TABLE OF CONTENTS

Software-Defined Networking for Internet of Things (IoT): A Report

Vaibhav Yadav, Student of Acropolis Institute of Technology and Research, Indore

Summary

SDN helps you transform your network, breaking away from its restrictive hardware constraints with improved agility, security, scalability and programmability. Kyndryl offers a consulting-led approach that helps you create the cloud-enabled, dynamic, and resilient network that your enterprise needs.

Internet of Things (IoT) is fast becoming a disruptive technology business opportunity, with standards emerging primarily for wireless communication between sensors, actuators and gadgets in day-to-day human life, all in general being referred to as "Things". This offers the capability to measure for understanding environment indicators. This paper addresses the internet of things (IoT) as the main enabling factor of promising paradigm for integration and comprehensive of several technologies for communication solution, Identification and integrating for tracking of technologies as wireless sensor and actuators. IoT as envisioned is billion sensors connected to the internet through the sensors that would be generate large amount of data which need to analyzed, interpreted and utilized. Context aware capturing enables modeling, interpreting and storing of sensor data which is linked to appropriate context variable dynamically. Building or home automation, social smart communication for enhancement of quality of life, that could be considered as one of the application of IoT where the sensors, actuators and controllers can be connected to internet and controlled.

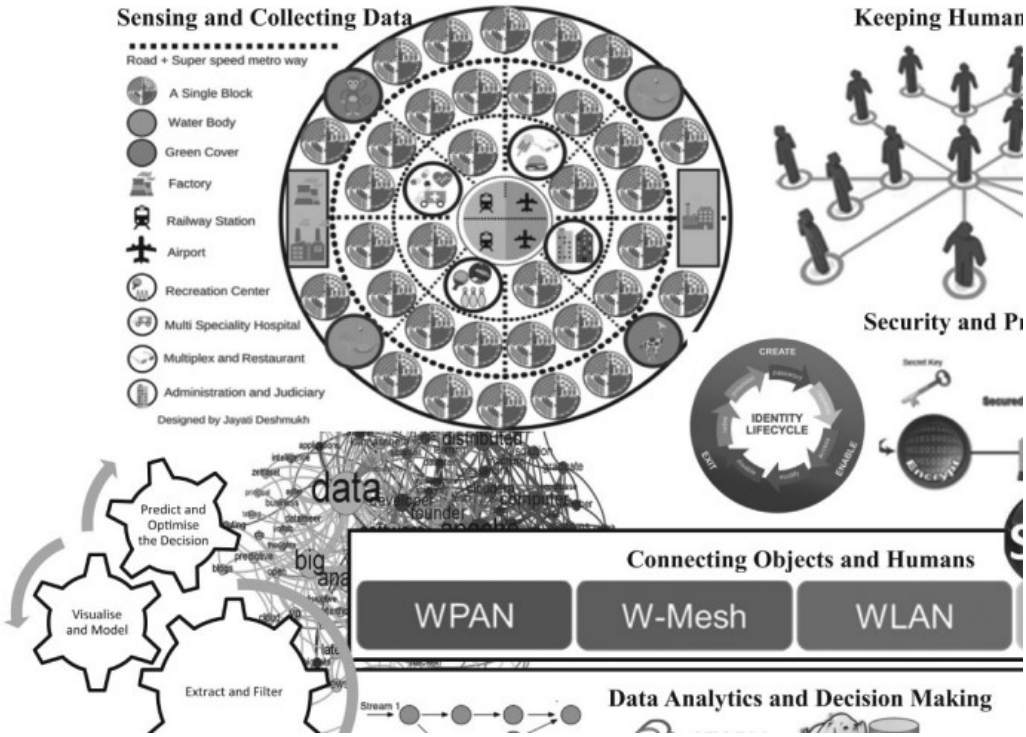
Published in: **International Conference on Computing, Communication & Automation**

CCS CONCEPTS • Networks → Network architectures • Networks → Network KEYWORDS SDN; IoT; Integration of SDN/IoT; WSN_SDN; Cellular SDN

Introduction

Internet of things (IoT) poses challenges that are different from traditional Internet in different aspects — heterogeneous communication technologies, application-specific QoS requirements, massive influx of data, and unpredictable network conditions. On the other hand, software-defined networking (SDN) is a promising approach to control the network in a unified manner using rule-based management. The abstractions provided by SDN enable holistic control of the network using high-level policies, without being concerned about low-level configuration issues. Hence, it is advantageous to address the heterogeneity and application-specific requirements of IoT.

