# SDN for IoT Environment: A Survey and Research Challenges

*Kamaran H.* Manguri[1*], *Saman M.* Omer[1]

[1]Computer Science Department, University of Raparin, Rania, Iraq,

**Abstract.** Recently, it has emerged that both Internet of Things (IoT), and Software Defined Network (SDN) are becoming popular technologies. The main goal of IoT is to link electronic devices via the internet, meanwhile SDN facilitates network arrangement for management of a network by distinguishing the control layer and the data layer from each other. The number of electronic devices over the internet is increasing constantly, therefore it is a complicated process to manage and control especially over the huge distributed network. IoT network can be reasonably flexible and programmable through The SDN without introducing any trouble to the previously implemented network infrastructure. This paper reviews various IoT domains and applications such as cellular network, wireless Sensor, IoT management, security and smart city framework and common IoT SDN solutions. Moreover, The IoT and SDN notion has been explored critically, with assessing the current contributions in the research field. Lastly, analyzing current available solutions for SDN-based IoT implementations comparatively helps easily understanding the emerging trends view.

**Keywords:** SDN, SDN Applications, IoT, Integration of SDN-IoT

## 1 Introduction

The Internet of Things (IoTs) is an emerging technology which enables smart ecosystem for leveraging heterogeneous technologies. Generally, in IoT network physical devices are connected to the internet such as RFID tags, actuators, wireless sensors, and/or wireless communication [1]. The IoT devices have the capability to observe, analyze and take intelligent decisions based on collected information from the surroundings and manipulation of the underlying network [2]. IoT has many applications such as unit controls, symptomatic gear, vehicles, airplane, and even atomic reactors. With regarding to secret and certain correspondences because of the nearness of the Internet of Things that provide reducing attacks and against assault. Two different models are used for security which including firewalls and system edge identification/moderation instruments to forestall outer assaults [3]. A huge data is generated and collected from IoT devices that made an issue with developers and researchers while managing, controlling, monitoring and securing of IoT devices in a heterogeneous network. In addition, heterogeneous network does not support completely in the traditional network that became an issue to fast development and

[*] Corresponding author: kamaran@uor.edu.krd

deployment and IoT full realization limited benefits, which are required for customers and service demands [2].

The proprietary nature of devices lead to the progress of innovation is very slow in the legacy network. Therefore, the infrastructure of traditional network and devices should be changed to realize full IoT benefits. In technologies terms, the integrated architecture may provide full IoT benefits [2]. Moreover, SDN is a new networking architecture that tries to decouple the control and data planes. This separation gives a global view of the net-work to the network controller, facilitating traffic engineering and network management at runtime [4].

In this review, different works highlighted that provide SDN based solutions for IoT environment. The recent studies during the period January 2016 - July 2021 have been reviewed by focusing on SDN applications and solutions in the IoT environment. The organization of this review is as follows. Section I provides an introduction of IoT and SDN. Background of SDN architecture addressed in Section II. Also, SDN and SDN enabled IoT architecture explained in Section III. In Section IV, the details of this review for the existing solutions are explained. The results and discussion are given in Section V. Finally, the last section remarks a conclusion.

## 2 SDN Architecture

The architecture of SDN includes six major components. The first component is SDN control logic which is managed by using management plane to give flexibility and easiness for implementing a new application and service. Second component is the control plane that includes one or numerous controllers and it is the most important intelligent layer. It forward various kinds of policies and rules through the Southbound Interface (SI) to the infrastructure layer. Third component, data plane represents forwarding devices on the network (routers, switches, load balancers, etc.), which is called infrastructure layer. The southbound APIs used to interact with the control plane by getting the forwarding policies and rules for applying them to the conforming devices. Fourth component, the management and control layers are allowed to communicate that are mainly a set of open source APIs using Northbound Interfaces (NI) [5]. Fifth component, east-west interfaces allows communication between various controllers that are not yet standardized. A messaging and notification system or a distributed routing protocol are used such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF). Sixth, the SI make an interaction between data plane and control plane that may be defined such as protocols summarily, which permits push policies from controller to the forwarding plane [6].

