Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 171 (2020) 1409–1418

Procedia Computer Science

www.elsevier.com/locate/procedia

Third International Conference on Computing and Network Communications (CoCoNet'19)

Software Defined Internet of Things using lightweight protocol

Meenaxi M Raikar[a], Meena S M[b], Mohammed Moin Mulla[c]

[a,b,c]K.L.E. Technological University, Vidyanagar, Hubballi, 580031, India

Abstract

The upsurge in the Internet of Things (IoT) has led towards an increasing interest in simplifying the control mechanism in the wireless network. The control mechanism is a challenge as it involves data acquisition and analysis, decision making, and actuation/control in IoT networks. This has led towards combining Software Defined Networks (SDN) and IoT for easy of controlling the network devices. The mobile application available at the tip of hands to control the connected devices to the internet has led to exponential growth in data. The management and handling the data intensive applications is a challenge to the network operators.

SDN is a paradigm shift that enables network programmability, control, and management of diverse networking devices. This paper describes the data transmission in SDN and integration of SDN and IoT. The light weight protocol Message Queue Telemetry Transport (MQTT) is used for data transmission between the IoT devices. The result analysis shows that the light weight protocol MQTT is 30% efficient for data transmission in SDN IoT architecture. The testbed for integrating virtual network in SDN and real-time network for IoT applications using lightweight protocol is described.

Keywords: broker, Message Queue Telemetry Transport (MQTT), mininet, sflow, Testbed

1. Introduction

The transition from voice data to video data has led to exponential growth in the data traffic. The shift is observed from wired to wireless devices for data access needs. To support the increase in the volume of the data the network operators expand the infrastructure which triggers power consumption in the wireless networks, that in turn has resulted in ever increasing the need for sustainable network management process. Thus power efficiency plays an important role in network design and planning. This research proposal presents energy-aware network design and planning for the next generation of wireless networks.

10.1016/j.procs.2020.04.151

The development of wireless technology is because of data driven services available on the internet. The next generation wireless networks envision ubiquitous connectivity between devices. The growth in data is enormous in recent years with the advent of the Internet of Things. The users receive real time updates by connecting the sensors/things to the internet. The network service providers face the challenge of meeting the user needs and striking a trade-off between the power consumption of the network devices and QoS parameters. The savings in capital expenditure (CAPEX) and operational expenditure (OPEX) is achieved by proposing the energy efficient solutions for network management.

The forecast presented by Cisco VNI presents an increase in connected devices to 11.6 billion by 2021. In the case of IoT scenario, the physical objects such as sensors, vehicles connect to the internet giving rise to the increase in the volume of the data. With the pressing need for energy-saving worldwide, the focus of the paper is to save power over wireless infrastructure and the user equipment. With the key technologies of the Next Generation Network (NGN) such as Power over Ethernet (PoE), SDN and IoT the optimization in network planning for energy saving in networks is proposed.

Why integrate SDN and IoT?

1. Integration of IoT and SDN eases the data acquisition, analysis, decision making, and actuation/control process.
2. The network resource utilization is optimized using SDN technology. The data intensive IoT applications in integration with SDN enable network operators to manage the users, devices, and groups.

The key contributions described in the paper are:

1. Integration of virtual network in SDN and real-time campus network for establishing connectivity between virtual and real-time network. The observations are that the results in the virtual network are similar as in real-time networks.
2. Perform integration of SDN and IoT for efficient utilization of network resources.
3. Publish subscriber communication model with lightweight protocol for efficient transmission in SDN IoT architecture.

The paper is put forth in the following sections. In section II the related work is stated, in section III description related to research questions addressed is presented, section IV on proposed work, section V includes the result/testbed setup, and in section VI the conclusion is presented.

2. Related work

The data intensiveness in different sectors such as academia and enterprise networks is described in the paper considering two categories, such as educational sector and enterprise network.

Educational sector: The change in teaching-learning pattern from textbooks to internet resources has led to data intensiveness in the academic sector. The proliferation of online courses for teaching-learning creates a need for network operators to upgrade the infrastructure to meet the user needs [6][10]. The step-to-step guidelines presented in the video enable the learner to reiterate the steps and simultaneously learn in cases such as installation which is difficult to present in the form of text.

Enterprise networks: The shift from client server architecture to cloud enabled architecture for achieving scalability, reliability, accessibility creates the challenge of how to process the data deluge in the network. The developers build the applications in the cloud development platforms using services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [9]. It creates data intensiveness in enterprise networks. The network service providers are looking towards migration from traditional networking to Software Defined Networking to meet the data intensive needs of internet users. The different IoT applications generate exponential data traffic growth in the network [7][11][13].