We study the application and impact of softwarization on IoT networks from different perspectives: **access networks, edge networks, and wide area networks**. We also develop and analyze models to characterize the performance of softwarized networks.



IoT ECOSYSTEM

The Internet of Things (IoTs) is an emerging technology which enables smart ecosystem leveraging heterogeneous technologies. Generally, physical devices equipped with RFID tags, actuators, wireless sensors, and/or wireless communication devices are connected to the Internet to form IoT network. These devices are specifically deployed in application context to participate in creating a smart environment ranging from cellular networks, to Machine-to-Machine (M2M) communication, from vehicular networks to wireless sensor networks, and in embedded systems, etc. Wide ranges of IoT application are stipulated to restructure the smart environment and to establish new computing paradigms to connect physical objects. Some of the application scenarios are health automation, first responder monitoring and safety system, smart homes and buildings, nifty traffic control and management, industrial control and monitoring system, and so on. IoT applications are shown in Fig. 1.

Figure 1. Overall IoT scenario

IoT follows a layered architecture comprising of three main layers; Perception layer: consists physical objects and sensing devices, Network layer: responsible for transmitting data from. physical objects to the gateway/edge of the network, and Application layer: deals with application/services of the user demand. The myriad implementation of IoT is extending Internet connectivity among billion of devices. According to Cisco report on IoT growth [1] currently, 6.4 billion devices are connected to the Internet which will rise to 50 billion in 2020. These connected devices produce a huge amount of data, such as data produced in the current year (6.2 Exabyte) is estimated to increase by 478% (30.6 Exabyte) in 2020. This estimated rise of 781% in the connected devices and 478% rise in data generation in 2020, anticipating intelligent network control and management solution. Many solutions have confronted to resolve existing issues in the IoT paradigm. However, the traditional network is not capable of handling such enormous number of connected devices and huge data manipulation.

Software Defined Network (SDN) is considered revolutionary network technology is supporting heterogeneous networking with rapid evolution and dynamism using programmable planes (control and data plane explained in section II). The main objective of the SDN is to separate the control plane from the data plane involving the forwarding devices. The SDN and IoT integration can meet the expectation of control and management in diverse scenarios. There are many research publications that comprehend the application, implication, challenges, issues, prediction and analysis of SDN in different domains of IoT and SDN as well. B. A. A. Nunes et al. briefly describe programmable networks and trends for SDN in past, present and future in [2]. Some other comprehensive surveys have also discussed the importance of SDNs [3-5]. Due to the important and centralized orchestration of SDN in another network, much emphasis is put in the integration of

SDN with wireless networks. In this regard, some articles survey the SDN in a wireless network like in [6, 7]. However, in this article, we focus on the existing SDN based solution for management and security in term of IoT and cellular networks and provide a comparative outcome of this solution.

Software-defined networking (SDN) is gaining prominence among technologists for its disruptive quality, vis-à-vis the traditional network. SDN is an approach to networking that enables network nodes to be managed through programming, rather than traditional system administration methods.

SDN will become important as IoT matures and its demands on the network increase. If you are wondering about how critical SDN will become, well, experts predict that IoT could comprise a whopping 21 billion devices by 2020. In order to better support these devices, the SDN market will burgeon to $132.9 billion by 2022, predicts a report by Allied Market Research, a global market research firm.

For SDN to become the norm, the growing number of mobile and other connected devices must begin to process the data they create between them. Additionally, the sectors interested in accessing data from these connected devices will need to create security related processes to transfer and store this data. Experts have a term to describe the changes the network will undergo to cope with IoT, and it is called *elasticity*. That's industry jargon for how a network responds in an agile way to data transfer.

SDN's elasticity becomes significant as we enter an era dominated by Big Data. Traditional networks are not equipped and certainly weren't designed to deal with the flow of Big Data into the average enterprise. Big Data must be parsed to help, not hinder, an organization. That's why SDN, with its flexibility, allows for the right kind of data management in this new age.

For an example, let's turn to the healthcare sector. In the near future, hospitals are likely to have a large presence of machinery and patient end-point devices. All of these are also expected to be IoT-enabled and connected. Thus, one may come across a patient hooked up to a medical imaging device that is bandwidth-heavy on the hospital's network. To cope with this real-time load on the network, hospitals and other medical enterprises will need to have flexible bandwidth.

