IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received December 10, 2020, accepted December 18, 2020, date of publication December 30, 2020, date of current version January 22, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3047996

Secure Software-Defined Networking Communication Systems for Smart Cities: Current Status, Challenges, and Trends

MOHAMED RAHOUTI[1], KAIQI XIONG[2], (Senior Member, IEEE), AND YUFENG XIN[3], (Member, IEEE)

[1]Department of Computer and Information Science, Fordham University, Bronx, NY 10458, USA
[2]ICNS Lab and Cyber Florida, University of South Florida, Tampa, FL 33620, USA
[3]RENCI, University of North Carolina, Chapel Hill, NC 27513, USA

Corresponding author: Kaiqi Xiong (xiongk@usf.edu)

This work was supported in part by the National Science Foundation (NSF) under Grant 1633978, Grant 1620871, Grant 1620862, and Grant 1636622; in part by the NSF/CNS Grant through the BBN/GPO Project under Grant 1936; and in part by the Florida Center for Cybersecurity (Cyber Florida).

ABSTRACT Smart city is a transformative and progressive vision that aims to revolutionize infrastructure systems and public services in an urban area with modern information technologies. Its ultimate goal is to greatly improve the livability Quality of Service (QoS) of its citizens and to optimize the utilization of its assets and natural resources sustainably. One of the key technical attributes in smart cities is to deploy a large number of sensors to collect data to enable real-time and intelligent decisions for various city functions and citizen needs. Many of the data have strict security requirements as they are either private to citizens or sensitive to critical infrastructures. As a result, how to securely and efficiently deliver and process the dramatically increasing volume of data becomes one of the grand challenges in materializing the smart city vision. In recent years, Software-Defined Networking (SDN) has emerged as a leading communication infrastructure candidate for smart cities. While many efforts have existed to research, prototype, and even deploy SDN on a small scale for some smart city applications, there is still a lack of cohesive understanding about SDN's impact on the secure communication need of smart cities. In this paper, we conduct a comprehensive survey of the core functionality of SDN from the perspective of secure communication infrastructure at different scales. A specific focus is put on the security threats and challenges in accordance with SDN plane-based architectures for various smart city-enabled applications. We further systematically categorize the state-of-art solutions and proposals to apply SDN to support typical smart city applications, such as transportation, health, and energy applications. Lastly, we cast a holistic view of future research trends.

INDEX TERMS Communication system, OpenFlow, security, smart city, software defined networks.

I. INTRODUCTION

The smart city initiative intends to provide innovative solutions that are primarily relying on information and communications technology (ICT) to enhance the urban area's daily life and improve local sustainability in terms of people, governance, economy, mobility, environment, and living [1]. Through the broad deployment of smart sensors and actuators, a smart city exploits physical and cyber spaces and involves various distributed systems and services implicated in complex linkages to other systems towards delivering new data-oriented intelligent functionalities [2]. A smart city may consist of many application components such as smart education, smart health, smart transportation, and so on, as shown in Figure 1. These components are classified in several main dimensions, including, but not limited to, a technological dimension, human dimension, and institutional dimension [1].

Smart city services rely on ubiquitous information connectivity and processing platforms to users with services and the

The associate editor coordinating the review of this manuscript and approving it for publication was Rentao Gu.

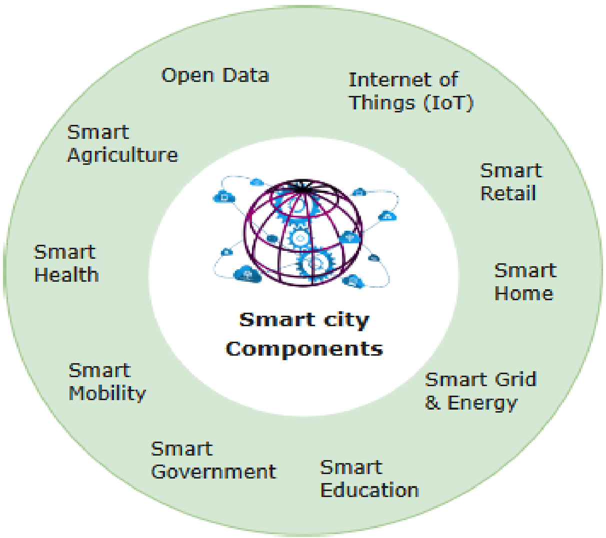

FIGURE 1. Main components of smart city applications.

things around them [3]. An advanced networking service platform is herein a prerequisite to render such services smarter to shape the smart city vision.

Security is a key requirement in networking environments. It ensures the capability to maintain and deliver an agreeable level of information and service protection in the face of attacks and failures. The issues for networking-enabled services typically include misconfiguration over scaled natural disasters, misimplementation of security policies, and targeted attacks.

The legacy local-area network (LAN) or Internet-based decentralized communication infrastructures are deemed to be not prospective in a smart city under the effect of data-burst, specifically, with rigorous security and real-time Quality of Service (QoS) requirements. The challenges only became more aggravated by the need to extend networking services into cloud computing, Internet of Things (IoT) system, and big data infrastructures in typical smart city settings.

To a great extent, recent community consensus is that Software-Defined Networking (SDN) is a remarkable paradigm choice in building the smart city communication infrastructure to meet the performance and security requirements of smart city services and applications [4].

A. NEED OF SDN IN SMART CITY COMMUNICATION INFRASTRUCTURES

Smart cities strive to enable a broad range of smart devices, applications, and systems to be embedded in an ambient environment. Smart devices range from sensors integrated into wearable equipment (e.g., watches and clothes), actuation and automation-enabled devices, to control systems in smart homes and buildings, sensors integrated into vehicles and on-board units for car maintenance and accident avoidance, and so on. These smart devices, control systems, automation technologies, and network elements, such as forwarding devices and routing devices, are merged together into the common communication platform that enables smart cities [5].

SDN was actually one of the leading foundational technologies being leveraged to shape the smart city vision. For example, Abhishek *et al.* [6] that presented a service priority adaptive approach to handling emergency traffic in smart cities and He *et al.* [4] proposed an SDN-based solution to improve the mobile edge computing and caching for a smart city using a big data deep reinforcement learning approach. In addition to its advantage in the most basic network functions such as the routing and end-to-end performance optimization [7], what makes SDN appealing to the smart city vision also lies in its three unique characteristics: (1) a logically centralized control plane to enable efficient global view and control, (2) programmability to enable in-situ configuration (3) virtualization that provides isolation and resource sharing between applications running in the same physical infrastructure.

However, the development of networking and security solutions leveraging SDN capabilities could present a platform for new attack vectors [8] for adverse users, and therefore network threats and exploitation. For example, Denial of Service (DoS) [9], Link Discovery Service (LDS) exploitation [8], [10], and Man-in-the-Middle (MITM) [8] have been proved serious attacks. SDN has been proven to provide flexible, simple, and programmable networking environments. Indeed, the programmability characteristic of the SDN infrastructure layer grants a dynamic and cost-effective configuration for networks in support of smart cities. For instance, SDN can be deployed to control and regulate IoT in smart city networked systems, by expanding connectivity to smart homes using capacity sharing [11], to assure security in smart city routing devices [5] and mobility control in clouds [12], [13].

Although researchers have been proactive in researching the latest SDN technologies to guarantee secure SDN-based communication systems, there still exist many technical challenges that need to be addressed:

1) In reality, SDN-enabled networks only account for some portions of the overall network infrastructure. In the foreseeable future, we believe that a wide-area network would be a hybrid environment consisting of some interconnected SDN domains around the cloud's sites or data centers.
2) The wide-area network will still consist of multiple domains, where multiple network segments would provision end-to-end security with possibly different QoS requirements.
3) In spite of many existing studies on SDN security, only a little work has been done to satisfy the need for reliable real-time communications in smart cities.

In legacy networks, security is regarded as *add-on* as it heavily depends on manual configuration-based solutions. Thus, in order to achieve high-level security applications, administrators need to configure each corresponding network entity according to vendor-particular low-level commands.

These manual security configurations (i.e., firewalls, IPSec, intrusion detection and prevention system (IDPS)) on a distributed set of network entities are vulnerable to inter-domain policy conflict and configuration and implementation errors, which may lead to earnest security ivulnerabilities and breaches [14].

Contrariwise, SDN improves security in a networking-enabled environment due to its centralized control of the network system and holistic visibility of the network behavior and run-time manipulation of inserting/pushing forwarding rules [15]. Therefore, the SDN non-distributed management of network allows for a more efficient enforcement of security policies and reduction of their conflicts. Additionally, security implementations such as security monitoring applications could efficiently inquire flow samples from data-paths via an SDN controller [16]. Once security analysis is finished, the monitoring application may guide the data path components to take action by either denying incoming traffic, redirecting the traffic to security-based middle boxes, or even restricting the traffic within a particular network authority. Moreover, SDN grants an efficient update of security applications and policy implementations. It allows for appending security modules at the controller platform instead of changing the hardware or even updating its firmware [16].

As the SDN controller detaches and centralizes the control plane of a network, it allows for the enforcement and automation of security policies due to the programmability features of the SDN controller. Therefore, SDN can deal with network threats and malicious traffic at runtime by leveraging applications of network security. To better represent an SDN architecture, Figure 2 depicts the main planes/layers of SDN and their functionalities. The three planes are shaped as follows:

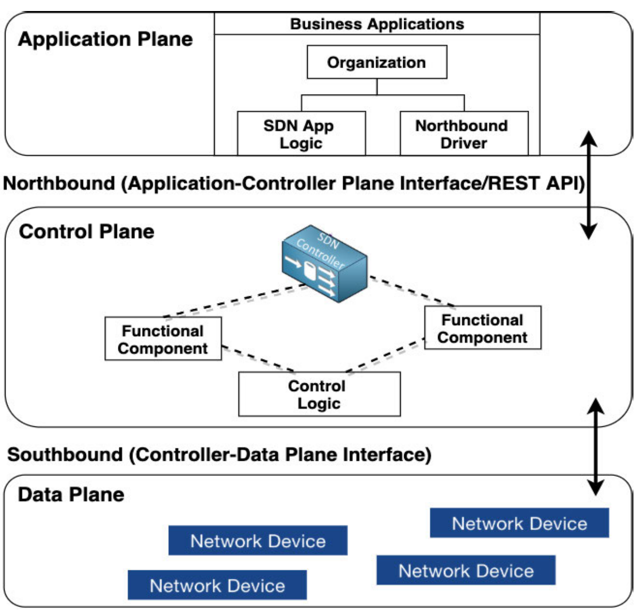

FIGURE 2. A high-level overview of SDN architecture layers.

TABLE 1. A list of acronyms used in this article and corresponding definitions.

Acronym	Description
ACL	Access control list
API	Application Programming Interface
BDDP	Broadcast Domain Discovery Protocol
CA	Certificate Authority
CoT	Cloud of Things
CPS	Cyber-Physical System
DCPP	Dynamic Controller Provisioning Problem
DDoS	Distributed Denial of Service
DoS	Denial of Service
DPI	Deep Packet Inspector
DSRC	dedicated short-range communication
DTLS	Datagram Transport Layer Security
E2E	End-to-End
GUI	Graphical User Interface
IBC	Identity Based Cryptography
ICS	Industrial control systems
ICT	Information and Communication Technologies
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IoT	Internet of Things
IoV	Internet of Vehicle
LAN	Local Area Network
LTE	Long term evolution
LDS	Link Discovery Service
MAN	Metropolitan Area Network
MANET	Mobile ad hoc network
MITM	Man-in-the-middle attack
MUD	Manufacturer Usage Description
MU-MIMO	Multi-user-multiple-input and multiple-output
NFs	Network functions
NFV	Network Function Virtualization
NOS	Network Operating System
ONF	Open Networking Foundation
OVS	Open vSwitch
P2P	Peer-to-peer
PaaS	Platform as a service
PUF	Physical unclonable function
QoS	Quality of Service
RAP	Rogue access point
RMU	Remote terminal unit
SDN	Software-Defined Networking
SDU	Software-Defined Utilities
SDVN	Software-defined vehicular network
SFC	Service Function Chain
SG	Smart Grid
STS	Spanning Tree Service
TCP	Transmission Control Protocol
TE	Traffic Engineering
TLS	Transport Layer Security
UE	User equipment
V2G	Vehicle-to-Grid
VANET	Vehicular ad-hoc network
VNF	Virtual Network Function
VoIP	Voice over IP
VoLTE	Voice over long term evolution
WLAN	Wireless Local Area Network
WoT	Web of Things

- Control Plane: It is a centralized control structure that embraces a network operating system (NOS). This layer provides hardware-based abstractions to SDN applications as well as a holistic view of the entire SDN-enabled network [15], [17].

TABLE 2. Comparison of existing survey papers about SDN integration in smart city communication systems. ✓, ✗, and ✱ indicate that the topic is well covered, uncovered, and partially covered, respectively.

Ref.	Year	Topic/Application of Smart City	SDN	Scalability	Security & Privacy	Research Directions
Gharaibeh et al. [18]	2017	Networks	✓	✱	✓	✓
Rehmani et al. [19]	2019	Smart grid	✓	✓	✓	✓
Dong et al. [20]	2015	Smart grid	✓	✱	✱	✱
Molina et al. [21]	2018	CPS	✓	✓	✱	✓
Ahmed et al. [22]	2016	IoT	✱	✱	✱	✱
Du et al. [23]	2019	Resource/communication management	✗	✱	✗	✓
Jawhar et al. [24]	2018	Networks	✱	✓	✱	✓
Petrolo et al. [25]	2015	CoT	✗	✓	✱	✓
Ijaz et al. [26]	2016	Smart city Infrastructure	✗	✱	✓	✓
Glass et al. [27]	2019	Smart grid communication	✓	✱	✗	✱
Yi et al. [28]	2015	Fog computing	✓	✱	✗	✱
Li et al. [29]	2018	5G and IoT	✱	✓	✱	✓
Bizanis and Kuipers [30]	2016	NFV and IoT	✓	✓	✗	✓
Oubbati et al. [31]	2020	UAV networks	✱	✓	✓	✓
Vu et al. [32]	2019	CPS	✱	✓	✓	✱
Ho et al. [33]	2019	Next-generation wireless for Smart city	✱	✓	✓	✓
Yurekten and Demirci [34]	2020	SDN-enabled cyber defense review	✓	✱	✱	✓
Our survey	-	Smart city-enabled SDN	✓	✱	✓	✓

- Data Plane: It is also called the infrastructure or forwarding layer. It consists of integrated forwarding components and a set of rules to direct networking traffic according to the instructions from the control plane [15], [17].
- Application Plane: It consists of SDN-based applications of different operations and functionalities, including, but not limited to, network security and policy services, as well as implementations [15], [17].