## 3 SDN and SDN Enabled IoT Architecture

In SDN, control plane and forwarding plane are decoupled, and APIs are used to communicate between two planes such as OpenFlow [7]. SDN is a layered architecture that includes three layers, which are control plane/controller, application layer and data plane. Data plane layer comprises dumb forwarding devices such as switches and routers that forward data only on the controller instructions. The controller acts as a brain and controls the whole network and possesses managed by controller which provides programmability, flexible management for flow forwarding state in the data plane [1]. The application layer abstracted to the customer needs, which is Northbound used to communicate with the controller APIs such as REST full API. All applications and programs are running above the controller. The controllers since its inception are many in the market for example, Floodlight [10], OpenDaylight [7], NoX/POX, and etc. The rule of incoming flows defined via SDN controller from the data plane. SDN Layers are communicate together through open APIs called SI and NI API [1].

## 4 Literature Review

IoT with SDN supervision is hot topic on different platforms. Several researches and investigations are carried out to make of the using programmability SDN in IoT network.

### 4.1 SDN Based Cellular Network

The more complex and grouped a telecommunication environment is, the more difficult it is to obtain the satisfied outcome that needs a radio technology to be physically intervene. EOPA and RNOPA are suggested to address the reduction in SDN relayed networks with the different cloudlets in the same locations with different APs in IoT linked devices [11]. SoftAir and adds software defined gateways (SD-GWs) are used to design SDN, which are performs a cross-layer optimization between various IoT electronic devices and radio based systems during communication functionalities [12]. The scalability and availability of IoT network have been considered to address an integration IoT with 5G network because of large number of connected devices in IoT [13].

### 4.2 SDN for Wireless Sensor Based IoT Devices

Wireless sensors need to reduce power usage and improve the scalability in the IoT environment. For this purpose, many efforts based SDN have been seen in the literature. µSDN had proposed in [15] to solve the problems caused by applying SDN in low-power Wi-Fi networks. A novel SDN framework based WSN infrastructure are empowered to cooperate effortlessly with cloud based environments in [16]. A simulation introduced in [17] for optimization infrequent and power consumption regarding lowest control traffic.

### 4.3 SDN Based IoT Management

IoT management includes improving flow control and mobility in crowded and heterogeneous networks, enhancing network scalability, maintainable control, fault and exception tolerance, enforce traffic management and etc. In [18] UbiFlow suggested that is used to separate the urban-scale SDN into different geographic locations through multiple controllers. In addition, a Trust List proposed in [19] that refers to the trust distribution among IoT-linked stakeholders and appropriate combination between SDN and blockchain to enforce traffic management at the edge of networks.

### 4.4 SDN Security Framework for IoT

Connecting to the internet lead to open some security issues such as malware attacks and access unauthorized users. The vulnerabilities and security threats were rises that are related to IoT devices. Security Authentication is provided by the Edge servers using a lightweight authentication scheme [22]. In Addition, an utilized SDN and blockchain techniques proposed in [23] to remove the unnecessary re-authentication. Also, in [24] granular policies enforced to secure the flows in the IoT network infrastructure with providing networking authentication for IoT device.

### 4.5 SDN Based IoT for Smart City Application

SDN that separates data plane and control plane for the purpose of supporting configuring network compared with existing network, which is suitable for smart cities requirement, even though in the reliability faces a problem but the highest impact have showed on the system. Quality of service (QoS) aware design such as SDN-IIoT, which deals with load on the server had been proposed in [27]. QoS aware Optimum Path Selection and Rule Caching Policy (QOPS-RCP) for SDN based IoT proposed in [28].

## 5 Discussion

The new idea of combination of IoT and SDN is still at the beginning pace, and standardizations attempts. In spite of having multiple efforts to dominate for universal standard, the practical solution is still not available. In other words, some of the aspects are remaining conceptual/theoretical. Different kind of SDN establishment for various IoT domains with respect to the cellular network, IoT management, wireless sensor, security and smart city are given in the Table 1. It can be said that the majority of the conducted studies are not validated practically. Yet, just representative proposals framework becomes center of attraction during the recent years.