Adding to this need, is that hospitals are dealing with personal data that is strictly regulated, and will thus have to factor in end-to-end data security. If the hospital machinery which in this case is a portable imaging device, needs to be moved around the premises, the instrument will have to be connected in the new spot immediately and the same network policies and controls it had in the earlier network will need to be pushed dynamically to the new location as well.

This is a flexible requirement and needs the network to be elastic and respond with agility. The need for elasticity around reams of Big Data is what has necessitated SDN; now you can see why this new way of dealing with an ultra-connected world is expected to have tremendous opportunity for growth in the near future.

I see SDN becoming significantly advantageous in a number of ways:

First, it will make the network aware of its applications. An IT specialist at the hospital in the above example can utilize a remote monitoring mechanism to realize the level of awareness of appropriate applications via SDN. The specialist leverages technology to deal with situations in a particular and specialized way.

If the network traffic is heavy during a certain time of day, the specialist can ensure he routes applications in ways that will deal with that heightened traffic level. What makes SDN so attractive

is that it allows the specialist to develop a policy to make apps central and optimized during such times of stress on the network.

The bandwidth that a network demands becomes much easier for an enterprise to govern when using SDN because of its elastic nature. Suppose your organization has both a field office and a switching device as part of the IT scenario. By using SDN, you can deal with these varied demands in an elastic manner, providing the bandwidth to the entity or office that needs it most at a certain moment.

There are many aspects of SDN that are dynamic, including QoS (quality of service). Specialty switching instruments can respond to QoS by making requests and creating preferential treatments of packets within the network. Better still is that the SDN controller can add the extremely advantageous application-awareness feature. Doing so lets the application become aware of the preferential treatment that is provided.

Coming back to the connected medical scenario and applying some of the capabilities outlined above. Application awareness enables the network to identify that the heavy data is coming from a critical medical device. If the network is running low on bandwidth at that point in time, either a preferential, application-aware routing or QoS remarking and treatment can be accomplished dynamically.

With self-learning the hospital will know that there are particular days of the week or hours of the day when there is heavy usage of the data exchange (such as remote patient consultancy). During these times, it can adopt an elastic bandwidth based on requirements through a simple-to-use interface.

Finally, to secure end-to-end data, SDN-enabled adapters are made available to close the end devices and dynamic policies can be injected in real-time. These adaptors can make the portable medical devices connect to the network very fast and download the policies automatically.

So there you have it: The IoT and SDN are two technologies that very much depend on each other. SDN technology can better prepare a network for a successful and robust IoT. It provides the agility and elasticity, which IoT demands. Moreover, it provides an open environment for application developers to develop innovative tools and software connecting the IoT more effectively. Both of these technologies supplement each other in bringing us a better — and vastly more connected — world.

Body

SDN technology is a network management technique that allows for dynamic, programmatically efficient network setup to increase network performance and monitoring, making it more like cloud computing than traditional network administration.

SDN was created to solve the problem that old networks' static design is decentralized and difficult, but today's networks demand more flexibility and ease of troubleshooting. By decoupling the forwarding of network packets (data plane) from the routing process, SDN tries to consolidate network intelligence in a single network component (control plane).

The control plane is made up of one or more controllers, which are considered the brain of the SDN network and contain all of the network's intelligence. The fundamental difficulty with SDN is that intelligent centralization has its own downsides in terms of security, scalability, and flexibility.

Operation Technology SDN

Operational Technology (OT) Software Defined Networking is a type of SDN technology that is now available for industrial control applications that require highly quick failover (SDN). OT SDN technology is a method of managing network access control and Ethernet packet delivery for critical infrastructure networks using environmentally hardened hardware. OT SDN removes control plane administration from switches, concentrating it in the flow controller and using SDN as the switch's underlying control plane.

OpenFlow Protocol

The transfer is simplified by removing the old control plane and centralizing control plane management. OpenFlow is a common control plane standard used in OT SDN, making it interoperable with other SDN solutions. The difference is that OpenFlow is the only control plane in the switch, and the switch retains through power cycles, and all flows and redundancy are proactively traffic-engineered so the switches can perform the forwarding they are configured to do with or without telecommunications. Industrial networks benefit from OT SDN in terms of performance, cybersecurity, and situational awareness.

Network control and forwarding operations are decoupled in SDN designs, allowing network control to be directly programmable and the underlying infrastructure to be distinct from applications and network services.

SDN technology can make use of the OpenFlow protocol.

