SDN-Based Approaches for Heterogeneity and Interoperability in Internet of Things: An Overview

Sihem Benkhaled, Mounir Hemam, and Moufida Maimour

Abstract The Internet of Things (IoT) and Software Defined Network (SDN) are two emerging technologies. The IoT aims to connect devices over the Internet. Networks on which these IoT devices operate will continue to be heterogeneous and the network becomes more complex. SDN paradigm provides efficient network management by decoupling the control plane and the data plane, it allows facing network heterogeneity and interoperability (networks-to-network communications) through a programmable manner, this paradigm allows the communication between various objects independently of their respective technologies and thus allows dealing with the problem of heterogeneity. The main objective of this chapter is to present an overview of SDN-based pertinent solutions that consider network level interoperability and heterogeneity in the IoT.

Keywords Internet of Things (IoT) · Interoperability · Heterogeneity · Software Defined Networks (SDN)

1 Introduction

Internet of Things (IoT) [1] is a novel emerging technology where any things from anywhere are connected together as well as to the Internet infrastructure at any time. IoT combines aspects and technologies coming from different disciplines. IoT devices such as laptops, smartphones, sensors and actuators are expected to exceed 45 billion by 2020. These devices may use various types of technologies and communication protocols and may produce large volumes of data. Hence, the need

S. Benkhaled (✉) · M. Hemam
Department of Computer Science, University of Khenchela, Khenchela, Algeria

M. Maimour
University of Lorraine, CRAN, UMR, 7039, Nancy, France
e-mail: moufida.maimour@univ-lorraine.fr

for installing new network access and core devices will increase and hence create several issues such as interoperability, heterogeneity, security, and scalability [2].

Particularly, in [2] the authors state that 40% of the potential benefits of IoT can be obtained with the interoperability between IoT systems. It is fascinating that this issue can be easily and dynamically resolved thanks to the paradigm of Software Defined Networking (SDN). It mainly allows hiding all the control and management operations by setting them inside a middleware layer, which alleviates the dependency from vendors.

In this chapter, we are interested in the use of Software defined networks technology to provide solutions to network level interoperability. Section 2 introduces the issue of network interoperability in the IoT and Sect. 3 presents the concept of SDN. Section 4 presents SDN-based IoT networks. Section 5 overviews research work where SDN-based technologies are used to overcome issues related to heterogeneity and interoperability in the IoT system.

2   Network Interoperability in IoT

The IEEE defines interoperability as the ability to interconnect and communicate different systems to form a cost effective and easy to implement network [3]. With respect to heterogeneity, interoperability can be seen from different perspectives, namely, device interoperability, network interoperability, syntactic interoperability, and semantic interoperability.

As networks on which IoT devices operate on will continue to be heterogeneous, network interoperability will continue to be more than required. Network level interoperability deals with mechanisms to enable seamless message exchange between systems through different networks (networks of networks) for end-to-end communication. In fact, IoT devices generally rely on various short ranged wireless communication and networking technologies [3]. To make systems interoperable, each system should be able to exchange messages with other systems through various types of networks. Due to the dynamic and heterogeneous network environment in IoT, the network interoperability level should handle issues such as addressing, management, routing, resource optimization, scalability, security, QoS, and mobility support [3].

In this level, protocol interoperability is the main focus. At the standardization level, the IETF has developed a set of standards for routing such as RPL, CORPL, and CARP and solutions for encapsulation including 6LowPAN, 6TiSCH, 6Lo, and Thread [3]. Another new solution to address interoperability in this level is software-based approaches such as Software Defined Networking (SDN) which hides all the control and management operations from the IoT devices by setting them inside a middleware layer, which alleviates the dependency from vendors [4].

3   Software Defined Networking (SDN)

SDN is a new networking paradigm that addresses the limitations of current network infrastructures. It brings flexibility allowing different objects connected to heterogeneous networks to communicate with each other. Simultaneous connections of various communication technologies can be handled.

Network management decisions such as routing, scheduling can be done at the SDN controller.

SDN architecture can be characterized by: (1) Decoupled data and control plans; (2) Routing decisions based on flow, rather than destination; (3) Control logic is moved to an external entity (SDN controller or network operating system); and (4) Network programmable by software applications that interact with data plane devices [4].

The separation of interests or concepts, introduced between the definition of network policies, their implementation in switching hardware, and the routing of traffic, is the key to the desired flexibility: by breaking the network control problem into manageable parts, SDN makes it easy to create and introduce new network abstractions, simplifying network management and making it easier to evolve.

