SOFTWARE DEFINED NETWORK FOR SMART HOME

Shujairi Murtadha

Doctoral Degree Programme (1), FEEC BUT

xshuja00@vutbr.cz

Supervised by: Vladislav Škorpil

E-mail: skorpil@feec.vutbr.cz

Abstract: As the world embraces Smart Home Technologies, there is a need for an efficient management platform for these services. Accordingly, this article proposes the Software-Defined Smart Home (SDSH) platform, which offers openness, virtualization, and centralization. The platform can integrate heterogeneous devices and offer flexibility between user demands and family scenes. This article offers a detailed explanation of SDSH and using it as a Firewall, explores potential applications, and identifies challenges and opportunities associated with its adoption.

Keywords: SDN, Smart Home, SDSH, IoT, Raspberry Pi

1 INTRODUCTION

Over the recent past, the world has witnessed the proliferation of Smart Home solutions. Smart home technologies are defined as digitally enhanced devices that provide high-quality services [1]. Moreover, Smart homes consider a promised approach for energy efficiency, climate change, and others [2]. the Office of Gas and Electricity Markets in the United Kingdom (UK) demonstrated that smart homes provided a solution for the decarbonization of electricity and other related programs [3]. the prevalence of smart homes' technology reached about 7.5% of households and the expected revenues about of 44.2 billion in 2018 [3]. Moreover, the expectations that the smart homes ached about 30% (84 million) of households by 2022; with France, Germany, and the United Kingdom leading the European market [4].

Indeed, the growth of the Smart Home market has continued to grow ever since. The field of academics has been examining the gap between the need and adoption of Smart Home applications. One of the key findings identified is that users are experiencing challenges managing the ever-growing list of devices in their homes [5]. The sheer diversity of smart home devices means that issues of interoperability and poor integration are common. As a result, Dixon et al. emphasized the need for the creation of dynamic smart home solutions [5]. As smart devices and the complexity of applications increase, the capability to meet the needs of common users for smart homes remains problematic.

2 SOFTWARE-DEFINED NETWORK (SDN)

The hierarchical network architecture that has been successful for open systems, is not able to deal with the complexities associated with closed systems. At the same time, global internet traffic has been increasing exponentially [6]. Today, the typical user demands greater bandwidth and additional services. Accordingly, there is a need for a scalable, high-performance network architecture to support the growing demand and enable flexibility. In 2018, McKeown presented the concept of Software-Defined Networking (SDN) that comprises data and control planes [7]. While the Data Plane comprises the hardware abstraction and physical Infrastructure Layers, the Control Plane consists of network applications and operating systems [7]. OpenFlow, which is a standardized communication protocol, decouples these two planes [8]. Some of the advantages of the SDN architecture include openness, the ability to deploy the network operating systems and applications on servers that adopt

X86 architecture and control data forwarding using OpenFlow, and the capacity to use OpenFlow to decouple the Control and Data Planes and virtualize the network [7]. As such, the concept of SDN has found applications in routers due to the need to develop flexible, open, and modularized devices [9]. The idea has also found application in cloud computing and data center applications [10,11]. Researchers have also explored the possibility of applying the concept of SDN to the Internet of Things [12]. The application of SDN could help in developing an IoT-oriented system structure design to address challenges such as service quality and network heterogeneity [13,14]. However, SDN does not adequately address two major issues: rapid developments in the Smart Home field and the complexity of application scenes. Accordingly, the Software-Defined Smart Home (SDSH) is proposed.

3 SOFTWARE-DEFINED SMART HOME (SDSH)

The Software-Defined Smart Home (SDSH) adopts an approach that comprises three levels: Application Layer, Controller, and Smart hardware layers. Whereas the three layers in SDN technology are similarly offset by the 3 layers in SDSH technology proposed with some additions.