- Because network control is separated from forwarding functions, it is directly programmable.
- Administrators can dynamically modify network-wide traffic flow to meet changing demands by abstracting control from forwarding.
- Software-based SDN controllers that retain a global view of the network are (logically) centralized in network intelligence which appears to applications and policy engines as a single, logical switch.

SDN allows network administrators to swiftly setup, manage, protect, and optimize network resources using dynamic, automated SDN programs that they may create themselves because the programs do not rely on proprietary software.

SDN is vendor-neutral and based on open standards, which simplifies network design and management by allowing SDN controllers to give instructions instead of numerous vendor-specific devices and protocols.

SDN AND SDN ENABLED IOT ARCHITECTURE IoT and SDNs are two distinct technologies. IoTs mainly consist of sensing devices attributing different communication networks; whereas SDN is associated with network routing and act as an orchestrator for network level management. SDN is a separation between the control plane and data plane and provides vendor independence, whereas IoT is layered architecture consisting of multiple technologies at each level. Hence IoT can leverage benefits from SDN control plane due to the fact, SDN promise to hold the traditional network with new service demands. In this section, an architectural detail of SDN and SDN enabled IoT is presented.

SDN Architecture and protocol In SDN, the control plane is decoupled from forwarding plane and communication between two planes is done through APIs e.g. OpenFlow [8]. SDN is basically layered architecture consist of three layers (1). Data plane, (2). Control plane/controller,

and 3). Application layer. Data plane consists of dumb forwarding devices i.e. router & switches which only forward data on the controller instructions. The controller acts as a brain and manages the network by having a global view of the network. The customer needs are abstracted over application layer which is communicated to the controller via Northbound APIs e.g. RESTfull API. The controller manages the whole network and possesses a global view of the network. All applications/programs run above the controller. Many controllers are in the market from its inception such as OpenDaylight [9], Floodlight [10], NoX/POX [11], etc. SDN controller defines a rule for the incoming flows from the data plane. SDN layers communicate with each other via open APIs called Northbound Interface (NI) API and Southbound Interface (SI) API. 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.

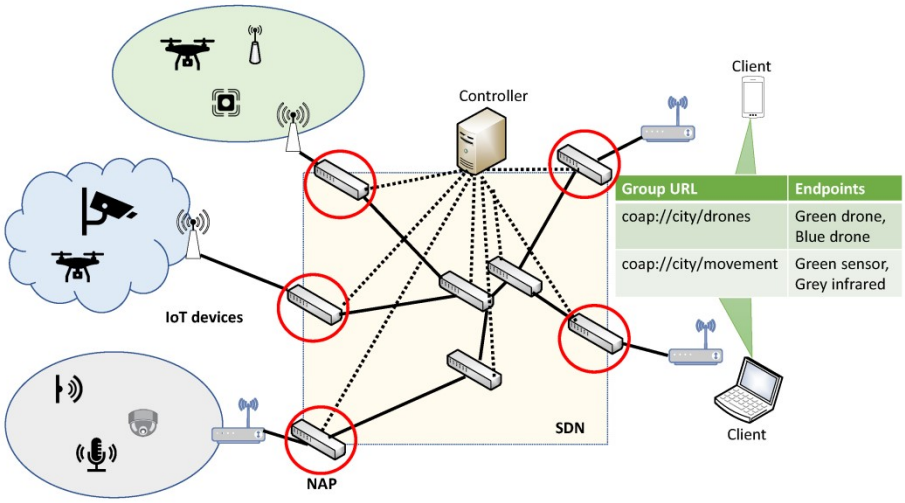


Figure 2: SDN based IoT network

SDN Based Cellular Network With the increasing complexity and aggregated telecommunication technologies, cross functionality in a cellular network is hard to obtain the desired result which requires a physically intervene in radio technologies. By providing software based radio manipulation, distinct management flexibility can uplift network performance. The first proposal for SDN based cellular network was presented by Li. Erran et. al in [17]. They name it as CellSDN, in which attribute based policies are formulated for an individual user in the LTE network and gain fine grain control over the network. In CellSDN, local agents on each switch perform deep packet inspection and reduce the excessive load on the controller SoftRAN is proposed by S. Tomovic et al. in [18], uses SDN principle in 4G LTE network. A centralized control plane abstracts the whole RAN into the geographical area. A big base station with centralized controller performs resource allocation in a grid of three dimensions i.e. space, time, and frequency slots. The controller decides to allocate resource in the domain of frequency, time and space slot. Radio elements/BS take some local decision to manage the delay. SoftCell [19], incorporate SDN in the cellular core network and provide fine grained policies for LTE network. In SoftCell architecture, traffic classification is done on the access switches instead of the gateway. Every access switch has a local agent which caches each UE profile to control packet classification access switch.