Unlike a legacy network, the SDN rules for data handling are placed and executed as a software module instead of decentralizing them in various firmware or hardware. This capability provides a run-time installment of security solutions and policies. Security solutions can be implemented and configured in the application layer of an SDN controller that inquires about networking resources and state, as well as packet samples from the control layer through an interface called *north-bound*. Therefore, these security implementations would lead to networking flow towards the security systems of a higher level through the *south-bound* interface via the SDN control layer. As an SDN controller guarantees a global view of the entire network with its logically centralized control, this leads to compromising the entire networking system once the SDN itself is compromised because it allows the control layer to interact with network applications.

B. CONTRIBUTION OF THIS SURVEY AND COMPARISON WITH RELATED ARTICLES

Existing studies, such as [16], [35] and [36], include an analysis of security issues and their associated solutions and frameworks in SDN. Nevertheless, these studies are limited in scope and do not include recent research advances. In our paper, we present an up-to-date and comprehensive analysis of our surveyed topic. Table 2 demonstrates the novelty of our work and presents survey articles related to communication infrastructures in smart city and smart city-enabled services and applications with regard to SDN. The literature review presented in Table 2 varies from definitions of smart city communication infrastructure [18], [24] to SDN-enabled smart services and devices in smart city [19], [22], [28], [37], and [30]. However, while SDN and its security in the context of smart city are either uncovered or partially covered in these literature reviews, our survey focuses on SDN applicability to smart city and security threats due to integration in the communication infrastructure.

Specifically, the contributions of our survey work is delineated as follows:

- We define concepts, architecture, and communication infrastructure of smart city.
- We motivate the need for SDN integration in smart city communication infrastructures.
- We review current security challenges in each SDN layer.
- We review current solutions and proposals to improve security in SDN with respect to each layer.
- We present SDN-enabled applications and smart services in the context of smart city.
- We discuss security vulnerabilities related to the integration of SDN in smart city communication infrastructures and services.
- We provide a taxonomic summary of existing proposals and solutions to improve security of SDN-enabled communication systems in smart city.
- We discuss open research problems and future research directions to enhance both resiliency and applicability of SDN in smart city communication infrastructures.

Our article contributes to open research problems on the integration of SDN into smart city communication architecture and design. It can comprehensively serve as a resource for information security and privacy, network reliability, and smart services and computing technologies efficiency in smart environments.

C. ARTICLE STRUCTURE

A list of acronyms used in this survey article is presented in Table 1 and Figure 3 presents the roadmap of our article whose organization is as follows:

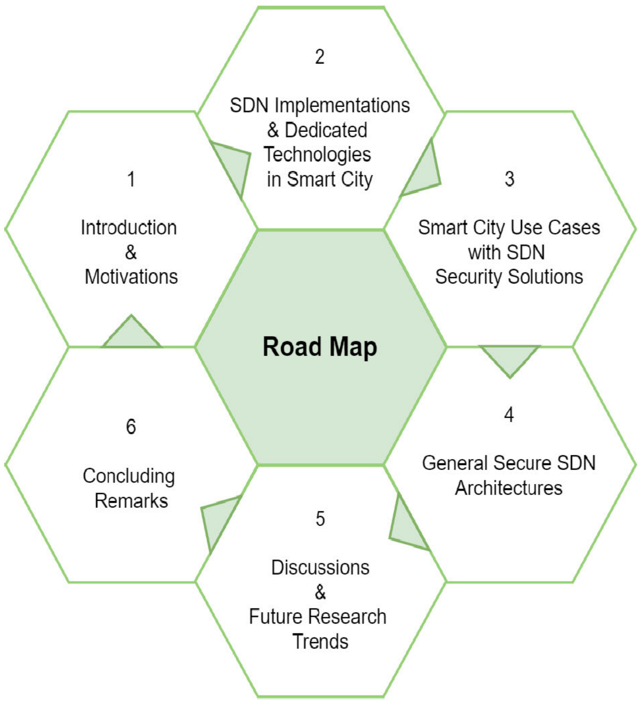

FIGURE 3. **Roadmap of the paper.**

Section II provides an overview and discussions about SDN components, implementations, and dedicated technologies in the smart city. Section III discusses research studies for smart city use cases along with SDN-based security solutions. The section also provides an up-to-date taxonomic classification of the presented research studies with regard to smart applications and services. While Section IV presents state-of-the-art secure SDN architectures for smart city communication networks, Section V gives research trends and future directions of this research. Lastly, Section VI presents concluding remarks and a summary of our article.

II. SDN IMPLEMENTATIONS & DEDICATED TECHNOLOGIES IN SMART CITY

SDN is an emerging paradigm of networking that intents to supersede the limitations of legacy networks. The worth of SDN lies in its capability to guarantee coherent policy enforcement, better scalability, and holistic visibility through centralized management and network programmability. The future generation of security solutions will benefit from the riches of network state and resource information available in SDN to enhance security policy enforcement, traffic abnormality revelation, and attenuation.

SDN separates the forwarding features from control and network management, which means that the network control traffic is detached from forwarding entities (e.g., OpenVswitch devices). Therefore, the SDN data layer is in charge of communicating with these individual forwarding entities that are eventually managed by the SDN controller. This plane-based abstraction allows for a programmability and efficient management of network services.

The vast majority of the proposed SDN security solutions, proposals, and frameworks consider OpenFlow [65] as a defacto protocol of SDN. Therefore, we present the SDN layers with regard to OpenFlow standardization. Figure 2 shows an SDN infrastructure and its layers decoupling. Based on the SDN planes decoupling aspect presented in Figure 2, the security applications and policies can be implemented and configured via the SDN application layer, whereas the network flows can be directed to another security applications (e.g., middle boxes) through the control layer.

According to OpenFlow protocol specifications, security systems need to be placed over the SDN control layer, and the SDN controller must grant a network view that is unified and clear in order to render security threats and violations easy to spot as well as security policies installment [66].

The existing SDN controllers can be classified into two sets, NFV-based infrastructure of a datacenter and historical-based for administering programmable networking switches. Table 3 presents a list of existing SDN controllers along with their relative features. The market for SDN is anticipated to reach more than 35 billion by the end of 2020. Thus, research scientist and networking industry (e.g., Deutsche Telekom, Facebook, Google, Microsoft, Verizon, and Yahoo!) launched the Open Networking Foundation (ONF) in 2011 in order to boost and advertise the SDN paradigm which then adopted SDN as an evolving paradigm in the technology of networking [16]. Therefore, based on these facts, both research scientists and networking industry could infer that the SDN architecture relishes future networking technology and infrastructure.

A. APPLICATION PLANE

As the SDN controller guarantees a global view of the network state and resources, the application frameworks profit from such a great controller visibility, allowing them to request and acquire the states of networking and resources in well-determined ways. The application layer is basically composed of end user business implementations (e.g., applications) that utilize SDN communications and services [67], such as network virtualization and security systems. Since decoupling applications from the underlying resources (i.e., physical or virtual) must fulfill OpenFlow protocol specifications, the network administrators aim to implement and administer networking policies by deploying a diverse configuration options and network control [68].

In order for the SDN controller to preserve a logically centralized map for the whole networking environment as specified by the OpenFlow protocol, it eliminates the complexity of network management, collects the network topology, state, and resources information using south-bound API. This collected network information is then forwarded to the networking applications via the SDN northbound API. Therefore, the OpenFlow protocol is regarded as an inbred option to

TABLE 3. Existing SDN controller software.

Controller	Language	Physically Distributed	OpenFlow	Multi-Threaded	TLS	Rest API	% Deploying	Other Features
Floodlight [38]	Java	✗	1.4	✓	✓	✓	11	GUI, forked from Beacon
ONOS [39]	Java	✓	1.3	✓	-	-	23	Built for service providers, supports OVSDB, BGP, Nteconf, and TLI
OpenDayLight [40]	Python/Java	✓	1.3	✓	✓	✓	61	GUI
NOX [41]	C++	✗	1.0	✗	-	-	-	Deprecated
Ryu [42]	Python	✗	1.5	✗	✓	-	15	Frequent switch certifications
SNAC [43]	C++	✗	1.0	✗	-	-	-	Built on NOX, GUI, closed source
HyperFlow [44]	C++	✓	1.0	✓	-	-	-	Built on NOX
OpenMUL [45]	Python	✓	1.4	✓	✓	✓	8	Supports Netconf and OVSDB, stable performance
Kandoo [46]	Go	✓	1.0	✓	-	-	-	-
OpenContrail [47]	Java/Python	✓	-	✓	✓	✓	14	Compatible with OpenStack. South-bound API: XMPP, BGP and Netconf
Trema [48]	C/Ruby	✗	1.3	-	-	-	-	-
Beacon [49]	Java	✗	1.0	✓	-	-	-	GUI, limited to STAR topology
POX [50]	Python	✗	1.0	✗	-	-	-	GUI, Development stagnated
Ryuretic [51]	Pyhton	✗	1.5	✗	✓	-	-	Built on Ryu
DIFANE [52]	C	✓	1.0	✓	-	-	-	Built on NOX
Pyretic [53]	Python	✗	1.0	✗	-	-	-	Deprecated built on POX
OPNFV [54]	Python/Java	-	1.3	✓	✓	✓	26	Compatible with NV/SDN, ODL, Open-Contrail, and ONOS
Disco [55]	Java	✓	1.3	✓	✗	✓	-	Built on top of Floodlight and AMQP protocol
HP VAN SDN [56]	Java	✓	1.5	✗	✓	✓	-	IPv6 traffic support
Onix [57]	Python/C	✓	-	✓	✓	-	-	Failure recovery support
Maestro [58]	Java	✗	-	✓	-	✗	-	Ad-hoc-based Northbound API
UniFI [59]	Python	✓	1.5	-	✓	✓	-	Compatible with NV/SDN, ODL, Open-Contrail, and ONOS
Ericsson Cloud [60]	Python/Java	✓	1.5	-	-	✓	✓	Intra & inter-datacenter connectivity based on OpenDaylight controller with routing capabilities
Lumina [61]	Python/Java	✓	-	✓	✓	✓	-	A common control plane over multiple domains based on OpenDaylight. Services are deployed using a single set of applications
NEC ProgrammableFlow [62]	-	✓	-	✓	✓	-	-	A packet processing pipeline capability for up to 10,000 switches networks
Faucet [63]	Python	✓	1.3	✓	✓	✓	-	Moves control functions to vendor independent server-based software
Open SDN [64]	Python/Java	✓	-	-	✓	✓	-	A commercial distribution of OpenDaylight offering automation of standards-based network infrastructure

build network applications in OpenFlow-based applications and functions.

B. CONTROL PLANE

This layer is also named a control layer. It is composed of various SDN controller software that grant unified and integrated control functionalities via open APIs to handle and manage the networking traffic behaviors throughout three open interfaces, north-bound, south-bound, and west-bound/east-bound interfaces [67]. The control layer is decoupled from network entities and built on top of a logically distinct and centralized layer.

Through the network operating system, the SDN controller manages the entire networking environment with a global and logically centralized control view of network state and resources. The control layer handles insertion/setup of flow rules according to OpenFlow protocol specifications of SDN controller-switches communication. Once an incoming packet arrives at the OpenFlow switch, it will first check its flow table and direct it according to the existing rule entry. If the switch does not find a matching entry in the flow table, it will then direct the packet to the SDN controller. Once the SDN controller receives the pushed packet, it will insert new rules (e.g. forward, drop, etc.) in the corresponding switching device's flow table. Hence, the processing of all networking traffic in datapath components in OpenFlow switching devices is based on the SDN controller's instructions.

C. DATA PLANE

This SDN plane is also named the data plane/layer. It is primarily decomposed of forwarding elements, including physical switches and virtual switches such as Open Vswitch (OVS). As an SDN controller detaches the control plane from the data plane, it renders the network forwarding entities such as OpenFlow switches unpretentious and straightforward with regard to remote control through open interfaces. There are several OpenFlow-enabled forwarding devices as presented in Table 4, and vary between open-source and commercialized platforms. However, OVS is an appropriate example of an SDN-enabled forwarding entity, which adheres

TABLE 4. Common OpenFlow switching devices and technologies.

Platform	Version	Details
Open vSwitch	2.15.x	Supports different datapaths on different platforms
DPDK	20.11.0	Provides a set of data plane libraries and network interface controller for TCP packet processing
VPP	-	Enables extension/addition of data path services with reliable performance
Tungsten Fabric	5.1	Automated secure multi-cloud network virtulization SDN for connecting virtual workloads
eBPF [69]	Kernel 5.9	Program the eXpress Data Path (XDP) via a kernel network layer that processes packets closer to the NIC
Pica8	-	OpenFlow compatible NOS runs on various white box switch hardware
Indigo	2	Used for hardware switching OpenFlow implementation on various physical switches

to OpenFlow specifications. An openFlow forwarding device maintains the flow entries for traffic forwarding rules and policies instructed/imposed by the SDN controller [65]. Since OpenFlow protocol grants a standard and open specifications mechanism for the OpenFlow switch to communicate with the SDN controller, OpenFlow switches are strictly required to maintain the following requirements;

- A trusted path to communicate networking packets and instructions with the SDN controller.
- A table called flow table that contains different actions' entries for flow processing.

D. A SECURE SDN-BASED COMMUNICATION MODEL FOR SMART CITY

In the past, ICT networking systems in smart city frameworks were attacked by adversaries. One of the recent vulnerable cyber infrastructure attacks occurred in United States in July 2015 where a centric electricity blackout took place in more than ten different states. The incident is a consequence of a cyber attack against the power grid in the United States [70]. Based on NIST recommendations, secure SDN-enabled communication frameworks need to be developed as the incorporation of SDN with ICT in smart cities will escalate security concerns to higher levels. Besides, current encryption and authorization policies are inefficient to guarantee an acceptable level of security in smart city communication systems.

To establish reasonable and appropriate resolutions regarding recovery measures and control in SDN-enabled ICT, it is exceptionally important to reign a comprehensive and clear understanding of the causes and consequential effects of possible cybersecurity threats in the smart city [71]. Hence, in this section, we present security threats and their relative impacts within the SDN-enabled smart city communication systems. The following threat classification is a combination of vulnerability categories pertinent to communication systems in smart city ICT infrastructure. The security threats are classified as follows.

