Volume XXIV 2021
ISSUE no.1
MBNA Publishing House Constanta 2021

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Software Defined (SDN) Based Internet of Things (IoT) networks

To cite this article: S. BÎRLEANU, M. PREDA, C. RĂCUCIU, Scientific Bulletin of Naval Academy, Vol. XXIV 2021, pg.103-110.

Submitted: 27.02.2021
Revised: 15.06.2021
Accepted: 22.07.2021

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-21-I1-012

Software Defined (SDN) Based Internet of Things (IoT) networks

S Bîrleanu, M Preda, C Racuciu
Bucharest, Romania
sorin.birleanu@mta.ro

Abstract: The exponential growth of IoT devices connected to the Internet has led to the need to develop a new technology for managing them. The challenges posed by the implementation of IoT networks have emerged in the control and management of IoT applications and networks that become difficult to maintain, the programming of IoT devices. In addition, IoT devices are not designed to allow centralized management and control. Things get even more complicated when the IoT administrator has to manually configure all distributed IoT devices to add each new feature to the network. Software-Defined Networking - SDN solves existing network-level problems by providing the ability to build increasingly complex IoT-based systems in a simpler and more flexible manner. The paper aims to detail the evolution of SDN and IoT networks and an analysis of the benefits and challenges of SDN and IoT integration.

1. Introduction

IoT follows a layered architecture comprising three main layers; Perception layer: consists of physical objects and detection devices, Network layer: responsible for transmitting data from physical objects to the network gateway / edge and application layer: handles the application / services of the user's request. These connected devices produce a huge amount of data, such as data produced in the current year (6.2 Exabytes) is expected to increase by 478% (30.6 Exabytes) in next years. This increase is estimated at 781% on connected devices and with 478% increase in data generation in next years, anticipating the intelligent network control and management solution. Many solutions have been faced to solve the problems in the IoT paradigm. However, the traditional network is not able to handle such a large number of connected devices and huge data manipulations. Software-Defined Networking - SDN solves existing problems at the network level by offering the possibility to build in a simpler and more flexible way increasingly complex systems based on information and communication technology (ITC). Software-defined networking - SDN transforms the network into a modern IT work environment that supports business, not a stopper. The concept of SDN consists in outsourcing the control plan to a centralized controller or other service. By centralizing the controller or service, opening APIs, and using network programming software, SDN can help eliminate manual processes, configuration inflexibility and latency challenges associated with device-centric networking.

SDN and IoT integration can meet the management expectations of various scenarios. Benzekki [1] briefly describes the networks and programmable trends for SDN in the past, present and future. Due to the important and centralized orchestration of SDN in another network, much emphasis is placed on the integration of SDN with wireless networks. This paper focuses on existing SDN solutions for securing IoT networks. Here, various studies are presented that offer SDN-based solutions for IoT technologies.

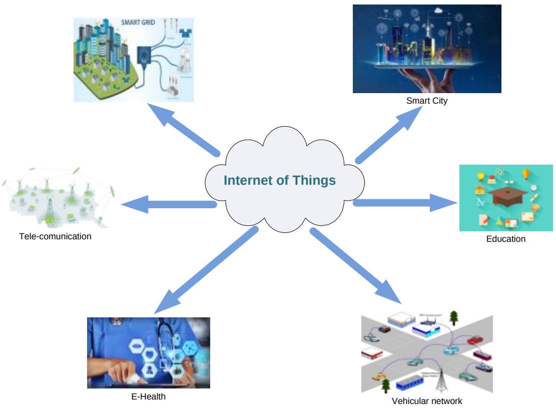

Figure 1. IoT scenario

2. Software Defined Network

SDN and IoT are two different technologies. IoTs consist mainly of detection devices that are assigned to different communication networks, and SDN is associated with network routing and acts as an orchestrator for network-level management.

2.1. Architecture and protocols

SDN presents a stratified architecture consisting of 3 layers, namely:

- Data plan - consists of redirection devices (router, switch) that redirect data from the controller instructions;
- Control / controller plan - manages the network with an overview of it;
- Application - here are found the needs of customers and transmitted to the controller.

