A Survey on SDN Based Security in Internet of Things

Renuga Kanagavelu(✉) and Khin Mi Mi Aung

Data Center Technology Division, A*STAR Data Storage Institute, Singapore, Singapore
{Renuga_k,Mi_Mi_AUNG}@dsi.a-star.edu.sg

Abstract. Internet of Things (IoT) is an emerging technology where tens of billions of devices that include everything from small wearable fitness bands, medical devices, smart devices to factory automobiles can be connected to the Internet which makes the life easy without or with little human intervention. Though IoT has proven to be more transformative, as its market size increases, it is really a big challenge to secure such a large number of devices that are connected by a complex heterogeneous network with a variety of access protocols. Software defined networking (SDN) decouples the control plane from the data plane, enabling fast reaction to security threats and security policy enforcement. IoT security can be achieved by the integration of SDN with IoT. SDN is an intelligent network paradigm which can open up ways to secure IoT and different access control mechanisms. This survey paper analyzes SDN based IoT security mechanisms to secure communications in IoT and present open research issues.

Keywords: Internet of Things · Software defined networking
Security · Access control

1 Introduction

With the rapidly growing Internet during the past decades, more and more devices are connected to the Internet. Gartner predicted that the number of devices connected to the Internet will grow exponentially up to 25 billion by 2020 [1]. The fact behind this growth includes smart devices that we use every day from small chips to large machines that are used on the industry floor are becoming the connected entities across the globe.

Internet of Things (IoT) refers to a network that connects not only smart phones and laptops but also the smart devices used at home automation, office, healthcare, e-learning, factories and even at nuclear reactors to the Internet [2]. These devices gathered and shared the required information autonomously between other devices. IoT provides the interaction between these devices by using different protocols. The common feature of IoT is to combine embedded

K. Arai et al. (Eds.): FICC 2018, AISC 887, pp. 563–577, 2019.
https://doi.org/10.1007/978-3-030-03405-4_39

sensory objects and ability to transfer data over a mix of wired and wireless networks without human-to-human or human-to-computer interaction [3]. Because of this, the physical devices are able to stay connected and without human intervention, machines can communicate with each other leading to a timely output.

While IoT brings in advantages in terms of time efficiency, money savings, and improved quality of life, it is prone to risks as the IoT devices can become the entry points to many critical infrastructures giving hackers and cyber criminals more entry points to exploit the sensitive information. The increase in automation may make the system more vulnerable. That is, more data will be transferred over IoT for automation. The greater the volume of sensitive data we transfer over the IoT, the greater the risk of data and identity theft, device manipulation, data falsification, IP theft and even server/network manipulation [4–6].

IoT consists of many heterogeneous devices which use different access protocols. Each protocol follows different access mechanisms and security measures according to the user requirements. Performance and security requirements vary considerably from one application to another. Apart from that most vendors only deal with the functionality and security of their products and pay less attention to the security and the privacy risks of the overall IoT architecture. A unified security mechanism is still not in place in IoT as it is really a great challenge. In IoT architecture, network will be the attractive attack target for leaking sensitive information as IoT devices will typically be embedded deep inside networks [7].

Traditional static network security approaches like Intrusion Detection and Prevention Systems (IDPS), Firewall are deployed at Internet edge devices. These mechanisms are meant to protect the network from external attacks. Such mechanisms do not provide effective security to IoT's borderless system architecture. Current approaches to secure IoT leverages communication protocol-based mechanisms, such as encryption for data-at-rest or in-transit. This may not be effective as the constrained endpoints themselves are susceptible to modification either by local access or remote connections. The other end-host based defenses like antivirus, and software patches from vendors like 'Patch Tuesday' are not well equipped to handle IoT security [8].

Software Defined Networking (SDN) [9] which is the new intelligent networking paradigm provides opportunities to solve issues related to IoT security. SDN provisions the security applications dependent on the service type and also allows the network to be agile against suspicious security attacks so that suspicious actions could be identified and either blocked or diverted to secure the users and the network. SDN can help only to reduce the risk as there are not enough resources to protect the entire increasing complex network at one time [11]. Additionally with the help of artificial intelligence and machine learning, the network could learn from attacks and find the ways to automate adaptive responses to prevent similar actions in future.