Keshav Sood et al., present the integration of IoT and Software Defined Wireless Networks for managing scalability and security issues. The benefits and opportunities in integrating SDN and IoT are highlighted [1]. Keshav Sood et al., describe the management of the network resources at the control layer of the SDN IoT network infrastructure. The game-theory approach is used to compute the controller's utility, thereby reducing the latency [2].

Slavica Tomovic et al., present the integration of Fog computing and SDN for solving scalability, data delivery in real-time and mobility issues in the IoT networks. Smart transportation, video surveillance, and precision agriculture are the use cases explained that include SDN and Fog integration for IoT [3]. Saba Al Rubaye et al., present usage of SDN in the management of Industrial Internet of Things (IIoT) with a case study example of smart grids. The resilience issue is put forward for managing failure occurrences and recovery in smart grid networks with the aid of real-time monitoring mechanisms [4].

Raul et al., propose the distribution of data analytic task at the edge network and cloud in integration with SDN for efficient utilization of network resources [5]. Energy harvesting technique, in combination with SDN IoT architecture, is employed to increase the network life of IoT devices [8]. The game theory Nash bargain concept is applied to maintain the balance between Quality of Service (QoS) parameters and energy consumption. The abstraction of energy plane along with the data and control plane in SDN is presented. The nodes in the network harvest energy from the environment, such as wind and solar energy. The mobile-charger is employed to charge the energy deficient nodes through “energy downlink.” The mobile-charger collects the surplus energy through “energy uplink”. The data queue and energy queue are maintained by Software Defined data switch, and Software Defined energy switch, respectively. The amalgamation of SDN and Network Function Virtualization (NFV) is proposed to enable network infrastructure sharing. The mathematical model for energy and cost analysis is presented for, with virtualization technique and without virtualization applied to the IoT network infrastructure [14]. The results state that cost and energy savings are obtained using virtualization techniques. The resource utilization is optimization is described by performing load balancing in SDN [12].

The different IoT applications and services in the smart city are presented in [15]. The IoT protocols such as CoAP in the transport layer and 6LoWPAN in network layer for building IoT applications are presented. The data formats, such as Efficient XML Interchange (EXI) is explained. The monitoring of traffic in the IoT network is performed for failure detection and security measures. The traffic patterns are analyzed using traffic time series algorithms. The anomalies in the traffic pattern are determined [16].

Edge computing is the solution proposed in [17] to handle the massive data traffic in IoT networks. Multicast transmission between publisher and subscriber using MQTT protocol is employed for minimization of transmission delays and efficient network resource utilization. The comparison of IoT middleware such as Constrained Application Protocol (CoAP), MQTT for Sensor Networks (MQTT-SN), and Data Distribution Service (DDS) is presented. The integration of SDN and direct multicast MQTT is proposed for minimization of delay between the edge broker nodes.

The leverage of SDN and Mobile Cloud Computing (MCC) is done to achieve energy optimization [18]. The computational offloading mechanism is applied for efficient utilization of processing, memory unit and for extending the battery life of the mobile devices. The co-operative mechanism to ensure security is proposed in SDN IoT network [19]. The data traffic growth in e-health service with captured data for including energy management distribution is presented in [20]. The service delivery challenges faced in IoT networks are resolved with the aid of SDN and NFV architecture. The technique of caching the frequently requested data and load balancing between the brokers for reducing the delay is presented in [21]. The Network Calculus theory and Genetic Algorithm (GA) are used to model the IoT networking scenarios. The solution comprising of SDN and IoT to manage the diverse IoT networks formed from cellular, WiFi, Bluetooth, and ZigBee is proposed [22]. The framework that integrates SDN and IoT for load balancing, energy management, fault tolerance, and security issues is presented [23].

The ubiquitous mobile devices such as tablets, laptops, smartphones in the digital era for real-time access to information has enabled people to connect instantaneously. In this era, it is merely not information access, it’s about network performance, reliability, and security that is the prime factor of revenue generation and productivity for network service providers. The key questions are deployment, maintenance, and management of the network resources without increasing the Capital expenditure (CAPEX) and Operational expenditure (OPEX).

