposed to WSN, leads to a reduction in packet transfer delay as the number of nodes increases.

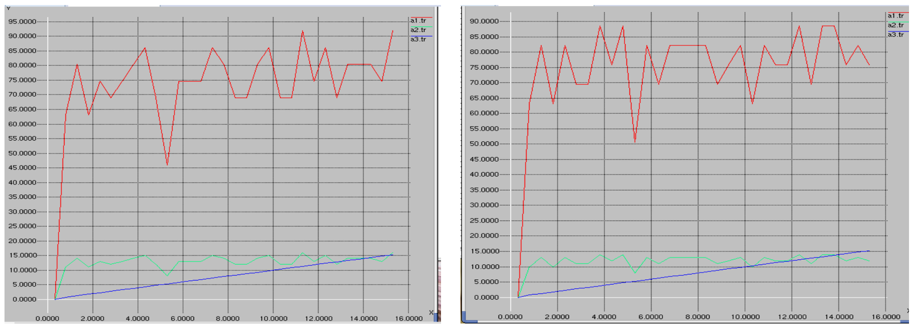


Figure 6. Analysis of delay

Latency. In the NS-2 simulator, at 0.4 sec, the packets are transmitted from 1 - 28 – 22. When the latency occurs, it reroutes the path at 7.4 sec to complete the transmission of the packet for communication. In packet transmission, the time required for a data packet to cross several devices, be received at its destination and decrease. The measurement of network latency can be accomplished by ascertaining the round-trip time (RTT) for a data packet to traverse to a designated endpoint and return.

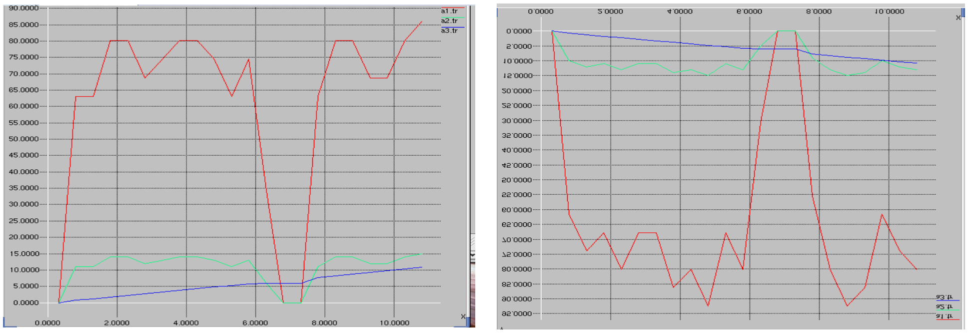


Figure 7. Analysis of latency

6. CONCLUSION

Software-defined networking (SDN) is a dynamic and progressive networking model that facilitates a uniform programming capability for governing network behaviour. The employment of Software-Defined Networking (SDN) represents a contemporary methodology in the field of Networking. This architectural framework has been leveraged to restructure a multitude of solutions to conventional network predicaments, albeit certain challenges persist. Whilst the genuine Software-Defined Networking (SDN) exhibits satisfactory response times and performance metrics, it is outperformed by the conventional network. The system exhibits exceptional performance in TCP data streams, achieving a throughput of 96.9 Mbits/sec, and in UDP data streams, achieving a throughput of 99.9 Mbits/sec. Furthermore, the mean response time is 17.48 ms, taking into account the immediate frame switching that occurs There exists a connection point between the virtual switch and the host node.

REFERENCES

[1] H. Kim and N. Feamster. Improving network management with software-defined networking. *IEEE Communications Magazine*, vol.13, no.4, 2021, pp. 3-14.

[2] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, Volume: 103, Issue: 1, January 2015, pp.14–76.

[3] A. Bradai, K. Singh, T. Ahmed, and T. Rasheed. Cellular software defined networking: A framework. *IEEE Communications Magazine.*, vol. 53, no. 6, June 2015, pp.36-43.

[4] T. Truong, Q. Fu, and C. Lorier. FlowMap: Improving network management with SDN. *Proceedings of the 15th IEEE/IFIP Network Operations and Management Symposium (NOMS 2016)*, pp. 821–824.

