STUDENT SESSION

SDN APPROACH IN DEVELOPMENT IOT ENVIRONMENTS

Stefan Biševac,(Student),
Marko Šarac, (Mentor)*

Singidunum University,
Belgrade, Serbia

Abstract:

SDN and IoT are two growing technologies that have been the focus of researchers around the world in recent years. Modern access to the network offered by SDN and the growing number of IoT devices shows that the integration of these two technologies as well as their adaptation to each other can significantly improve the interoperability of the whole environment. IoT security issues can also be bridged by the idea of integrating modern firewall or IDS/IPS solutions through an SDN controller or as an independent entity within an SDN environment. The paper aims to show the work done so far on the implementation of SDN in the IoT environment as well as to provide overview for further development of SDN in the IoT communication service.

Keywords:

SDN, IoT, Integration, Programability, Security.

INTRODUCTION

SDN stands for Software Defined Network created by Martin Cassado in 2005 [1]. SDN is a different approach to network management that allows dynamic, programmability and efficient network configuration, all in order to improve network performance and monitoring, thus making the network more of a cloud-computing component than a component of traditional computer systems.

Despite the fact that traditional networking devices are evolving, the disadvantages of the traditional approach are the impossibility of massive scalability, multi-tenant networking, as well as virtualization. This further implies the difficulty of proper configuration, the difficulty of adding new functionalities (upgrades) as well as the difficulty in finding potential errors on the system (it is necessary to analyze all devices in the network).

A new approach to computer networks - SDN, provides a new workspace in which network engineers can automatically and fully dynamically manage and control a large number of network devices, services, different topologies and even packages using a higher programming language and APIs. The needs of SDN are virtualization and orchestration. Virtualization because there is no need to worry about where the logic of the network is really physically located, how big it is and how it is organized.

Correspondence:
Marko Šarac

e-mail:
msarac@singidunum.ac.rs

DOI: 10.15308/Sinteza-2022-449-456

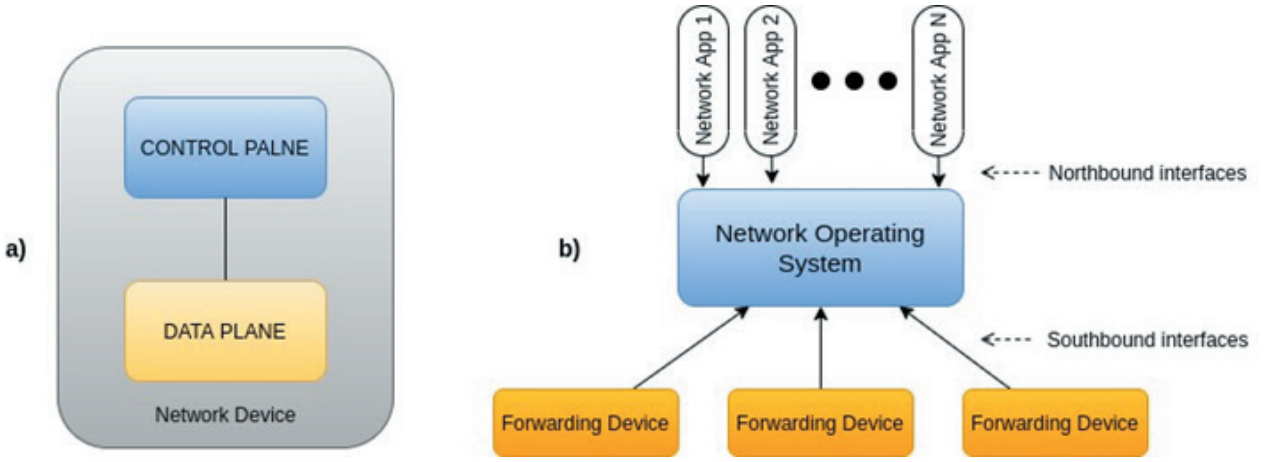

Figure 1 - a) Traditional network model, b) SDN network model

Orchestration means the control and management of a large number of devices through a single command. On the other hand, the Internet of Things, together with SDN, is presented as one very important development technology that seeks to connect different objects via the Internet. By implementing SDN in the IoT network, centralized control of IoT devices such as sensors, actuators, RFID tags, etc. is achieved. The main purpose of integrating SDN into IoT is to organize streams using SDN controllers which further reduces human activity on the network.

