International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 11 | Nov -2017 www.irjet.net p-ISSN: 2395-0072

Software Defined Networking Architecture for Empowering Internet of Things & Enhancing Security Features Using Software Defined Networking: Survey & Discussion

Ms. Arundhati Ubhad[1], Dr.Prof Parikshit Mahalle[2]

[1]Department of Computer Engineering Smt Kashibai Navale College of Engineering Vadgaon, Pune, Savitribai Phule Pune University Maharashtra(India)
[2]Professor & Head, Dept of Computer Engineering Smt Kashibai Navale College of Engineering Vadgaon, Pune, Savitribai Phule Pune University Maharashtra(India)

Abstract - *The Internet of things has gained enormous attention in today's world. Most of the organizations have started showing interest in IoT and has resulted in deployments in various areas such as IoT subnetworks where multiple heterogenous wireless solutions co-exist. As the devices in the IoT environment are geographically distributed and open they need to be managed and especially in dynamic environment where the end user's need changes is a key technical challenge. Today's IT industries are growing exponentially, the programmability of network will be critical for business growth. In this systematic survey on SDN, we investigate the need for SDN, its architecture and the new features provided by SDN which proves to be useful in enhancing the network security.*

***Key Words*: SDN, IoT, OpenFlow**

1.INTRODUCTION

The concept of the IoT became popular in 1999, through the Auto-Id centre at MIT and related market analysis publications. Radio frequency identification (RFID)was seen as a perquisite for IOT at that point[17]. If all the objects and people in daily life were equipped with identifiers, computers could manage and inventory them. Besides using RFID tagging of things may be achieved through such technologies as near field communication, barcodes, QR codes, Bluetooth and digital watermarking. The internet of things is not the result of single novel technology; instead several complementary technical developments provide capabilities that taken together help to bridge the gap between the virtual and physical world [10].

Basically, IoT is an technology which aims towards connecting physical objects, devices through the internet. The physical devices can be connected to the internet through Wi-Fi (802.11),3G, 4G network, LTE network and Bluetooth. As the millions of devices are connected to the network, the complexity of connecting these millions of devices increases. Also, the networks has to find these devices and connect with them and then route the traffic and make the rules about how each individual device will be used followed by monitoring each of these connections and the data that will be generated by them. So SDN becomes important in internet of things to avoid this growing level of complexity. SDN helps in finding and connecting with these devices and then routing their traffic. Contrast to that with a single router we might have to write thousand lines of code to accomplish this but with SDN it can be handled with few mouse clicks.

Software defined networking is an emerging technology and proves to be promising for future networks. It uses OpenFlow protocol for its implementation [10]. OpenFlow is the key component to understand the SDN concept and many research ideas based on SDN/OpenFlow have been proposed and are still emerging [12] [13] [14]. In the traditional methods of management i.e. configuration is done device by device or system- by- system using manual methods and simply cannot scale at the rate required today. Thus, automation via network programmability is one of the ways in which IT combat the cost associated with rapid growth without burning out engineers. Thus, we can say that software defined networking is not only good for networks but also for business. SDN allows us to maximize the security, performance while keeping up with ever changing business needs. As sdn has the ability to cope up dynamically with the changing user needs or the new traffic patterns, security incidents and policy changes will enable IoT environments to deliver on their promise.

2. MOTIVATION

Software defined networks were created in response to demands from large data centers who found problems coping with unpredictable traffic patterns. These traffic patterns would cause very high demands for particular resources that couldn't meet with existing infrastructure. So, there were two choices either to scale the network infrastructure to meet the peaks which is very expensive or to build a network which can reconfigure itself automatically to cope with those peaks and channel the resources to meet the appropriate demands.

2.1 Traditional networking architecture

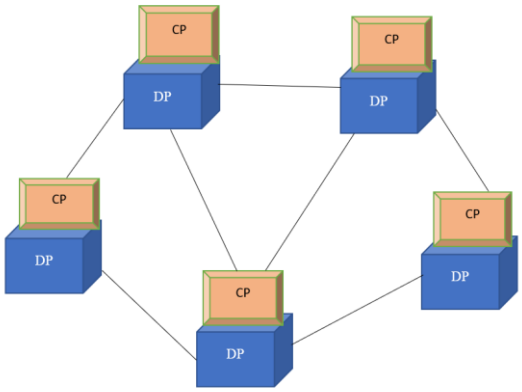

Fig 1: Traditional n/w architecture

Here in the above figure (1), we can see that there is separate control plane (CP) and data plane(DP) for each device. Each plane has a separate task that provides overall switching and routing functionality. Thus, network manager needs to configure each device separately which is very time consuming task. In addition to that, there is no complete network view. Also, the network needs changes dynamically and thus cannot meet to the end users demands.