SDN is composed of three layers: Data plan layer, Control layer, and application layer [5]. The *data plan layer* is composed of various networking equipments which form the underlying network that forward network traffic. It could be a set of network switches and routers in the data center. This layer would be the physical one over which network virtualization would be laid down through the control layer (where SDN controllers would sit and manage underlying physical network).

The control layer is an intermediate between the infrastructure (data plane) layer and the application layer. It is implemented in a logically centralized controller (or network operating system), simplifying policy enforcement and network configuration and evolution. It can manage physical devices with various features and functions via different interfaces from lower layer (southbound API).

The application layer is an open area to develop as much innovative application as possible by leveraging all the network information about network topology, network state, network statistics, etc. There may be several types of applications which can be developed like those related to network automation, network configuration and management, network monitoring, network troubleshooting, network policies and security. Such SDN applications can provide various end-to-end solutions for real world enterprise and data center networks.

Traditional networks are usually rigid, fixed and complex which is difficult to manage and configure. Heterogeneity, scalability, and interoperability have been major challenges. SDN is a promising paradigm to provide solutions to network interoperability and heterogeneity issues through virtualization [4].

SDN is applied to the IoT to facilitate networking applications (heterogeneity of protocols, QoS management, and security). Even though the devices have different protocols, the forwarding devices in the router are able to convert them in an understandable form by the receiver [4].

4   IoT Systems with Software Defined Networking (SD-IoT)

In recent years, the SD-IoT has become one of the main topics of IoT-related researches. It deals with several issues for deploying and managing numerous nodes of IoT infrastructure by adopting the idea of SDN [6].

The IoT aims to connect objects over the Internet and the SDN is expected to resolve traditional network issues like heterogeneity, interoperability, and scalability by allowing orchestration for network management and network interoperability by decoupling the control plane and the data plane [3].

Integrating IoT and SDN will increase network efficiency as it will make it possible for a network to respond to changes or events detected at the IoT application layer through network reconfiguration. It allows routing efficiency, high data transmission, network management and resource allocation for the IoT devices to meet the growing need of the user demands [7].

The general architecture for SDN-based IoT is shown in Fig. 1 redrawn from [1]. SD-IoT architecture deals with clear separation of concern between services provided in the control plane and the data plane. Control plane specifies the management of network traffic and data plane specifies the mechanisms to forward traffic to desired destination. SDN-based IoT management specifies how the applications on top of the Management Layer interact with the control plane and the coordination among them.

There are three layers in the SD-IoT architecture. The data plane includes sensors which sense and forward data in the network. The control plane that consists in the

Fig. 1 IoT architecture based SDN technology [1]
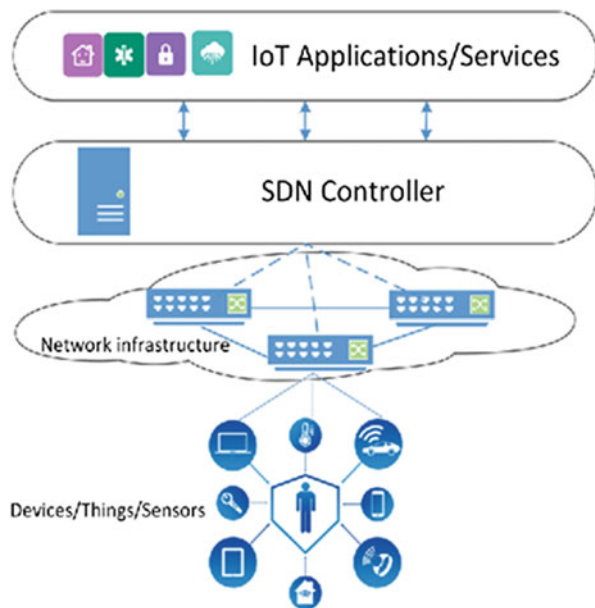
controller which controls the whole network. The application plane includes diverse network applications such as routing.

IoT networks need to be based on a robust architecture to answer these requirements and inspired by SDN to make them more flexible.

The SDN controller provides programmability and flexible management for flow forwarding state in the data plane by having a global view of the network. SDN can facilitate high data transmission, spectral efficiency, resource allocation and network management for the IoT devices for fulfilling growing need of the customer demands (Fig. 1).

5   Overview of SDN–Based Solutions to Network Heterogeneity and Interoperability in IOT

SDN has been applied to IoT to facilitate networking applications while dealing with heterogeneity, network and device management, routing, and security issues. In order to have an interoperable network and overcome these issues, it is necessary to create and manage the network devices efficiently so an interoperable network is obtained with efficient data exchange [8].