2.1. Power over Ethernet switches for energy cost reduction in the edge networks

The edge network devices include wireless APs, IP phones, or any other PoE enabled devices. The Energy Proportionality Index (EPI) is defined to establish the relation between data traffic load and energy consumption [24]. The routers and switches do not include the values for different parameters for energy consumption. The different parameters for energy consumption variations such as the base chassis power, number of line cards, active ports, port capacity, Ternary Content Addressable (TCAM), firmware and port utilization are presented.

The Energy Efficient Ethernet (EEE), 802.3az standard low power idle (LPI) saves 1W per Ethernet link. In EEE the Power over Ethernet (PoE) is not included as the power saving measure. The PoE technology reduces the cable installation as well as remote control of the network devices for power saving, such as the camera connected can be turned off during the inactivity period to save power. During low utilization period, the 802.11 WLAN access points are turned off. The network devices are powered over the same Ethernet cable used for data transmission in PoE technology. Thus eliminating the installation of AC outlet, and conservation of power during device off state.

2.2. Embedding Intelligence into Network edge devices

The analysis is carried out to find the energy consumption of the PoE devices. The PoE switch budget is efficiently utilized based on the power requirements of the connected devices. The power usage of the network devices is visible on the dashboard per device in kilo Watts unit for monitoring and management. The combination of machine learning (ML) and networks is planned to be adopted for increasing the network performance. The network optimization is planned by embedding intelligence in the networking system for efficient organization, management, and maintenance. The combination of SDN and ML is employed for route optimization, traffic classification, Quality of Experience (QoE) prediction, network resource management, and security.

The application of artificial intelligence (AI) and deep learning technology for wireless networks is presented in [29]. These techniques enable finding the network dynamics such as congestion point, interference distribution, hotspots, availability of spectrum, and traffic bottlenecks. The different network parameters considered are a delay, link Signal to Noise Ratio (SNR), and loss rate.

In the wireless network, the Access Points (APs) are placed at the edge to enable the user devices to connect wirelessly to the network [25]. The network administrators need to discover all the APs in the wireless network for configuration of these devices centrally. To ease the deployment and management, the network administrator look for remote AP management. The template based configuration of APs needs to be enabled for remote configuration of the APs. The different parameters in the AP template are Virtual LAN (VLAN) ID, channel, Service Set Identifier (SSID) name, and security features. The firmware update and management, Rogue AP detection, AP load balancing are the other features for network in-operation monitoring/maintenance. Traffic shaping, setting the firewall rules, and QoS priorities are the techniques applied for user traffic profiling and management. The downtime of the AP is reduced by monitoring the status of the APs and sending the notification to the network administrator for action initiation and rectification.

The programmable solution for wireless network AP management using SDN is proposed [26]. The different techniques described are AP configuration, channel interference minimization, and load balancing. The mixed-integer programming concept is applied to minimize energy as well as latency in SDWN [27]. The evolution of multiple Radio Access Technologies for data access in the wireless network has created control and management of the network devices a challenge [28]. SDN technology is proposed as a solution to cater to the needs of the data intensive application. The network slicing technique is applied in multi-RAT network architecture. The integration of SDN and IoT to achieve energy efficient architecture is described in [30]. The analysis of video traffic in wireless personal area network is described in [31]. The power consumption model for the various components of the IoT network is proposed in [32].

3. Research focus

The needs of internet users are changing with the advancement in networking technologies. The gap between the exponential growth in the volume of the data and the network infrastructure deployment to ensure the Quality of Experience (QoE) is to be bridged. The research focus is to satisfy the QoE needs of the users by using SDN technology. The authors have attempted to provide a solution by addressing these research questions.

Research Questions

1. Whether SDN technology can be employed to handle the massive growth in data volume because of the connected devices to the internet?

2. Whether the amount of data sent can be reduced per transmission to save power?
    - Publish Subscribe communication model.
    - Lightweight protocol used for transmission of data.

4. Proposed work

The Software Defined Networks (SDN) technology is chosen to solve the issue of energy saving in wireless networks due to the following characteristics:

Centralized controller: The controller is a program that gathers the status of the network elements dynamically.

Network Programmability: The network administrators can program the data forwarding devices.

Vender Independent: The data plane and the control plane are separated in SDN. The programs are written for different functionalities of the network devices. The software components can be added to the network devices independent, of which vender the device is purchased.

The drawback of the network simulation is it does not integrate with the real-time networks. Hence the network emulation is used to implement the proposed framework. The network architecture for co-operative transmission between the nodes is shown in fig 1. The different network applications in the framework are traffic monitoring, traffic optimization, energy manager, and topology manager. The southbound interface is used for communication between the network elements and the controller.