Some benefits of SDN and IOT integration are implementing intelligent routing decisions, simplification of information collection, analysis and decision making, visibility of network resources which include network management simplification based on user, device and application specific requrements or implementing intelligent traffic pattern analysis and coorinated decisions. The main feature of the SDN network model is the separation of Control and Data Plane, which allows independent development of each individual. A comparative view of models are given in Figure 1.

2. AN OVERVIEW OF CURRENT SDN SOLUTIONS

Many professional and scientific communities have been involved in the development of SDN, as well as many manufacturers of network devices. The course of development of open source SDN solutions constantly follows the development of SDN solutions of vendor companies. One of the major differences is the technology of creating SDN controllers and components that join the controllers, while from the aspect of network application development the situation is completely identical, both communities offer a well-defined API, thus providing independent access to the system in relation to the programming language.

2.1. OPENSOURCE SOLUTIONS

ONOS - Open Network Operating System is a java-based SDN solution that is being actively developed by the ONF community. ONOS network operating system, framed by a software controller implemented in next-generation SDN/NFV environments. It has been developed to satisfy the flexibility in creating and implementing dynamic network services with a simple programmable interface. ONOS supports pre-configuration and real-time network configuration, eliminating the need to run routing and switching control protocols within network devices [2].

OpenDayLight is a modular open platform for configuring and automating networks of any size and distribution. ODL is a part of LF networking that aims to develop the Open Networking ecosystem. It is designed as a general-purpose platform for delivering a wide range of network services. ODL provides all the benefits of SDN and NFV providers, research institutions and organizations such as smart cities or metropolitan areas. Its SDN controller is called OpenDayLight Phosphorus [3].

Open vSwitch is a multi-layer switch licensed under the Apache 2.0 license. It is designed to enable massive network automation through programmable interfaces, supporting both standard management interfaces and protocols such as NetFlow, sFlow, LACP, 802.1ag, etc. In fact, it is designed to support the distribution of network services across multiple physical servers, similar to VMware VDS or Cisco Nexus 1000v series switches [4].

Ryu is a component-based software-defined network

framework. Ryu delivers software components with a well-defined API, which facilitates the development of network management and network applications. Ryu supports various protocols for managing network devices such as OpenFlow, NetConf, OF-config, etc. Unlike ONOS and ODL, Ryu is a python-based SDN solution [5].

2.2. VENDOR SOLUTIONS

Cisco ACI (Cisco Application Centric Infrastructure) is an SDN solution from Cisco, the world's leading network equipment manufacturer. This solution works with the APIC (Application Policy Infrastructure Controller) software controller and Nexus 9000 switches. What characterizes the Cisco ACI is a much higher throughput, 5 times less latency compared to competing technology, 2 times faster data backup, supports micro-segmentation thus providing a higher level of security. In addition to full automation, it also offers a unique management console [6].

When it comes to Data Centers, VMware currently offers a leading SDN solution related to Data Center technology. NSX is basically an overlay network technology and can work with any hardware switch. NSX offers a wide range of network functionalities in virtualized form, which means that it is possible to create a large number of Overlay networks, Virtual routers, Edge gates, Switches, Firewalls, Load Balancers, VPNs, etc., without the use of additional hardware. VMware offered NSX in two variants: NSX-V and NSX-T, where NSX-V is exclusively for vSphere hypervisors, while NSX-T supports most modern infrastructures such as OpenStack, KVM, Kubernetes, AWS, etc. [7].