This section gives a general overview of how applied SDN to IoT in order to solve heterogeneity and interoperability issues in the connectivity and network level. We focus on the pertinent approaches (summarized in Table 1) which can be potentially fulfilled by SDN technology.

In this context, Jie. Li, et al. proposed a general framework for IoT based on SDN with distributed controller and managing. Another conceptualization of generic IPv6-based IoT devices architecture based on SDN for smart cities is presented in [15]. Hung et al. [10] propose SDN-based management framework for the IoT devices, as the 6LoWPAN protocol gains momentum, particularly in view of the IoT new network management solutions are developed to cater for these devices.

Jia Qiang Liu, et al. proposed an SD-IoT architecture in [9], for the smart management of IoT devices. In [13], A. Desai et al. proposed an architecture for IoT integrated into SDN in which IoT devices are managed by OpenFlow based management devices. Wu et al. in [19], presents UbiFlow framework which provides the integration of the SDN and the IoT, proposed an efficient flow control and mobility management in urban multi-networks using SDN distributed controllers. In UbiFlow architecture, IoT network is partitioned into small network chunks/cluster. Each partition is controlled by a physically distributed SDN controller, the IoT devices in each partition may be connected to the different access point for different data requests. In [12] the authors propose SDN-based cloud platform approaches for IoT network connectivity. The work in [14] presents general SDN-based architectures to facilitate the scalability, heterogeneity, and interoperability among IoT devices or nodes.

Table 1 Proposed IoT approaches based on SDN for heterogeneous networks

Approaches	Goals	Proposition	Control plane decoupling	Advantage
Liu et al. [9]	Device management High level management capabilities Low latency and heterogeneity Mobility using fog computing	Edge computing enabling the IoT	Distributed ODL, Onix, and ONOS controllers SD fog gateways, OF-switches	Supports multiple identification and communication Technologies Multiple SD fog gateways ensure interoperability Centralization leading to security enhancement to some extent
Huang et al. [10]	Scalability Efficient interoperability and traffic Engineering	Framework for monitor IoT devices	Centralized SDN controllers	Architecture based on independent IoT system and efficient management IoT devices
Hakira et al. [11]	Networking, mobility, standardization, security, QoS	IoT architecture combining SDN with message-based publish/subscribe DDS middleware	Centralized SDN controller	Filtering and fusion mechanism for efficient traffic engineering
Desai et al. [12]	Heterogeneity, IoT device to cloud communication	OF-enabled management device	Distributed NOX, POX, ODL	Proposed an OF-enabled management device, which will make network simpler
Salman and Jain [13]	Single solution for multiple challenges: Scalability, heterogeneity, QoS, latency, reliability, security	Centralized SDN control network for IoT with decentralized data management Layered model: Works in application, control, network, and device layers Implements SD-gateways in the fog with specialized algorithms	Distributed SDN controller	Inter-controller communication. Intelligent fog nodes SDN controller uses management protocols (i.e., NetConf and Yang, OF-Config and extended OF) Use of unified application for communication

Table 1 (continued)

Approaches	Goals	Proposition	Control plane decoupling	Advantage
Lin et al. [14]	Heterogeneity, interoperability, scalability, security, QoS	Centralized global view Heterogeneous devices with various data formats for information modeling	Centralized layered IoT controller	Adaptable network state Minimized latency and optimized interoperability and scalability Better performance and flow scheduling
Li. et al. [15]	Heterogeneity, interoperability, scalability, availability, security	IoT gateways and SDN switches. Distributed network OS	Distributed SDN controller	Distributed OS providing centralized control Global view of the underlying physical distributed network environment
Iyer et al. [16]	Heterogeneity, interoperability, latency, scalability, reliability, security	SDN gateway/router	Distributed network OS Distributed POX	Discovering IoT devices from different domains Real time evaluation for latency in IoT devices and sensors, using Raspberry Pi
Mann et al. [17]	Interoperability, device discovery, scalability, security, efficiency management, flexibility	An SDN-IoT architecture with NFV implementation	SDN controller and virtualized IoT gateways	Enhanced performance and management of hardware, software and virtual resources Device discovery with enhanced connectivity
Qin et al. [18]	Heterogeneity, scalability, mobility	Replacement of traditional gateway with SDN gateway	Distributed ONOS, ODL	Improved network efficiency and agility SDN-enabled gateway Intelligent routing protocols and caching techniques Architecture only

Table 1 (continued)