Architecture	Management	Architecture	Control/data plane decoupling	Protocol used	Scalability	Benefit
SDN-WISE[23]	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	Medium	The state-full approach, reducing information exchange. Mobility, reconfigurati and localizati of
WSN-SDN[24]	Sensor network flow management	WSN cluster with centralized controller monitored and controlled by Master SDN controller	Centralized master controller	OpenFlow/ distance aware routing protocol	Low	Optimal path selection, rou strategy adjustment
SD-WSN[25]	Infrastructure management and reconfiguration	FPGA	Micro-controller	COAP	Low	Programmab reconfigurati network
Integrate WSDN[26]	Management platform for using virtual machine	Local controller in each sensor node which interacts with a centralized controller. INNP	Centralized controller and local	Contiki OS on each local	Low	Flexibly usin commodity o the shelf dev

The controller assigns policy tag, hierarchical IP address and UE identifiers and embed into packet header to avoid reclassification of traffic. SDN and SDR integrated architecture for the 5G network is proposed in [20], called Hybrid SDN/SDR architecture. The architecture is cross layer combination of SDN and SDR for exploiting frequency spectrum and link information in the 5G network. The cross-layer controller is used to request frequency spread spectrum and make the decision for flow traffic. This architecture also manages user authorization in the cross-layer controller and grant access to a better band.

SoftAir [21], by Ian F. Akyildiz et al., proposed the integration of SDN principals in 5G network exploiting virtualization for a resilient network. SoftAir provides mobility aware load balancing and resources efficient allocation through virtualization. The aggregated control is provided by NFV creating multiple virtual networks with independent protocols and resource allocation algorithms. SD-RAN and SD-core network nodes are OpenFlow enabled and monitored through OpenFlow and Common Public Radio Interface (CPRI). All management policies are defined at central control plane which enables cloud orchestration and provides end-to-end QoS guaranty. In SDN&R [22], a merger of SDN and SDR for IoT network is presented for the integrated management of the cellular network. SDR is used to maintain radio status information in the control plane implemented in a base station (BS). The OpenFlow enabled control plane performs radio allocation on the BS and cognitive edges (CE). The CE obtains the complete view of the radio spectrum. The packet processing is done on the controller connected to BS via a secure channel. This architecture is the detailed footprint of SDN integration in a cellular network for managing

resources in IoT network. Table 1 discusses the existing SDN based cellular architectures and present their comparison.

The most common contributor in the IoTs is sensor network. Much work in done for the integration of IoT and SDN, few are given below. In the context of WSN management, L. Galluccio, et al. in proposed SDN-WISE in [23], in which SDN based WSN support duty cycle and data aggregation and provide a state-full solution. The adoption layer performs translation between the sensor node and WISE-Visor. SDN-WISE defines its policies on the basis of state description. Software-Defined Wireless Sensor Network Framework [24] and leverage SDN programmability in the WSNs. The architectural components of this approach consist of a Base Station (BS) and several sensor nodes. SDN controller operates on BS took routing decision in lieu of dumb sensor nodes. Sensor nodes contain flow table as in the SDN concept which is populated by SDN controller. In [25], T. Miyazaki et al. proposed an architecture for reconfigurable WSN network on the basis of customer need by using role injection and delivery mechanism. The role compiler generates scenarios which are injected through wireless communication. The change in the sensor nodes is carried by field programmable array (FPGA) and a microcontroller unit (MCU). The multi-purpose sensor network is also addressed in [26]. I. Leontiadis et al. exploited NFV for sharing single infrastructure for many applications in a sensor network. They proposed a framework for multiple application scenarios on a common build infrastructure. Each node has an abstraction layer for a shared hardware which works on the overlay network and creates multiple virtual sensor networks (VNS).

SDN for wireless sensor based IoT devices

Approach	Security parameter	Network	Description	Limitations
secured SDN framework [26]	Authentication	Ad hoc network	SDN controller block all switch port on receiving new flow and start authentication	Not prove simulation, framework
DISFIRE[27]	Authentication & authorization	Grid network	hierarchal cluster network with multiple SDN controllers implement a dynamic firewall to ensure authorization	Evaluation c The protoco not practical
Black SDN[29]	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	Scalability create hazar security
SDP[35]	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	Scalability performance

SDN based IoT Management The configuration, reconfiguration, resource allocation and even the pattern of inter communication become extremely difficult. SDN play a vital role in the management of such heterogeneous network. Table 2 present some of the management frame work for SDN based IoT networks. In [28], Qin et al. enhanced the idea of Multi-network controller architecture for heterogeneous IoT at the campus level. MINA is basically a middleware whose working principle is self-observing and adaptive, and manage the pervasive heterogeneous network.