In this paper, we first provide a brief overview of the beneficial features of SDN in IoT security. We present a comprehensive survey on the existing SDN-based technologies in the context of IoT. Finally, we present different open research issues to be addressed for a secure IoT environment.

Rest of the paper is organized as follows: Sect. 2 discusses the security and privacy concerns in IoTs. Section 3 discusses how the SDN features are beneficial to IoT network security. Section 4 discusses various SDN-based IoT frameworks. Section 5 reviews the existing solutions and discusses the open issues that are needed to be solved. Section 6 concludes survey study with references at the end.

2 Security Concerns in Internet of Things

IoT is defined as a global network infrastructure that is used to connect medical equipment, factory machines, and domestic appliances at diverse locations around the globe with self-configuring features [12]. The interconnected nature of IoT provides the room for the Internet resources to get attacked from any location in the world and this makes security and privacy key the issues at IoT architecture [13].

The IoT architecture consists of three important layers Perception layer, Network layer and Application layer as shown in Fig. 1. The functionality of the perception layer is to collect, process and distinguish the object information in the physical world. It comprises of sensors, radio frequency Identification (RFID) tags, cameras, laser devices. This layer is also responsible for converting the collected data in to digital signals for network transmission [13,14]. Nano technologies and embedded intelligence play a key role at the perception layer.

The middle layer is the network layer which is responsible for processing the data received from perception layer. This layer aims to transfer data over different types of media such as FTTx, 3G/4G, Wifi, bluetooth, Zigbee, UMB, infrared technology, etc. by wired/wireless technologies. The network layer is also responsible for reliable transmission of processed data to application layer. Cloud computing is used as a middleware in this layer to store and process the massive amount of data.

Application layer is meant to provide services to the users. It uses the processed data by the network layer. This layer provides the required tools to realize the IoT vision. This layer analyzes the received data and makes the control decisions and provides an interactive display by making use of cloud computing and middle ware business management.

Figure 1 shows the security problems associated with different layers and across the layers [10]. Perception layer's physical nodes do not have enough power and storage to implement complex security techniques, so they are vulnerable to variety of attacks. The possible threats at this layer are sensor attacks (key nodes like gateway nodes can be easily controlled by the hackers), fake node (the attackers introduce a fake node in the system and inject malicious data which will destroy the whole network), radio interference (attacker inject the fake routing information which will create routing loops and increase the end-to-end delay), Side Channel Attack (the attacker attacks the encrypted device) and Denial of Service (DoS) threats [15]. The high level cryptographic algorithms and protocols are implemented at this layer to achieve physical security and secure routing.

Network layer is more vulnerable to hackers [16] as it has different access methods like sensor, wired and wireless access. Different access methods lead

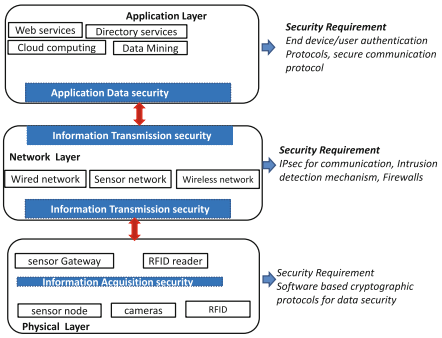

Fig. 1. IoT architecture with security requirements.

to heterogeneous environment with different switching technology and different location management strategies. In wireless networks, nodes can be moved freely and they may join/leave the network at any time which makes them vulnerable to attacks. Wired and wireless networks face traditional network security threats like denial-of-service attack (DoS), man-in-the- middle attacks, network congestion, authentication, etc. In addition to that the number of nodes deployed at IoT is very huge, which make the attackers easily hack the network and block the network. Further, huge amount of data transmission across huge number of nodes lead to network congestion and data loss. Traditional static network security approaches like Intrusion Detection and Prevention Systems (IDPS), Firewall are deployed at internet edge devices, to protect the network from external attacks are not providing effective security to IoT's borderless system architecture. The other end-host based defenses like antivirus, and software patches from vendors like 'Patch Tuesday' are not well equipped to handle IoT security.