- Confidentiality threats: Typical vulnerabilities to the confidentiality of data include the illegitimate and unlawful gathering of information through eavesdropping mechanisms or even the analysis of communication flows [71].
- Integrity threats: Typical vulnerabilities include the unauthorized access to restrictive data, which could be feasible through launching malware or masquerade attacks as well as wastage, modification, and corruption of unprotected data [71], [72].
- Availability threats: Vulnerabilities in the continuous behavior and availability of SDN-enabled communication systems in the context of smart city such as DoS threats [18].
- Accountability and non-repudiation threats: Accountability and non-repudiation are of great importance to guarantee no party can deny that specific traffic flow (e.g., message) was transmitted or received, or that particular service or information was manipulated [71], [73], [74].
- Authenticity threats: These are the primary security vulnerabilities in smart communication systems since typically, all entities, smart devices, and system stations can transmit, extradite, and replay broad message types [71].

The simplified view of the ICT architecture of smart cities describes five layers (from bottom to top):

- Field components
- Data transmission network
- Data processing
- Data aggregation connectivity
- Smart processing

Although SDN integration into smart city is highly beneficial in advancing the communication infrastructure and smart city-enabled applications, it also raises various challenges including non-security ones. Such non-security challenges include, but not limited to, reliability, interoperability, consistency, scalability, and single point of failure [75]. However, in this article we mainly focus on the security-related issues and challenges.

E. SDN FOR SECURE CLOUD AND NFV IN SMART CITY COMMUNICATION SYSTEMS

There is a broad range of embedded smart entities/devices in the smart environment on one end of the smart city's architectural design. These entities are used for various applications and purposes (e.g., embedded sensors) [5]. On the other end of the smart city spectrum, there are scalable and high-performance cloud datacenters, where smart applications and networking-enabled services are hosted. Hence, clouds play an essential role for service providers and smart city residents to deploy and elaborate on various smart city applications and services [5].

TABLE 5. VNF/SDN in smart city.

Ref.	Smart City Application	Details
SmartCityWare [76]	Cloud and fog-enabled middleware	Propose a service-oriented middleware for cloud and fog-enabled smart city services with the possibility of SDN extension
Wu et al. [77]	Safety extension	Propose a safety extension for critical cyber-physical systems using SDN
Munir et al. [78]	QoS improvement	Propose a resilient SDN-based mechanism for QoS fulfilment of smart services
Taylor et al. [79]	Resiliency	Propose a cloud-based SDN design for residential networks
SUPC [80]	Policy checking	Propose an SDN/NFV-enabled approach for universal policy checking in cloud networks
Condoluci et al. [81]	Softwarization/virtualization	Discuss Softwarization and virtualization in 5G networks for smart cities and implications of SDN resiliency
DistBlackNet [82]	IoT communication architecture	Propose an SDN-enabled distributed secure black IoT architecture for smart cities
Xu et al. [83]	Data management	Propose an SDN-based DDoS defense solution to improve data management in smart city networks by leveraging NFV and traffic classification strategy

However, substantial hardware differences, communication standards disparity, and vendor-based software specification restrain the smart city attainment. Nowadays, the softwarization and virtualization progress in the network and transportation layers, in particular, can address some of such challenges. Key softwarization technologies include SDN, Network Function Virtualization (NFV), and cloud computing [84], [85]. These softwarization enabling technologies can be deployed to integrate smart devices into smart city systems and simplify information management in smart city communication infrastructures. Additionally, SDN and NFV enable various data management services (i.e., all the L2-L7 services and applications) [86].

Substantially, the telecommunication industry employs dedicated network hardware to elaborate network functions (NFs), which offer specific services, such as deep packet inspection (DPI) and security firewalls at the networking level. Under NFs deployment, networking flows are pushed through multiple functions in a pre-defined order called the service function chain (SFC). An SFC can be, for instance, a security firewall, an IDS, and a DPI, respectively. Hence, SFC consists of a defined set of middle boxes, which handle networking traffic. An SFC must be implemented optimally to operate network hardware efficaciously [76].

NFs are considered software implemented in virtual hardware, i.e., Commercial-off-the-Shelf (COTS) networking hardware. Moreover, an NFV management and orchestration (MANO) software is deployed to establish, configure, manage, and monitor Virtual Network Functions (VNFs) and the Network Functions Virtualization Infrastructure (NFVI) [87]. It is interesting to note that NFVs do not need vendor-specific hardware nor specialized operators and grants prompt maintenance and integration of new NFs. Nowadays, NFV is being efficaciously integrated into network layer functions and expanded to deliver E2E applications for smart city communication systems [87].

Furthermore, NFV simplifies the integration of IoT-enabled applications in the smart city via IoT-Clouds [88] and SDN-enabled NFV to implement a platform as a service (PaaS) for IoT [89]. Gember *et al.* proposed OpenNF [90] and Stratos [91]. While OpenNF is an adjusted SDN control layer for VNF through the extension of the forwarding layer of the SDN controller to enable steering networking flows via VNF instances, Stratos is a VNF orchestrator to administer VNFs at the cloud level through traffic engineering (TE) and scaling techniques, respectively. Qazi *et al.* [92] and Fayazbakhsh *et al.* [93] deployed TE techniques to handle VNFs in SDN-enabled environments. Specifically, they aimed at steering network flows throughout a defined set of VNFs using middle boxes, which adjust packet headers and modify flow signature.

As the smart city is a coherent integration of residential, municipal, commercial, and equipment (e.g., smart devices, homes, systems) into a broad range of safety and reliability services, cloud, SDN, and NFV all together can facilitate and enhance the development of networking-enabled services in smart cities communication systems [86]. Figure 4 depicts organizational tiers of the SDN, cloud, and NFV-enabled smart city networking system [86].

Figure 4 presents three networking layers. The first layer contains diverse entities inter-connected via a physical link or a wireless access network, converged edges [94], and networking-enabled applications and or services. Layer 2 consists of converged edges to link resources in the cloud (e.g., storage) to end devices. These edges are capable of comprising Metropolitan Area Network (MAN) edge points [86], fog nodes, cloudlets [88], [95], and NFV/SDN-enabled edges [94], [96]. Lastly, the third layer contains clouds that are interconnected through a backbone architecture. It is important to note that the backbone infrastructure can be virtualized and or softwarized for diverse L2-L7 functions.

Table 5 presents a summary of existing research studies about SDN, cloud, and NFV deployment to improve communication systems and applications and services for the smart city context. Among the presented studies, Taylor *et al.* [79] proposed a cloud-based SDN design for improving the resiliency in residential networks. Islam *et al.* [82] introduced

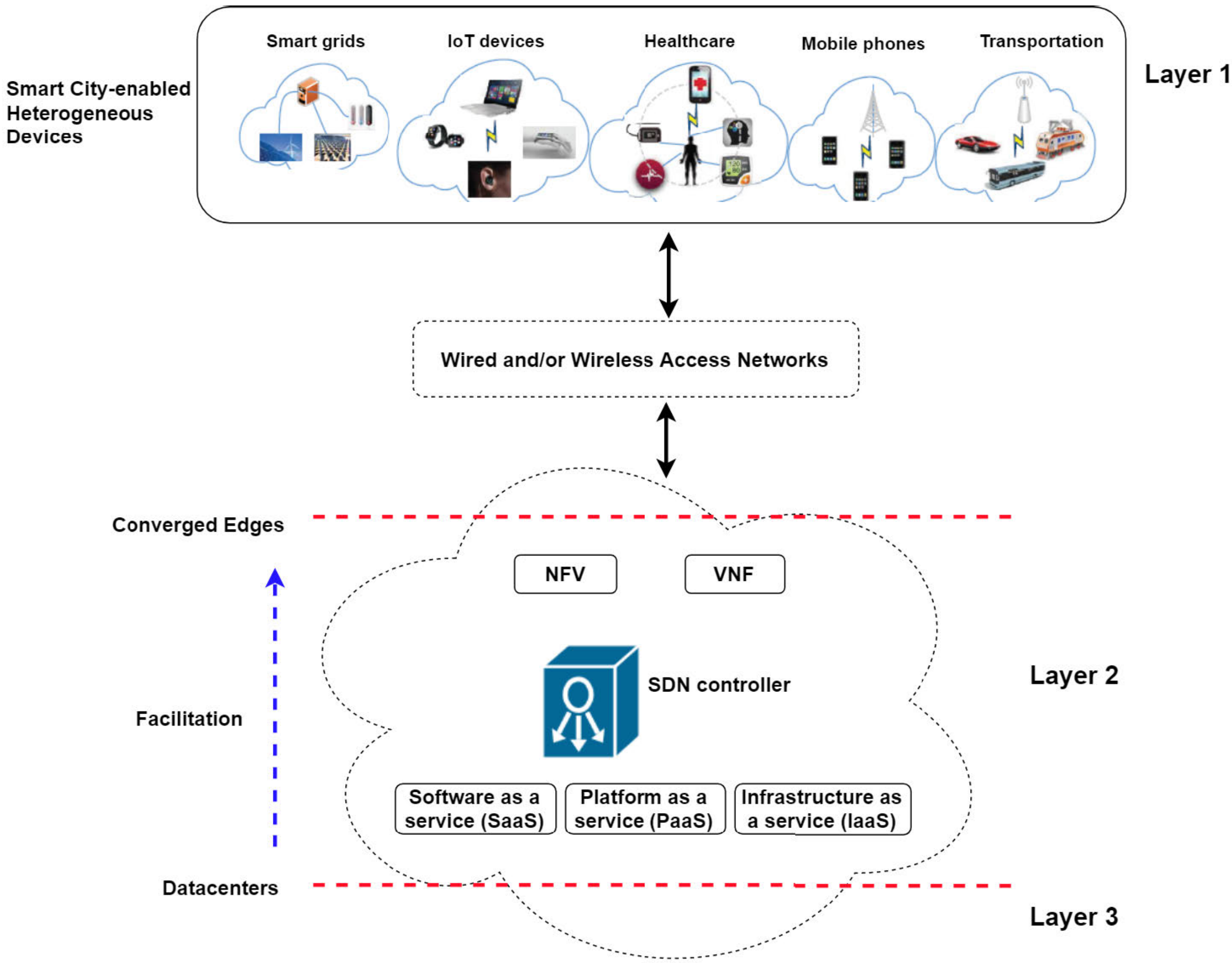

FIGURE 4. Smart city facilitated by cloud, SDN and NFV.

and implemented DistBlackNet, a distributed secure black SDN-IoT framework using NFV implementation for smart city applications. The proposed solution leverages black SDN to improve the security of both metadata and traffic payload within SDN layers. A multi-distributed SDN controller architecture is also proposed to enhance network layers' security using black network providers [82]. Chowdhary *et al.* presented SUPC [80], an SDN-enabled mechanism for universal policy enforcement in cloud networks. The proposed mechanism provides flow composition and ordering via the translation of service functions rules to compatible OpenFlow rules format. Such an approach eliminates redundant rules and ensures policy compliance in SFC. Additionally, SUPC allows for analysis of flow conflicts to detect conflicts in header space and actions within service function rules.

F. SDN SECURITY IN SMART CITY WIRELESS COMMUNICATIONS

Nowadays, mobile devices, such as laptops, smartphones, and tablets, require ubiquitous and substantially available wireless networks, such as Wireless Local Area Network (WLAN) or Wireless Fidelity (WiFi) [97]. The dramatic increase of mobile devices imposes various requirements, including QoS, trusted authentication management, load-balancing capabilities, etc. [98]. Furthermore, advances in connection abilities of multi-user-multiple-input and multiple-output (MU-MIMO) and high-performance hardware render the infrastructure of wireless networks complex [99]. In particular, the significant boost in mobile devices and upgrades of connection standards, such as 802.11ac, impose new challenges like the need for providing comprehensible authentication of users or suitable control of users' association state [98].

The smart city paradigm can be regarded prospective hybrid networks that are mission-critical linking citizens and smart objects to deliver a wide range of smart applications and services via reliable, high performance, and low latency broadband networking systems [81]. Next generation mobile networks, i.e., 5G networks, can fulfill smart city needs for such hybrid networks through their programmability and cognition features [100]. The programmability and cognition are the main features of 5G networks and are attained through virtualization and softwarization of the E2E chain of radio, applications, and services [101]. Therefore, SDN and NFV are promising technologies in such network advances, e.g., enabling multiple users to partition a physical infrastructure. When consisting of a broad range of inter-related infrastructures, a smart city can significantly benefit from such a multi-tenant design [81].

Moreover, in the past, hybrid optical-wireless networks and mobile ad hoc networks (MANETs) have been regarded independently without joint management solutions [102]. The MANET's focus is mainly on dispatching networking traffic between mobile entities in an infrastructure-less and more dynamic networking environment. Simultaneously, the hybrid optical-wireless networks strive to provide low latency and high bandwidth access to cellular-equipped mobile entities. It is crucial to claim that SDN capabilities and features have helped integrate flexible control and monitoring for such networks [102].

Nowadays, to fulfill the QoS needs for mobile users in smart city communication infrastructures, both academic and industrial research studies are striving to ensure dynamic management and high-performance [103]. This can be attained throughout two directions; (1) resilient and dynamic connectivity by providing peer-to-peer (P2P) services through multi-hop and infrastructure-less mobile networks [102], and (2) wide coverage and high bandwidth, which can be achieved over Internet access in the hybrid optical-wireless networks (i.e., infrastructure-based networks) [104].

The facilitation and simplification of associated networks' management are the critical goals of the underlying networked systems in a smart city. However, networking technologies, such as MANET and Wi-Fi, are traditionally managed distinctly through TE operators (e.g., Wi-Fi is managed in a totally decentralized manner that is different from MANET) [81]. In the smart city context, this stringent separation prevents the full exploitation of various novel scenarios that require flexibility, resiliency, and high performance. One scenario is about sparse smart cities, characterized by collaborative users' smartphone applications for remote control and monitoring of mobile devices [105]. Recent research studies focused on adopting mobile node collaboration to improve the distribution of computation tasks and QoS in content delivery [106]. Herein, SDN-enabled FiWi and MANET domains can facilitate the deployment of such an approach, while optimizing the performance and overhead produced by frequent mobile device movements and related re-connections/disconnections attempts [81]. Therefore, softwarization through SDN can help with addressing such networks' integration challenges [101]. The adoption of NFV along with SDN in smart city wireless networks does not only address challenges related to resource limitation and power supply (i.e., that render the satisfaction of the increasing amount of mobile devices infeasible), but also optimization, heterogeneity, and security challenges caused by the various specifications of wireless access equipment [107].