One of the world's telecommunications companies is Nokia, which offers the Nuage Networks Virtualized Services Platform (VSP) SDN solution based on its own Virtualized Services Container (VSC) as well as two other key elements: Virtualized Services Directory (VSD) and Virtual Routing and Switching (VRS). Like other vendors, Nokia Nauge Networks provides a full range of products optimized for Data Center, Cloud and SDN operations [8].

3. OVERVIEW OF RELATED RESEARCH AREAS – INTEGRATION OF SDN INTO THE IOT ENVIRONMENT

The starting point for this paper was a publication that thoroughly described the application of SDN and virtual technologies and their integration into the IoT environment [9]. The idea of the authors was to systematize all the knowledge related to the support of SDN in the IoT environment, from physical computer network to wireless and mobile sensor networks. The authors conclude that the advantages of SDN are numerous, especially when it comes to sensitive and mission-critical IoT applications that require a certain level of security. What determines all scientific papers is what they deal with SDN and its integration into the IoT. The following subsections provide some topics on which there is a large amount of research.

3.1. NETWORK MANAGEMENT EFFICIENCY

Research shows the potential inefficiencies of traditional network technology when it comes to the large number of IoT devices on the network. In general, they analyzed the implementation of SDN in production networks, after which they came to the conclusion that SDN is one of the good ways to improve the management of the entire network infrastructure [10].

Based on results in Table 6 [11] it is shown that the SDN-based framework in relation to tables that handle environments such as network management protocols for IoT low power networks Cloud-based frameworks, Semantic-based frameworks and machine learning based frameworks in advantage by the following parameters Scalability, Fault tolerance, Energy efficient, QoS, Security.

What is specific of SDN-based frameworks in according to the IoT with traditional networks, is the flexible topology which is changeable. So if the traditional gateway breaks down, the networks can not continue to work by adjusting themselves. But in the introduced SDN, the network can reconfigure according to the change of environment [12].

SDN-based frameworks for IoT networks management have been proposed in order to centralize network management operations on a central entity and so, reduce computational operations on IoT devices

3.2. SECURITY

Due to the weaker processing power of IoT devices, a large number of papers have been published on the topic of researching the security aspect of the IoT environment. Some security risks of SDN integration into the IoT environment have been defined and provide a distributed control plan solution as one of the effective solutions to protect the network, both from external attacks and from internal attacks [13].

Authors of the paper "Security improvement in IoT based on Software Defined Networking (SDN)" [14] in the service of improving security, and due to the fact that not all IoT sensors can be SDN eligible, introduces the term IoT agents and IoT controllers who need to connect SDN-incompatible resources with IoT devices that they did.

The paper "An approach to adding a simple interface as a security gateway architecture for IoT device" [15] provides an interface that deliver security to the IoT environment without overloading end IoT resources, and this solution provides security that is compatible with remote Internet services.

The popularity of SDN and IoT technologies, as well as their mutual integration, is growing, which indicates the commitment of the scientific and professional community to provide new directions for the development of these technologies [16].

4. POSSIBILITY OF IMPROVING RESULTS IN IOT RESEARCH

Based on the previously shown research, there is no doubt that SDN completely provides a new approach in the development of IoT environment, which enhances research in various areas such as improving security aspects, performance measuring, development of network applications, etc. This paper aims to provide an overview of some directions in which the development and improvement of the IoT environment in line with SDN potentials can take place.

IoT devices as well as IoT network are applied on the southbound interface of SDN architecture. According to the Figure 2, IoT device can be connected directly to the SDN Controller or using a Forwarding device. Depending on the network topology but also the specific requirements of IoT communication, SDN can be configured to meet all needs in order to provide network services through network applications that are applied to the northbound interface [17].