Approaches	Goals	Proposition	Control plane decoupling	Advantage
Desai et al. [13]	Scalability, heterogeneity, agile and inexpensive	SD solution for IoT to forward store, and secure data	Distributed (multiple SDN controllers)	Maniples SD application modules to facilitate IoT network
Wu et al. [19]	Interoperability, device discovery, scalability, security, efficiency management, flexibility	An SDN-IoT architecture with NFV implementation	SDN controller and virtualized IoT gateways	Enhanced performance and management of hardware, software and virtual resources Device discovery with enhanced connectivity
Julia and Skarmeta [8]	– Efficient routing – Cost-effective deployment	Resolves CAPEX issues in IoT	Centralized SDN controller	Efficient inter-domain routing Less connected and deployed devices, hence cost-effective
Qin et al. [18]	Low cost IoT Enhanced scalability and interoperability	An SDN/NFV-enabled edge node, which orchestrates end-to-end SDN-IoT services	Distributed SDN controller IoT gateways OF-switches	ODL and OpenStack Nova/Havanna service controller GMPLS controlled optical network Multi domain network architecture

Salman and Jain [13] proposes architecture, with layered model, for IoT with decentralized data and centralized control. Authors also discuss IoT challenges like scalability, big data, heterogeneity, and security. The proposed four layered model consists of Application, Control, Network, and Device Layer.

The architecture uses unique identifiers in device layer that ensures interoperability, security, and quick address. Software Defined Gateways (SD-Gateways) [20], a virtualized abstraction of a common gateway supporting extended OpenFlow protocol to communicate with the SDN controllers.

Li et al. [16] discusses issues like interoperability from the perspective of devices, data, communication protocols, and re-usability of data generated from IoT devices. Moreover, authors suggest resource utilization, openness and interoperability by using a layered architecture which includes Device Layer (responsible for collecting data), Communication Layer (contains SDN-enabled switches and

gateways), Computing Layer (having SDN Controller), and Service Layer (which provides services). The IoT devices communicate with the SDN gateway/router through sinks, like Raspberry Pi. The gateway/router then forwards the data to the SDN controller. The SDN controller manipulates the data as per the application requirements located at the service layer. This is done by programming the SDN controller. Limitations of this work include sink and sensing devices, which work independently while only responsible for aggregating and caching the data received from IoT devices. Its architecture lacks security mechanisms and routing algorithms both in SDN controller and IoT Gateway.

Ojo et al. [17] proposes a replacement of traditional IoT gateways, with specialized SDN-enable gateways, these gateways are capable of managing wired and wireless devices, and claims to be more flexible, efficient, and scalable. Authors also claim that the gateway can perform efficient traffic engineering with intelligent routing protocols and caching techniques across less constrained paths. However, the work is limited in defining intelligent routing algorithms, and performance evaluation or implementation in real time which is considered a future direction. Hakiri et al. [11] discusses five key network related challenges of IoT, such as current standardization efforts, mobility management, recurring distributed systems issues, communication protocols, and security and privacy. They outline an IoT architecture that combines SDN with message-based publish/subscribe Data Distribution Service (DDS) middleware to solve variety of issues like networking, mobility, standardization, and QoS (Quality of Service) support. In this framework, smart devices are linked with SDN-based IoT gateways to communicate with SDN forwarding devices. Furthermore, an SDN controller connects to the forwarding devices using southbound APIs allowing asynchronous, anonymous, and many-to-many communication semantics.

Martinez-Julia and Skarmeta [8] used SDN to allow different objects from different networks to communicate with each other using IPv6 and at the same time simplify the management and control operations of various objects types by adding an additional IoT controller over the SDN controller. Thus, even so the devices have different protocols; the forwarding devices in the router convert it in a form understandable by the receiver. This enables the communication of diverse devices in the network.

A middleware is designed and implemented by Qin et al. [18], which is composed of a layered IoT SDN controller to manage distributed, heterogeneous, and dynamic IoT multi-network. In their research, a central controller monitors the existing resources and schedules the data streaming according to the specific service requirement e.g., a minimum data rate, maximum tolerable delay or packet loss for each separate flow.

Finally, in the same [18] Multi-network information architecture (MINA) proposed with reflective self-observing that maintaining proactive plans approach to address this problem of heterogeneity for multi-network IoT environment by providing a centralized global view much like SDN for overlay structure and can perform analysis of the network state.

6 Discussion

In this chapter, we agree that the lack of interoperability is a consequence of several problems such as the heterogeneity in the objects, the communication protocols and the network routing protocols.

The different approaches, based on SDN, presented in this chapter, give certain advancement in research. It should be noted that the most SD-IoT approaches are neither implemented nor validated. So, we should contribute with an implemented approaches, this should address the transparent mobility of intelligent objects between different IoT architectures, research on routing mechanisms to overcome the disadvantages of traditional routing protocols and use the virtualization of network.