The proposed device in the Control layer is an SDSH Controller that consists of an Arduino Microcontroller or a Raspberry Pi. One of the benefits of this controller is that if the SDN Controller falls, the Microcontroller can manage the Home Network, store its information, and add a level of security by verifying the identity of the User also it can work as a firewall separating the home network from the SDN Controller.

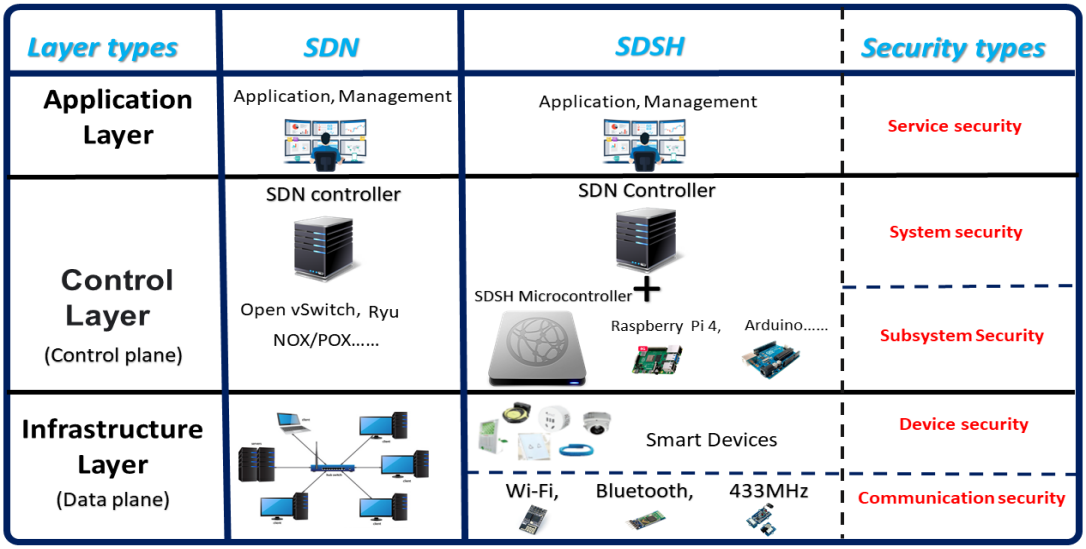

Figure 1: Architecture SDN vs SDSH

4 SDSH MICROCONTROLLER AS A FIERWALL

Due to the inability of the sensors to contain the software such as the firewall as an example, or the ability to programing, it represents one of the vulnerabilities that could cause penetration through it and entering the network to the main SDN Controller and tampering fully networks In this section the suggestion is the device (SDSH Microcontroller) to function as a Firewall, not just for home network management as the main part of the SDSH Microcontroller is the Raspberry Pi.

In other words, Raspberry Pi is a small computer (Microcontroller) the size of which does not exceed the size of credit cards with a low cost that can be connected to a computer screen or TV screen, and a mouse and keyboard can be connected to it to facilitate control, and to perform many tasks such as home automation: it can be controlled By turning on and off the lights, temperatures, and humidity in the home using smartphone applications, and storing all the data related to that easily through

some sensors, Raspberry Pi and some coding. The important thing is that it is a programmable control device that could contain the software as well as open-source. Figure 2 Shows the SDSH Firewall in the Home Network. Figure 3 represents the Flowchart for SDSH Firewall Implementation