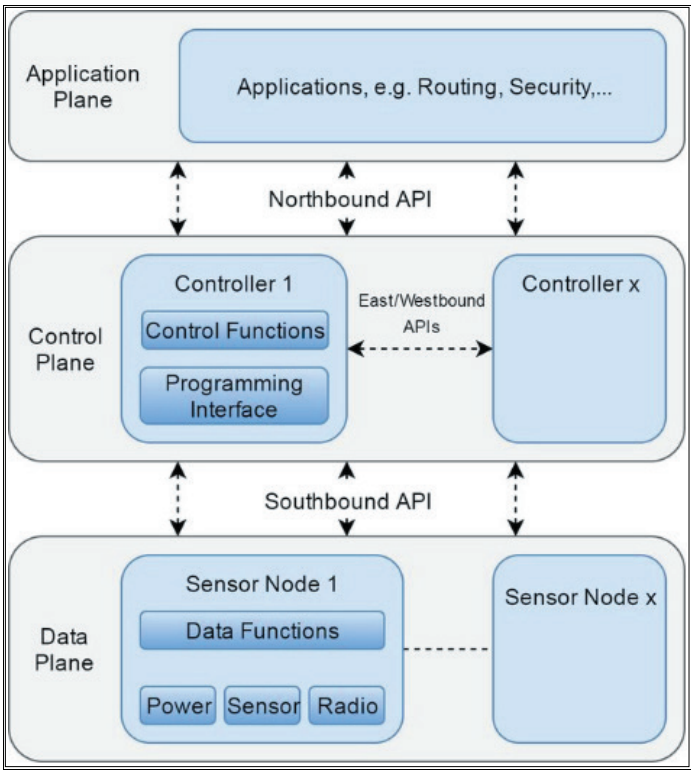

Figure 2 - SDN model adapted to IoT environment

4.1. PROGRAMMABILITY

Compared to traditional networks, SDN can be programmed at all levels: Data Plane, Control Plane and at the level of network applications [18]. Many network models are analyzed on "bottom-up" principle, starting from the physical to the application level. Within the Infra project, the Open Network Foundation community has developed the P4 - Programming Protocol-independent Packet Processors is an open source, domain-specific programming language for network devices, specifying how data plane devices (switches, routers, NICs, filters, etc.) process packets [19]. XDP (eXpress Data Path) is designed for users who want programmability as well as performance. XDP allows users to write a C-like packet processing program and loads into the device driver's receiving queue. It is more performance compared to P4 and adapted to the new upcoming 6G networks, but has a less intuitive programming language as show in paper work [20]. The difference between the two technologies is quite significant, with XDP clearly in favour. If there is a plan to implement light forwarding devices that can be part of the IoT environment then this fact should be taken into consideration. The conclusion that can be drawn from this part is that it is possible to create and form flow tables on devices operating at the Data Plane level, using one of these two programming languages to meet the specific need with a detailed flow of data and all in order to provide communications between two or more IoT entities. One of possible forwarding device block diagram with flow tables and IoT sensors are given in Figure 3.

The SDN Controller serves as an aid to dynamically populate forwarding tables with precisely defined rules. Also, development of SDN Control Plane, ie. SDN Controller, means the development of a service for distributed management of forwarding devices, a service for accepting network applications, but also a service for clustering the SDN controllers themselves. In accordance with the SDN network model, different types of OpenFlow, PCEP, etc. protocols can be developed on the southbound interface. While on the northbound side, API or REST / HTTP services are most often developed. On the controller it is possible to develop monitoring services for devices, topology, and service discovery mechanism; a path computation system; and potentially other network-centric or resource-centric information services. The conclusion that can be seen here is that the SDN controller can be considered as a network operating system that can be upgraded in accordance with the applicable rules of upgrading and currently up-to-date computer operating systems. In the IoT service, the SDN controller is considered to be the data flow editor in the IoT network. A possible but not final model of the SDN controller in the IoT environment is given in the Figure 4.