Problems associated with traditional networking architecture

->Scalability
->Classification of data and routing traffic
->Time Consuming
->Multi-vendor environment requires high level of expertise
->Decentralized network control

Thus, to address the problems associated with traditional networking architecture, the concept of Software defined networking architecture was introduced.

2.2 Software defined networking architecture

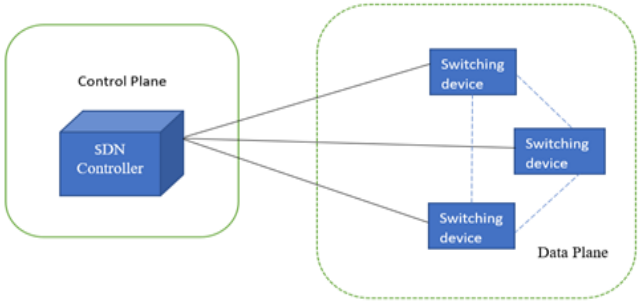

Fig 2: SDN Controller

Figure (2) shows the SDN architecture in which both the control and data planes are decoupled having only one centralized controller. A programmable interface is provided to the separated control plane having intelligence added to them. Software defined networks are dynamic and resilient, coping with the real time demands of IoT.

SDN controller features:

- **Network Programmability**: As the SDN controllers can be programmed it is possible to apply the sophisticated filters to the packets and control the incoming and outgoing traffic.
- **Scalability**: As the SDN deals with heterogenous network, SDN controller interacts with the different devices and number of devices can be added or removed to the network without affecting its performance.
- **Centralized Monitoring**: SDN controller enables the IT organization the end-to-end network flow visibility. An SDN controller uses the OpenFlow data to identify the problem on a given flow and changes the path of the flow that it takes.
- **Visualization:** SDN controller provide visualization of the multiple virtual networks that run on the physical network. Controller also allow the organization to see the flow from both the physical and virtual network perspective to get the detailed information.
- **Performance:** SDN controller pre-populate the flow tables to its maximum possible extent and have good processing and I/O capability that ensures centralized controller is not the bottleneck.

3. LITERATURE SURVEY

a) Haopei Wang, Lei Xu, Guofei Gu[1] focuses on the reactive controllers and consequent security threats against them. A defence framework for sdn networks known as floodguard which is scalable, efficient, lightweight and protocol independent is proposed in this paper to prevent data-to-control plane saturation. Floodguard system uses proactive flow rule analyser and proactive migration for preventing data-to-control plane saturation attack. Impact on bandwidth under different attack rates with and without floodguard is evaluated.

b) Mohan Dhawan, Rishabh Poddar, Kshiteej Mahajan, Vijay Mann [2] explains SPHINX - controller agnostic tool that takes advantage of the flow graphs to detect the security threats on network topology and data plane forwarding emerging within software-defined-networks. SPHINX

incrementally updates the flow graph and detects the attacks in real time that some controllers are vulnerable to.

c) Vandana C.P [15] explains the overview of the current state of the IoT with the security challenges like object identification, privacy and integrity, authentication and authorization and malware in IoT. Software-defined-networks concept along with the Software-defined-networks based IoT architecture is discussed. Also, the security mechanism based on the concepts of segment controller and gateway controllers are highlighted.

d) Seungwon Shin, Lei Xu, Sungmin Hong, Guofei Gu [3] explains the features provided by software-defined-networks such as dynamic flow control, network wide visibility with centralized control, network programmability and simplified data plane. In addition to these features, how network security benefits from these above mentioned features is illustrated with examples. Thus in-depth-investigation is done in this paper on how software defined networking features can bring benefits to security illustrated with state-of-art research in related areas.

e) Shiva Rowshanrad, Sahar Namvarasl, Vajihe Abdi, Maryam Hajizadeh, Manijeh Keshtgary [4**]** presents the software-defined-networks capabilities, deployment, applications and the challenges faced giving the broader view of the concept. Also, the brief introduction to the history of programmable networks and different protocols which are used for communication such as OpenFlow, XMPP, OnePk is given.