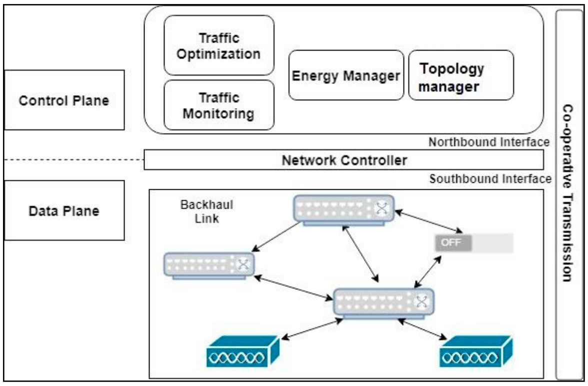

Fig 1 Network Architecture for co-operative transmission between the nodes.

The OpenFlow protocol is used as the southbound interface for communication. It maintains a table on every switch/Access point. The contents of the table are determined solely by the controller. The table contains the match action entries which are used to inspect and act upon the traffic entering the switch/Access points. The northbound interface is used for communication between the controller and the application. The different network applications functionalities are as follows:

Traffic monitoring / Classification application: The statistics related to real-time dynamics is collected at the controller for monitoring and analysis of the power usage at the network devices.

Traffic optimization: The traffic optimization techniques are to be applied to reduce the number of packets transmitted and to handle the link failures. The traditional network is designed such that the energy consumption remains the same irrespective to the data traffic variations in volume.

Energy Manager: The challenges in the design of the proposed algorithm are to meet the energy constraints of the wireless nodes. Each node in the wireless network topology consumes power depending on whether it is in the following states:

- asleep mode (i.e, no transmission)
- idle mode (i.e, listening but not sending)
- transmitting mode

Topology Manager: The topology manager stores the network information related to the number of host nodes/stations, bandwidth for the link, port status, and network connectivity. The global information of the topology is discovered by the controller using the Link Layer Discovery Protocol (LLDP).

5. Results and Discussions

In this section, the testbed setup for integrating virtual SDN with real-time network is presented. It is further extended for integrating SDN and IoT infrastructure. The lightweight protocol is used to minimize the transmission delay between the communicating nodes.

Testbed Setup: The hybrid network composing of the real-time network and the virtual network is represented in the fig 2. The college campus network is chosen to represent the real-time network. The campus network is segregated into eight sections to represent the different departments using the Virtual Local Area Network (VLAN) concept, as shown in Table 2. Among the eight VLANs, two VLANs representing computer science department and the campus WiFi are shown in fig 2. To connect the virtual network to the real-time network emulation tool mininet, third party mobile application, and the mosquito broker for lightweight protocol setup is employed. The different sub-sections in the testbed setup are virtual network setup, traffic analysis, connecting the virtual network and the real network, communication model, lightweight protocol, mobile application, and the packet sniffer. These sub-sections are discussed in the further sections.

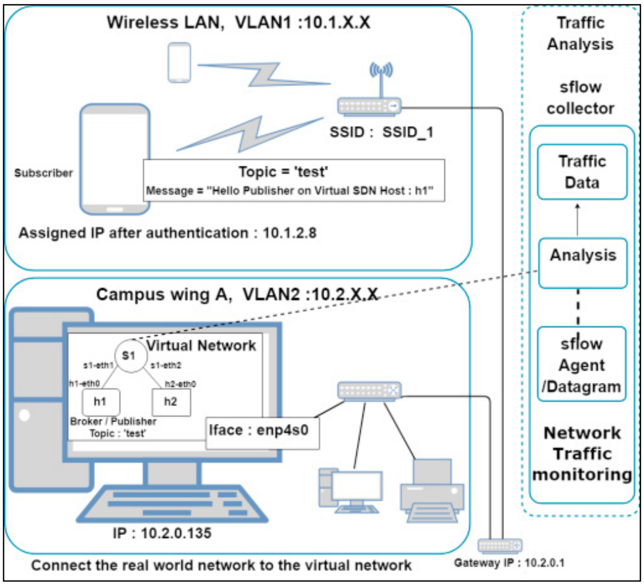

Fig 2 Interconnecting virtual network and the real-time network.

Table 1 VLAN for representing eight departments in the campus.

