An SDN Based Distributed IoT Network with NFV Implementation for Smart Cities

Bivash Kanti Mukherjee[1(✉)], Sadiqul Islam Pappu[2], Md. Jahidul Islam[1], and Uzzal Kumar Acharjee[1]

[1] Jagannath University, Dhaka, Bangladesh
mshunnohridoy@gmail.com, jahidul.jnucse@gmail.com, uzzal@cse.jnu.ac.bd
[2] Daffodil International University, Dhaka, Bangladesh
sadiqul15-9769@diu.edu.bd

Abstract. The Internet of Things (IoT) is an arrangement of connected numerous digital devices usually contained Unique Identifiers (UIDs) and have the capability to exchange data over a network without any human interaction. Another new paradigm Software-Defined Networking (SDN) comes in for the organization and control of the large amount of data produced by IoT devices. It separates the data plane from the control plane of network devices which enables easy configuration and management of those devices. Furthermore, Network Function Virtualization (NFV) is emerged to optimize and secure the SDN-IoT network. It enables network devices to be deployed as virtualized components via software. In this research, the authors have proposed an SDN based distributed IoT network with NFV implementation for smart cities. Where smart city is a residential area which utilizes Information and Communication Technology (ICT) as well as IoT network to develop the standard of living of its residents. The integration of NFV in the SDN-IoT network improves the network performance by increasing throughput, and time sequence while mitigating the round trip time as well. Moreover, the authors have used multiple distributed controllers and a clustering scheme to improve load balancing, scalability, availability, integrity, and security of the whole network.

Keywords: IoT · SDN · NFV · Smart City · OpenFlow · Controller · Cluster etc

1 Introduction

Nowadays, a rapid evolution of IoT is seen with plenty of physical objects connected to the Internet. IoT technology can connect each and everything throughout the world via the internet [1]. It can sense or monitor surroundings through sensor networks and can identify things by scanning an RFID tag [2]. Potential areas where IoT technology is utilized include home automation, industrial

T. Bhuiyan et al. (Eds.): ICONCS 2020, LNICST 325, pp. 539–552, 2020.
https://doi.org/10.1007/978-3-030-52856-0_43

automation, health care, smart grid, smart cities, etc. As the number of connected objects to the internet are rising day by day so the management and control of IoT becomes a very challenging task. Here, SDN comes in to give the flexibility and programmability of the IoT network instead of modifying the structure of existing implementations. Moreover, it can simplify network operations, reduce cost and accelerate service delivery by separating the control plane from the data plane of traditional network devices. In addition, NFV is introduced to develop the flexibility of network service provisioning and to diminish the time to market the latest services [3]. It also reduces Operating Expenses (OpEx) and Capital Expenses (CapEx) significantly.

A recent survey says that over 50% of the world's population now living in towns [2] that has a significant impact on city resources and infrastructure. For the proper utilization of city resources as well as to improve the quality of life for all inhabitants smart cities are now becoming IoT dependent. Because of the rising acceptance of IoT system, multiple challenges have arisen in terms of security, availability, and management. Common security mechanisms i.e. firewalling, intrusion detection system, etc. are no longer enough to secure the vast IoT network. Billions of devices are now connected to the IoT network and sharing sensitive data so they are becoming more vulnerable to security attacks. Moreover, any delay in response time through the communication will be resulting in a negative impact on the overall performance and accuracy of the network system, especially in cases of real-time transaction. To minimize the response time while improving the security system SDN is used in IoT applications. Recently, multiple controllers are used in SDN instead of using a centralized controller which helps to distribute traffic loads of IoT devices among the controllers. Resources will be available instantly when they are required by the user by means of SDN-IoT network. Furthermore, using an SDN controller a network can be configured in a dynamic way. One of the most common protocols used by SDN is OpenFlow [4]. In recent years, NFV is introduced as a promising technology that has the ability to virtualize the network functions replacing traditional network devices like switches, routers, firewalls, etc. with software running on commercial off-the-shelf servers [5]. So it enables service providers to implement network functions in virtual server rather than in conventional hardware. Therefore, it improves network scalability, load balancing, and power consumption as well.