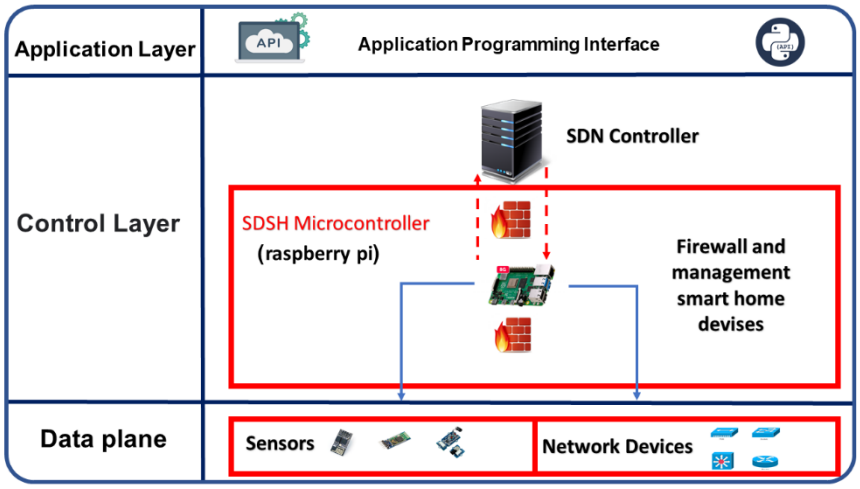

Figure 2: SDSH Firewall for the Smart Home Network

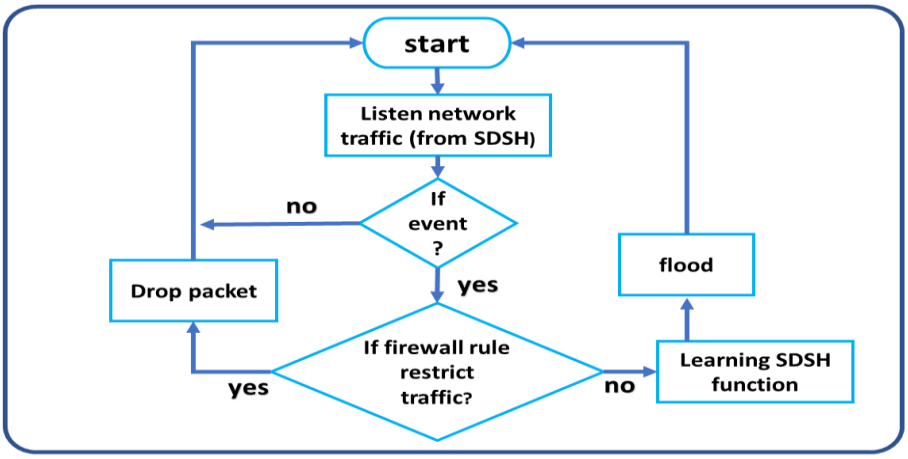

Figure 3: Flowchart for SDSH Firewall Implementation

5 CHALLENGES AND OPPORTUNITIES

Besides the technological gaps, the adoption of SDSH is likely to encounter several problems and present some opportunities. The main challenge is the risk of privacy infringement. Indeed, the Internet of Things (IoT) paradigm has been criticized because of poor family privacy protection. Devices such as sensors and cameras collect vast quantities of personal information, which are fed into machine learning algorithms to support automation [15]. Although measures such as the removal of personal identifiers such as names and addresses are often employed, hackers can reconstruct this information [16]. The SDSH model also proposes an interconnected approach which means that one intrusion could have far-reaching consequences within a network in terms of security and safety. Accordingly, strong security mechanisms must be adopted together with this architecture. The security should not just be limited to technical aspects but must also consider human-related system vulnerabilities [18].

A final opportunity is that SDSH can be integrated with the current Smart Home platform. A key aspect of SDSH is its openness, which allows interconnections with other platforms [17]. It also

includes virtualization technology that minimizes the heterogeneity and complexity associated with connecting different protocols or systems [19]. The SDSH platform can also offer different services for all external services or other platforms hence improving user experience.

6 FUTURE WORK

The future work will be conducting a practical study of the implementation of SDSH Microcontroller integrated into smart home sensors, the study will be considering several performance parameters that will be discussed and analyzed. to design an efficient system that capable of self-recovery in the case of the SDN-failure, artificial intelligence algorithms will be integrated into the system for error detection and correction and to prevent and predict a cyber-attack.