The SDN controller defines a rule for the input flows in the data plane. SDN layers communicate with each other through open APIs called the Northbound Interface (NI) API and the Southbound Interface (SI) API. The SDN controller provides programmability and flexible management for the flow redirection state in the data plan, with an overview of the network. SDN can facilitate high data transmission, spectral efficiency, resource allocation and network management for IoT devices to meet the growing needs of customer requirements. IoT devices are used to detect, collect, process, deduce, transmit, notify, manage and store data; however, its limitations are not limited to sensor devices. Billions of connected devices, thousands of communication protocols and network architectures help create the complexity and inoperability of IoT. Jie Li [7] proposed in his paper a general framework for distributed-based SDNs with distributed management. S. Namal [12] has proposed an SDN-integrated IoT architecture in which IoT devices are managed by OpenFlow-based management devices. The following figure shows the general IoT architecture based on SDN.

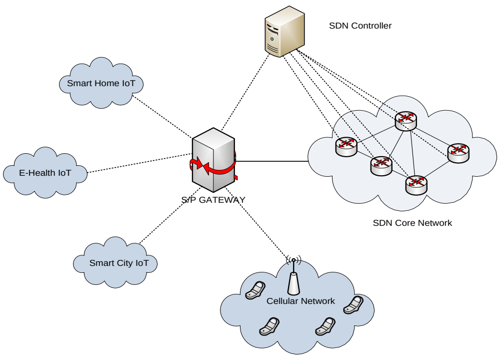

Figure 2. IoT architecture based on SDN

2.2 SDN Based Cellular Network

The first proposal for the SDN-based cellular network was presented by Li. Erran in his work *Toward software-defined cellular networks*. I call it CellSDN, in which attribute-based policies are formulated for an individual user in the LTE network and gain fine-grained control over the network. In CellSDN, the local agents on each switch perform the deep inspection of the packets and reduce the excessive load on the controller. SoftRAN is proposed by S. Tomovic in *SoftRAN: Software defined radio access network, Uses the SDN principle in the 4G LTE network*. A centralized control plan abstracts the entire RAN in the geographical area. A large base station with centralized controller performs the allocation of resources in a three-dimensional network, ie spaces, time and frequency slots. The controller decides to allocate resources in the field of frequency, time and space. The radio / BS elements make a local decision to manage the delay. SoftCell incorporates SDN into the core cellular network and provides fine-grained policies for the LTE network. In the SoftCell architecture, traffic classification is done on access switches instead of gateways. Each access switch has a local agent that caches each UE profile to control packet classification is the access switch. The controller assigns the policy label, the hierarchical IP address and the EU identifiers and is incorporated in the package header to avoid reclassifying the traffic. The integrated SDN and SDR architecture for the 5G network is proposed in [20], called the hybrid SDN / SDR architecture. The architecture is a combination of SDN and SDR cross-layers for the exploitation of the frequency spectrum and connection information in the 5G network. The cross-layer controller is used to request the frequency spread spectrum and to make the flow traffic decision. This architecture also manages user authorization in the multilayer controller and provides access to better bandwidth. Ian F. Akyildiz proposed the integration of the main SDNs into the 5G network by exploiting virtualization for a resilient network. SoftAir offers load-conscious mobility balancing and efficient allocation of resources through virtualization. Aggregate control is provided by NFV by creating several virtual networks with independent protocols and resource allocation algorithms. SD-RAN and SD-core network nodes are OpenFlow enabled and monitored through OpenFlow and the Common Public Radio Interface (CPRI). All management policies are defined in the central control plan, which allows cloud orchestration and provides end-to-end QoS security. The following table provides a comparison of existing SDN-based cellular architectures.