In this research, the authors have proposed a distributed SDN-IoT network with NFV implementation for smart city usage. Besides, to develop cost-effective, scalable, reliable, and resilient smart cities the authors have implemented NFV in that SDN-IoT network. The authors have also introduced a clustering approach for the efficient management of large IoT network which will enable reliable communications while consuming less power. Besides, for the proper distribution of communication traffic at the same time improving security in SDN-IoT environment, the authors have proposed multi-functional distributed controllers in the network. Moreover, the implementation of NFV in SDN-IoT architecture increases the overall network efficiency which will give more flexibility to the network operators to control their networks dynamically.

The authors have organized the paper as follows: Authors discuss related works in Sect. 2. Section 3 introduces the proposed NFV implemented SDN-IoT Network architecture and also explains the working principle of it. After that, simulation results and findings are illustrated in Sect. 4. Section 5 includes the conclusion of the research with future research scopes.

2 Related Works

Several researches have carried out in this field. Some of them are listed below:

The research in [6] provides a detail view of different SDN-IoT frameworks and security solutions, current trends in research and therefore the futurist contributory factors. However, no new methodology had been proposed. Further, three architectures are proposed in [7] which are designed to work with all existing platforms like OpenFlow, OpenStack, and OpenDaylight. The authors focused on controller security throughout the research but couldn't give any solution for the challenging management task of vast IoT devices. A comprehensive survey presents in [1] showing the security mechanisms that SDN technology can serve for the IoT environment. The authors also proposed a role-based security controller architecture (called Rol-Sec) for the SDN-IoT environment. But they didn't simulate it in an SDN environment and also not provided any performance analysis of the proposed architecture. Another survey in [8], the authors introduced the software-defined NFV architecture as the state of the art of NFV and presented relationships between NFV and SDN. They also provided a historic view of the involvement from the middlebox to NFV. The authors discussed various challenges and problems of NFV but didn't provide any suitable solution in their research. The research in [9] focused on driving mobile network evolution towards cost-efficient IT-based solutions using standardized hardware and software-based ideas like SDN and NFV. The authors also highlighted some other limitations for integrating IT concepts in telecommunication networks. However, more granular and customizable network architecture is needed to deal with the challenge of network service automation through softwarization and cloudification.

Further, in the research [10,11], the authors introduced a highly secured SDN called Black SDN and designed an NFV integrated distributed IoT network with that SDN for more efficient network performance and security. Though the authors didn't provide any simulation data and also not clarified performance analysis information. Besides, in the research [12], the authors concentrated on investigating the security issues of SDN along with the limitations of the proposed solutions. Another group of researchers in [13] used an SDN gateway for monitoring the traffic originating from and directed to IoT based devices. But still, energy-efficient better routing mechanism is required for IoT nodes to minimize resource usage. Moreover, researchers in [14] analyzed the challenges associated with IoT technology and proposed a software model based on SDN that can prevent different attacks in the IoT environment. However, implementation of the proposed algorithm and the result analysis for different security attacks was not shown. Furthermore, in the research [15], authors presented a study that

is focused on an efficient method to build a cluster network using SDN, network virtualization, and OpenFlow technologies. But the performance of the proposed clustered routing approach for SDN-IoT network is not measured.

Moreover, authors in the research [16] presented a framework to exploit security features of SDN/NFV and made efficient integration with existing IoT security methods. They also explored the opportunities that NFV and SDN jointly offer in coping with security threats against IoT services. An SDN/NFV packet/optical transport network named ADRENALINE testbed was proposed in [17] and the authors also figured out an edge/core cloud platform for end-to-end 5G and IoT services. Similarly, the authors in the research [18] focused on investigating the roles of SDN/NFV in deploying IoT services and proposed an SDN/NFV architecture for applying in IoT framework. Where the components of the proposed architecture are physically used and some of them are accessed from the local server instead of deploying them in the cloud. Furthermore, a new approach was presented in [19] for comprehensive monitoring of software-defined 5G mobile network by using IoT based framework which provides easier implementation of a monitoring system for mobile network operators. In another research [20], the authors discussed major security challenges in IoT networks and also presented two secured SDN-IoT integration technique termed as loosely and tightly coupled. The security framework of the proposed SDN integrated networks should be improved to develop more efficient IoT networks that can be applied in real industrial applications. A network slicing concept was presented in [21], which had a particular focus on its application to 5G systems. The authors also gave a short overview of the SDN architecture proposed by the Open Network Foundation (ONF) and additionally presented a scenario that couples SDN and NFV technologies to address network slices. However, any analysis of the security and privacy concerns that are risen from 5G slicing has not been seen. Besides, in the research [22], a comparison was conducted in between a proposed SDN/NFV network and a typical 4g network that was represented through mathematical illustration. However, no new theory has been given on how to reduce cost and save energy in the SDN/NFV based IoT networks.