Additionally, it is immensely vital to note that there is a necessity to consider the E2E requirements and capabilities of SDN-enabled wireless networks in line with 5G guidelines [108]. The service requirements in 5G networks, according to the latest specifications published by the 3rd Generation Partnership Project (3GPP), specified that user equipment (UE) must support at least one of the following mechanisms of connectivity; (1) conventional direct network connectivity and or (2) indirect connectivity based on other UEs that are utilized as relays (i.e., relays can range from traditional mobile devices to smart sensors and devices deployed in a smart city IoT environment) [109].

On the one hand, the adoption of SDN architecture has remarkably improved wireless networks' security and changed how they are managed. For instance, The integration of SDN capabilities into Wi-Fi networks allows for various management solutions to be used even from outside the access network, while granting suitable approaches for enforcing mobile nodes' privacy. On the other hand, the SDN availability in smart city-based spontaneous networks will help achieve centralized management in the decentralized-based multi-hop networked systems and an effortless control by embracing dedicated mechanisms of traffic monitoring and TE [110].

In the past, various remarkable research efforts have been presented to improve resiliency and security by adopting and leveraging SDN technology capabilities in smart city wireless communication systems and related smart applications, such as smart homes and smart grids. Table 6 presents a taxonomic summary of existing security research studies addressing a wide range of security challenges in different wireless networking systems.

To address the heterogeneity and authentication challenges in 5G networks, Fang *et al.* [108], proposed an SDN-based security architecture, which analyzes and manages identities and handles authentication in the network. Fang *et al.* [108] explored a novel handover mechanism and a signaling-based load scheme to demonstrate the proposed security scheme's efficiency. As the management of smart home networks that consist of disjoint network segments handled by multiple technologies can be problematic, Gallo *et al.* [103] discussed such an interoperability challenge and explored shortcomings in the reliability and resiliency of current approaches. Moreover, to address these challenges, Gallo *et al.* [103] defined SDN@home, a flexible SDN-enabled architecture, in which wireless protocols and capabilities are not restricted to particular technologies and can be deployed by any general-purpose SDN-enabled device.

Various research efforts have recently been carried out to detect and mitigate conventional security attacks in wireless-enabled networks. Yan *et al.* [111] proposed an IDPS solution for identifying DDoS attacks and mitigating them using a fuzzy synthetic evaluation decision-making approach. Sweatha and Vijayalakshmi [112] also designed

TABLE 6. Secure SDN in smart city wireless networks.

Ref.	Smart City Application	Details
Liang and Qiu [119]	5G networks	An SDN-based secure architecture for smart city 5G networks
Siddiqui, et al. [120]	NFV-enabled 5G networks	A policy based-security architecture for smart city 5G networks
Hyun, et al. [122]	VoIP/VOLTE	Network security functions based on SDN for VoIP and VoLTE services
Bellavista, et al. [102]	Hybrid FiWi-MANET networks	A federated and reliable architecture for the interaction of multi-domain MANET and FiWi SDN controller
Artman and Khondoker [98]	Security Analysis	A security analysis of SDN-WiFi-enabled applications
Usman, et al. [123]	5G networks	A resilient architecture based on software-defined device-to-device communication in 5G-enabled safety applications
Sweatha and Vijayalakshmi [112]	WSN	Propose a security framework for DDoS against WSN in smart city where SDN is used for attack mitigation
Irfan, et al. [118]	LTE-enabled grids	Propose an SDN/LTE-based architecture for smart city grid security
Wu, et al. [117]	Sensor networks	Propose an SDN-based hierarchical security framework for defending against attacks on wireless smart city sensor networks
Condoluci, et al. [81]	5G networks	Discuss Softwarization and virtualization in 5G networks for smart cities and implications of SDN resiliency
Ding, et al. [116]	Wireless SDN	Provide proposals about SDN for security enhancement in wireless mobile networks
Liyanage, et al. [121]	LTE	Propose security enhancement solution for LTE through SDN and NFV
Zhou, et al. [115]	WSN/actor networks	Propose an application framework for resiliency improvement in WSN and actor networks using SDN
Yan, et al. [111]	Wireless SDN	Propose an IDPS for DDoS prevention using fuzzy synthetic evaluation decision-making approach
Huang, et al. [114]	Wireless SDN	Propose a physical unclonable functions (PUFs)-based group key distribution scheme
Cox, et al. [113]	Wireless access points	Propose an SDN and WebRTC-based solution for rogue access point security

and implemented a security framework for DDoS attacks against WSN in smart city networks where SDN centralized capabilities are leveraged for traffic monitoring and attack mitigation. Moreover, Cox *et al.* [113] proposed a novel framework using SDN and WebRTC technology to enhance security in rogue access points. The rogue access points (RAPs) are the unauthorized nodes connected to a networking environment and strive to grant unauthorized wireless access to other users.

To solve the key distribution challenges in wireless networks, Huang *et al.* [114] designed and implemented a security framework for group key distribution management and control. The proposed solution [114] adopts the physical unclonable functions (PUFs), where the PUF challenge is saved in the mobile devices in order to minimize the associated communication overhead. While benefiting from the centralized feature of the SDN controller, the proposed scheme [114] attains group key delivery with a two-way authentication function based on one communication interaction only. The scheme can efficiently identify multiple threatening scenarios, including eavesdropping and cloning.

Other remarkable research studies have also been presented to improve resiliency in particular smart city wireless networks through SDN capabilities. Most notably, Zhou *et al.* [115] proposed an application framework for resiliency improvement in WSN and actor networks. Ding *et al.* [116] presented multiple proposals about SDN adoption for security enhancement in wireless mobile networks. Wu *et al.* [117] proposed a hierarchical security framework for defending against attacks on WSN. Other efforts have further aimed to design security architectures based on the integration of SDN infrastructure. Namely, Irfan *et al.* [118] proposed a long term evolution (LTE) networks-based architecture for smart city grid security, Liang and Qiu [119] proposed a secure architecture for smart city 5G networks, Siddiqui *et al.* [120] presented a policy based-security architecture for smart city 5G networks. Artman and Khondoker [98] further provided a security analysis of SDN-WiFi-enabled applications.

Lastly, as discussed above, SDN and NFV can be adopted as innovative concepts to enhance the overall security and resiliency in the LTE network infrastructure. Liyanage *et al.* [121] leveraged these concepts to design an architecture for enhancements of the traditional security mechanisms. They [121] proposed a novel security application dedicated to SDN-enabled LTE network security, where its performance evaluation is only conducted with simulation tools. While Hyun *et al.* [122] presented a network security function based on SDN/NFV for Voice over IP (VoIP) and Voice over Long-Term Evolution (VoLTE) services, Condoluci *et al.* [81] discussed the integration of softwarization and virtualization in 5G networks for smart cities and resiliency implications of SDN/NFV in networks. Condoluci *et al.* [81] presented a security guideline for benefiting from SDN and NFV to improve resiliency and security enforcement in smart city 5G networks.

III. SMART CITY USE CASES WITH SDN SECURITY SOLUTIONS

A. SDN IN SMART CITY GRIDS & SECURITY IMPLICATIONS

To ensure the smooth operation of critical services, such as transportation, energy, health, and power substations in the smart city [138], one must provision timely logistics and information by all means to the public, while conserving efficiency and security of information and resources [139]. A smart grid (SG) is another essential component in a smart city to assure an efficient supply of energy and empower assortment between resources and infrastructure operators [140]. A SG consists of a set of control, electrical, and electronic entities that range from phasor measurement units (PMUs) to smart meters and from information acquisition systems to distribution units [19]. The evolution of SGs depends on the reliability, efficiency, and globalized management of the underlying communication infrastructure.

Furthermore, SG is a critical infrastructure, and it must be resilient when networking-enabled attacks and malicious behaviors take place [20]. Dong *et al.* [20] conducted a comprehensive study about the integration of SDN with smart city grids. Dong *et al.* [20] demonstrated how SDN is capable of enhancing SG security. However, such an integration presents security risks and challenges, which can be classified to three classes; (1) compromising power devices such as a SCADA slave, or a remote terminal unit (RTU), (2) compromising SDN forwarding devices, and (3) compromising applications at the SDN controller level. SDN technology is indeed considered an essential alternative to address the communication challenges of SGs [129]. Martín de Pozuelo *et al.* [141] and Dong *et al.* [20] demonstrated an SDN-enabled architecture where the controller interconnects communication between end devices, such as remote terminal units (RTUs) and management interfaces (e.g., supervisory control). Additionally, Dong *et al.* [20] discussed security threats with regard to SDN applicability in SGs development.

There are various further case studies of SDN-enabled SG, such as utility in M2M applications [142]. In [142], Zhou *et al.* presented an SDN-M2M case study while considering the centralized controller as a single-point-of-failure performance bottleneck, which results in a collapse of both the energy and communication system. Zhou *et al.* [142] also presented a mechanism for efficacious management of trust over M2M entities using SDN capabilities. Moreover, Molina and Jacob [21] discussed emerging trends across SDN integration into cyber-physical systems (CPSs). However, an in-depth discussion of an SDN applicability in the SG environment is not provided. Molina and Jacob [21] discussed the general benefits of applying SDN architecture to CPSs and how to deploy SDN capabilities to achieve mission-critical infrastructure. While SDN technology facilitates network and resource management, it can also form a closed-loop feedback control for routing and QoS policies configuration with regard to the dynamic changes in CPSs, while ensuring security and reliability requirements [21].

To attain self-configurable SGs, researchers recommended the deployment of closed-loop feedback SDN systems, whereas the Monitor, Analyze, Plan and Execute (MAPE) process adapts resources with the dynamicity of networking environments [19]. Additionally, the logically centralized controller facilitates networking awareness and provides QoS support for critical SG-supported applications [21]. Besides the traffic and resource management benefits, an external SDN controller can enhance security in SG systems. For instance, such a controller can be used to enforce filtering policies to protect smart grid entities from malicious attacks [143]. Genge *et al.* [143] introduced an external SDN controller-based approach for preventing DDoS attacks against sensitive streams in the industrial control systems (ICS). The proposed approach is capable of rising alerts at the controller level prior to block or re-route malignant traffic.

Presently, vehicle-to-grid (V2G) is another substantial component in a smart city. Although V2G provides various benefits to smart cities such as efficient scheduling and energy storage, security challenges hinder smooth operations of V2G-enabled communication systems. In particular, there are two key challenges regarding V2G security. Current security solutions (1) are based on static strategies, and thus they are unable to efficiently prevent highly dynamic and sophisticated attacks, and (2) they are short of a unified information modeling mechanism [131]. Wang *et al.* [131] introduced an SDN-based security solution for V2G. The proposed solution [131] utilizes transfer learning and IEC 61850 standards to provide a dynamic security policies configuration while dynamically updating security policies. Maziku and Shetty [130] proposed and implemented an SDN-based security score framework for substation communication systems. The proposed mechanism incorporates a security risk score model while benefiting from the SDN centralized control and global view to attain cyber resilience.

While SDN technology offers new opportunities to improve reliability in the underlying communication networks of smart grids (i.e., by enabling new mechanisms for detecting and preventing attacks against smart grids [27], it also augments the vulnerability surface and current standards do not solve authorization and authentication issues [133]. Namely, the allowance of new network applications augments system complexity, and thus, it becomes challenging to highlight applications responsible for flow entries' modification. Moreover, the centralized SDN controller acts as a single point of failure, degrading the entire smart grid communication system reliability and becoming a significant target for DoS attacks.

To summarise research efforts on improving SGs in the context of smart cities using SDN, we present a taxonomic classification of related studies in Table 7. Among these research studies, Antonioli and Tippenhauer [128] presented an emulation tool based on the OpenFlow-enabled SDN controller that serves as IDPS of security attacks. The networking environment in [128] is generated through Mininet emulator, and connected to both simulated and physical industrial protocols. The proposed tool depends on constant monitoring that permits the central service to capture abnormal adversary behaviors (e.g., DoS and MITM) prior to attack mitigation and network reconfiguration.

TABLE 7. Secure SDN in smart grid communication.

Ref.	Smart City Application	Details
Irfan et al. [118]	Smart grid communication	Propose an SDN/LTE-based architecture for smart city grid security
Ghosh et al. [124]	Security framework	Propose a security framework for SDN-enabled smart grids
Chaudhar et al. [125]	Smart grid communication	Propose an SDN-based framework to secure multi-attribute communication in IoT and smart grid environment
Gonzalez et al. [126]	Security framework	Propose an SDN-based security framework for smart grid-enabled IoT
Chaudhary et al. [70]	Security framework	Propose an SDN-based multi-attribute security framework for IoT-enabled smart grids
LACSYS [127]	Cryptosystem	Propose an SDN-enabled lattice-based cryptosystem for securing smart grid communication
NLES [77]	Safety extension	Propose a safety extension for crtitical cyber-physical systems using SDN
MiniCPS [128]	CPS networks	Propose a toolkit for SDN-based CPS networks security research assessment
Zaballos et al. [129]	SDU	Propose an approach for a reliable SDU based on SDN
Maziku and Shetty [130]	Substations communication	Propose a resilient SDN-based solution for smart substation communication system
SSDS [131]	V2G communication	Propose a smart software-defined security mechanism for V2G using transfer learning
Rehmani et al. [132]	Smart grid communication	Propose a multi-armed bandit approach by leveraging SDN capabilities to enhance smart grid resilience
Jung et al. [133]	Smart grid networks	Investigate implications of SDN-collected information on anomaly detection in smart grid networks
Aydeger et al. [134]	Smart grid teleprotection	Propose an SDN-based recovery solution for smart grid teleprotection applications of disaster handling
Liu et al. [135]	Smart grid network	Propose an SDN-defined survivability-aware routing restoration solution for large scale failures in smart grid networks
Von et al. [136]	Smart grid controller	Propose an SDN-based solution to enhance reliability of the controller by reducing power equipment redundancy
Zhao et al. [137]	SCADA Systems	Propose an SDN mechanism to identify security threats in SCADA design using a vulnerability pattern database

B. SDN SECURITY IN SMART CITY IoT

The Internet of Things (IoT) is a technology striving to connect networking-enabled objects, such as vehicles, bulbs, and computers, at any place, at any time [144]. These objects are connected to the so-called IoT ecosystem and they must be addressable, possess a unique ID, and connect to Internet [145]. IoT is indeed a technology that offers a virtualized image of networking-enabled objects that are connected to the Internet. Contemporary advances in networking technologies, such as radio frequency identification, WSN, and M2M communication, have significantly shared in IoT's evolution [146].