Sl. No	VLAN	IP address	Department
1	VLAN1	10.1.X.X	Campus Wifi
2	VLAN2	10.2.X.X	CSE
3	VLAN3	10.3.X.X	E&C
4	VLAN4	10.4.X.X	Mechanical
5	VLAN5	10.5.X.X	Biotechnology
6	VLAN6	10.6.X.X	Office
7	VLAN7	10.7.X.X	Hostel
8	VLAN8	10.8.X.X	Management

Virtual network setup: The virtual network composing of the switch and two hosts are created using the command *'sudo –mn'*.

Traffic Analysis: The sflow application is used for traffic monitoring at the network devices. The different applications of sflow are to determine the network outages, network planning, intrusion detection, and route profiling.

The traffic information of the virtual network topology created using mininet is shown in fig 3. The dashboard displays the time series charts for top flows, top ports, and the topology diameter. In top flows the active flows during that time instances is displayed. The top port shows the ingress ports that are active during that time instance. The sflow agents run as a network management module in the switch or router of the network topology. The sflow datagram is formed of flow samples and interface counters. The sflow agent sends the sflow datagrams to the sflow collector. Packet sampling is performed to obtain wire-speed performance.

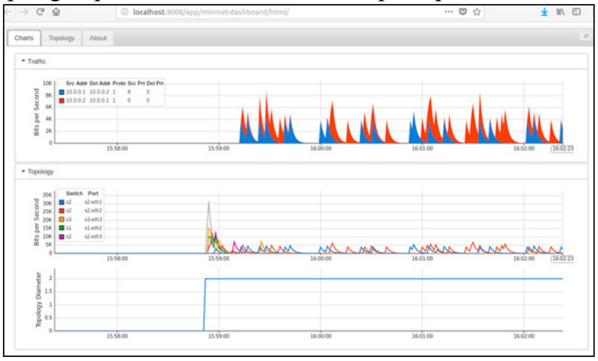

Fig 3 Traffic monitoring in the virtual network using sflow application.

Connecting the virtual network to the real network: The virtual network is created on the host machine with IP *'10.2.0.135'* as shown in fig 2, in a real network. This host is in VLAN2 of the campus network. The command *'sudo mn'* is used to create a virtual network. The test for connectivity using the ping command to google server IP 8.8.8.8 at mininet> prompt is reachable as shown in table 2. The command *'h1 ping 8.8.8.8'* fails the connectivity test. The route command is used to find the destination, gateway and the Iface value of the virtual host h1. Table 3 shows the gateway and Iface value of the host h1 in the virtual network.

Table 2 Test for connectivity from a host in the virtual network

Command	Reachability
mininet>sh ping 8.8.8.8	Yes (reachable)
mininet>h1 ping 8.8.8.8	Not reachable

Table 3 Route information details.

Command	Destination	Gateway	Iface
mininet>sh route	default	10.2.0.1	enp4s0
mininet>h1 route	10.0.0.0	*	h1-eth0

The administration of the OpenFlow switch is performed using the ovs-ofctl command. The ifconfig command is employed to change the network interface configuration. The dhclient command is used to obtain a dynamic IP address of the virtual host as shown in table 4.

Table 4 Network interface configuration and obtaining a dynamic IP address.

Command	Description
mininet>sh ovs-vsctl add-port s1 enp4s0	Add a port
mininet>sh ifconfig enp4s0 0	Configuration of the network interface
mininet>sh dhclient s1	Use DHCP to obtain a dynamic IP address
mininet>h1 ifconfig h1-eth0 0	Configuration of the network interface
mininet>h1 dhclient h1-eth0	Use DHCP to obtain a dynamic IP address

Communication model: The Publish-subscribe communication model is deployed for connecting the mobile device to host in the virtual network. The publishers publish using a topic name. The subscriber subscribes to the topic for receiving the published data.

Lightweight protocol: The lightweight protocol MQTT is chosen for sending the messages from the publisher to subscriber. The mosquitto broker is used for data transmission between the publisher and the subscriber. The command '*sudo systemctl restart mosquitto'* is used to enable the services of the mosquitto broker. The command '*mosquitto –v*' is used to set the verbose mode of interaction. The virtual host h1 is configured as the broker as well as the publisher, as shown in fig 2. The default port for the broker is 1883. The CONNACK, PUBLISH, DISCONNECT are the messages exchanged between the broker and the publisher. The CONNACK, PINGREQ, PINGRESP, SUBSCRIBE are the messages exchanged between the subscriber and the broker. The command '*mosquito_pub –h 10.2.0.135 –t "test" –m "Hello Publisher on Virtual SDN Host: h1"*' is used by the publisher to publish the message to the subscribers. The topic here is "*test*", the message sent is "*Hello Publisher on Virtual SDN Host: h1*" and the host IP of the broker is 10.2.0.135.