Application Layer is vulnerable to privacy data leakage because of integration of various applications. Since different applications have different users, illegal user intervention needs to be prevented. Further, the user private data leakage should be prevented by identity authentication, which will prevent the unauthorized access to the user private data [17].

Table 1. IoT layers and security issues

IoT layer	Components	Security issues
Perception Layer	RFID,Sensors,Cameras,Smart Devices	Sensor attack, fake node, radio interference,DoS
Network Layer	Sensor, Wired, Wireless	DoS, man-in-the- middle attacks, congestion, authentication
Application Layer	Web services, Directory Services	Illegal user intervention, Private Data Leakage

Table 1 summarizes the IoT layers and their associated security issues. It is important to point out that the current security means and measures for each

separate layer in the IoT are independent of each other so that it is not sufficient to provide security assurance for the whole IoT application.

3 Software-Defined IoT

In this section, we discuss the SDN architecture and how SDN technologies are beneficial to IoT security.

3.1 Software-Defined Networking for IoT Security

The IoT architecture consists of variety of devices including network routers, switches, health monitoring wearable devices that are needed to be managed and secured. The explosive growth of IoT devices imposes two major issues. They are huge data traffic and network security threats. The common encryption techniques may not be sufficient to secure some of these devices as they don't have sufficient memory. For on-line commerce applications, these devices must be secured without any interruption.

The SDN technique [18] which decouples the control plane from data plane possess the following essential properties authentication, availability, confidentiality and integrity to secure the communication network. SDN allows the automation and centralized management of network resources. Figure 2 shows the SDN architecture. A central software program, called SDN controller (POX [20], NOX [19], Ryu [21]), which is in the control plane, manages the overall network behavior. The centralized SDN controller has the global network view and communicates with OpenFlow enabled switches using the OpenFlow protocol. Every OpenFlow switch maintains a flow table with entries for the flows. An entry in the table specifies a few packet fields and associated action to be carried out in the event of a matching with the incoming packet. In the event when a switch is unable to find a match in the flow table, the packet is forwarded to the controller to make the routing decisions. After deciding how to route the new flow, the controller installs a new flow entry at the required switches, so that the desired actions can be performed on the new flow.

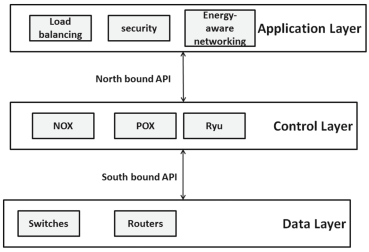

Fig. 2. Software defined networking architecture.

The northbound APIs in SDN architecture are the interfaces between the software modules of the controller and the SDN applications running on the top of the network platform. These northbound APIs supports applications like enabling firewall, intrusion protection and dynamic provisioning of Quality of service(QoS) to end users.

The southbound APIs provide the communication between the controller and the deployed devices(switches, routers) in the data plane. The OpenFlow protocol most used south bound protocol which is used to send the messages between controller and data plane.

3.2 Network Management

It is evident that [1] millions of devices will be connected worldwide through IoT technology. The huge data will be generated from these devices. An efficient IoT network management is required to manage enormous number of these IoT devices and also the huge data generated by them. The network management should be able to distribute and control the traffic flows in the network in such a way to minimize the network delay and achieve load balancing. Since, SDN technology supports fine-grained flow classification and flexible routing management, IoT requirements can be fulfilled by it. The programmability of the SDN along with the complete network view makes SDN to provide the feasible, cost effective security solution for IoT [22].

3.3 Security and Privacy

Traditionally network security is implemented by deploying middle boxes at different locations in the network. Different mailboxes are served for different purposes. It is hard to customize the middle box's security polices as they are vendor specific and it is hard to have one middle box to serve different network security polices. Deploying different middle boxes for different security purposes increase the overall cost. The SDN programmability feature enable a cost effective software network security solution by providing an efficient security functions in the control plane [22].