IoT ecosystems produce big data, from which a wide range of knowledge and information is induced. The extracted knowledge presents value-added benefits in various smart city applications [144]. Typical smart city IoT applications include, but are not limited to, industrial and home automation, car industry, smart energy management, SG control, and health care. Governments, residents, and the industrial sector can benefit from these smart applications and services given the QoS that smart cities aim at providing to citizens while optimizing administrative management overhead via efficacious and reliable resource management [146]. Therefore, in order to design reliable, resilient, and scalable smart cities, IoT ecosystems should be simple and grant a secure communication system [144].

Two of the existing key security challenges in IoT infrastructure are scalability and heterogeneity [147]. Unlike typical networking-enabled devices with sufficient storage, computing, and processing abilities, IoT entities (e.g., mobile sensors) are resource-restrained. In addition to the need for processing and storing a massive amount of data produced by a wide range of IoT entities, scalability is also a key challenge in an IoT system because its environment needs to support and handle communications between billions of devices [147]. Besides heterogeneity and scalability challenges that render IoT networked systems more defying than traditional ones, there are several other security challenges, such as identity management and trust management, that need to be addressed.

As SDN's architecture offers a programmable and dynamic networking environment, its characteristics and features can be leveraged to process the IoT networked system challenges particularly scalability and heterogeneity. For the past several years, the integration of SDN technology into IoT environments for the purpose of resiliency enhancement has been attracting researchers and service providers' attention, e.g., the adoption of SDN technology to boost IoT's bandwidth.

Herein, we present and summarize remarkable research studies on SDN-based solutions strive for enhancing smart city IoT security and IoT-enabled applications for the context of smart cities. Table 8 presents a summary of existing work on SDN deployment to improve IoT security. To address the heterogeneity issue, Salman *et al.* [148] developed and implemented an authentication mechanism for identity control in

TABLE 8. Secure SDN in smart city IoT.

Ref.	Smart City Application	Details
Tselios et al. [154]	Blockchain-enabled architecture	An SDN-based secure architecture IoT devices deployment via blockchain
Islam et al. [82]	SDN/NFV-based architecture	Propose an SDN-enabled distributed secure black IoT architecture for smart cities
Ahmed et al. [22]	IoT communication	Survey on IoT integration in smart city where related SDN security is partially covered
Chakrabarty et al. [5]	IoT environment	Propose a secure IoT architecture based on a black network, trusted SDN controller, and key management and unified registry system, while enabling a smart city-based secure IoT-centric blocks
Mazhar et al. [155]	IoT communication	Conceptualization of SDN layers over IoT for smart cities applications
DSS-SL [156]	Signage system	A secure SDN-based dynamic signage system for IoT/smart buildings
Liu [157]	Data transfer	An SDN-based architecture for secure data transfer in IoT
Karmakar et al. [158]	Communication architecture	An SDN-based architecture for secure communication in IoT
Flauzac et al. [153]	Security architecture	An SDN-based architecture for smart devices security improvement
SHSec [159]	Security architecture	A security architecture for IoT based on SDN-enabled smart home network
IoT-SDNPP [160]	Security/privacy preserving	A security method for privacy preserving in smart city IoT through SDN
Kalkan et al. [145]	IoT communication	Propose an SDN-based security classification approach for smart city IoT
Gonzalez et al. [161]	Security architecture	Propose an SDN-based distributed architecture for smart devices security improvement
DistBlockNet [162]	IoT communication	Propose a distributed blockchain-enabled secure SDN architecture for smart devices
Shif et al. [163]	IoT communication	Propose a security and scalability improvement for smart services network using SDN/VPN
Gonzalez et al. [126]	Security framework	Propose an SDN-based security framework for smart environment-enabled IoT
Abreu et al. [164]	Communication architecture	Propose a resilient architecture for smart city IoT with regard to SDN
Hamza et al. [165]	Intrusion detection	Propose an IDS framework through combining SDN capabilities and MUD
Volkov et al. [166]	SDN segmentation	Propose a SDN-enabled segmentation for IoT traffic in a smart city model
Nobakht et al. [149]	IDPS	Propose a host-based IDPS solution IoT-enabled smart homes using SDN
Chakrabarty et al. [150]	IoT communication	Propose an SDN-based architecture for enhancing IoT communication security
Bull et al. [152]	IoT communication	Propose a mechanism for IoT flow security through SDN gateway
Derhab et al. [167]	Industrial IoT	Propose an IDS for SDN-enabled Industrial IoT networks by leveraging blockchain chain technology and subspace learning
Wang et al. [168]	IoT-enabled smart city and home	Propose an SDN solution to address network invasion in smart city IoT applications by leveraging path filtering and IoT devices classification
Lin et al. [169]	IoT and smart transportation	Propose a spatio-temporal congestion-aware path planing for smart transportation systems by leveraging smart city-based SDN and IoT
Li et al. [170]	IoT and healthcare	Propose an SDN-based solution to address authentication and healthcare data privacy at the edge server level

the IoT environment by leveraging SDN capabilities and features. In this study [148], identity formats generated by various communication protocols are mapped to a shared identity record, which is elaborated using addresses from virtual Internet Protocol version 6 (IPv6). Additionally, the certificate authority (CA) is carried out by the centralized controller and handles all security parameters via a security protocol in order to authenticate all enabled devices and gateways in the environment. However, the proposed solution [148] was evaluated by simulation tools, and communication overhead was not examined.

Nobakht *et al.* [149] presented IoTIDM, a host-based IDPS solution for smart city IoT networked systems using SDN controller properties. The developed solution [149] captures and mitigates attacks against target hosts. It is implemented in an SDN controller software, where remote security management is attained through third-party entities (i.e., entities offering security as a service). While optimizing computation and communication overhead, the solution [149] ensures host-based detection rather than network-based intrusion detection. It monitors and extracts features from malignant behaviors to improve the threat identification module. Once an attack source is identified, the required flow rules are installed in SDN-enabled forwarding devices to mitigate the attack on IoT-enabled targets.

Chakrabarty *et al.* [150] designed a networking mechanism for security enforcement in IoT networking infrastructure using Black SDN. Specifically, the proposed mechanism addresses data gathering and networking traffic analysis. Chakrabarty *et al.* [150] encrypt both the payload and header (including the source and destination IP addresses), but such complete encryption leads to routing overhead and challenges. Thus, a broadcast routing protocol needs to be implemented in the SDN controller software.

Moreover, DoS and DDoS are other traditional security threats that impact availability in networking environments [151]. Among proposed solutions to address these security challenges, Bull *et al.* [152] proposed a flow-based security solution for IoT environments. The proposed solution [152] utilizes the SDN gateway and strives for mitigating DDoS attacks. The SDN gateways are vitally used as dumb forwarding devices only. However, in this work [152], the IoT gateways are merged with SDN gateways, where the networking traffic is monitored and analyzed. It is important to note that enabling SDN-enabled forwarding devices with such intelligence may impact the key paradigm of SDN centralized infrastructure.

In addition to the research studies mentioned earlier, Flauzac *et al.* [153] developed a multi-domain SDN framework for improving IoT network security, where each SDN controller acts as an edge security guard. The presented solution [153] supports multi-domain controllers, and all active IoT devices must associate with an OpenFlow device linked to one of the SDN controller domains. As discussed in this subsection, IoT networked systems have various security challenges, particularly scalability and heterogeneity. Thus, the flexibility and dynamism of the SDN nature can intuitively remediate some of the key security challenges in IoT environments for smart city communication systems and smart applications.

C. SDN SECURITY IN SMART CITY VEHICULAR COMMUNICATIONS

Recently, advances in vehicular communication have led to what is so-called software-based configurable hardware, which smoothed the evolution of software-defined vehicular networks (SDVNs). The characteristic functions of SDN, such as its programmability and plane decoupling, can meet the performance requirements for vehicular ad-hoc networks (VANETs) [171].

The considerable advances in smart city communication systems and smart devices have led up to VANETs that assist with ensuring vehicular communication efficiency and enhancing road safety [171]. Vehicular-enabled networking consists of diverse communication standards and technologies, such as Wi-Fi, 4G/5G, dedicated short-range communication (DSRC), and TV white space. While such technologies are deployed in VANETs to provide ubiquitous and efficient mobile coverage and service, various prominent features of VANETs present shortcomings and defiance, e.g., ineffective utilization of network resources and traffic unbalancing [172], [173]. Hence, programmable networking environments such as SDN can address these challenges in VANETs.

The integration of SDN architecture into VANETs provides vital mechanisms to address the aforementioned communication challenges in vehicular networks. Figure 5 depicts a visual illustration of the SDVN. In such integration,

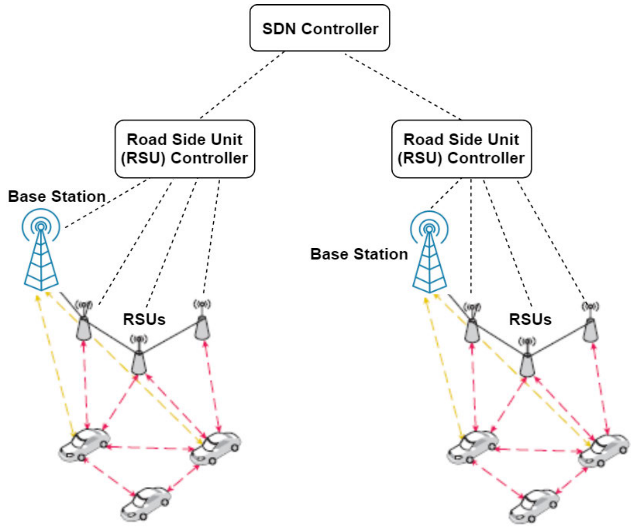

FIGURE 5. A visual illustration of a software-defined vehicular network.

devices and smart networking devices can be flexibly reconfigured using the SDN programmability and centralized control advantages along with external implementations and applications [171]. Furthermore, OpenFlow-enabled SDN advances have recently turned to wireless scenarios [172]. Yap *et al.* [174] proposed OpenRoads, a mechanism to anticipate the moves of users between various ranges of wireless infrastructure. Schulz-Zander *et al.* [175] presented cloud-medium access control (MAC), which provides virtual access points. Although the evolving interest in SDN technology has led to improve its applicability to VANETs, the enhancement of security and resiliency is a stringent requirement for SDVNs. Because of its centrality feature, the SDVN controller must be perfectly secured as its failure or unauthorized access may lead to severe road-related accidents [171].

Table 9 presents a summary of existing research studies about SDN, cloud, and NFV deployment to improve communication systems and applications and services for the smart city context. Remarkably, Yaqoob *et al.* [171] identified and discussed key requirements (including security requirements) for SDVNs realization along with related challenges. Wang *et al.* [131] presented and implemented a smart software-defined security mechanism for V2G communication using the transfer learning approach. The proposed architecture establishes a dynamic security protection offers a dynamic configuration of security policies. Mendiboure *et al.* [176] proposed an SD-IoV-enabled mechanism for application authentication and trust management in vehicular networks through the centralized SDN and blockchain technologies. The proposed solution also plays the role of a trust establishment system and aims at managing the identity of applications and their behavior. Moreover, Wang *et al.* [177] proposed an approach for rule installation and verification for real-time query services through SD-IoV.

TABLE 9. Secure SDN in vehicular communication.

Ref.	Smart City Application	Details
Wang, et al. [131]	V2G communication	Propose a smart software-defined security mechanism for V2G using transfer learning
Di, et al. [178]	VANETS	Survey on security impacts
SD-IoV [176]	blockchain-enabled communication	An approach for trust management and application authentication in vehicular networks through SDN and blockchain
Wang, et al. [177]	Rule installation/validation	An approach for rule installation and check for real-time query services through SD-IoV
Yaqoob, et al. [171]	Investigation article	Discuss SDVN advances and provide requirements for reliable and resilient integration with smart services

The proposed model is a destination-driven in the wired infrastructure layer and minimizes the number of flow rules in SDN-enabled forwarding devices at a real-time.

IV. GENERAL SECURE SDN ARCHITECTURES

The smart city spectrum aims to integrate smart application pillars, such as transportation, smart grid, and mobility, for the purpose of optimizing the resources management and minimizing the computation overhead and energy footprint of big cities. To achieve this, the integration of the centralized SDN-enabled heterogeneous communication systems is recommended to provide a peer to peer connectivity of services and applications exposed by smart devices (e.g., actuators and embedded sensors) within smart city. Moreover, the SDN adoption will not only allow for a dynamic configuration of forwarding/switching rules of data outputted by devices in the smart city, but also offer dedicated bridges to efficiently manage heterogeneous communication media and distribute time to edge nodes [179].

A. AN SDN-ENABLED ARCHITECTURE FOR SMART CITY COMMUNICATION SYSTEMS

The programmability and logically centralized view of the network carried out by the SDN allow for the deployment of network services and security, implementing network security policies and forensics at real-time [16]. Furthermore, SDN is able to easily mark and locate traffic paths as the traffic forwarding and management decisions are carried by the logically decoupled control layer [17], [73].

To reliably transfer information and data generated by different entities at run time and deliver QoS-aware services in a smart city such as emergency response traffic [188], Web of Things (WoT) [189], video surveillance [190], the communication systems must provide centralized management of network resources where QoS-aware routing mechanisms and astute scheduling could be attained [71]. This is quietly challenging to achieve via traditional networking infrastructures where centralized control is not upheld [184]. Thus, SDN is a good fit into smart city communication systems and will allow planners of its ICT to develop efficacious and dynamic security mechanisms and policies to enhance both efficiency and security of the ICT framework [191]. Figure 6 presents a detailed SDN-based architecture for communication systems in a smart city. As shown in Figure 6, the SDN controller is devoted to managing and handling the data transmission in a centralized manner, including traffic and device monitoring through the network control module. Moreover, the SDN controller is capable of upholding QoS-aware routing, TE, allocation of resources by cogging the forwarding devices (i.e., hardware and software switches) in the network unit, which render the user communication and data transmission controllable in smart city networks.