Mobile application: The mobile device is chosen as a subscriber as shown in fig 2. After authentication by the firewall, the dynamic IP address *'10.1.2.8'* is allocated to the mobile device. The VLAN ID of the mobile device is *10.1.X.X.* The third-party mobile application is used by the subscriber. The broker IP is set as *10.2.0.135* using the mobile app. The dashboard in the mobile app receives the message sent by the publisher.

Packet Sniffer: The packet sniffer Wireshark is used to capture the OF (OpenFlow) packets to view the packet header details and analysis.

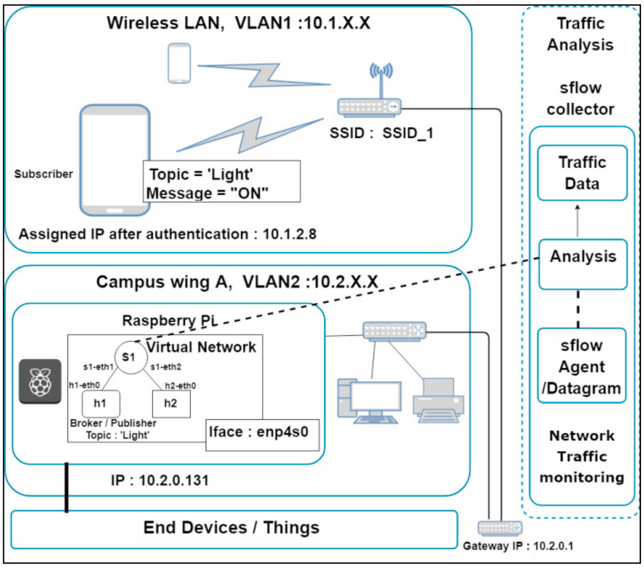

Fig 4 Software Defined Internet of Things using light weight protocol.

Integration of SDN and IoT: The host machine in VLAN2 is replaced with Raspberry pi 3 for connecting the things to the internet in fig 4. The Raspberry pi 3 is a system on a chip that supports wireless connectivity to the internet. The things can be a bulb, temperature sensor, rain sensor, PIR (Passive Infra-Red) sensor used for motion detection, ultrasonic sensor (HC-SR04) to measure the distance, MQ-135 gas sensor to detect the harmful gases in the environment or any other thing.

The lightweight protocol MQTT is used to control the things over the internet. The topic chosen by the publisher here is 'Light' as shown in fig 4. The subscribers subscribe to the same topic. The message 'ON' is sent by the subscriber to ON/OFF the thing connected to the Raspberry pi controller. The packet capture is performed using the Wireshark tool. The filter is applied to compare the number of bytes used in packet transmission using "HTTP" and "MQTT" protocol, as shown in fig 5.

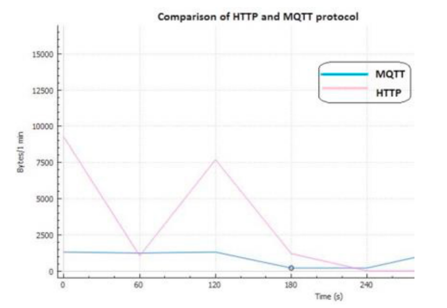

Fig 5 Comparison of HTTP and MQTT protocol.