4 Securing IoT with SDN Architecture

There has been several research work towards defining the SDN based IoT reference architecture models for present and future IoT deployments. In this section, we briefly summarize the recent SDN based IoT security studies under the following categories.

- SDN based IoT architectures.
- SDN virtualization based IoT architectures.
- SDN based DDos mitigation in IoT.

Figure 3 presents an overview of SDN-based IoT networks aspects, which are considered in the existing works.

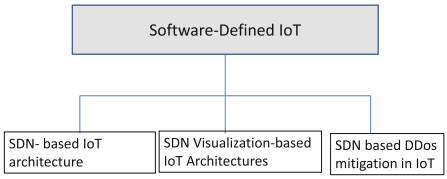

Fig. 3. Overview of SDN-based IoT solutions.

4.1 SDN Based IoT Architectures

Black SDN [23] is a secure SDN IoT network architecture designed for secure IoT communication. It secures both the meta-data and the payload by encrypting them. It uses the SDN centralized controller as a trusted third party for secure routing and optimized system performance management. It mitigate a range of attacks,including traffic analysis/inference attacks.

An enhanced SDIoT is a secure SDN-based IoT framework (SDIoT) [24] is shown in Fig. 4, in which the SDN control plane is designed to provide security services such as authentication/access control, IDS/IPS, and lightweight encryption.

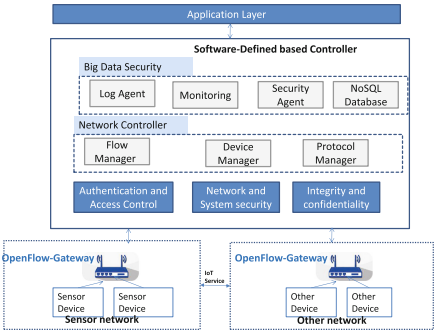

Fig. 4. Enhanced SDIoT architecture.

The control Layer in the framework has three major components to enhance the security:

- Authentication and Access Control: When a new device attempts to access the network, the authentication and access control module authenticates the device for the required service to be provided. The security password authentication (SPA) technique is used to determine whether or not to authenticate a device and allow it to network access.When the new sensor device is registered, a secret SPA information in advance goes through a safe communication channel. Each device transmits the SPA information to the gateway before

it is connected to the network. The controller checks this information and establishes a mutual transport layer security (TLS) connection. If the SPA information is not transmitted, the TLS connection is not executed even if it is requested by the device.

- Network Security: An Intrusion detection System (IDS), Intrusion Prevention system (IPS), and a firewall, which are used for network security, are provided in the network environment as software in the controller, not as network devices.
- Data Integrity: When providing an IoT service, during the process of collecting and storing data, data leakage/falsification may occur. There is a need for ensuring the integrity and confidentiality of data. Lightweight encryption and a hashing algorithm are used in an IoT environment.

To deploy this proposed framework on the IoT echo system, additional studies are required on the detailed system configuration and means of efficiently operating the system.

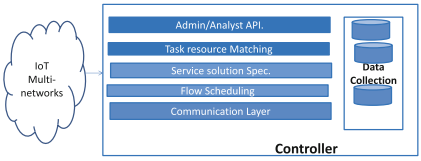

Fig. 5. Layered SDN IoT controller.

Figure 5 shows the layered IoT controller Architecture [25]. It is based on a software-defined networking concept. It is designed to dynamically achieve differentiated quality levels to different IoT tasks in a heterogeneous wireless network. The developed SDN IoT Controller translates the specific service requirements into network requirements like minimum data rate, or a maximum tolerable delay or packet loss for each separate flow. Network calculus and genetic algorithms [25] are used to model the multi-network environment and to schedule flows, respectively in order to optimize end-to-end flow performance.