However, the massive amount of data produced by a broad range of devices and entities in the smart city dramatically augments the encumbrance of underlying SDN infrastructure [70]. Therefore, to obtain dependable data flows at run time, the implicit SDN-enabled communication systems must deliver customized control mechanisms of the network that helm interoperability between different kinds of smart city devices [192]. In contemporary proposals including, but not limited to [193] and [194], SDN is efficiently adopted to address the challenges discussed above in heterogeneous networking environments as an adequate solution to handle the massive volume of data produced by the smart city entities and frameworks. However, SDN may also lead up to both service reliability and security challenges in smart city networks from the scalability perspective.

B. CONVENTIONAL THREATS IN SDN-SUPPORTED SMART CITY COMMUNICATION SYSTEMS

As the layers in SDN are dependent, security threats or attacks on one particular layer will most likely impact the remaining layers. Security vulnerabilities that might direct to incidents do not surely have to be linked with only one particular vulnerability category. Thus, segregation is elaborated on whether they were brought about accidentally or intentionally. In this article, we discuss resiliency challenges in SDN-enabled smart city communication systems from the perspective of information exchange, information transmission network, and information ingathering connectivity [16].

The particular resiliency vulnerabilities associated with information exchange between different devices in a smart city vary according to the maturity of the concerned party/entity. From the communication systems point of view, vulnerabilities seem to appear multifaceted and pointed towards information and applications as well as the entire technology infrastructure [71]. Figure 7 presents a visual taxonomic overview of the vulnerability landscape in the context of

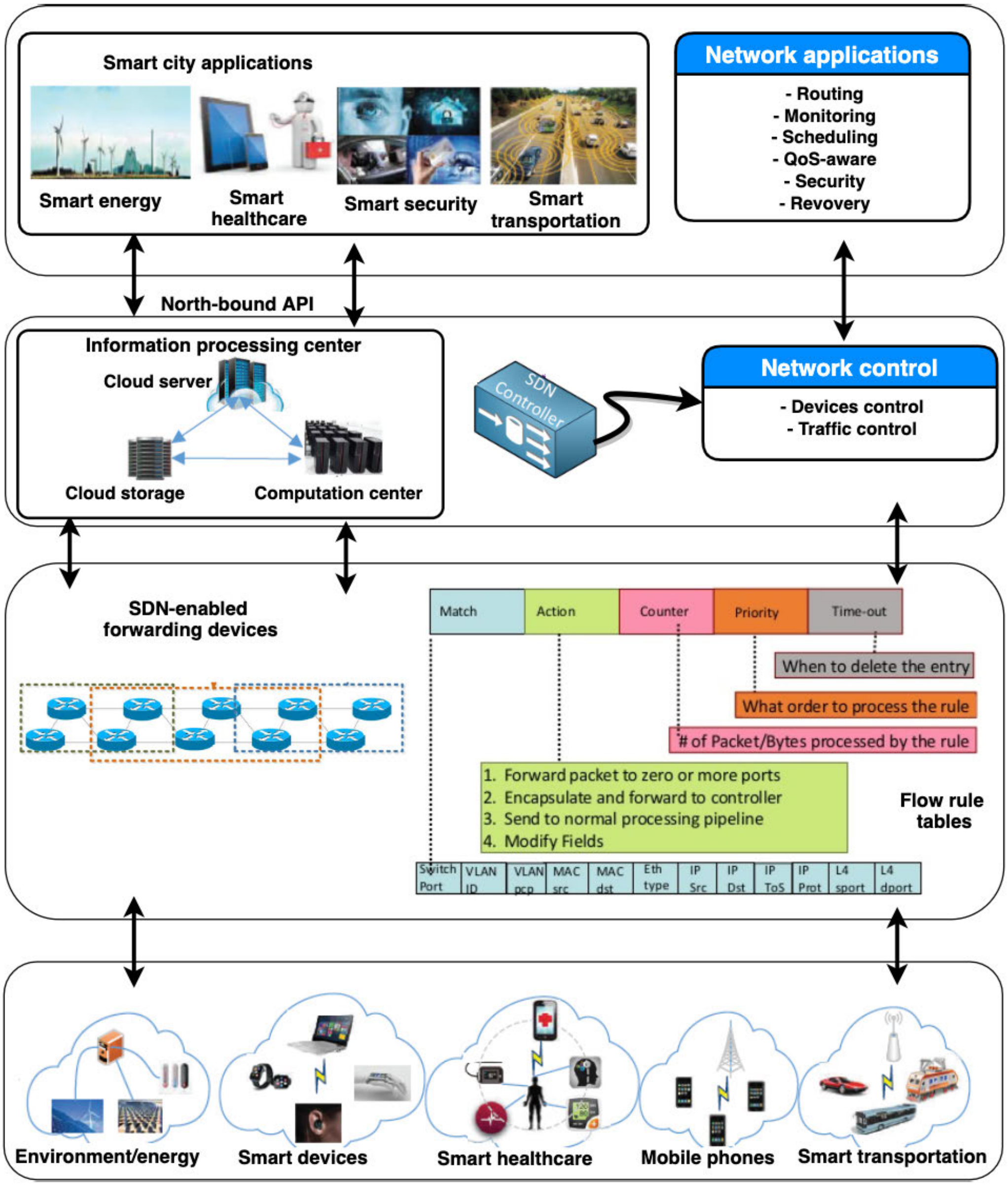

FIGURE 6. An SDN-enabled architecture for smart city.

SDN-enabled smart city communication systems differentiating between vulnerabilities from both accident occurrences and intentional attacks.

Incidents resulting from threats in this group are caused intentionally. The key threats from intentional attacks are eavesdropping/wiretapping, theft, tampering, and unauthorized access [71] that are detailed next.

- Eavesdropping: Eavesdropping and/or wiretapping is intentional conduct of apprehending network flows and hearkening to communications between parties in an unauthorized manner [71]. This is the major threat in the context of information exchange and can helm to follow-up vulnerabilities and therefore, could impact confidentiality, availability, and integrity of the entire information and communication system. For example, capturing credentials to comprehend the network configuration details and how end user devices are linked. The map of a network is a stringent information segment to any adversary. Hence, the better attached communication systems are, the highly critical and earnest follow-up threats are [16]. The severity of eavesdropping threats varies from one type of connection to another and might lead to a purposed disclosure of sensitive personal, financial, and proprietary information [18].
- Loss of Reputation: It stratifies to unprotected communication systems and personnel and hence, slashes the scale of trust in a smart city services. A purposed attack may target a particular framework in smart city

TABLE 10. Security extensions and solutions for improving reliability in SDN-enabled smart city applications.

Ref.	Smart City Application	Details
Zhou et al. [142]	Smart energy management	Propose an efficient approach for privacy and trust management across a massive number of M2M devices by leveraging SDN infrastructures
Molina and Jacob [21]	CPS	A survey paper
Kim et al. [140]	Smart grids	Emergence from ICT sub-system to SDN-enabled smart grid architectures
Genge et al. [143]	CPS	Propose an experimental assessment of network SDN-based design approaches for protecting smart CPS
Antonioli et al. [128]	CPS	Propose a toolkit for the security assessment of SDN-based CPS networks
Ndonda and Sadre [180]	Industrial networks	Propose an SDN-based countermeasure to eavesdropping in industrial networks
Tarai and Shailendra [181]	Controller placement	Propose a secure controller placement mechanism while dynamically optimize flow setup time and fault tolerance based on Master-Equal-Slave (M-E-S) controllers combination
Rametta et al. [182]	Surveillance systems	Propose a resilient SDN-enabled surveillance system for smart city
Boussard et al. [183]	Smart devices interconnection	Propose a secure software solution for interconnecting devices in smart environments according to user services request
Bi et al. [184]	Big data transfer	Propose a time-Constrained big data transfer for SDN-enabled smart city through dynamic flow control and multi-path transfer scheduling
Abhishek et al. [185]	Smart homes	Propose an architectural vision of a software defined home alert management system for smart cities
He et al. [186]	Network architecture	Propose SDN-based mobile edge computing and caching for smart cities through a big data deep reinforcement learning approach
Arbiza et al. [187]	Smart service delivery	Propose a resilient SDN-based architecture for services delivery in smart environments

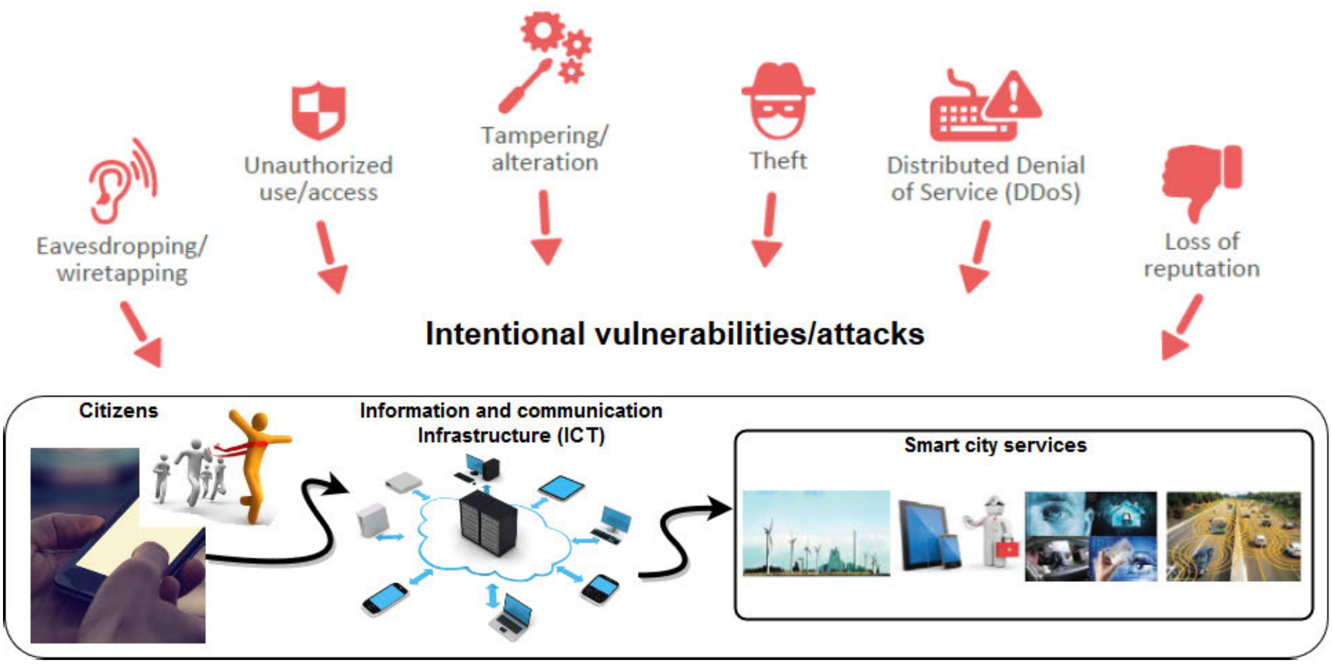

FIGURE 7. Intentional threats in smart city communication systems.

(e.g., smart grid) for different reasons, which will affect the trust between the smart city planners (including suppliers and municipalities) and citizens [71].

- Tampering/alteration: It attempts to manipulate information and applications with a forthright impact on integrity and availability. Information tempering demands direct access to assets of the target through several ways (e.g. data leakage, reply attacks, black holes, etc.) [16]. Concerning information exchange among end user devices, the MITM attack is specifically pertinent. Furthermore, any purposed adjustment, insertion, removal of information by unauthorized or authorized parties, which compromises the information, is regarded as information tempering [18]. Information tempering can affect authenticity and confidentiality. For example, fabricated messages in the form of reply attacks might be transmitted to the network and trick end users to render them ratify that another party was accountable

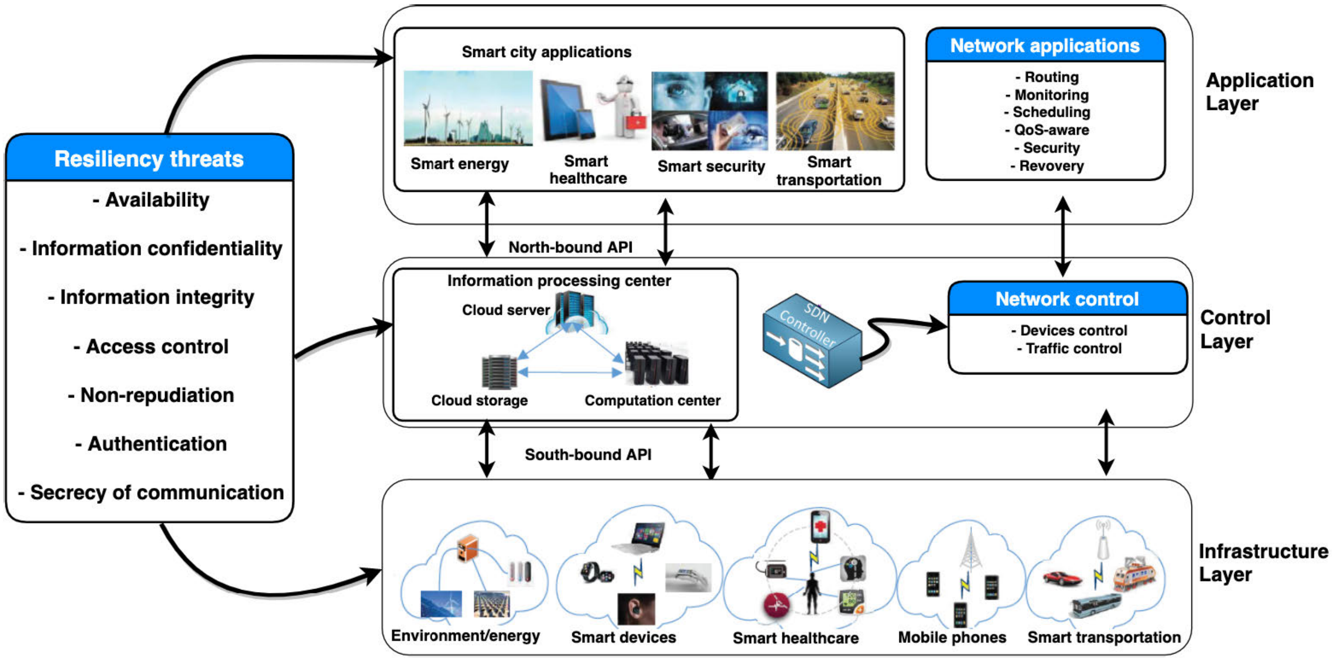

FIGURE 8. Applying ITU-T security dimensions to SDN-enabled smart city communication systems.

for transmitting these false flows. Furthermore, as the linkage of website services with other smart city systems is dramatically increasing, they have turned into being an essential gateway for more earnest vulnerabilities [71].