**Table 1.** Summary of the SDN based proposed model for IoT environment.

| Application | Referen ce | Architecture/ Protocol/ OS | Contribution(s) |
|---|---|---|---|
| Cellular Network | [11] | EOPA and RNOPA | Produce optimum performance of reducing average cloudlet access latency and consistency |
| | [12] | SoftAir | Cross-layer optimization performed between IoT devices and radio based systems. |
| | [13] | MEC, D2D | Integrating heterogeneous IoT networks with the 5G networks and enabling dense deployment. |
| | [14] | NB-IoT | The proposed queueing models can be properly applied in different case scenarios. |
| Wireless Sensor | [15] | RPL-based IEEE 802.15.4-2012 | Improving the scalability. |
| | [16] | WSN, MQTT | WSN infrastructure is used to develop a novel framework for the purpose of cooperating effortlessly with cloud based environments. |
| | [17] | - | Optimization issue is introduced using the simulation with regarding lowest control traffic. |
| IoT Management | [18] | UbiFlow | Suggested to use distributed hashing as supervising structure to improving network scalability and mobility controlling |
| | [19] | PoC | Proposed a Trust List that refers to the trust distribution among IoT-linked stakeholders |
| | [20] | ONOS and ODL | Developed different SDN management approach of SDN controllers. |
| | [21] | - | Introducing a hierarchical structure for the control plane |
| Security Framework | [22] | Edge computing | Proposed a framework to authorized access to the IoT devices by the Edge servers. |
| | [23] | Lightweight protocol | Unnecessary re-authentication is removed in repeated handover among heterogeneous cells. |

| | | | |
|---|---|---|---|
| | [24] | ONOS and Raspbian Virtual Machines | Granular policies enforced to secure the flows in the IoT. |
| | [25] | SDNWISE | A novel framework proposed for the detection of DDoS attacks. |
| | [26] | OVS | Proposed an efficient solutions to provide device classification and malicious traffic detection based on SDN and Machine Learning. |
| Smart City | [27] | SDN-IIoT and QoS | Proposed a switch application using the POX controller. |
| | [28] | QoS and QOPS-RCP | Proposed a QoS aware Optimum PS and RC Policy (QOP-RCP) for SDN-IoT. |

## 6 Conclusion

The IoT seems to have a profound impact on the communication approach between human and electronic devices in the next decades. Today, the view is exceeding the limit of only connecting tangible objects via the internet. Nevertheless, as IoT is in early start of its era, it has been faced with several obstacles such as, security, programmability, flexibility, and data management. It is highly likelihood to include both programmability and centralized control in management of IoT with SDN integration. In this review the improvement of network performance with SDN has been shown for the promising solutions for current IoT. The results of these review show that solutions are not fully integrated into SDN for IoT environment. Also, most of models are evaluated and tested on the simulation models and they are not implemented on the real IoT environment. Finally, despite of many efforts had been done to build frameworks based on SDN still comprehensive architecture and framework are the challenge for researchers.

## References

1. S. K. Tayyaba, M. A. Shah, O. A. Khan, and A. W. Ahmed, "Software defined network (sdn) based internet of things (iot) a road ahead," in Proceedings of the International Conference on Future Networks and Distributed Systems, 2017, pp. 1-8.
2. S. K. Tayyaba, M. A. Shah, N. S. A. Khan, Y. Asim, W. Naeem, and M. J. n. Kamran, "Software-defined networks (SDNs) and Internet of Things (IoTs): A qualitative prediction for 2020," vol. 7, no. 11, 2016.
3. A. H. Mohammed, R. M. KHALEEFAH, and I. A. Abdulateef, "A Review Software Defined Networking for Internet of Things," in 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2020, pp. 1-8: IEEE.
4. O. Salman, I. Elhajj, A. Chehab, and A. J. C. N. Kayssi, "IoT survey: An SDN and fog computing perspective," vol. 143, pp. 221-246, 2018.
5. D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. J. P. o. t. I. Uhlig, "Software-defined networking: A comprehensive survey," vol. 103, no. 1, pp. 14-76, 2014.
6. O. Blial, M. Ben Mamoun, R. J. J. o. C. N. Benaini, and Communications, "An overview on SDN architectures with multiple controllers," vol. 2016, 2016.
7. W. Braun and M. J. F. I. Menth, "Software-defined networking using OpenFlow: Protocols, applications and architectural design choices," vol. 6, no. 2, pp. 302-336, 2014.
8. J. Li, E. Altman, and C. J. Z. c. Touati, "A general SDN-based IoT framework with NVF implementation," vol. 13, no. 3, pp. 42-45, 2015.
9. J. Medved, R. Varga, A. Tkacik, and K. Gray, "Opendaylight: Towards a model-driven sdn controller architecture," in Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, 2014, pp. 1-6: IEEE.