f) Hai Huang1, Jiping Zhu1**, Lei Zhang2[5]** proposes a network management framework in which software-defined-network is combined with IoT. The devices in the network can be managed and configured dynamically based on SDN. It also improves the reconfiguration and flexibility of devices and the proposed framework mainly focuses on M2M transactions. Thus, the authors addresses the integration solution between the IoT devices and SDN.

g) Muhammad H. Razaa, Shyamala C. Sivakumarb, Ali Nafarieha, Bill Robertsona [6] presents the two types of SDN implementation strategies i.e. proprietary and open source. Author compares and comes out with some notable differences between them such as network control, feedback from physical layer to logical layer, stability and vendor support and standardization.

h) Eun Joo Kim, Jong Arm Jun, Nae-Soo Kim [16] provides the method for configuring the data traffic paths in IoT based SDN and configuring function for each switch node constituting the configured data traffic paths. It also provides the terminal with path list information where the user can select the most appropriate path suitable for a service demanded by the user. Thus, this overall activity enhances the performance and service quality.

i) Ola Salman Imad Elhajj Ayman Kayssi Ali Chehab[7] focuses on the control plane of the SDN architecture. A study is carried out on new controllers such as ONOS and Libfluid based controllers are tested using Cbench, an OpenFlow testing tool in this paper. Also, the comparison of multiple controllers is carried out based on several different parameters and found that OpenDayLight is a good choice as a full featured controller.

j) Yaser Jararweh1, Mahmoud Al-Ayyoub1, Ala' Darabseh1, Elhadj Benkhelifa2, Mladen Vouk3, Andy Rindos4 [8] proposes the framework for SDIoT exploiting the several software defined systems such as SDN, SDStore andSDSec. SDIoT solution accelerates and facilitates the IoT control and management operations. Also, the three main components of the proposed architecture i.e. physical layer, control layer and application layer are illustrated.

4.GAP ANALYSIS

Table -1: Gap analysis

Paper ↓	Authentication	Authorization	Scalability	Security	Performance
a	YES	NO	YES	YES	GOOD
b	NO	NO	YES	YES	GOOD
c	NO	NO	YES	YES	MODERATE
d	YES	NO	NO	YES	GOOD
e	NO	NO	NO	LESS SECURE	MODERATE
f	YES	YES	NO	LESS SECURE	MODERATE
g	NO	NO	NO	YES	GOOD
h	YES	NO	YES	LESS SECURE	GOOD
i	NO	NO	YES	LESS SECURE	GOOD
j	YES	NO	NO	LESS SECURE	MODERATE
Proposed System	YES	YES	YES	YES	GOOD

The above table shows the gap analysis which is carried out using some parameters like authentication, authorization, scalability, security and scalability. When it comes to providing security to the SDN authentication and authorization plays vital role. Also the performance of the controller needs to be evaluated. Thus Paper[1], [4], [6], [8], [10] does the authentication of the arrived packets . Also the system needs to be scalable as the SDN network is dynamic and user needs changes and number of devices keep on adding or removing the system should work effectively without affecting the overall performance.

Thus, the proposed architecture must be scalable, secure, preserve the integrity of data and have low performance overhead.