Most of the research works focused on improving IoT security and controller security for the SDN-IoT network. Several researches are done on NFV implementation in SDN-IoT architecture to give more flexibility to network operators in controlling their network while reducing the capital and operational expenses as well. Different researchers proposed many SDN-IoT architecture with NFV implementation but very few of them are presented simulation works in this field. To solve various challenges in the IoT network many researchers are still trying to find optimal solutions for providing smart citizens with a network that will be more secure, handy and optimized.

3 Proposed SDN-IoT Network with NFV Implementation

The authors have designed an IoT network for smart city applications. To build a dynamic, programmatically efficient IoT network Software-defined Networking (SDN) technology is used in the network. Moreover, to simplify the architecture of physical networks and at the same time to improve the scalability and adaptability of the network, the authors have also implemented Network Functions Virtualization (NFV) method in these proposed network architecture.

The authors have divided the entire network scenario into four layers. They are-

- Infrastructure Layer
- Control and Virtualization Layer
- Application Layer
- NFV Management and Orchestration

3.1 Infrastructure Layer

The infrastructure layer is divided into two parts. One is the clustered IoT nodes and another is the data plane. Handling a large IoT network efficiently is a very challenging task without any properly organized structure. So the authors have

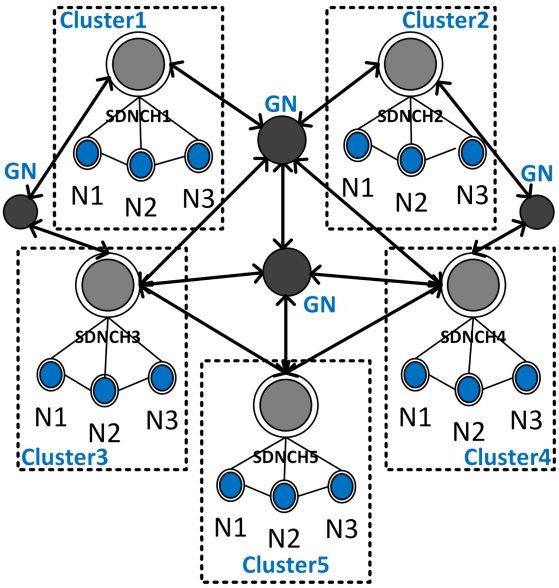

Fig. 1. IoT clustering

proposed a clustering method to organize the IoT nodes in an efficient way. A cluster consists of several IoT nodes (N1, N2, N3..., n). These IoT nodes have the sensing capability to collect data from their surroundings. Every cluster is managed by a Cluster Head (CH). Cluster heads are selected randomly by the respective cluster's IoT nodes based on the highest energy presented in the node. To develop this design authors tend to place an SDN controller within each cluster head (SDNCH) [15]. The main purpose of SDNCH is to control and monitor the cluster domains. Moreover, it secures all cluster domains from internal and external threats. Several nodes are selected as common nodes in between the clusters called Gateway Nodes (GNs). GNs are used to maintain communication between the cluster domains.

The graphical illustration of these clustering scheme is depicted in Fig. 1. Further, the data plane involves a group of basic network devices including router, switch, firewall, and cloud infrastructure. The data communication between the cluster heads and the control plane is maintained by some SDN-IoT gateways over the data plane. After a complete routing on the data plane, the traffic is passed to the control and virtualization layer through SDN OpenFlow routing protocol.