[5] A. El-hassany and L. Vanbever. SDNRacer : Concurrency analysis for software-defined networks. *in ACM SIGPLAN Conference on Programming Language Design and Implementation*, *PLDI*, 2016, pp. 402–415.

[6] M. Afrin and R. Mahmud. Software defined network-based scalable resource discovery for Internet of Things. *EAI Endorsed Transactions on Scalable Information Systems*, vol. 14, no. 4, 2017, pp. 1–6.

[7] A. Duque-torres, F. Amezquita-su, O. Mauricio, C. Rendon, A. Ord, and W. Y. Campo. An approach based on knowledge-defined networking for identifying heavy-hitter flows in data centre networks. *Applied Science,* vol. 9, art. 4808, 2019, pp.1–19.

[8] Lawal BH, Nuray AT. Real-time detection and mitigation of distributed denial of service (DDoS) attacks in software defined networking (SDN). *In 26th Signal Processing and Communications Applications Conference (SIU),* 2018, pp. 1-4.

[9] Rahman A, Islam MJ, Montieri A, Nasir MK, Reza MM, Band SS, et al. Smart block-SDN: An optimized blockchain-SDN framework for resource management in IoT. *IEEE Access,* vol. 9, 2021, pp.28361-28376.

[10] Almohaimeed A, Asaduzzaman A. Introducing edge controlling to software defined Networking to reduce processing time. *in IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC),* Las Vegas, NV, USA, 2019.

[11] Jiang, F., Zhou, Y., & Chen, Y. (2023, March). MaMED: ML-assisted minimum end-to-end delay routing in SDN-IoT networks for IoT monitoring. In *IEEE Wireless Communications and Networking Conference (WCNC)*, March 2023, pp. 1-6.

[12] Rahman, A., Islam, M. J., Band, S. S., Muhammad, G., Hasan, K., & Tiwari, P. Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. *Digital Communications and Networks*, vol. 9, no. 2, 2023, pp. 411-421.

[13] Bargayary, B., & Medhi, N. (2023, March). A blockchain-assisted authentication for SDN-IoT network using smart contract. In *4th International Conference on Computing and Communication Systems (I3CS)*, 2023, pp. 1-6.

[14] Asaithambi, S., Ravi, L., Kotb, H., Milyani, A. H., Azhari, A. A., Nallusamy, S., & Vairavasundaram, S. An energy-efficient and blockchain-integrated software defined network for the industrial Internet of Things. *Sensors*, vol. 22, vol. 20, 2022, pp.7917.

[15] Sasikumar, A.; Senthilkumar, N.; Subramaniyaswamy, V.; Kotecha, K.; Indragandhi, V.; Ravi, L. An efficient, provably secure DAG based consensus mechanism for industrial internet of things. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, vol. 16, no. 4, 2022, pp.1–11.

[16] Ammi, M.; Alarabi, S.; Benkhelifa, E. Customized blockchain-based architecture for secure smart home for lightweight IoT. *Information Processing & Management,* vol. 58, no. 3, art. 102482, May 2021.

[17] Atanasov, I., Pencheva, E., Nametkov, A., & Trifonov, V. On functionality of policy control at the network edge. *International Journal on Information Technologies and Security*, vol. 11, no. 3, 2019, pp. 3-24.

[18] Romansky, R. Evaluation of experimental data from monitoring and simulation of network communication parameters *International Journal on Information Technologies and Security*, vol. 14, no. 2, 2022, pp. 75-86.

Information about the authors:

Dr. B. S. E. Zoraida is an Assistant Professor in the Department of Computer Science, Bharathidasan University, Tiruchirappalli, India. She did her Ph. D at National Institute of Technology, Trichy. She has more than 29 years of teaching experience and 15 years of profound experience in Research. She has more than 50 research publications to her credit. Her areas of interests include DNA Computing, Bio-inspired Algorithms in Energy Management and Semantic Web

G. Indumathi is an Assistant Professor in the Department of Computer Science, AVVM Sri Pushpam College,Poondi, India. She does her Ph.D. at Bharathidasan University, Tiruchirappalli. She has more than 8 years of teaching experience. Her areas of interests include Networking, SDN, Blockchain and Machine Learning.

Manuscript received on 07 June 2023