The SDN based architecture for Horizontal IoT [26] is shown in Fig. 6. It is proposed based on the expectation that Internet of Things (IoT) architecture is going to evolve into a horizontal model containing various open systems, integrated environments, and platforms. The architecture is proposed with an aim to support multiple services with different scenarios and in different domains. Though the existing application specific vertical IoT architecture is beneficial in terms of operation and maintenance of IoT applications in one domain, it has the limitation in terms of interpretability and reusability. In order to overcome this, the Horizontal IoT architecture is designed to support data provision and interpretability at different levels by making devices, gateways and data open to service operators and application developers. This architecture does not provide any extra security mechanism which is important to protect the SDN

controller, establish trust among entities, and creates a robust policy mechanism. The authors intend to implement more functions and algorithms for calculating routing paths by considering the caching in the gateways and some security strategies on SDN controllers and gateways, in future.

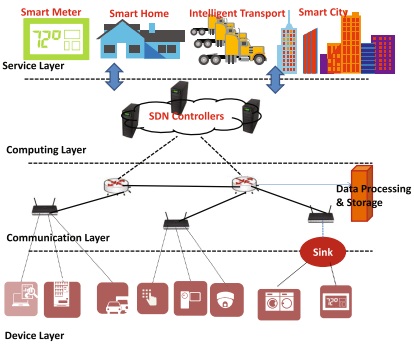

Fig. 6. Horizontal IoT architecture based on SDN.

In [27], SDN-based IoT gateway is designed to detect and mitigate anomalous behaviour. The SDN gateway is used to monitor the traffic originating from and directed to IoT based devices. The adaptive mechanism designed at the gateway will perform dynamic analysis on these traffic patterns to determine when devices are acting in a malicious manner, or are being the target of external exploitation. Once anomalous behaviour is detected, then it performs three possible mitigate actions (blocking, forwarding, or applying Quality of Service) to deal with it.

In [28], Flauzac et al. pointed out that the traditional Ad-Hoc network is lack of traffic monitoring and access control, due to the absence of the network infrastructure. The SDN-based IoT architecture proposed by them is designed to establish and secure both wired and wireless network infrastructure and also includes Ad-Hoc networks and network object things such as: sensors, tablets, and smart phones. Security controllers are used to monitor traffic and execute security polices in the Ad-Hoc network.

Sandor et al. [29] try to improve the communication performance and resilience of IoT systems. They adopt hybrid network infrastructures composed of SDN and redundant non-SDN segments. They designed a mechanism at the SDN controller that automatically performs dynamic switching between the redundant non-SDN communication edges.

4.2 SDN Virtualization-Based IoT Architectures

The SDN based secured framework for IoT(SDIoT) [31] is shown in Fig. 7.

This framework provides the SDN based IoT security by utilizing network function virtualization (NFV). The proposed framework has three main components.

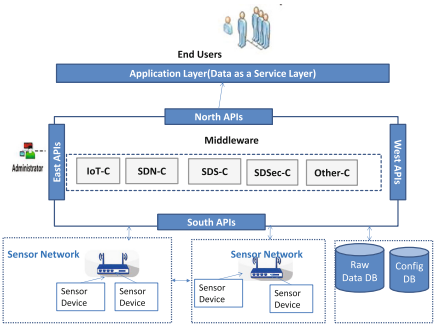

Fig. 7. SDIoT architecture.

- Physical Layer: All the physical devices in the system are residing in this layer. They can be classified in to sensor cluster, data base cluster, switch/router cluster and security appliance cluster.
- Middle ware layer: This is the core of the framework. Software defined controllers like IoT controller, SDN controller, SDStore controller, and SDSec controller are located and integrated inside this middleware layer. SDSec module provides the security of SDN based IoT network by utilising NFV.
- Application layer: This acts as a communication interface between controller and applications using north bound APIs.

Though the work discussed about a high-level architecture of an IoT controller to handle heterogeneous IoT flows, the concrete design of the inner workings of the controller and an experimental evaluation of the proposed high-level architecture are not done.

SDN-based IoT framework with NFV implementation [32] is shown in Fig. 8. This is a classic architecture. This IoT architecture has three layers:

- Sensing layer consists of IoT devices.
- Network layer consists of network switches.
- Service layer providing data analytic and application processing services.