4.PROPOSED ARCHITECTURE

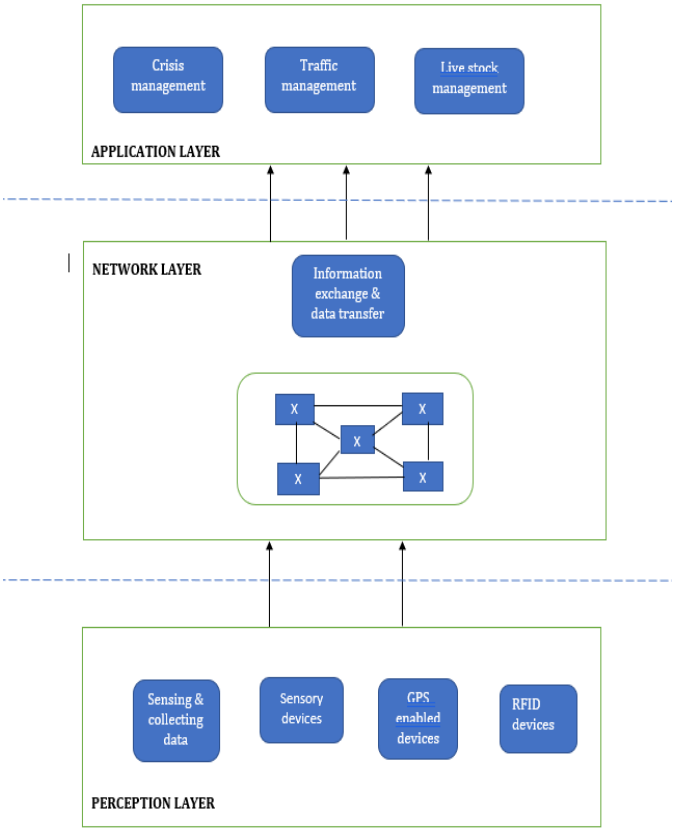

Fig 3: SDN working based on IoT layers

The three IoT layers are perception layer, network layer and application layer are shown in fig (3). Perception layer senses the data from physical as well as human worlds in IoT. RFID devices, GPS and camera enabled devices, sensor devices comprises this layer and main functionality of this device is things identification and intelligent acquisition. This layer is the core layer of the IoT structure due to this functionality.

Network layer is responsible for exchanging the information and data transfer and the SDN controller processes the data here.

Application layer runs the particular application and it provides human - machine interface. Thus the proposed architecture tries to be scalable, and have low performance overhead with the authentication and authorization security features.

5. CONCLUSIONS

In this paper, we discussed the need for SDN and showed how IoT and SDN are related to each other. Some of the features provided by SDN are also discussed. In this survey an in-depth investigation is carried out on how SDN works on the IoT layers. By decoupling the control plane from data plane SDN can cope up dynamically with the changing user needs and it can maximize the performance and IT organizations can benefit from it.

REFERENCES

[1] Haopei Wang,Lei Xu, Guofei Gu, " FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks"

[2] Mohan Dhawan, Rishabh Poddar, Kshiteej Mahajan, and Vijay Mann. SPHINX: Detecting Security Attacks in SoftwareDefined Networks. In NDSS'15, 2015.

[3] Seungwon Shin,Lei Xu, Sungmin Hong, Guofei Gu, "Enhancing Network Security through Software Defined Networking (SDN)"

[4] Shiva Rowshanrad , Sahar Namvarasl, Vajihe Abdi, Maryam Hajizadeh, Manijeh Keshtgary, "A survey on SDN, the future of netwoking" Journal of advanced computer science and technology, doi: 10.14419/jacst.v3i2.3754

[5] H. Huang, J. Zhu, and L. Zhang, "An sdn based management framework for iot devices," in Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). 25th IET. IET, 2013, pp. 175–179.

[6] Muhammad H. Razaa, Shyamala C. Sivakumarb, Ali Nafarieha, Bill Robertsona, "A Comparison of Software defined network(SDN) Implementation Strategies" doi:10.1016/j.procs.2014.05.532

[7] Ola Salman Imad Elhajj Ayman Kayssi Ali Chehab, "SDN Controllers: A Comparative study" doi:10.1109/MELCON.2016.7495430

[8] Y. Jararweh, M. Al-Ayyoub, A. Darabseh, E. Benkhelifa, M. Vouk, and R.Andy,"Sdiot:a software defined based internet of things frame work," Journal of Ambient Intelligence and Humanized Computing, 2015.

[9] What is docker? [Online]. Available: https://www.docker.com/ what-docke

[10] B. Eleonora, "The internet of things vision: key features, applications and open issues," Computer Communications, 2014 - Elsevier, 2014.

[11] OpenFlow. Innovate Your Network. http://www.openflow.org.

[12] R. S. Braga, E. Mota, and A. Passito. Lightweight DDoS Flooding Attack Detection Using NOX/Open Flow. In Proceedings of the35th Annual IEEE Conference on Local Computer Networks, LCN, 2010.

[13] Ankur Nayak, Alex Reimers, Nick Feamster, and Russ Clark. Resonance: Dynamic Access Control for Enterprise Networks. In Proceedings of WREN, 2009.

[14] Sungmin Hong, Robert Baykov, Lei Xu, Srinath Nadimpalli, and Guofei Gu. Towards SDN-Defined Programmable BYOD (Bring Your Own Device) Security. In NDSS'16, 2016.

[15] Vandana C.P, "Security improvement in IoT based on Software defined networking" ISSN:2278-7798

[16] Eun Joo Kim, Jong Arm Jun, Nae-Soo Kim, " A Packet scheduling Strategy for Heterogeneous Traffic of Internet of Things".

[17] Bose I, Pal R, "Auto-ID: managing anything, anywhere, anytime in the supply chain", Communications of the ACM, vol. 48, no. 8, 2005, pp 100-106.