The development of network applications, given the existence of the northbound interface, should allow developers to create their own protocols without knowing the technology of SDN control and forwarding devices. This allows developers to write applications or entire app-systems in any programming language (Python, JAVA, C++, etc...) that will communicate with the SDN controller via the API/HTTP or any other northbound

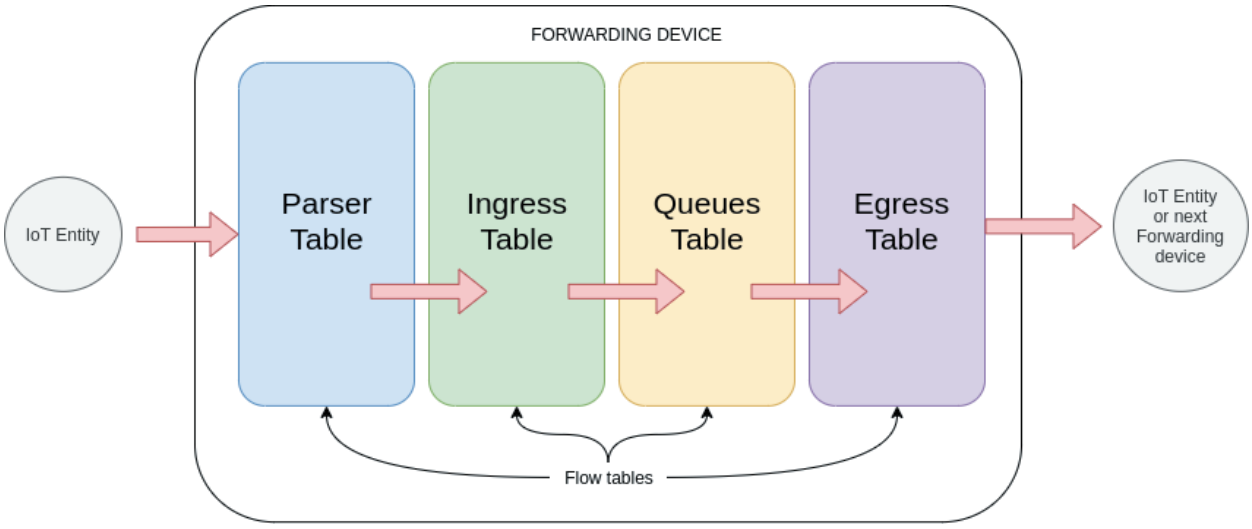

Figure 3 - Overview of Data Plane model of Forwarding device and Flow tables with position of IoT entities