This IoT framework is combined with the well-known SDN architecture to produce a general SDN-IoT framework. This work emphasizes the importance of designing an efficient distributed operating system (OS) using visualization techniques in the control plane for the SDN-based IoT architecture. With such distributed OS for the SDN-based IoT framework, it is possible to provide a centralized control and visibility of different IoT services for different IoT users. The distributed OS for the SDN-based IoT is under development in [34].

4.3 Existing SDN Based DDos Mitigation in IoT

A Denial of Service (DoS) attack is an attack to make a network resources unavailable by overwhelming it with traffic from multiple sources. In [30], the

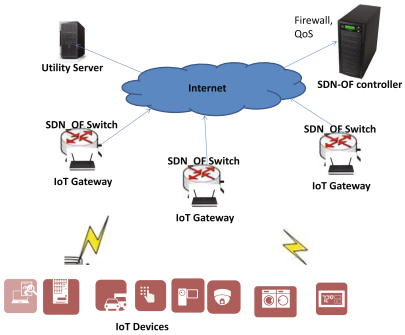

Fig. 8. Network architecture using SDN and NFV technologies.

SDNs features such as software-based traffic analysis, logical centralized control, dynamic flow insertion and deletion at remote switches, and global view of the network, can be leveraged to detect the malicious flows contributing to the DDoS flooding attack and effectively mitigated.

Cheng et al. [33] focus on the security issues of OpenFlow channel. They investigated the threat of Man-in-the-Middle attacks on the openflow channel and proposed a countermeasure to detect MitM attacks by leveraging Bloom filter. The protocol developed by them is lightweight and monitor the system based on SDN for such attacks. It does not require additional hardware or maintenance.

A summary of different SDN based IoT architectural frameworks presented in this survey is given in Table 2.

5 Discussion on Open Issues

In the previous section, we presented the literature on the integration of SDN and IoT. All these frameworks are designed considering the programmability benefits of SDN. An important thing observed in this study is that most of the frame works are not experimentally validated except SDIoT.

The SDN technologies are mainly designed to be used at Data Center networks (DCN) today is in DCNs [35,36], where the focus is on the collection of specific network statistics (e.g., bandwidth consumption) from network switches and efficient routing among them within the datacenter. A typical IoT Multinetworks setting is contrast to DCN, where diverse devices are located at different locations and are connected by a heterogenous network. The heterogenous nature of IoT system requires unique object addressing which is not discussed so far in the SDN based IoT frameworks [37].

An IoT traffic pattern is completely different from Data Center traffic pattern. To merge the SDN with IoT, a detailed analysis about traffic pattern and buffering mechanisms need to be addressed.

SDN based IoT controller design is still at the infant stage. There is a need for lots of effort to change the SDN controller's south bound APIs to communicate

Table 2. Summary of SDN based IoT architectural frameworks

Framework	Technology	Summary
BlackSDN [23]	SDN	It secures both the meta-data and payload by encrypting them. It uses the SDN centralized controller as a trusted third party for secure routing and optimized system performance management
Layered IoT controller [25]	SDN-IoT Controller	It is designed to dynamically achieve differentiated quality levels to different IoT tasks in a heterogeneous wireless network
Horizontal IoT [26]	SDN	It is proposed based on the expectation that Internet of Things architecture is going to evolve into a horizontal model containing various open systems, integrated environments, and platforms
SDN based IoT gateway [27]	SDN	It is designed to detect and mitigate anomalous behaviour. Once anomalous behaviour is detected, it performs three possible mitigation actions (blocking, forwarding, applying Quality of Service)
SDN based IoT Security [28]	SDN	The SDN based IoT architecture is designed to establish and secure both wired and wireless network infrastructure. Security controllers are used to monitor traffic and execute security polices in the Ad-Hoc network
Resilient IoT system [29]	SDN	SDN controller automatically performs dynamic switching between the redundant non-SDN communication edges to ensure resilience
SDIoT [31]	SDN/NFV	SDN controller is designed for heterogenous traffic flows.
SDN-based IoT Framework with NVF Implementation [32]	SDN/NFV	This IoT framework is combined with the SDN architecture to produce a general SDN-IoT framework This work emphasizes the importance of designing an efficient distributed operating system using virtualization techniques in the control plane for the SDN-based IoT architecture
SDN based DDos mitigation in IoT [30]	SDN	It leverages SDN features such as software-based traffic analysis, logical centralized control, dynamic flow insertion and deletion at remote switches, and global view of the network, to detect the malicious flows contributing to the DDoS flooding attack and effectively mitigate it
Man-in-the-Middle attack mitigation in IoT [33]	SDN	It proposes Counter measure to detect MiM attacks on OpenFlow channel by leveraging Bloom filter