Table 1. SDN-IoT cellular solution frameworks

Architecture	**Resource management**	**Interface API**	**Control/data plane decoupling**	**Benefit**
SoftRAN	Resource management, mobility support, traffic off loading	Controller API/ Femto API	Centralized controller and local agent at eNBs slicing forming big base station	Radio resource management, mobility support, Traffic offloading, Reduced delay
Hybrid SDN-SDR	Spectrum management	-	Centralized controller	Power saving and optimization
SoftCell	Fine grain policies management.	OpenFlow API	Logically centralized controller, local agent SD-RAN (BS)	Dynamic traffic offloading, efficient routing, minimizing the state in the core network
SoftAir	Distributed traffic classification, network management	OpenFlow & CPRI	SD-BS, SD-switch, BS-clustering	Flexible platform for fully & partially

				centralized architecture
cellSDN	Mobility management and policy control	NOS	Centralized control plane, local control agent ate BS	Seamless mobility management and fine grain control due Local agent and virtualization

2.3 SDN for wireless sensor

L. Galluccio in *SDN-WISE: Design, prototyping and experimentation of a stateful SDN solution for Wireless SEnsor networks* [13], proposes SDN-based WSN, supports the operating cycle and data aggregation and provides a complete state solution. The adoption layer performs the translation between the sensor node and the WISE-Viewfinder. SDN WISE defines its policies based on the description of the state. The work Smart wireless sensor network management based on software-defined networking presents the programmability of SDN in WSNs. The architectural components of this approach consist of a base station (BS) and several sensor nodes. The SDN controller running on the BS made the routing decision instead of the dumb sensor nodes. The sensor nodes contain the flow table as in the SDN concept, which is populated by the SDN controller.

Miyazaki [15] proposed a reconfigurable WSN network architecture based on customer needs, using the role injection and delivery mechanism. The role compiler generates scenarios that are injected via wireless communications. The sensor nodes are modified by the field programmable array (FPGA) and a microcontroller unit (MCU). The multifunctional sensor network is also addressed in SenShare: transforming sensor networks into multi-application sensing infrastructures by I. Leontiadis. NFV exploited for sharing a single infrastructure for many applications in a sensor network. They proposed a framework for several application scenarios on a common construction infrastructure. Each node has an abstraction layer for shared hardware that works on the overlay network and creates multiple virtual sensor networks (VNS). The concept of reprogramming and re-activation in WSN was proposed in Sensor OpenFlow: Enabling Software-Defined Wireless Sensor Networks. The modules in the SOF control layer are the "sensor reconfiguration" module and the "query strategy control" module and perform flow-based redirection in the sensor nodes that contain the data plane.

Table 2. SDN based IoT management frameworks

Architecture	**Management**	**Architecture**	**Control/ data plane decoupling**	**Protocol used**	**Benefit**
SDN-WISE	Localization of distributed sensor, energy management,	Centralized controller with dumb sensor node having flow table like OpenFlow flow table which is preinstalled flow rules	Centralized controller, dumb data plane	OpenFlow	The state-full approach, reducing information exchange. Mobility, reconfiguration and localization of

WSN-SDN	Sensor network flow management	WSN cluster with centralized controller monitored and controlled by Master SDN controller	Centralized master controller	OpenFlow/ distance aware routing protocol	Optimal path selection, routing strategy adjustment
SD-WSN	Infrastructure management and reconfiguration	FPGA	Micro-controller	COAP	Programmable reconfiguration of network
Integrate WSDN	Management platform for using virtual machine (INNP)	Local controller in each sensor node which interacts with a centralized controller. INNP is done through VM in the node platform	Centralized controller and local controller	Contiki OS on each local controller	Flexibly using commodity off the shelf device, reducing cost
SOF	Flow management	INNP in data plane and flow based packet forwarding	Centralized controller and distributed data plane	Sensor OpenFlow (SOF)	handling peer compatibility, address classification,