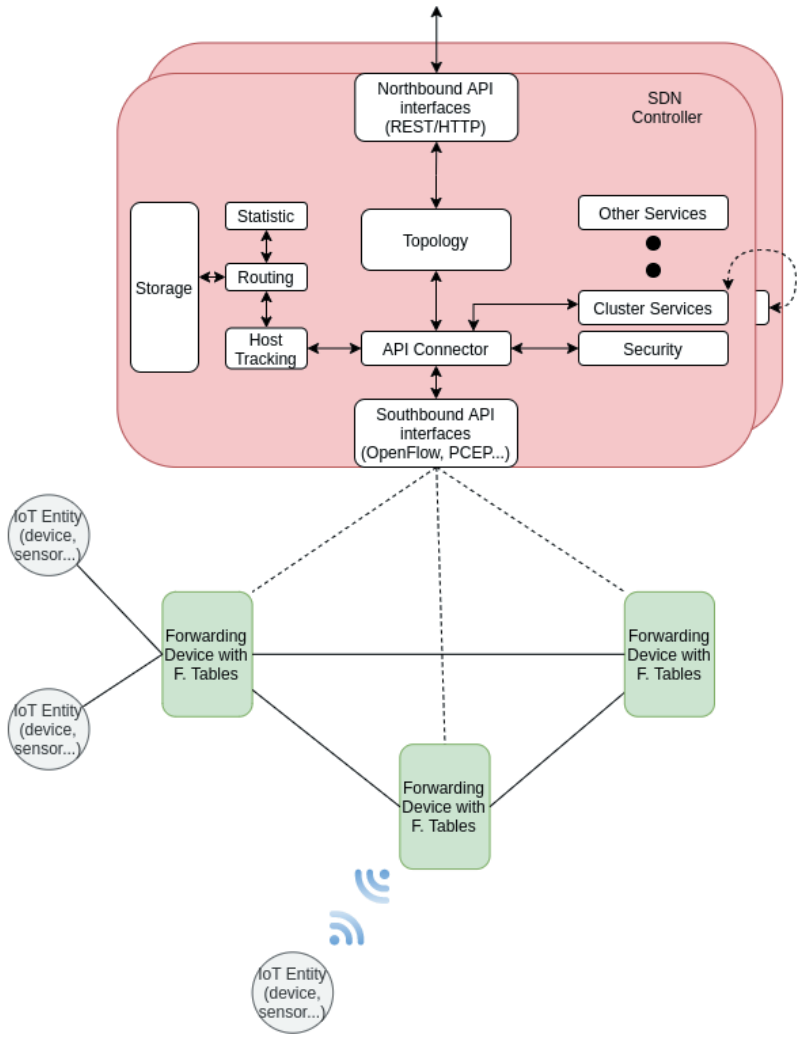

Figure 4 - Overview of SDN Controller block model for IoT environment

interfaces that are developed for specific communication. There are a lot SDN applications that can bi associated to IoT environment including monitoring and measurement, security, cloud, big data, wireless etc.. [21]. Therefore, researchers are given the opportunity to, using any programming language, independently develop potential algorithms that will solve current problems that occur in IoT environments.

This subsection more closely determines the position of the IoT entity in relation to SDN components, shows the direction of development of each layer of the SDN model and how it is possible to improve communication between SDN entities and the rest of the network.

4.2. SECURITY

Some authors have shown how it is possible to integrate a blockchain architecture to protect IoT networks whether it is a centralized or distributed network system [22][23]. This works describes how to deploy security measures, including threat prevention, data protection, and access control, and mitigate network attacks such as cache poising/ARP spoofing, DDoS/DoS attacks, and detect security threats.

Since the most SDN controllers are OpenSource, a number of firewall policies or IPS / IDS systems can be integrated with the controller itself to block or identify malicious traffic. Some authors explain that for the purposes of SDN, IDS / IPS functionality is provided through external systems, such as Suricata [24]. This allows the implementation of various security services: Firewall, network scan detection, abnormal traffic detection, intrusion detection, intrusion prevention.