3.2 Control and Virtualization Layer

This layer consists of a group of multi-functional controllers and virtualized resources which is shown in Fig. 2. It provides the control of the forwarding data behavior and the virtualized resources for smart city apps. To eliminate the bottleneck issues [23], it is necessary to distribute the functions of the SDN controller. So, the authors proposed multiple controllers for specific roles to play [1,7] in the proposed network architecture. Authors utilize three basic types of controllers in the network namely application, packet, and security controller. The application controller is designed for tracing the malicious applications within the network. Packet controller is responsible for load balancing and packet security monitoring. The security controller introduces three additional controllers such as key controller, intrusion controller, and crypto controller. These controllers are used to maintain integrity, privacy, and confidentiality throughout the whole network operation. For the implementation of NFV, all the resources e.g. storage, networking, and computing are virtualized here which are known as NFV Apps. These Apps are considered as high-level applications.

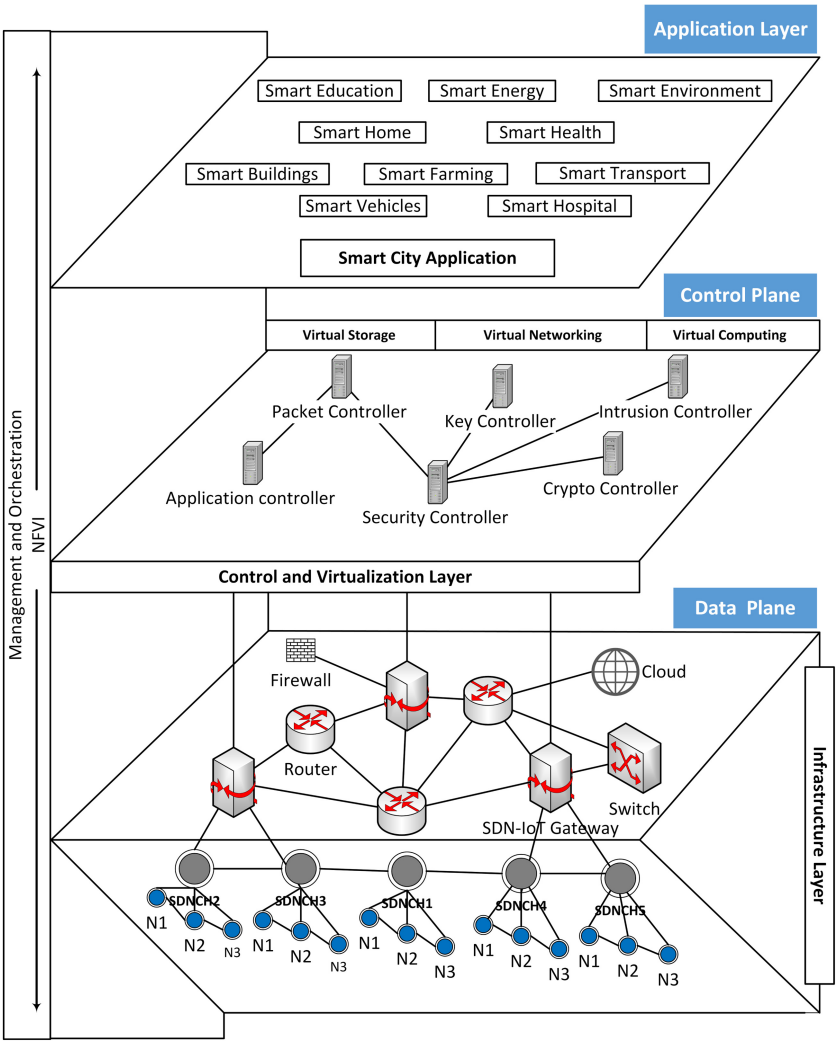

Fig. 2. Proposed network architecture

3.3 Application Layer

This is the upper layer of the network architecture where the application fields of the developed network are enlisted. The authors have proposed this network architecture, especially for smart city applications. This layer covers an array of smart city applications like smart home, smart vehicle, smart education, smart healthcare, smart transportation, etc. Moreover, it includes server and cloud infrastructures that share content and provide real-time services to the user. Data processing and providing services are also the most vital functions of this

layer. Overall, this layer provides a large-scale management of IoT system for smart cities as shown in Fig. 3.