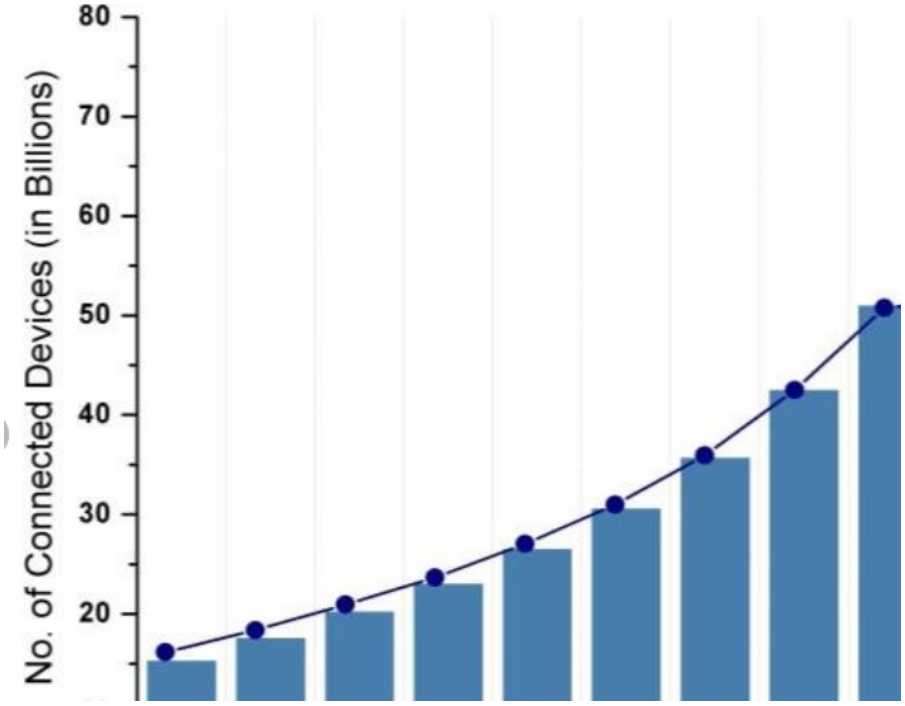
MINA follows SDN like layered architecture and flows matching principle which reduces the semantic gap between IoT and task definitions in a multi-network environment. This architecture aims flow scheduling and management of Wi-Fi and WiMAX environment which is optimized by utilizing resource sharing. Di. WU et al. in [29], presents UbiFlow framework which provides the integration of the SDN and the IoT. UbiFlow proposed an efficient flow control and mobility management in urban multinetworks 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. MINA perform per-device flow management and optimization of access. M. Boussard et al. [30], proposed SDN based control and management framework for IoT devices in a smart environment. The management framework, called as "Software-Defined LANs (SD-LAN)", organize devices and group these devices in the order of requesting services from the user.

This framework uses Universal Plug and Play (UPnP) and Simple Service Discovery Protocol (SSDP) for discovering new device in the SD-LAN network and create a virtual topology for service requirement. Y. Jararweh et al. in [31] proposed a framework model for SDN based IoT management and control. In this framework, data is collected from the sensor board and aggregated on the IoT Bridge. Then collected data is sent to SDSec controller for security checking. Access is provided only to an authorized device by using authentication and authorization. Rules are defined on the basis of collected data for routing and controlling policies by the SDN controller and stored into SDStore module of the framework.

SDN security framework for IoT The IoT devices become more vulnerable to security risks in a heterogeneous network. Few considerations of security aspect are witnessed in SDN based IoT network. In [32], K. S. Sahoo et al. proposed a secure architecture for IoT network based on SDN. This security architecture focuses on the authentication of 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 controller block all the port when the connection is established, and controller starts authenticating that device. If the user is authentic, the controller starts pushing flow to that user. Few controllers in the network serve as a security guard and exchange information with each other about the user authentication. In the case of guard controller failure, some other border controller is selected as security controller. In Gonzalez et al. proposed a dynamic firewall named as Distributed Smart Firewall (DISFIRE) for secure architecture in SDN based grid network. The architecture consists of hierarchal cluster network with multiple SDN controllers. These cluster head SDN controllers implement a security policy. For this purpose, they used Cisco defined policy agent opFlex in the controller instead of OpenFlow. The device information is exchanged between devices, and any unauthorized potentially malicious device flow rule policy is deleted.