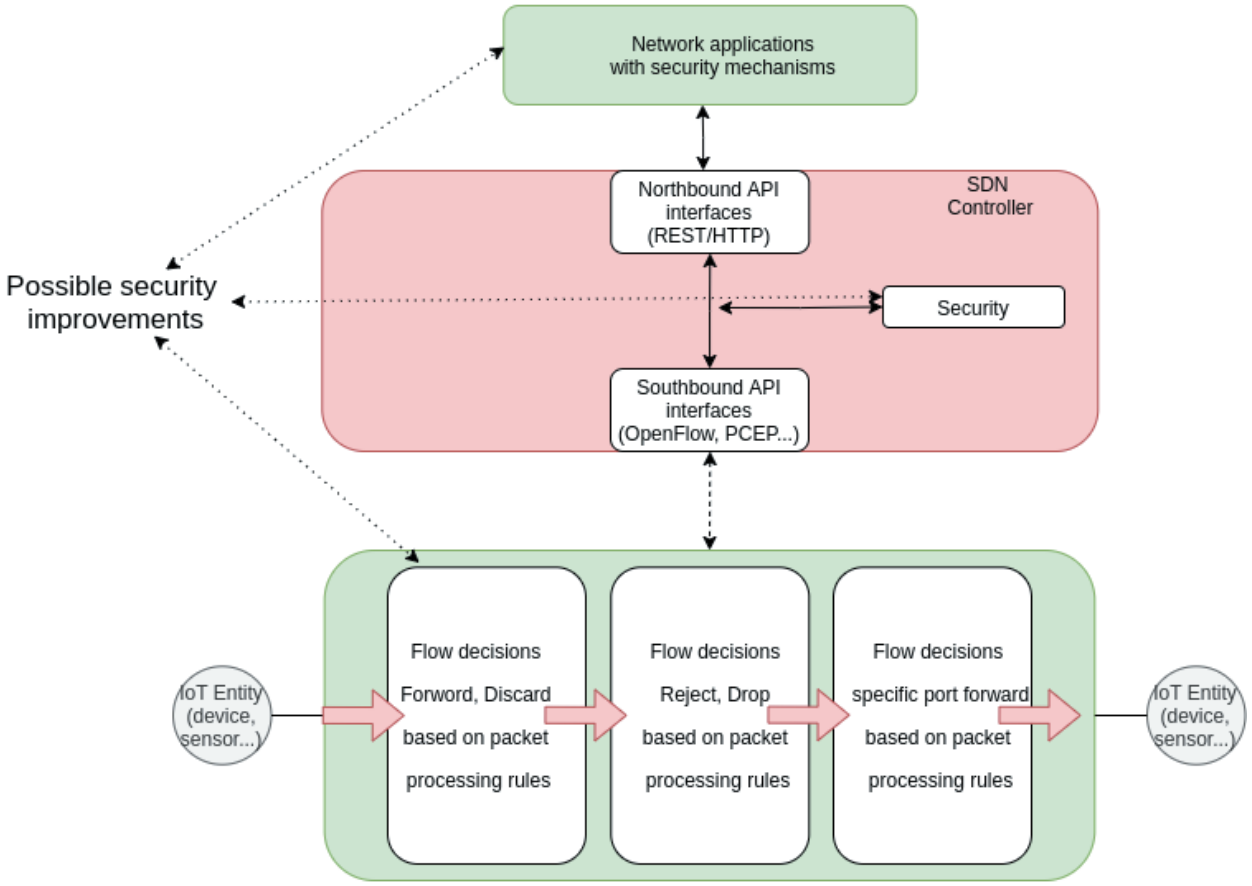

Figure 5 - Overview of possible security improvement

In accordance with the previously proven security improvements of the IoT environment, the following Figure 5 shows the directions in the development of security solutions at all levels of the SDN model or their integration with all layers of this model.

In conclusion, the fact that the SDN platform is extremely suitable for further development of security protocols in the IoT environment as well as relatively simple integration with external security solutions.

Given all the facts presented so far, it can be concluded that the SDN platform is largely suitable for the IoT environment. All the specific requirements of specific IoT communication can be realized through the development of applications at all levels of the SDN network model.

5. CONCLUSION

This paper provides an overview of current researches on the topic of IoT and SDN integration. The systematization of the material is based on the available open source SDN solutions that are most often used in research. Parameters such as network programmability and security that are important for the IoT environment were evaluated. It has been shown that in most cases the SDN architecture provides better opportunities in IoT communication, gives developers the freedom to develop their own applications, provides better control over system behavior as better security solutions. The paper also showed possible software and security points in the development of SDN architecture in service of IoT needs.

In the time to come, SDN will become a technology that will be much more responsive, fully automated and highly secure, as well as one of possible directions for improving IoT services by SDN technology.

6. REFERENCES

[1] OpenFlow Inventor Martin Casdo on SDN, VMware, and Software Defined Networking Hype [Online]. Available: https://www.enterprisenetworkingplanet.com/standards-protocols/openflow-sdn-inventor-martin-casado-on-sdn-vmware-and-software-defined-networking-hype-video/ [Acessed 15.02.2022.]

[2] Open Network Foundation, Open Netowrk Operating System [Online]. Available: https://opennetworking.org/onos/. [Accessed 21.02.2022.]