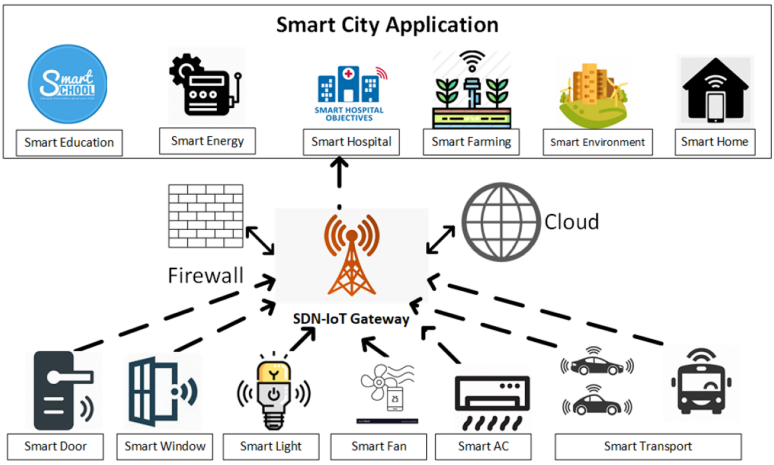

Fig. 3. Smart city application

3.4 NFV Management and Orchestration (NFV MANO)

NFV MANO is applied to the entire system to virtualize all the functions of the network. Some of the NFV management and orchestration features include network service onboarding, monitoring, and scaling. Another vital role is played by the NFV MANO that is the deployment of the Virtualized Network Functions (VNFs) over the Network Function Virtualization Infrastructure (NFVI). NFVI includes the combination of both hardware and software resources which form the environment where VNFs are deployed. All virtualization-specific management tasks needed in the NFV framework are done by NFV MANO.

4 Results and Discussions

The authors have built three network topology with 10, 20, and 50 IoT nodes. Entire simulation is done on Mininet-WiFi, a tool to emulate wireless OpenFlow scenarios allowing high-fidelity experiments that replicate real networking environments. Moreover, the authors have used the Wireshark packet analyzer for analyzing network packets and determining throughput, round trip time, and time sequence (tcptrace) of the three network topologies respectively. In this section, at first, the authors have compared their three network topologies with respect to three simulation parameters i.e throughput, round trip time, and time sequence (tcptrace). Then, the authors have compared their best efficient network topology with another two reference papers performance regarding the simulation parameters and present the analysis result.

4.1 Throughput for Different Number of Nodes

Figure 4 shows that the average throughput of 10, 20, and 50 nodes topology is approximately similar during 0–5 s. But after 6s the average throughput for 10 and 20 nodes topology drops while throughput for 50 nodes topology grows identically. As the cluster heads can utilize multiple gateways to pass the data traffic to the control plane, it significantly lessens the possibility of traffic congestion or bottlenecks in a single gateway even if the number of nodes increases. For this reason, 50 nodes topology comparatively gives better throughput delivery compared to others.

Further, the authors take the best performer in throughput comparison (50nodes) and compare it with an extended version of the Multinetwork Information Architecture (MINA) [24]. Figure 5 shows that the average throughput

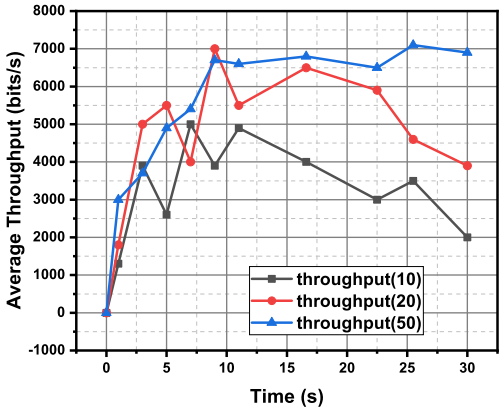

Fig. 4. Average throughput comparison (10, 20, 50 nodes)