- Access control: Unauthorized access to network resources and services might be at the source of various vulnerabilities where the information and applications are accessed in an illegitimate way. This includes, but is not limited to, the non-licensed/entitled access to networks, information leakage, files browsing, and so on. Furthermore, the unauthorized access or usage might directly impact non-repudiation and accountability, confidentiality, authenticity, and integrity and thus, follow-up attacks can impact information exchange between different connected devices to smart city services [16], [195].
- Distributed Denial of Service (DDoS): This typical threat ordinarily prevents an attacked entity from Internet connectivity and might be precursory to different security vulnerabilities. As the IP-connected entities dramatically increase, DDoS are a major vulnerability to SDN-enabled communications systems in the smart city. The ICT framework infrastructure is commonly attacked by DDoS attacks; however, it might unknowingly participate and be a part of a DDoS attack as well if smart city communication systems are defenseless.

C. RECOMMENDED SOLUTIONS AND PRACTICES FOR IMPROVEMENT OF NETWORKS SECURITY IN SMART CITY VIA SDN

ITU-T [214] provides various security dimensions to enhance the network security aspects through various security measures [215]. The proposed security measures are composed of a combination of different security aspects to preserve the maximum network resiliency while considering all primary security vulnerabilities. In this section, we discuss different security mechanisms, platforms, and solutions that are feasible to adopt by SDN-enabled smart city communication systems with regard to ITU-T recommendations. Figure 8 depicts SDN security mechanisms discussed according to ITU-T specifications and Table 12 presents common platforms and solutions for SDN security, which tends to apply to the context of SDN-enabled networking systems for smart cities. The presented platforms are sorted according to security aspects.

Per Figure 8, recommended security measures can be taxonomically classified into different categories ranging from resource and service availability, information confidentiality and integrity, and access control to authentication. While recommended security measures range from detection and prevention to mitigation, implemented security solutions can involve any combination of these three measures. It is essential to note that these SDN-enabled security solutions are commonly deployed on the controller platform. However, implementations can also be integrated as extension applications on the switching devices.

1) ACCESS CONTROL

In the smart city context, access and authorization control measures will ensure that solely legitimate parties might have access to network services and resources. Furthermore, illegitimate access to OpenFlow-enabled forwarding devices and/or SDN node in which applications can store users' credentials could lead to dilapidation across the entire

TABLE 11. A taxonomic overview of practical attacks against SDN-enabled smart city communication systems.

Threatened Service	Violations	Descriptions
3*Banking and E-commerce	Phishing	To impersonate trusted reputable party for gaining critical information such as passwords and credit cards n40bers via emails and instant messages
	Spoofing	To duplicate data by third malicious and send it to the reader after revealing the security protocol [26].
	Attacks to information integrity	Get information about customers and networks and inject false data to system's monitoring center
Citizen to smart city communications and 6*Machine-to-machine communication	Eavesdropping	To spy on all kinds of conversations and recordings and to listen to communication channels; or we may say reading data by unauthorized readers
	DoS	To block all system's operations by using its radio signals for broadcasting devices for malicious purposes; or we may say to blind smart cities [196]
	MITM	Intercept communication channels to manipulate transmitted data, and falsified operators' actions [26].
	Side Channel Attacks	To use whatever reached information about the physical implementation of computing tasks such as power consumption and execution time
	Identification	Linking data and information to whom they belong.
	Secondary use	Using data and information collected according to specific permission and particular use for another unpermitted purposes

TABLE 12. Recommended security platforms and solutions for adaptive SDN-enabled smart city communication systems.

Proposed Solution	Security Aspect	Approach/Mechanism
DISCO [55], [197]	Availability	SDN control layer distribution
McNettle [198], [199]	Availability	Processing abilities extension
Maestro [200], McNettle [198]	Availability	Parallelism-based multi-core processors
PermOF [201]	Access control	Access control enforcement on SDN-enabled applications
FRESCO [202]	Access control	Framework for designing security application in ACL
FSL [203]	Access control	Enforcement of access control policies
Resonance [204]	Access control	Enforcement of dynamic access control policies
OF-RHM [205]	Confidentiality	Random host transformation/mutation
FortNOX [206]	Confidentiality	Information confidentiality enforcement via rules legitimacy
IBC [207]	Confidentiality	Cryptographic mechanism based on identity
FortNOX [206]	Authentication	Framework for authorization and authentication enforcement based on role
FSL [203]	Authentication	Uses admission control to monitor authentication policies
TLS [208]	Communication security	Framework for communication security assurance between SDN and forwarding devices (e.g. OVS)
[209]	Non-repudiation	Deploys perpetual identities of end user devices
OFHIP [210]	Non-repudiation	Deploys HIP for perpetual identities
VAVE [211]	Non-repudiation	Framework to validate the traffic flows based on the source address
[212]	Information integrity	Mechanism for data integrity check based on traffic isolation
OFHIP [210]	Information integrity	Utilizes the IPSec encapsulated security payload
VeriFlow [213], FortNOX [206]	Information integrity	Mechanisms to ensure information integrity based on flow rule legitimacy

communication system. As a consequence, adversaries can clone or swerve communication flows to insert fake traffic forwarding rules in the SDN-enabled forwarding devices or even to launch DoS attacks through transmitting fabricated flow requests to the SDN. In [204], Nayak *et al.* presented a platform for dynamic access control enforcement using traffic information and real-time alerts. The presented framework dynamically enables forthright development of access control policies in the device standard, whereas the upper layers will have very little accountability. A proposed solution in PermOF [201] can be adopted. In PermOF [201], Wang *et al.* implemented a mechanism based on a customized authorization approach and segregation of OpenFlow-enabled applications to protect resources in the network from malignant applications. FSL [203] provides an efficient deployment of access control and reduces the risk of security policies conflict based on traffic flows in the OpenFlow controller.

2) AUTHENTICATION

From the smart city communication systems perspective, mechanisms of authentication enforcement will assure identity of communication entities. Therefore, smart city users are unable to aim at a masquerade or even an illegitimate replay of preceding traffic. In the SDN context, all implemented applications need to be authenticated before allowance for access to network resources and SDN interfaces, particularity, control interface [71]. Similarly, the SDN infrastructure layer needs to possess security enforcement for SDN controllers authentication in order to evade malicious and fake flow rules injections [16]. In a multi-domain communication environment, multiple SDNs might be deployed such that the forwarding devices such as OVS entities must be able to authenticate the SDN controllers and preserve the essential controller replication. Moreover, all servers/hosts of applications need to authenticate users and user nodes prior to sending any critical information/credentials. Recent SDN security mechanisms can be feasibly adopted to address the authentication challenges in SDN-enabled smart city communication systems. Particularly, FortNOX [206] provides an extension of NOX software to guarantee a role-based authentication and authorization mechanism. The presented solution inhibits attackers from manipulating or injecting false traffic rules into the OpenFlow-enabled forwarding devices. Different schemes of authentication mechanisms might be suitable for this context and could be selected based on network architecture and communication framework abilities [216].

3) NON-REPUDIATION

Non-repudiation is a highly important security aspect that must be enforced in smart city communication systems to assure specific conduct/behaviors were carried out by particular end-devices by keeping track of their appropriate identities. Eventually, the SDN controller has to assign appropriate identities to OpenFlow-enabled switches in order to reduce the jeopardy of malignant and fake requests. Further, the SDN needs to maintain the trace of applications identities authorized to access the network services and functionalities or make changes to resources in the network. In [211], an approach for validation of source addresses is proposed. The proposed solution aims to inspect all incoming traffic and verify the identities of sources in order to mitigate security faults. In [210], Namal *et al.* introduced an OpenFlow-Host Identity-based scheme that is a cryptographic name-space for device identity enforcement. In [209], YuHunag *et al.* deployed the perpetual locator/identifier separation protocol (LISP) [217] (i.e., where the perpetual identifier does not change when user location changes) to develop a mechanism to preserve accountability in SDN-enabled environment.

4) INFORMATION CONFIDENTIALITY

From a confidentiality perspective, access control policies and encryption schemes need to be reinforced to guarantee information protection from illegitimate access in communication systems. OpenFlow specifications offer a volitional security policy to block impersonation-based attacks where adversaries attempt to impersonate an SDN controller or SDN-enabled forwarding device [16]. This optional feature deploys TLS where authentication certificates are verified and enables control interface encryption to prohibit eavesdropping from taking place. In [212], Gutz *et al.* proposed a technique to reinforce slice isolation-based confidentiality, where flows in diverse slices are isolated based on the functionality of flow processing. Jafarian *et al.* in OF-RHM [205] presented a moving target-based defense approach to transform IP addresses of user devices to avert scanning vulnerabilities. FortNOX [206] is a solution to enforce content confidentiality through traffic legitimacy. In [207], Santos *et al.* presented a technique to reinforce confidentiality within a hybrid OpenFlow network through the deployment of Identity Based Cryptography (IBC). A demonstration of HIP efficiency is presented in OFHIP [210], where HIP [218] offers cryptographic identities to boost networking flow confidentiality via specific techniques for authentication.

5) INFORMATION INTEGRITY

To ensure information accuracy and content integrity between devices and applications in different frameworks of smart city, integrity measures must be properly implemented. Innately, the SDN controller encloses content integrity via demonstrable traffic rules, virtualization methods, and a holistic view over content destination and source. VeriFlow [213] elaborates dynamic run-time mechanisms to verify traffic rules pro-actively to enforce the traffic rules integrity while OFHIP [210] utilizes transport mode-based Encapsulating Security Payload (ESP) to prevent DoS threats (i.e., authenticity of traffic origin). In Splendid [212], an integrity approach is proposed based on flow isolation. The efficiency of the proposed approach is not guaranteed as no particular security platform is adopted to enforce the integrity of networking traffic. FortNOX [206] also addressed the data integrity challenges in the SDN-enabled communication systems role-based authentication for determining the security authorization of OpenFlow applications through an extension of NOX platform [219] to uphold digital signatures. The proposed extension also provides an avoidance mechanism of traffic rules conflict through alias-based set of rules algorithm, assuring that the information is transmitted only to legitimate entities.

6) AVAILABILITY

Like the traditional networking environment, in the SDN-enabled smart city communication systems, availability must be ensured so that a denial of legitimate access to applications and network services and resources is prevented. In the smart city context, events such as natural disasters and hardware failures are very likely to occur. However, these events should not restrict authorized access to resources. Therefore, availability can have various measures, and there are indeed several research efforts to boost scalability of the centralized SDN. Namely, [220] and [52] that are approaches to enhance SDN availability through reducing the charge/duty of the centralized controller.

Availability measure requires a rapid recuperation when natural disasters or hardware failures take place. In [221], a swift recuperation technique is presented for SDN-enabled communication systems. The approach aims at redirecting the traffic flow through a different route within an optimal time slot once hardware or software failures occur. In [222], a mechanism is presented to upgrade the SDN controller to avoid service interruption with optimal overhead. Guaranteeing the availability of the SDN application layer is a further challenge and limitation in SDN-enabled smart city as services delivered by various network operators could ambush in the cloud and need to be available upon clients' requests. This availability limitation might even aggravate once commercial networks move towards SDNs.

Furthermore, it is greatly important to assure the availability of flow rules tables in the forwarding devices for all new forthcoming flows. However, the forwarding devices have limited tables and thus will lead to a rejection of valid requests. Lastly, the centralized controller and link failure (e.g., natural disaster-based link failure) can degrade the QoS in the underlying communication networks of smart city [223].

Once threats in SDN-enabled communication systems are characterized, vulnerability analysis and assessment need to be performed in order to carry out appropriate decisions on mechanisms and policies to place. These elaborated security measures will supply network operators and smart city planners with guidance to present acceptable security practices with regard to resiliency enforcement, recovery from attacks, and implementation of new mechanisms to mitigate the intentional attacks. Presently, network operators in smart cities do not have efficient security policies set in place and do not deploy codified and institutionalized determinations for critical assets, where awareness of cybersecurity in SDN-enabled smart city communication systems seems to be quietly limited.

Since stringent mechanisms and policies are not wholly exploited yet, response to intentional attacks is in the early stages and on the making. Instantaneous response to cyber attacks appears to be diversified with the widely prevalent responses from traditional networks such as maintaining back-ups, monitoring hardware/software faults, and security by design. Retaining traditional communication networks is a constraint in smart city infrastructures from the perspective of communication systems resiliency, and thus establishing new OpenFlow-based testbeds with a particular focus on validation of SDN policies and security solutions is another recommended practice in SDN-enabled smart city networked systems [224].

V. FUTURE RESEARCH TRENDS

In this section, we discuss future research trends and existing security challenges. We first detail research directions with regard to general integration of SDN technology into smart city networks. Building upon this, we then summarize those research trends in security with accordance to smart city specific applications.

The SDN controller allows developers and networking administrators to implement advanced and efficient networking architectures, models, and operational network applications. This flexibility will eventually carry out creativity inventions and present security threats and challenges in the networking industry and research. In this section, we present a detailed discussion about open research problems and future research opportunities for secure integration of SDN architecture in smart city communication systems. The key research directions are summarized as follows and detailed afterward.

- Examination of the controller software implementations prior to integration into smart city communication systems to identify possible exposures to common pitfalls and design vulnerabilities
- Enforcement of authorization and access control of SDN-enabled applications according to the demands of the distinguished operations while preserving the networking overhead constraints
- Scalability enhancement to prevent adversaries from elaborating attacks based on the immersing controller-to-OVS communication
- Cascading deficiency caused by multi-SDN controllers deployment

A. TOWARDS SDN-ENABLED SMART CITY COMMUNICATION SYSTEMS

Yoon *et al.* [225] examined different implementations of OpenFlow SDNs to demonstrate their exposure to common sets of pitfalls and design weaknesses, which allow for an intensive amount of security threats. Thus, the SDN-based independent applications might utilize the functionalities of various SDN elements at a time, and therefore could introduce serious security vulnerabilities. Besides, when an SDN application, whether a user or administrator based, is implemented in the control plane in a detached system/SDN environment, the SDN is rendered to be prone to security challenges, such as policy integration complexity and policies collision.