7 CONCLUSION

The next phase of improvements in smart home technologies should focus on addressing challenges such as differences in user requirements, diverse hardware, and the need for monitoring. Accordingly, this paper presents SDSH, which is based on the SDN's strategies of optimization, centralization, and virtualization. SDSH is based on a controller that integrates with external services and connects with different smart devices. It also allows APIs to connect to third-party services. Some of the technologies central to the operation of SDSH include demands-acquiring technology, system recourse virtualization, network formation, and AI-based decision-making. In addition to discovering the requirements of users, SDSH offers a smart platform for controlling devices. Although SDSH is a promising architecture, key challenges such as the possibility of cyber-attacks and privacy infringement must be addressed.

REFERENCES

[1] Strengers Y, Nicholls L. Convenience and energy consumption in the smart home of the future: industry visions from Australia and beyond. Energy Res. Soc. Sci. 2017; 32:86–93.

[2] ovacool, Benjamin K., and Dylan D. Furszyfer Del Rio. "Smart home technologies in Europe: a critical review of concepts, benefits, risks and policies." Renewable and sustainable energy reviews120 (2020): 109663.

[3] Ofgem. Upgrading our energy system: smart systems and flexibility plan: progress update. 2018.

[4] Sforza M. Twenty-two million smart homes in Europe: from science-fiction to reality. cityfied. Jan-2019 [Online]. Available: http://www.buildup.eu/en/new.

[5] McKeown, N.: Software-Defined Networking, INFOCOM keynote speech, vol. 17, no. 2, 2009, pp. 30–32.

[6] Masayoshi, K., et al.: Maturing of OpenFlow and software-defined networking through deployments, Computer Networks vol. 61, 2014, pp. 151-175.

[7] Xu, K. et al.: Toward a Practical Reconfi gurable Router: A Software Component Development Approach, IEEE Network, vol. 28, no. 5, 2014, pp. 74–80.

[8] Yang, H. et al.: Cso: Cross Stratum Optimization for Optical as a Service, IEEE Commun. Mag., vol. 53, no. 8, Aug. 2015, pp. 130–39.

[9] Banikazemi, M. et al.: Meridian: an SDN Platform for Cloud Network Services, IEEE Commun. Mag., vol. 51, no. 2, Feb. 2013, pp. 120–27.

[10] Valdivieso, Á., L. et al.: SDN: Evolution and Opportunities in the Development IOT Applications, Int'l. J. Distrib. Sensor Networks, vol. 2014, 2014.

[11] Qin, Z.: A Software Defi ned Networking Architecture for the Internet-of-Things, 2014 IEEE NOMS, 2014, pp. 1–9.

[12] Jararweh, Y. et al.: Sdiot: A Software Defi ned Based Internet of Things Framework, J. Ambient Intelligence and Humanized Computing, vol. 6, no. 4, 2015, pp. 453–61.

[13] Lee, H.: Home IoT resistance: Extended privacy and vulnerability perspective, Telematics and Informatics, vol. 49, 2020, pp. 101377.

[14] H. J. et al.: February. De-identification and privacy issues on bigdata transformation, in 2020 IEEE International Conference on Big Data and Smart Computing (BigComp), 2020, pp. 514-519.

[15] Alam et al.: IoT virtualization: A survey of software definition & function virtualization techniques for internet of things, arXiv preprint arXiv:1902.10910, 2019.

[16] Abomhara, M. and Køien, G. M.: Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks, Journal of Cyber Security and Mobility, 2015, pp. 65-88.

[17] Zhang, D. et al.: Heteroedge: taming the heterogeneity of edge computing system in social sensing, in Proceedings of the International Conference on Internet of Things Design and Implementation, 2019, (pp. 37-48).

[18] Dixon, C. et al.: An Operating System for the Home, Proc. 9th USENIX Conf. Networked Systems Design and Implementation, 2012, pp. 25–25.

[19] C. V. N. Index, "Forecast and Methodology, 2013–2018, 2013."