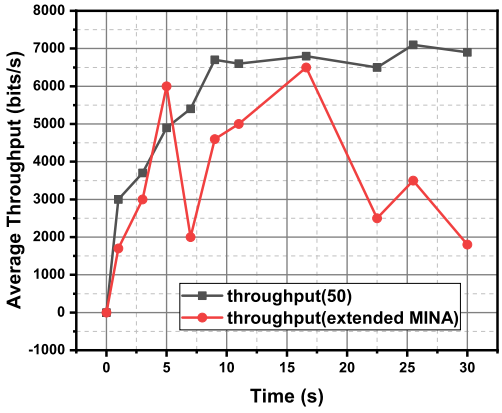

Fig. 5. Average throughput comparison (50 nodes vs extended MINA)

of both networks increases identically until they reach 6000bits/s but after 5s the throughput of extended MINA suddenly falls down meanwhile the throughput of 50 nodes topology progresses similarly. As the authors have used multiple controllers in the proposed network architecture for proper distribution of network traffic among respective controllers, it minimizes the delay time and improves network performance. Besides, the management and orchestration of network functions virtualization improves the load balancing of the network resulting in a greater throughput delivery.

4.2 Round Trip Time for Different Number of Nodes

Round-Trip Time (RTT) is the time that need for a signal to be sent plus the time it takes for an acknowledgment of that signal to be received. At first, the authors compare their three build topology with each other. From Fig. 6 it is shown that round trip time decreases when the number of nodes increases. Since the network is fully distributed so, multiple controllers are available for handling specific task and thus reduces the response time. That has a great impact on the round trip time even the number of nodes increases in the network. As a result, 50 nodes topology requires the lowest period for a round trip.

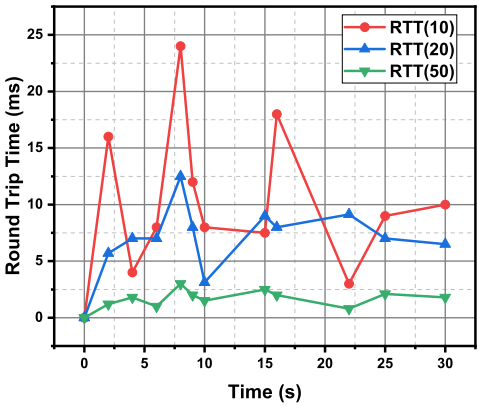

Fig. 6. RTT comparison (10, 20, 50 nodes)

Further, the authors compare the RTT of 50 nodes topology with another OpenFlow-based protocol [25]. The result is illustrated in Fig. 7. It shows that 50 nodes topology requires a little bit long time for round trip before 9s compare to the OF-based protocol. But after 10s RTT of 50 nodes topology decreases smoothly compare to the OF-based protocol. For applying the clustering method in the network, the IoT nodes can easily communicate with SDN-IoT gateways via multiple cluster heads preventing network congestion. As a result, it reduces the network latency and improves the round trip time as well.

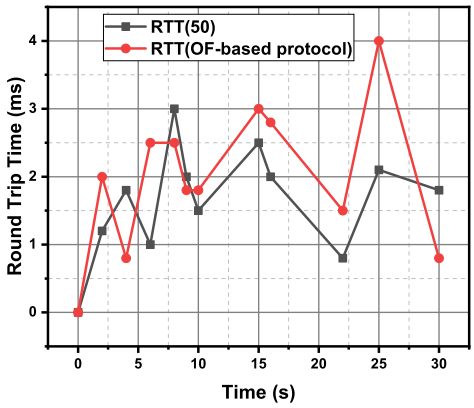

Fig. 7. RTT comparison (50 nodes vs OF-based protocol)

4.3 Time Sequence (tcptrace) for Different Number of Nodes

Time Sequence (tcptrace) illustrates the TCP metrics including forwarded segments and acknowledgments. Figure 8 indicating that sequence number increases with time if the number of nodes increases. For this reason, the increment of sequence number for 50 nodes topology is greater than 10 and 20 nodes topology. As we know that time sequence indicates the TCP flows so this tcptrace comparison symbolizes the progress of TCP flows in the particular network. Moreover, this comparison is performed to show how the TCP flow behaves for a varying number of nodes.