[3] The Linux Fondation Projects, OpenDaylight, OpenDaylight Phosphorus [Online]. Available: https://www.opendaylight.org/current-release-phosphorus [Accessed 21.02.2022.]

[4] Production Quality, Multilayer Open Virutal Switch [Online]. Availabel: https://www.openvswitch.org/ [Accessed 01.03.2022.]

[5] Component-based software defined networking framework – Ryu [Online]. Available: *https://ryu-sdn.org/* [Accessed 01.03.2022.]

[6] Cisco ACI solution [Online]. Available: *https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/solution-overview-c22-741487.html* [Accessed 01.03.2022.]

[7] Vmware NSX [Online]. Available: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-datasheet.pdf (accessed 05.03.2022.)

[8] Nauge Networks Virtualizes Services Platform [Online]. Available: *https://www.nuagenetworks.net/platform/virtualized-services-platform/* [Accessed 05.03.2022.]

[9] N. Bizanis and F. A. Kuipers, "SDN and Virtualization Solutions for the Internet of Things: A Survey," in *IEEE Access*, vol. 4, pp. 5591-5606, 2016

[10] A. Caraguay, A. Peral, L. López and L. Villalba, "SDN: Evolution and Opportunities in the Development IoT Applications", in International Journal of Distributed Sensor Networks, vol.10, 2014.

[11] M. Aboubakar, M. Kellil, P. Roux, "A review of IoT network management: Current status and perspectives", in Journal of King Saud University – Computer and Information Sciences, March 2021

[12] H. Huang, J. Zhu and L. Zhang, "*An SDN_based management framework for IoT devices,*" in 25th IET Irish Signals & Systems Conference and China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), pp. 175-179 , 2014

[13] O. Flauzac, C. Gonzalez, A. Hachani and F. Nolot, "*SDN Based Architecture for IoT and Improvement of the Security*", in IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, 2015.

[14] C. Vandana, "Security improvement in IoT based on Software Defined Networking", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 5, 2016

[15] N. Pavlović, M. Šarac, S. Adamović *et al. "An approach to adding simple interface as security gateway architecture for IoT device"*, in Multimed Tools Appl, 2021.

[16] "Forecast end-user spending on IoT solutions worldwide from 2017 to 2025" [Online]. Available: *https://www.statista.com/statistics/976313/global-iot-market-size/* [Accessed 10.03.2022.]

[17] S. Pritchard, R. Malekian, G. Hancke and A. Abu-Mahfouz, "*Improving Northbound Interface Communication in SDWSN*", in 43rd Annual Conference of the IEEE Industrial Electronics Society (IES), 2017

[18] B. Astuto, M. Mendonça, X. Nguyen, K. Obraczkaand T. Turletti, "*A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks*". Communications Surveys and Tutorials, IEEE Communications Society, Institute of Electrical and Electronics Engineers, pp.1617 – 1634, 2014.

[19] Programming Protocol-independent Packet Processors(P4) [Online]. Available: *https://opennetworking.org/p4/* [Accessed 10.03.2022.]

[20] D. Carrascal, E. Rojas, J. Alvarez-Horcajo, D. Lopez-Pajares and I. Martínez-Yelmo, "*Analysis of P4 and XDP for IoT Programmability in 6G and Beyond*" [Online]. Available: https://www.mdpi.com/2624-831X/1/2/31 [Accessed: 11.03.2022.]

[21] SDN applications [Online]. Available: *https://opennetworking.org/sdn-resources/sdn-reading-list/sdn-applications/* [Accessed 16.03.2022.]

[22] P. K. Sharma, S. Singh, Y. S. Jeong and J. H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," in *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78-85, 2017

[23] M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman and S. Adamović, "*Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device Security Gateway Architecture*", in Energy Reports, 2021

[24] K. Nam and K. Kim, "*A Study on SDN security enhancement using open source IDS/IPS Suricata,*" 2018 International Conference on Information and Communication Technology Convergence (ICTC), pp. 1124-1126, 2018.