with IoT devices. Single point of SDN-based IoT controller is prone to security attacks and failures which need to be addressed.

Another open issue that need to be addressed while integrating the SDN with IoT is, the size of the flow table in the SDN enabled switches. As IoT has huge volume of end devices and their rapid entering and leaving the network, may require large flow tables at SDN enabled switches. Optimization of buffering at SDN enabled switches is an important problem that need to be addressed [37].

6 Conclusions

IoT is a smart system used to interconnect mechanical, digital devices and humans to improve the quality of life. However, IoT lacks programmability, agility, security and data management due to large number of heterogeneous devices and the amount of data produced. SDN which decouples control plane from data plane is a potential candidate for providing centralized management for IoT with security enhancements. In this paper, we discussed IoT architecture, IoT security requirements, SDN architecture and the benefits of integrating SDN with IoT for enhanced security. We also discussed their limitations and the open issues that remain to be addressed.

References

1. Gartner Says 4.9 Billion Connected "Things" Will Be in Use (2015). http://www.gartner.com/newsroom/id/2905717
2. Bremner, D.: Analysing the IoT ecosystem: the barriers to commercial traction. In: Embedded World Exhibition & Conference 2016, Nuremberg, Germany, pp. 23–24 (2016)
3. Tarkoma, S.: The Internet of Things Program: the finnish perspective (2013)
4. Hewlett-Packard, Internet of things research study 2015 report. http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf
5. Roman, R., Najera, P., Lopez, J.: Securing the Internet of Things. Comput. Soc. **44**, 58 (2011). https://www.nics.uma.es/sites/default/files/papers/1633.pdf
6. Escribano, B.: Privacy and security in the Internet of Things: challenge or opportunity. http://www.olswang.com/media/48315339/privacy_and_security_in_the_iot.pdf
7. Wu, C.: A preliminary investigation on the security architecture of the Internet of Things. Bull. Chin. Acad. Sci. **25**(4), 411–419 (2010)
8. Yu, T., Sekar, V., Seshan, S., Agarwal, Y., Xu, C.: Handling a trillion (unfixable) flaws on a billion devices: rethinking network security for the Internet-of-Things. In: Proceedings of the 14th ACM Workshop on Hot Topics in Networks, HotNets-XIV (2013)
9. Openflow.org. Pantou. Pantou: OpenFlow 1.0 for OpenWRT. http://www.openflow.org/wk/index.php/
10. Stout, W.M.S., Urias, V.E.: Challenges to securing the Internet of Things. In: Proceedings of IEEE International Carnahan Conference on Security Technology (ICCST) (2016)