IoT connected devices worldwide

A security proposal for smart cities is presented in. S. Chakrabarty et al. proposed a secure architecture based on trusted SDN controller, Black Network, Unified Registry and Key Management System in an IoT network. The security architecture ensures authentication of the heterogeneous devices. SDN controllers act as a Trusted Third Party (TTP) and provide security properties i.e. confidentiality, privacy, integrity and authentication and routing between IoT devices. The unified registry is responsible for Identity management, availability, accounting, authentication, authorization. The shared key is used for secure communication.

A security architecture is presented in [35] where each node is connected to a domain controller through an embedded virtual switch. This controller is on the edge of the network and acts as a domain controller and provide authentication of the network devices. For Valid authorization profile, flow entries are pushed in the access switch. F. Oliver et al. [36] proposed an SDN based IoT architecture for infrastructure and infrastructure-less network where a virtual switch is embedded in each node bounded to a controller in a domain. Some of the border switches are selected as security controller. The security controllers provide dynamic network configuration and security policy deployment.

CONCLUSION

The new era of IoT is changing the way of communication between human and machines. Now thinking are getting beyond the connectivity among every physical object with the Internet. However, IoT is in infancy and lack programmability, agility, security and data management to meet the need of customer requirement, it is highly anticipated to use programmability, and centralized control for IoT management and integration with SDN is required. In this paper, a survey of the existing solution of IoT leveraging SDN control and data plane programmability is presented. In this work, architectural details and contributing a framework of SDN based IoT are discussed, summarizing architectural details and its evolution, and then some of the unresolved issues in this merger are reported. Lastly, some predictions for the world in 2020 is made in the context of SDN based IoT.

RECOMMENDATIONS

Here are 11 key enterprise IoT security recommendations

1. Create a Strategy

Effective IoT security has to be organized so that no stone is left unturned. This means you will need to create and document a security strategy that is tightly integrated with both your general IT strategy and your overall business plan.

Your IoT security strategy should cover all areas that utilize the IoT network. It should set out, for each situation, the security measures that will be taken and how they will be monitored and reviewed.

As mentioned above, the IoT can appear in many different forms and you must take an in-depth look at your IT architecture and endpoints to ensure you catch everything in your net.

2. Invest in Ongoing Training

Most IT breaches include a human element, so a critical part of your IoT security strategy will be setting out an ongoing training program for both existing and new recruits.

IoT training should include a topic on the dangers of a shadow IoT, which is being fueled by the aforementioned commoditization of IoT devices. If employees are connecting home devices to the company network, they could be opening the door for hackers. They need to be taught whether a device might have a limited function (e.g. a smart kettle) has no bearing on its utility as a hacking device: the smallest of windows can be enough to allow a criminal to access your business. More in-depth training might include using anomaly detection and granular audit trails to detect threats.

3. Physical Security

The most basic level of IoT security is the physical protection of connected devices. Wherever possible, sensors and appliances should be kept under constant guard to protect them from being tampered with or reconfigured (e.g. passwords being reset, etc.)

When an IoT device isn't being used, it should be turned off and the immediate area secured. Physically covering ports, cameras, and microphones will add another layer of protection. The physical security of IoT devices or groups of devices could be assigned to specific individuals or teams in your operational manual.

4. Endpoint Hardening

Staying at the device level, endpoint hardening plugs vulnerabilities by blocking high-risk ports (e.g. TCP/UDP, serial ports, etc.), unencrypted communications and wireless connections. Measures should also be taken to protect devices from malicious code injection.

5. Manage Updates

All companies should include IoT in their password management process. Where possible, IoT devices, like all IT software, should be set up to receive automatic updates to minimize the attack window between patches.

At the very least, IoT devices should be capable of manual updating with the IoT vendors on top of the latest threats. It is best to upgrade on at least a monthly basis and to avoid devices that are incapable of being upgraded or are poorly supported.

You should also ensure that the details of the device lifecycle are recorded and acted upon. For example, you should replace any device once its support period is over.