2.4 SDN based IoT Management

Table 2 presents a part of the management framework for SDN-based IoT networks. Qin has improved the idea of multi-network control architecture for heterogeneous IoT on campus. MINA is practically a middleware whose working principle is self-observation and adaptation and manages the ubiquitous heterogeneous network. MINA follows the SDN principle as a layered and streamlined architecture, which reduces the semantic gap between IoT and task definitions in a multi-network environment. This architecture aims at flow planning and management of the Wi-Fi and WiMAX environment, which is optimized through the use of resource sharing. Di. WU in *UbiFlow: Mobility management in urban-scale software* defined IoT. The IEEE Conference on Computer Communications presents the UbiFlow framework that provides SDN and IoT integration. UbiFlow proposed efficient flow control and mobility management in multiple urban networks using SDN distributed controllers. In the UbiFlow architecture, the IoT network is partitioned into small pieces of network / cluster. Each partition is controlled by a physically distributed SDN controller. IoT devices in each partition can be connected to a different access point for different data requests. MINA manages the flow per device and optimizes access. M. Boussard [22] proposed an SDN-based control and management framework for IoT devices in a smart environment. The management framework, called "Software-Defined LANs (SD-LAN)", organizes the devices and groups these devices in the order of service request from the user. This framework uses Universal Plug and Play (UPnP) and Simple Service Discovery Protocol (SSDP) to discover a new device in the SD-LAN and create a virtual topology for service requirements.

Table 3. SDN based IoT Security solutions

Approach	Security parameter	Network	Description
secured SDN framework	Authentication	Ad hoc network	SDN controller block all switch port on receiving new flow and start authentication
DISFIRE	Authentication & authorization	Grid network	hierarchal cluster network with multiple SDN controllers implement a dynamic firewall to ensure authorization
Black SDN	Location Security, Confidentiality, Integrity, Authentication and Privacy.	Generic IoT/M2M communication	secure the meta-data and the payload by encryption in the link layer and use SDN controller as TTP
SDP	Authentication	Ad hoc network/M2M communication	SDP collect the IP addresses of all M2M communication capable devices and store into a logical network. Authenticate based on information stored
SDIoT	Authentication	Generic IoT network	It utilized SDSecurity mechanism leveraging NFV and SDP for ensuring secure access in the network by authentication.

2.5 SDN security framework for IoT

IoT devices are becoming more vulnerable to security risks in a network. Few security considerations are observed in the SDN-based IoT. K. S. Sahoo [23] proposed a secure architecture for the SDN-based IoT network. This security architecture focuses on authenticating the IoT device on the controller. In this architecture, IoT is an ad hoc network in which when a wireless object establishes a connection with the controller and the controller blocks the entire port when the connection is established, and the controller starts authenticating that device. If the user is genuine, the controller starts pushing the stream to that user. Few network controllers serve as security guards and exchange information with each other about user authentication. If the security controller fails, another border controller is selected as the security controller. Gonzalez in *SDN-based security framework for the IoT in distributed grid* [21] proposed a dynamic firewall called Distributed Intelligent Firewall (DISFIRE) for the secure architecture in the SDN-based network. The architecture consists of a hierarchical cluster network with several SDN controllers. These SDN cluster head controllers implement a security policy. For this purpose, they used the Cisco policy agent defined opFlex in the controller instead of OpenFlow. Device information is exchanged between devices and any unauthorized policy of potentially harmful device flow rules is deleted.

Olivier, F. [20] in New Security Architecture for IoT Network presents SDN-based IoT network security by implementing the SDSec module that used NFV to create a virtual topology for the connected device and for authentication by blocking the entire switching port when it received a request for to a new flow. SDSec stores information in the security database and identifies an object tracking the authentication database. Another security framework is proposed in the Novel Wireless Sensor Networks Structure Based on the SDN. IoT is divided into segments with its own SDN controller. The IoT agent and IoT controller are responsible for connecting to the SDN-enabled heterogeneous network.

The IoT agent is an agent registered with the IoT controller. The SDN controller performs authentication and routing based on information collected from IoT agents.

3. Issue

The whole concept of IoT-SDN is in its infancy and standardization efforts are still ongoing. Although several competing alliances try to dominate for a global standard, these efforts are more like a theoretical result, and the concrete solution is missing. The diversity of SDN incorporation in different IoT domains in the context of the cellular network, IoT management and security are discussed in Table 1, Table 2 and Table 3. However, the existing solution is not fully integrated in SDN, and an architecture and framework comprehensive are not established so far. Few efforts are admirable, such as SoftRAN, SoftAir, SDN-WISE, SDIoT, BlackSDN, etc., which presents a complete framework for IoT devices that provide resource allocation strategies, operating system for the SDN sensor network, SDStorage, SDSystem and SDSec for management, security and architectural details of IoT interaction in SDN. The major factors for the lack of a comprehensive SDN-based IoT architecture is the absence of a concrete IoT architecture framework. Existing transport protocols fail in IoT scenarios from connection configuration and congestion control mechanisms require high bandwidth and control flow in network and the TCP connection requires excessive buffering, which is a major limitation in IoT constraint devices. In a network, control traffic consumes bandwidth and therefore degrades the spectral efficiency of IoT devices. Battery power is also extremely vulnerable to this massive traffic control. Therefore, the security of the well-known traditional network cannot be applied in IoT. Also, the SDN centralized control plan may suffer from denial of service attack and human attack in the middle.