11. Kloti, R., Kotronis, V., Smith, P.: OpenFlow: a security analysis. In: Proceedings of the 8th Workshop on Secure Network Protocols (NPSec 2013) (2013)
12. Conner, M.: Sensors empower the "Internet of Things", pp. 32–38 (2010). ISSN 0012-7515
13. Xiaohui, X.: Study on security problems and key technologies of the Internet of Things. In: International Conference on Computational and Information Sciences (2013)
14. Yan, L., Zhang, Y., Yang, L.T.: The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems. Auerbach Publications, Boston (2008)
15. Jose, C.: Internet of Things (IoT) - security challenges and possible security approaches (2016)
16. Amine, A., Mohamed, O.A., Benatellah, B.: Network Security Technologies: Design and Applications. IGI Global, Hershey (2014)
17. Weber, M., Boban, M.: Security challenges of the Internet of Things. In: Proceedings of MIPRO (2016)
18. McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., Turner, J.: OpenFlow: enabling innovation in campus networks. SIGCOMM Comput. Commun. Rev. **38**, 69–74 (2008)
19. Tavakoli, A., Casado, M., Koponen, T., Shenker, S.: Applying NOX to data center. In: Proceedings of 8th ACM Workshop on Hot Topics in Networks (2009)
20. The Pox Controller. https://github.com/noxrepo/pox
21. The Ryu Controller. https://osrg.github.io/ryu/
22. Shin, S., Xu, L., Hong, S., Gu, G.: Enhancing network security through software defined networking (SDN). In: ICCCN (2016)
23. Chakrabarty, S., Engels, D.W., Thathapudi, S.: Black SDN for the Internet of Things. In: Proceedings of the IEEE 12th International Conference on Mobile Ad Hoc Sensor System (MASS), Dallas, TX, USA, October 2015, pp. 190–198 (2015)
24. Choi, S., Kwak, J.: Enhanced SDIoT security framework models. Int. J. Distrib. Sens. Netw. **2016**, 1–12 (2016)
25. Qin, Z., Denker, G., Giannelli, C., Bellavista, P., Venkatasubramanian, N.: A software defined networking architecture for the Internet-of-Things. In: Proceedings of the IEEE Network Operations and Management Symposium (NOMS) (2014)
26. Li, Y., Su, X., Riekki, J., Kanter, T., Rahmani, R.: A SDN-based architecture for horizontal Internet of Things services. In: Proceedings of IEEE International Conference on Communications (ICC) (2016)
27. Bull, P., Austin, R., Popov, E., Sharma, M., Watson, R.: Flow based security for IoT devices using an SDN gateway. In: Proceedings of the IEEE 4th International Conference on Future Internet Things Cloud (FiCloud), Vienna, Austria, August 2016, pp. 157–163 (2016)
28. Flauzac, O., González, C., Hachani, A., Nolot, F.: SDN based architecture for IoT and improvement of the security. In: Proceedings of the IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Gwangiu, South Korea, March 2015, pp. 688–693 (2015)
29. Sándor, H., Genge, B., Sebestyén-Pál, G.: Resilience in the Internet of Things: the software defined networking approach. In: Proceedings of the IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, September 2015, pp. 545–552 (2015)
30. Ahmed, M.E., Kim, H.: DDoS attack mitigation in Internet of Things using software defined networking. In: 2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService) (2017)

31. Jararweh, Y., Mahmoud, A., Darabseh, A., Benkhelifa, E., Vouk, M., Rindos, A.: SDIoT: a software defined based Internet of things framework. J. Ambient Intell. Humaniz. Comput. **6**(4), 453–461 (2015)
32. Li, J., Altman, E., Touati, C.: A general SDN-based IoT framework with NVF implementation. ZTE Commun. **13**, 42–45 (2015). ZTE Corporation
33. Li, C., Qin, Z., Novak, E., Li, Q.: Securing SDN infrastructure of IoT-fog networks from MitM attacks. IEEE Internet Things J. **4**, 1156–1164 (2017)
34. Open Network Operating System Project. http://onosproject.org/
35. Curtis, A.R., Mogul, J.C., Tourrilhes, J., Yalagandula, P., Sharma, P., Banerjee, S.: Devoflow: scaling flow management for high-performance networks. In: Proceedings of the ACM SIGCOMM 2011 Conference (2011)
36. Al-Fares, M., Radhakrishnan, S., Raghavan, B., Huang, N., Vahdat, A.: Hedera: dynamic flow scheduling for data center networks. In: Proceedings of the 7th USENIX Conference on Networked Systems Design and Implementation, NSDI 2010 (2010)
37. Bizanis, N., Kuipers, F.A.: SDN and virtualization solutions for the Internet of Things: a survey. IEEE Access **4**, 5591–5606 (2016)