Further, the authors have compared the time sequence of 50 nodes topology with the OpenFlow-based protocol once again. The result is depicted in Fig. 9. From Fig. 9, it is easily noticeable that 50 nodes topology gives a smoother time

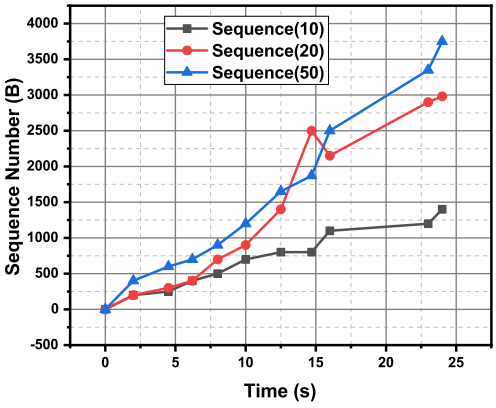

Fig. 8. Time sequence comparison (10, 20, 50 nodes)

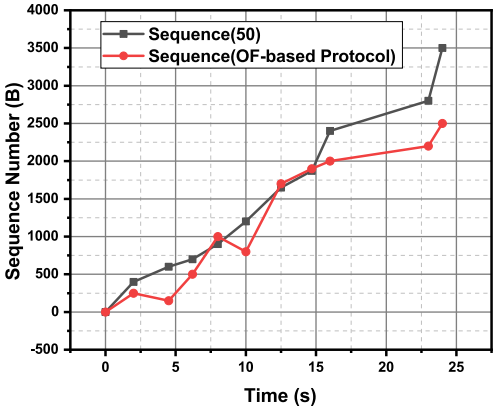

Fig. 9. Time sequence comparison (50 nodes vs OF-based protocol)

sequence increment compared to the OF-based protocol. In the proposed network multipurpose distributed controllers are used to accept and transfer data packets via multiple gateways that diminish the possibility of single-point failure in the network resulting in a higher data transmission rate. That's why the TCP flow of the 50 nodes topology comparatively higher and smoother than the conventional OF-based protocol.

5 Conclusion

The implementation of NFV is essential for the balance and orchestration of virtual resources in SDN-IoT environment. Despite the immense speed at which NFV is being accepted by both academia and industry, it is still in the early stage. Besides, the optimization of algorithms for real streaming in SDN/NFV architecture is a challenging task. Based on this premise, the authors have proposed an SDN based distributed IoT network with NFV implementation for smart cities. Authors believe that their NFV implemented distributed SDN-IoT network inherently supports heterogeneity and gives flexibility to smart citizens to manage IoT multi-network more efficiently and dynamically.

This research is conducted in a simulation environment. Practical application and performance analysis will be the future research work. Additionally, blockchain technology can be implemented in the proposed network to have a peer-to-peer network where non-confident members can't interact with each other without a trusted intermediary.