4. Conclusion

The new trend of technology development changes to a great extent the way of communication between man and devices. IoT technology is in its infancy and has no programmability, security being at a low level, being a very large amount of information, their management becomes difficult to meet user requirements. In this paper, a study of the existing IoT solution using SDN control and data plan programmability is presented. In this paper, architectural details and the contribution of an IoT framework based on SDN are discussed, summarizing the architectural details and its evolution, and then some of the unresolved issues in this merger are reported.

References

[1] Benzekki, K. and Elbelrhiti Elalaoui, 2016 *Software-defined networking (SDN): A survey*

[2] Karakus 2017 *Quality of Service (QoS) in Software Defined Networking (SDN): A survey*

[3] Abu-Ghazaleh 2016 *Wireless Software Defined Networking: A Survey and Taxonomy*

[4] Krishnamachari B. 2014 *Software-Defined Networking Paradigms in Wireless Networks: A Survey*

[5] Braun W. 2014 *Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices*

[6] Evans D. 2011 *The Internet Is Chang. Everything Whitepaper Cisco Internet Bus*. Solutions Group IBSG

[7] Li J. and Touati, C. 2015 *A general SDN-based IoT framework with NVF implementation*

[8] Chen, M. and Jin D. 2015. *Software-defined internet of things for smart urban sensing*

[9] Gudipati A. and Katti S. 2013 *SoftRAN: Software defined radio access network*

[10] Jin X. and Vanbever L. 2013 *Softcell: Scalable and flexible cellular core network architecture*

[11] Akyildiz I. and Wang P. 2015 *SoftAir: A software defined networking architecture for 5G wireless systems*

[12] Namal S, Saud S. and Gurtov 2015 *A Implementation of OpenFlow based cognitive radio network architecture: SDN&R*

[13] Galluccio L. and Morabito 2015 *GSDN-WISE: Design, prototyping and experimentation of a stateful SDN solution for WIreless SEnsor networks*

[14] Gante D. and Matrawy A. 2014 *Smart wireless sensor network management based on software-defined networking*

[15] Miyazaki T. and Kitamichi J. 2014 *A software defined wireless sensor network*

[16] Leontiadis I. and Crowcroft J. 2012 *SenShare: transforming sensor networks into multi-application sensing infrastructures*

[17] Luo, T., Tan, H. and Quek, T. 2012 *Sensor OpenFlow: Enabling Software-Defined Wireless Sensor Networks*

[18] Qin Z., Giannelli C. and Venkatasubramanian N. 2014 *A software defined networking architecture for the internet-of-things*

[19] Wu, D. and Zhijing, *Q* 2015 *UbiFlow: Mobility management in urban-scale software defined IoT*

[20] Olivier, F., Carlos, G. and Florent, N. 2015. *New Security Architecture for IoT Network. Procedia Computer Science*, p1028-1033.

[21] Gonzalez, C., Charfadine, S., Flauzac, O. and Nolot, F. 2016 *SDN-based security framework for the IoT in distributed grid*. International Multidisciplinary Conference on Computer and Energy Science (SpliTech), p1-5.

[22] Boussard, M., Bui, D., Ciavaglia, L., Douville, R., Le Pallec, M., Le Sauze, N., Noirie, L., Papillon, S., Peloso, P. and Santoro, F. 2015 *Software-defined LANs for interconnected smart environment* p219-227.

[23] Sahoo, K., Sahoo, B. and Panda, A. 2015 *A secured SDN framework for IoT*. International Conference on Man and Machine Interfacing (MAMI) p1-4.