We can try to integrate this approach in a whole IoT architecture by considering the other interoperability levels like semantic data. Each layer of IoT interoperability model is the prerequisite for upper layers.

7 Conclusion and Perspectives

In this chapter, we have answered two questions, what are the different levels of IoT interoperability and how the SDN technology can face one of this levels that is network level.

We have presented the most pertinent SD-IoT approaches. Those approaches trend to focus more on communicating and networking layers by exploit the characteristics of SDN technology. All these presented approaches focus on designing solutions to solve the interoperability in network functions, only in one level without considering the other upper IoT levels.

Finally, we consider it is necessary to develop an interoperability approach which covers different layers in the same IoT architecture. Each layer of IoT interoperability model is the prerequisite for upper layers; not only the networking level but the semantic data level also it's a very important challenge.

References

1. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787–2805.
2. Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the internet of things. *Cluster European Projects on the Internet Internet Things, European Commission, 3*(3), 34–36.
3. Hahm, O., Baccelli, E., Petersen, H., & Tsiftes, N. (2016). Operating systems for low-end devices in the internet of things: A survey. *IEEE Internet of Things Journal, 3*(5), 720–734.
4. Ashton, K. (2009). The internet of things. *RFID Journal, 22*(7), 97–114.

5. Bizanis, N., & Kuipers, F. (2016). *SDN and virtualization solutions for the internet of things: A survey* (pp. 5591–5606). IEEE Access.
6. Kreutz, D., & Ramos, F. (2015). Software-defined networking: A comprehensive survey. In *Proceeding IEEE* (pp. 14–76).
7. Han, Z., & Ren, W. (2014). A novel wireless sensor networks structure based on the SDN. *International Journal of Distributed Sensor Networks, 10*(3), 1–8.
8. Julia, P. M., & Skarmeta, A. F. (2014). *Extending the internet of things to IPv6 with software defined networking*. White Pap.
9. Liu, J., Li, Y., Chen, M., Dong, W., & Jin, D. (2015). Software-defined internet of things for smart urban sensing. *IEEE Communications Magazine, 53*(9), 55–63.
10. Huang, H., Zhu, J., & Zhang, L. (2014). An SDN-based management framework for IoT devices. In *Proceeding 25th IET Irish signats systems cong. China. Ireland international conference on information and communication technology (ISSC, CIICT)* (pp. 175–179).
11. Hakiri, A., Berthou, P., Gokhale, A., & Abdellatif, S. (2015). Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications. *IEEE Communications Magazine, 53*(9), 48–54.
12. Gharbaoui, M., Martini, B., Adami, D., Antichi, G., Giordano, S., & Castoldi, P. (2014). On virtualization-aware traffic engineering in OpenFlow Data Centers networks. In *Proceeding of the IEEE network operations and management symposium (NOMS)* (pp. 1–8).
13. Salman, T., & Jain, R. (2013). *Networking protocols for internet of things* (pp. 1–28).
14. Li, D., Shang, Y., He, W., & Chen, C. (2014). EXR: Greening data center network with software defined exclusive routing. *IEEE Transactions on Computers, 64*(9), 2534–2544.
15. Li, J., Altman, E., & Touati, C. (2015). A general SDN-based IoT framework with NVF implementation. *ZTE Communications, 13*, 342–345.
16. Iyer, A., Kumar, P., & Mann, V. (2014). Avalanche: Data center multicast using software defined networking. In *Proceeding of international conference on communication systems and networks (COMSNETS)* (pp. 1–8).
17. Mann, V., Vishnoi, A., Kannan, K., & Kalyanaraman, S. (2012). CrossRoads: Seamless VM mobility across data centers through software defined networking. In *Proceeding of network operations and management symposium (NOMS)* (pp. 88–96).
18. Qin, Z., Iannario, L., Giannelli, C., Bellavista, P., Denker, G., & Venkata, N. (2014). MINA: A reflective middleware for managing dynamic multinetwork environments. In *Proceeding of network operations and management symposium (NOMS)* (pp. 1–9). IEEE.
19. Wu, D., Arkhipov, D. I., Asmare, E., Qin, Z., & McCann, J. A. (2015). Ubi flow: Mobility management in urban scale software defined IoT. In *IEEE conference on computer communications (INFOCOM)* (pp. 208–216).
20. Diaz-Montes, J., Diaz-Granados, M., Zou, M., Tao, S., & Parashar, M. (2015). Supporting data-intensive workflows in software-defined federated multi-clouds. *IEEE Transactions on Cloud Computing*. https://doi.org/10.1109/TCC.2015.2481410