References

1. Kalkan, K., Zeadally, S.: Securing internet of things with software defined networking. IEEE Commun. Mag. **56**(9), 186–192 (2017)
2. Chakrabarty, S., Engels, D.W.: A secure IoT architecture for smart cities. In: 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 812–813. IEEE (2016)
3. Han, B., Gopalakrishnan, V., Ji, L., Lee, S.: Network function virtualization: challenges and opportunities for innovations. IEEE Commun. Mag. **53**(2), 90–97 (2015)
4. McKeown, N., et al.: Openflow: enabling innovation in campus networks. ACM SIGCOMM Comput. Commun. Rev. **38**(2), 69–74 (2008)
5. Rahman, A., Islam, M.J., Sunny, F.A., Nasir, M.K.: Distblocksdn: a distributed secure blockchain based SDN-IoT architecture with NFV implementation for smart cities. Technology (ICIET) **23**, 24 (2019)
6. Tayyaba, S.K., Shah, M.A., Khan, O.A., Ahmed, A.W.: Software defined network (SDN) based internet of things (IoT): a road ahead. In: Proceedings of the International Conference on Future Networks and Distributed Systems, p. 15. ACM (2017)
7. Chourishi, D., Miri, A., Milić, M., Ismaeel, S.: Role-based multiple controllers for load balancing and security in SDN. In: 2015 IEEE Canada International Humanitarian Technology Conference (IHTC 2015), pp. 1–4. IEEE (2015)
8. Li, Y., Chen, M.: Software-defined network function virtualization: a survey. IEEE Access **3**, 2542–2553 (2015)
9. Hoffmann, M., et al.: SDN and NFV as enabler for the distributed network cloud. Mob. Netw. Appl. **23**(3), 521–528 (2018)
10. Islam, M.J., Mahin, M., Roy, S., Debnath, B.C., Khatun, A.: Distblacknet: a distributed secure black SDN-IoT architecture with NFV implementation for smart cities. In: 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), pp. 1–6. IEEE (2019)
11. Chakrabarty, S., Engels, D.W., Thathapudi, S.: Black SDN for the internet of things. In: 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems, pp. 190–198. IEEE (2015)
12. Feghali, A., Kilany, R., Chamoun, M.: SDN security problems and solutions analysis. In: 2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), pp. 1–5. IEEE (2015)
13. Bull, P., Austin, R., Popov, E., Sharma, M., Watson, R.: Flow based security for IoT devices using an SDN gateway. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 157–163. IEEE (2016)
14. Al Shuhaimi, F., Jose, M., Singh, A.V.: Software defined network as solution to overcome security challenges in IoT. In: 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 491–496. IEEE (2016)
15. Gonzalez, C., Charfadine, S.M., Flauzac, O., Nolot, F.: SDN-based security framework for the IoT in distributed grid. In: 2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech), pp. 1–5. IEEE (2016)
16. Farris, I., et al.: Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems. In: 2017 IEEE Conference on Standards for Communications and Networking (CSCN), pp. 169–174. IEEE (2017)

17. Muoz, R., et al.: The adrenaline testbed: an SDN/NFV packet/optical transport network and edge/core cloud platform for end-to-end 5G and IoT services. In: 2017 European Conference on Networks and Communications (EuCNC), pp. 1–5. IEEE (2017)
18. Sinh, D., Le, L.V., Lin, B.S.P., Tung, L.P.: SDN/NFV–a new approach of deploying network infrastructure for IoT. In: 2018 27th Wireless and Optical Communication Conference (WOCC), pp. 1–5. IEEE (2018)
19. Maksymyuk, T., Dumych, S., Brych, M., Satria, D., Jo, M.: An IoT based monitoring framework for software defined 5G mobile networks. In: Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication, p. 105. ACM (2017)
20. Krishnan, P., Najeem, J.S., Achuthan, K.: SDN framework for securing IoT networks. In: Kumar, N., Thakre, A. (eds.) UBICNET 2017. LNICST, vol. 218, pp. 116–129. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-73423-1_11
21. Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Munoz, J.J., Lorca, J., Folgueira, J.: Network slicing for 5G with SDN/NFV: concepts, architectures, and challenges. IEEE Commun. Mag. **55**(5), 80–87 (2017)
22. Almustafa, K., Alenezi, M.: Cost analysis of SDN/NFV architecture over 4G infrastructure. Procedia Comput. Sci. **113**, 130–137 (2017)
23. Ojo, M., Adami, D., Giordano, S.: A SDN-IOT architecture with NFV implementation. In: 2016 IEEE Globecom Workshops (GC Wkshps), pp. 1–6. IEEE (2016)
24. Qin, Z., Denker, G., Giannelli, C., Bellavista, P., Venkatasubramanian, N.: A software defined networking architecture for the internet-of-things. In: 2014 IEEE Network Operations and Management Symposium (NOMS), pp. 1–9. IEEE (2014)
25. Wang, Y., Bi, J.: A solution for IP mobility support in software defined networks. In: 2014 23rd International Conference on Computer Communication and Networks (ICCCN), pp. 1–8. IEEE (2014)