6. Organize Device IDs

It is difficult to stay in control of IoT devices if you and your IT team don't recognize them on the network. An effective way to avoid shadow IT and stay on top of threats from IoT devices is to set up an official naming convention for the devices. As soon as a new IoT device is configured on your network, use the naming rules to give it a device ID that everyone in the company can recognize. That way, any unauthorized devices will immediately jump out.

7. Use Encryption

Moving on from devices to the network as a whole, it is crucial that data is kept secure from interception both while in transit and during storage. A data audit is the first step to ensure you can account for all data within your IT ecosystem.

Ideally, only devices which support encryption should be connected to your network and you may need to set up a VPN rather than connecting over the internet. This will also give you the benefit of increased performance.

8. Segment the IoT Network

One strategy that may work for you, particularly in industrial IoT (IIoT) settings, is to use network segmentation to isolate IoT devices from your core IT network. This can be done in a way similar to setting up a guest network. This way, even if a hack should happen, it won't cross over into your core network and your IT emergency response team can cut off the affected segment and avoid the danger of a company-wide disaster.

There are various models (e.g. The Purdie Model) that can be used for segmentation. But whatever method you use, ensure that you set up firewalls and monitoring software to help profile your IoT traffic and check for anomalies.

This has the added advantage of helping you to identify and disarm sources of attack with little or no risk to your business.

9. Strengthen Access Management

If you don't already have robust access and identity management system, now is the time to work on it. Such a system ensures that employees change passwords regularly, use two-factor authentication where possible, and are only able to access the IT systems they are authorized to use for their tasks. APIs can also be included for automated connections. Even if you already have identity management in place, you should ensure it is compatible with your IoT devices.

10. Use a Commercial IoT Platform

Most of the IT professionals who were surveyed by 451 Research revealed that they planned to use dedicated commercial IoT platforms to manage their IoT devices. Although this is a good idea in principle, it is very important that IT experts do their due diligence on the companies selling these products as there is likely to be a lot of variation in quality as vendors join the IoT gold rush.

11. Keep up to Date with Online Trust Alliance Guidance

In common with many new technologies, the IoT is currently poorly regulated with plenty of guidance and advice published but little in the way of standardization. Although the inevitable merging of organizations and advice is beginning to move us in the right direction, with thousands of pages of documentation produced by dozens of global organizations, knowing where to go for advice can be a challenge.

Some of the steps listed above apply to most industries. They have come from the IoT Trust Framework published by the Online Trust Alliance (OTA). The Alliance is an initiative of the Internet Society and is tasked with providing advice for security best practice and increasing consumer confidence in IT.

In the fast-paced world of cloud computing and the IoT, such guidance is regularly updated and expanded. The OTA publishes regular blog posts featuring the latest news on breaches, security best practice, and other security-related information. Keeping current with this will allow you to update your procedures and training materials so they remain relevant.

By following these 11 tips, your company should be able to keep itself safe from the worst of the threats that compromised IoT devices pose to your IT networks. You can then relax and look forward to the many benefits that connected devices are sure to bring to your business from improved data analytics to more efficient operations.

Appendices

1. https://ieeexplore.ieee.org/document/7148413
2. https://www.kyndryl.com/in/en/services/network/software-defined
3. https://www.researchgate.net/publication/319602888
4. https://www.tutorialspoint.com/what-is-software-defined-networking-sdn
5. "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 White Paper," Cisco.
6. Sreekanth. S.S is a Principal Technology Architect at Infosys. For more posts, visit InfyTalk
7. Nunes, B., Mendonca, M., Nguyen, X., Obraczka, K. and Turletti, T. 2014. A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. IEEE Communications Surveys & Tutorials. 16, 3 (2014), 1617-1634.
8. 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. (2015), 219-227.
9. Benzekki, K., El Fergougui, A. and Elbelrhiti Elalaoui, A. 2016. Softwaredefined networking (SDN): a survey. Security and Communication Networks. 9, 18 (2016), 5803-5833
10. Sahoo, K., Sahoo, B. and Panda, A. 2015. A secured SDN framework for IoT. International Conference on Man and Machine Interfacing (MAMI) (2015), 1- 4.
11. Robert, E. 2015. "Building the Internet of Everything (IoE) for first responders. Systems, Applications and Technology Conference (LISAT) (2015), 1-6.
12. Olivier, F., Carlos, G. and Florent, N. 2015. New Security Architecture for IoT Network. Procedia Computer Science. 52, (2015), 1028-1033.
13. https://www.altexsoft.com/blog/business/11-key-enterprise-iot-security-recommendations/