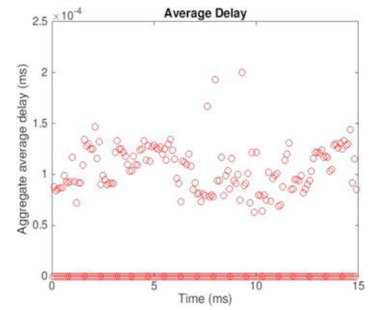

Fig 6 IoT traffic delay performance

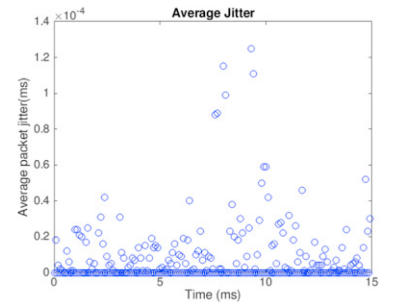

Fig 7. IoT traffic jitter performance

The result analysis presented in fig 5 shows that the number of bytes transferred per min is approximately 1500 bytes using lightweight protocol MQTT compared to 7500 bytes (peak value) using the hypertext transfer protocol. The obtained ratio for the number of bytes transferred per minute is 1:5 that is one-byte data is sent in case of MQTT protocol compared to five bytes using HTTP. Thus a saving of four bytes is obtained using lightweight protocol for data transmission per minute. It is assumed that one unit of power consumption occurs for one byte of data transferred per minute. It requires one unit of power for lightweight protocol compared to five units of power using HTTP. Hence a power saving of four units is obtained per minute of data transfer using MQTT. The percentage saving obtained using lightweight protocol for data transmission is 80%. The comparison of MQTT and CoAP the IoT protocols could be the future work.

Simulation setup for IoT traffic analysis: The evaluation of the experimental setup is performed using mininet, the network emulator, and POX software defined controller. The experiments are carried out on desktop machine having Intel ® Core ™ i3-7100 CPU @ 3.90 GHz processor with 4GB RAM on Ubuntu 16.04 operating system. The tree topology is used to represent the data center scenarios. The modeling of the IoT traffic is performed using the Distributed Internet Traffic Generator (D-ITG). The ITGSend, ITGRecv, and ITGDec components are used as a sender, receiver, and decoder component in IoT traffic generation. The UDP is chosen to represent the IoT traffic. The resulting log files are decoded using the ITGDec component for the result analysis. The ‘*.dat” files are generated for measuring the network performance based on bitrate, delay, jitter, and packet loss. The plotting of the graphs is carried out using online MATLAB R2019a version. The throughput (bitrate) of 16Kbps is obtained for the experimental setup with no packet loss. The plot of the aggregate average delay in ms and average packet jitter (ms) are represented in fig 6 and fig 7, respectively.

6. Conclusion

In this paper, integration of SDN and IoT for massive data access and connectivity is presented. The light weight protocol MQTT is used for energy efficient data transmission between the devices. The proof of concept is presented by setting up a testbed of SDN and IoT devices. The virtual network in mininet is connected with real-time campus network. The Publish subscribe communication model is used for data transmission among the devices.

The combination of SDN and IoT for network monitoring and management is envisioned in the future. Due to the data intensiveness, the challenges posed in the network infrastructure maintenance are energy management, fault tolerance, security, and load balancing. A look-ahead solution towards energy management in data intensive networks is a combination of PoE, IoT, and SDN along with the lightweight protocols.

References

[1] 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.

[2] Sood, Keshav, Yu, Shui, Xiang, Yong and Peng, Sancheng 2016, Control layer resource management in SDN-IoT networks using multi-objective constraint, in ICIEA 2016: IEEE, Piscataway, N.J., pp. 71-76.

[3] 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.

[4] 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*.

[5] R. Muñoz *et al.*, "Integration of IoT, Transport SDN, and Edge/Cloud Computing for Dynamic Distribution of IoT Analytics and Efficient Use of Network Resources," in *Journal of Lightwave Technology*, vol. 36, no. 7, pp. 1420-1428, 1 April1, 2018.

[6] M. S. Patil et al., "Leveraging Student Project through MOOC on UX: Case Study," 2016 IEEE 4th International Conference on MOOCs, Innovation and Technology in Education (MITE), Madurai, 2016, pp. 8-13.

[7] M. M. Raikar, P. Desai, V. M and P. Narayankar, "Upsurge of IoT (Internet of Things) in engineering education: A case study," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, 2018, pp. 191-197.

[8] X. Huang, R. Yu, J. Kang, Z. Xia and Y. Zhang, "Software Defined Networking for Energy Harvesting Internet of Things," in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1389-1399, June 2018.

[9] M. M. Raikar, P. Desai, M. Vijayalakshmi and P. Narayankar, "Augmenting Cloud concepts learning with Open source software environment," (ICACCI), Bangalore, 2018, pp. 1405-1411.

[10] M. Vijayalakshmi, P. Desai and M. M. Raikar, "Packet Tracer Simulation Tool as Pedagogy to Enhance Learning of Computer Network Concepts," IEEE 4th International Conference on MOOCs, Innovation and Technology in Education (MITE), Madurai, 2016, pp. 71-76.