10. J. Liu, Y. Li, M. Chen, W. Dong, and D. J. I. c. m. Jin, "Software-defined internet of things for smart urban sensing," vol. 53, no. 9, pp. 55-63, 2015.
11. L. Zhao, W. Sun, Y. Shi, and J. Liu, "Optimal Placement of Cloudlets for Access Delay Minimization in SDN-Based Internet of Things Networks," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1334-1344, 2018.
12. L. Tello-Oquendo, I. F. Akyildiz, S. Lin, and V. Pla, "SDN-based architecture for providing reliable Internet of Things connectivity in 5G systems," in 2018 17th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), 2018, pp. 1-8.
13. A. A. Ateya, A. D. Algarni, M. Hamdi, A. Koucheryavy, and N. J. E. Soliman, "Enabling Heterogeneous IoT Networks over 5G Networks with Ultra-Dense Deployment—Using MEC/SDN," vol. 10, no. 8, p. 910, 2021.
14. X. Chen et al., "Traffic modeling and performance evaluation of SDN-based NB-IoT access network," vol. 32, no. 16, p. e5145, 2020.
15. M. Baddeley, R. Nejabati, G. Oikonomou, M. Sooriyabandara, and D. Simeonidou, "Evolving SDN for Low-Power IoT Networks," in 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), 2018, pp. 71-79.
16. C. Çeken and M. Al-Hubaishi, "Integrating SDN-enabled wireless sensor networks into the Internet," in 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2019, vol. 2, pp. 1090-1094: IEEE.
17. K. Choumas, D. Giatsios, P. Flegkas, and T. J. E. Korakis, "SDN Controller Placement and Switch Assignment for Low Power IoT," vol. 9, no. 2, p. 325, 2020.
18. D. Wu et al., "Towards distributed SDN: Mobility management and flow scheduling in software defined urban IOT," 2018.
19. K. Kataoka, S. Gangwar, and P. Podili, "Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN," in 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), 2018, pp. 296-301: IEEE.
20. I. Bedhief, M. Kassar, T. Aguili, L. Foschini, and P. Bellavista, "Self-Adaptive Management of SDN Distributed Controllers for Highly Dynamic IoT Networks," in 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 2019, pp. 2098-2104: IEEE.
21. Z. Eghbali and M. Z. Lighvan, "A hierarchical approach for accelerating IoT data management process based on SDN principles," Journal of Network and Computer Applications, vol. 181, p. 103027, 2021/05/01/ 2021.
22. J. Li et al., "A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System," IEEE Access, vol. 8, pp. 135479-135490, 2020.
23. A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K. R. Choo, "Blockchain-enabled Authentication Handover with Efficient Privacy Protection in SDN-based 5G Networks," IEEE Transactions on Network Science and Engineering, pp. 1-1, 2019.
24. K. K. Karmakar, V. Varadharajan, S. Nepal, and U. Tupakula, "SDN Enabled Secure IoT Architecture," IEEE Internet of Things Journal, pp. 1-1, 2020.
25. J. Bhayo, R. Jafaq, A. Ahmed, S. Hameed, and S. A. Shah, "A Time-Efficient Approach Towards DDoS Attack Detection in IoT Network using SDN," IEEE Internet of Things Journal, pp. 1-1, 2021.
26. H. Gordon, C. Park, B. Tushir, Y. Liu, and B. J. a. p. a. Dezfouli, "An Efficient SDN Architecture for Smart Home Security Accelerated by FPGA," 2021.
27. H. Babbar, S. Rani, A. Singh, M. Abd-Elnaby, and B. J. J. S. Choi, "Cloud Based Smart City Services for Industrial Internet of Things in Software-Defined Networking," vol. 13, no. 16, p. 8910, 2021.
28. H. M. Mahantesh, M. Nageswara Guptha, and M. S. Hema, "Optimized Path and Reduced Rule Caching Cost for Software Defined Network (SDN) Based Internet of Things (IOT)," Wireless Personal Communications, 2021/07/03 2021.