[11] M. M. Raikar, P. Desai, N. Kanthi and S. Bawoor, "Blend of Cloud and Internet of Things (IoT) in agriculture sector using lightweight protocol," 2018 (ICACCI), Bangalore, 2018, pp. 185-190. doi: 10.1109/ICACCI.2018.8554406

[12] Mulla M.M., Raikar M.M., Meghana M.K., Shetti N.S., Madhu R.K. (2019) Load Balancing for Software-Defined Networks. Emerging Research in Electronics, Computer Science and Technology. Lecture Notes in Electrical Engineering, vol 545. Springer, Singapore.

[13] M. M. Raikar, P. Desai and J. G. Naragund, "Active Learning Explored in Open Elective Course: Internet of Things (IoT)," 2016 IEEE Eighth International Conference on Technology for Education (T4E), Mumbai, 2016, pp. 15-18.

[14] Mamdouh Alenezi; Khaled Almustafa; Khalim Amjad Meerja, "Cloud based SDN and NFV architectures for IoT infrastructure", Egyptian Informatics Journal, ISSN: 1110-8665,2018, DOI10.1016/j.eij.2018.03.004

[15] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for Smart Cities," in IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22-32, Feb. 2014.

[16] Izal, Mikel et al. "Computation of Traffic Time Series for Large Populations of IoT Devices" Sensors (Basel, Switzerland) vol. 19,1 78. 26 Dec. 2018, doi:10.3390/s19010078.

[17] Park, J.-H.; Kim, H.-S.; Kim, W.-T. DM-MQTT: An Efficient MQTT Based on SDN Multicast for Massive IoT Communications. Sensors 2018, 18, 3071.

[18] Elhadj Benkhelifa, Thomas Welsh, Loai Tawalbeh, Yaser Jararweh, Mahmoud Al-Ayyoub, "Leveraging Software-Defined-Networking for Energy Optimisation in Mobile-Cloud-Computing", Procedia Computer Science,Volume 94,2016,Pages 479-484,ISSN 1877-0509.

[19] G. Grigoryan, Y. Liu, L. Njilla, C. Kamhoua and K. Kwiat, "Enabling Cooperative IoT Security via Software Defined Networks (SDN)," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, 2018, pp. 1-6.

[20] C. Jacquenet M. Boucadair "A software-defined approach to IoT networking" ZTE Commun. vol. 14 no. 1 pp. 61-66 2016.

[21] X. Sun and N. Ansari, "Traffic Load Balancing Among Brokers at the IoT Application Layer," in IEEE Transactions on Network and Service Management, vol. 15, no. 1, pp. 489-502, March 2018.

[22] Z. Qin, G. Denker, C. Giannelli, P. Bellavista and N. Venkatasubramanian, "A Software Defined Networking architecture for the Internet-of-Things," 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, 2014, pp. 1-9.

[23] Farzad Kiani, "A Survey on Management Frameworks and Open Challenges in IoT," Wireless Communications and Mobile Computing, vol. 2018, Article ID 9857026, 33 pages, 2018. https://doi.org/10.1155/2018/9857026.

[24] Mahadevan, Priya et al. "A Power Benchmarking Framework for Network Devices." Networking (2009).

[25] Roam Kleinerman, "Power over Ethernet (PoE) : An energy-efficient alternative, https://www.marvell.com/switching/assets/Marvell-PoE-An-Energy-Efficient-Alternative.pdf

[26] 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.

[27] 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

[28] Akshatha Nayak and et al, "Control and Management of Multiple RATs in Wireless Networks: An SDN Approach", arXiv:1801.03819 [eess.SP], 6 Dec 2018.

[29] Q. Mao, F. Hu and Q. Hao, "Deep Learning for Intelligent Wireless Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 2595-2621, Fourthquarter 2018.doi: 10.1109/COMST.2018.2846401.

[30] N. Kaur and S. K. Sood, "An Energy-Efficient Architecture for the Internet of Things (IoT)," in IEEE Systems Journal, vol. 11, no. 2, pp. 796-805, June 2017.doi: 10.1109/JSYST.2015.2469676.

[31] K. S. Shilpa, D. G. Narayan, S. Kotabagi and M. Uma, "Suitability Analysis of IEEE 802.15.4 Networks for Video Surveillance," 2011 International Conference on Computational Intelligence and Communication Networks, Gwalior, 2011, pp. 702-706.

[32] B. Martinez, M. Montón, I. Vilajosana and J. D. Prades, "The Power of Models: Modeling Power Consumption for IoT Devices," in IEEE Sensors Journal, vol. 15, no. 10, pp. 5777-5789, Oct. 2015.doi: 10.1109/JSEN.2015.2445094.