The majority of networking operations are perceived to be installed as networking-enabled applications in software within the SDN control plane (i.e., control layer-application layer). While particular implementations in SDN software might require network statistics about load-balancing, other applications could require flow samples, and so on. Thus, each particular type of SDN applications needs to have a valid and safe authorization and access control according to their distinguished operations' demands in order to maintain a determined jurisdiction and utilize a reliable traffic route while preserving the networking overhead constraints as discussed in [68]. A categorization of SDN applications that affect the SDN resiliency is therefore needed based upon specific criteria; packaged services of network, services for the network system, and networking-based critical applications [68]. According to the authors, authorization and access control mechanisms should not be unified for all SDN

TABLE 13. Security practices in SDN-enabled smart city communication systems.

Security Practices	
Security Practice	Description
Access control	Refers to the methods by which a system grants/denies access approval to a subject based on the successful authentication. Access control is usually a combination of physical measures (e.g., key, lock, etc.) and logical measures (e.g., authentication, access-control list, etc.). Access control limits unauthorized access and provides evidence in case of tampering
Implementation of an information security policy	Information Security Policy/Framework is implemented to effectively manage information security throughout an organization. Such policy defines for example, the elements to protect, the procedures to follow, the organization of security
Creation of activity logs	Activity logs, audit trails, and error logging record actions onto a log file. These logs offer evidence and analysis capacity in case of an incident. They provide a good indicator of what happened and how a threat materialized effectively
Maintenance of backups	Maintain backups of data, ideally in secure off-site servers that allow for data recovery in the case of corruption/loss. Proper maintenance of backups ensures that data recovery retains integrity (i.e., no loss of data)
Regular auditing	Faulty flow rules
Deploy NIDS	Inspect all inbound and outbound network activity and identifiy suspicious patterns that may indicate a network or system attack. To perform efficiently, network intrusion detection systems shall be configured appropriately (e.g., monitor key data exchange, know authorized connections, etc.)
Encryption of data	The conversion of electronic data into cipher-text, which cannot be easily understood by anyone except authorized parties. Sensitive data need to be protected with (preferably strong) encryption at-rest and in-transit. Encryption guarantees data confidentiality as it protects against unauthorized access (e.g., wiretapping)

applications. Otherwise, the control layer may experience a bottleneck because of the tremendous quantity of arriving requests to gain entry to networking elements and resources.

Scalability is another concerning challenge in the centralized SDN controller since the quantity of control flows augments as the topology (i.e. network and resources) size increases. As a result, the response time of the flow rules setup significantly increases [44]. Furthermore, the scarcity of SDN scalability might allow adversaries to establish attacks based on the immersing controller-to-OVS communication to saturate the SDN control layer [226]. Moreover, the exhausted OVS devices can further lead to a networking environment compromise [227]. Despite several studies proposed the employment of multiple SDNs to resolve the availability challenges in SDN, such a deployment can however, lead to cascading deficiency [228]. Thus, the corresponding scalability to SDN resiliency must be taken into consideration in order to grant a reliable SDN availability.

Additionally, the SDN controller offers control and application layer-based services for a broad range of SDN-enabled traffic forwarding entities [229]. However, such an SDN mechanism can lead to a controller-to-entity and entity-to-entity latency increase when reciprocating the network state and resource inquiries, and therefore introducing new vulnerabilities related to SDN availability. It is also feasible that the larger the number of connected OVS devices in SDN topology becomes, the higher the SDN response time of installing traffic rules is because more incoming traffic requires additional setup demands from the controller [230]. Hence, a smart trade-off between the infrastructure and control layers is recommended as an eventual criteria to optimize the OVS reliance on the SDN and improve both scalability and delay through internal decision-making abilities (e.g., traffic analysis and routing decisions). Besides, the relocation of the control layer's functionalities is further challenging if these functionalities are critical and require fast reaction decisions (e.g., link failure detection, forwarding path calculation). Moreover, the security of OpenFlow networks does not only rely on the fault tolerance over the infrastructure layer, but also on the high availability of the non-distributed control layer functions.

The security of a network environment is a crucial structural component of network management [14], and resilient policy adoptions demand a comprehensive analysis of policies' configurations in order to avert policy conflicts, and therefore minimize the risks of security vulnerabilities and maintain the network flows alive when a security breach occurs. Like in traditional networks, networking flow characteristics, features, and statistics in SDN-enabled networks can be utilized to capture DoS threats. Several studies such as, [151], [231], and [232], where precisely the control-to-data layers saturation attacks are addressed in reactive controllers via lightweight protocol implementations for independent detection and mitigation mechanisms. However, the holistic and centralized networking view in SDN and the flexible programmability of its infrastructure layer are likely to allow for interdependent and mutual policies deployment. Thus, it is recommended to design interdependent policies for both security and flow forwarding that guarantee a secure forwarding of networking flow and fully benefit from the SDN features.

SDN further allows for introducing languages and controllers that have the ability to dynamically react under the network state alterations [233]. SDN controllers provide a framework for efficient automation and monitoring of the networking environment, therefore rendering the design of new tasks automation-based applications simple (i.e., manually performed tasks) [234]. As a result, the communication and SDN operations cost can be minimized through dedicated automation mechanisms [235] and [236]. Such mechanisms can be elaborated and developed based on platforms dedicated to automated policies and autonomous control implementations. However, no practical mechanism for policy automation has been tested in SDN yet.

Furthermore, the logical centralization of the SDN brings in more charges for network operators as the scarcity of the operator's awareness and familiarity could render the networking environment prone to bottleneck threats. Thus, autonomous recovery applications as well as automated, flexible, and advanced security mechanisms, are recommended to be placed on the top of the SDN controller so that the operators only need to provide minimal involvement to secure the communication system.

B. SDN SECURITY IN SMART CITY IoT NETWORKS

From the IoT perspective, the IETF specifications seek the standardization of the Manufacturer Usage Description (MUD) mechanism and grammar for designating IoT devices' demeanor in order to narrow down the security threats surface. In this context, SDN can be deployed to control the internal communication between IoT devices through implementations of access control lists (ACLs) [165]. Additionally, SDN can also be employed in a distributed manner to enforce distributed security roles in a large scale IoT environment by mapping different controllers to different security roles [145]. Moreover, SDN-IoT is indeed a hot topic. To date, only light work has been conducted over leveraging SDN capabilities to improve resiliency and security in IoT-enabled environment and applications. Because of the resource constraints in some IoT devices, SDN can present more challenges to IoT environments because of the limited flow table size of SDN-enabled forwarding devices (e.g., OVS devices) [237]. Besides this challenge, the centralized management of SDN can suffer from single-point-of-failure vulnerability. In order to overcome such a challenge, reliable back-up solutions need to be considered. It is important to state that it is still unclear how such solutions can be elaborated when SDN is adopted in IoT networked systems.

C. SECURITY OF SDN-ENABLED SMART GRIDS

As for SDN-enabled smart grids, any cyber-resilient infrastructure needs comprehensive risk speculation mechanisms. Likewise, in order for a smart city grid to fulfill the resiliency requirements, the security of its networked systems should be feasibly quantified in both the absence and presence of attacks. Thus, when deploying SDN for smart grids communication management, an implementation of a risk assessment model is recommended to quantify security in the communication systems [130].

Furthermore, when deploying multiple SDN controllers in a communication infrastructure, methods for quantifying security in terms of number of controllers should be elaborated. Using diversity modeling and attack graphs can assure that adding more controllers enhance the resiliency and security of the network [238]. Additionally, the majority of existing SDN-enabled security solutions are limited by a centralized framework, which presents remarkable overhead (at the control layer in particular), and thus, helm to control links congestion. Therefore, distributed security platforms that leverage the capabilities of SDN control and monitoring along with the scalability of distributed systems must be deployed [239]. It is important to note that several existing security services in SDN require complex configuration, which may impact packet inspection performance, bandwidth, and network propagation delay. One solution can be the action-based abstraction for security services instantiation at the data plane level [240]. It is important to add that the system control and monitoring future is emerging towards a cyber-social-physical microgrid resilient communities. A substantial research trend in this area is the incorporation of SDN and human behavior into secure smart city communities (e.g., human errors, reliable social networks, client-centric demand response). Therefore, further security issues must be taken into account for future research on SDN-enabled control microgrids in smart city networked systems [32].

D. SDN & SECURE NFV-ENABLED SMART CITY NETWORKS

Various research proposals deal with authorization and access control using SDN. However, SDN combined with NFV features have not been remarkably shed light on these security applications. Unlike SDN, NFV/SDN platform provides heterogeneous services as it allows for handling control access to operations over networking flows on virtual resources [241]. Moreover, none of the existing security solutions address resiliency issues related to VNF operations. As discussed in previous sections, SDN can be deployed to provide bridges for efficient routing of data in the smart city communication systems. However, such deployment requires assessing the time synchronization of the differently implemented bridges using a low-cost platform [179]. Furthermore, SDN can be regarded as an essential component of information security support in smart city service-oriented infrastructures, datacenters, and cloud [242]. The service-oriented infrastructures are presented in the form of a sequence of tasks and-or subtasks managed by scheduling mechanisms. Thus, it is recommended to integrate an information security solution of such services, where the interaction among various tasks/subtasks is handled by the SDN controller.

E. SDN FOR SECURE VEHICULAR NETWORKS IN SMART CITY

Besides, In a smart city SDVN networked system, the distribution and dispatch of illegitimate data from unauthorized parties/devices can helm severe incidents (e.g., collisions). Thus, the SDN controller in such a critical environment should be highly secured. Furthermore, in SDVN-enabled networking systems, various security threats may compromise the centralized SDN control, infrastructure, and application layers. In particular, the centralized controller in SDVN should be secured against conventional security threats, such as DoS/DDoS, MITM, malignant applications, unauthorized access, and flow rules conflicts. Such security threats typically occur because of the lack of security enforcement in the transport layer and the injection of reactive flow rules, respectively. To thwart such challenges, physical network security in SDVNs should be enhanced. Although several remarkable research studies, such as [131], [171], [176], and [177] have been conducted over this topic, they cannot be efficiently applied to VANETs because of their mobility characteristics. Herein, future security solutions must fulfill the VANET system nature needs.

Lastly, a further future direction is the integration of blockchain technology and SDN into smart city applications. An integration example can be blockchain As-a-Service [243]. In this direction, a permissioned blockchain can be deployed to provide malware injection against not only the SDN planes, but also the intermediate communication paths.

VI. CONCLUSION

Networking infrastructures in the smart city have to fulfill the heterogeneity and interoperability requirements. Such stringent requirements span a wide range of essential components in smart city systems, ranging from user smart devices, network equipment, vendor proprietary software, communication technologies and protocols, and smart services and smart city applications. While for the last several years SDN has evolved as a part of the promising resilient future Internet architecture and has been comprehensively studied, a tremendous amount of existing studies has shed light on the SDN adoption in smart cities' communication networks to enhance their resiliency and security. In this article, we conducted a comprehensive and in-depth survey to discuss the core functionality of SDN from the perspective of security resilience, followed by a detailed discussion of existing security threats and challenges per SDN plane-based classification. Furthermore, we presented an inclusive probe of the current state-of-art that will facilitate the development of reliable, secure, and resilient SDN communication systems for the smart city.

ACKNOWLEDGMENT

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied of NSF.

REFERENCES

[1] L. G. Anthopoulos, *Understanding Smart Cities: A Tool for Smart Government or an Industrial Trick?* (Public Administration and Information Technology Book Series (PAIT)) vol. 22. Springer, 2017.

[2] E. Cavalcante, N. Cacho, F. Lopes, T. Batista, and F. Oquendo, "Thinking smart cities as systems-of-systems: A perspective study," in *Proc. 2nd Int. Workshop Smart*, vol. 9, Dec. 2016, pp. 1–4.

[3] S. H. Bouk, S. H. Ahmed, D. Kim, and H. Song, "Named-data-networking-based ITS for smart cities," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 105–111, Jan. 2017.

[4] Y. He, F. R. Yu, N. Zhao, V. C. M. Leung, and H. Yin, "Software-defined networks with mobile edge computing and caching for smart cities: A big data deep reinforcement learning approach," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 31–37, Dec. 2017.

[5] S. Chakrabarty and D. W. Engels, "A secure IoT architecture for smart cities," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2016, pp. 812–813.

[6] R. Abhishek, S. Zhao, and D. Medhi, "SPArTaCuS: Service priority adaptiveness for emergency traffic in smart cities using software-defined networking," in *Proc. IEEE Int. Smart Cities Conf. (ISC)*, Sep. 2016, pp. 1–4.

[7] J. H. Cox, J. Chung, S. Donovan, J. Ivey, R. J. Clark, G. Riley, and H. L. Owen, "Advancing software-defined networks: A survey," *IEEE Access*, vol. 5, pp. 25487–25526, 2017.

[8] S. Hong, L. Xu, H. Wang, and G. Gu, "Poisoning network visibility in software-defined networks: New attacks and countermeasures," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2015, pp. 8–11.

[9] R. Wang, Z. Jia, and L. Ju, "An entropy-based distributed DDoS detection mechanism in software-defined networking," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 15, Aug. 2015, pp. 310–317.

[10] T.-H. Nguyen and M. Yoo, "Analysis of link discovery service attacks in SDN controller," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, 2017, pp. 259–261.

[11] A. Mckeown, H. Rashvand, T. Wilcox, and P. Thomas, "Priority SDN controlled integrated wireless and powerline wired for smart-home Internet of Things," in *Proc. IEEE 12th Int. Conf. Ubiquitous Intell. Comput., IEEE 12th Int. Conf. Autonomic Trusted Comput., IEEE 15th Int. Conf. Scalable Comput. Commun. Associated Workshops (UIC-ATC-ScalCom)*, Aug. 2015, pp. 1825–1830.

[12] W. F. Elsadek and M. N. Mikhail, "Inter-domain mobility management using SDN for residential/enterprise real time services," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW)*, Aug. 2016, pp. 43–50.

[13] I. Khalil, A. Khreishah, and M. Azeem, "Consolidated identity management system for secure mobile cloud computing," *Comput. Netw.*, vol. 65, pp. 99–110, Jun. 2014.

[14] H. Hamed and E. Al-Shaer, "Taxonomy of conflicts in network security policies," *IEEE Commun. Mag.*, vol. 44, no. 3, pp. 134–141, Mar. 2006.

[15] R. Masoudi and A. Ghaffari, "Software defined networks: A survey," *J. Netw. Comput. Appl.*, vol. 67, pp. 1–25, May 2016.

[16] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in software defined networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2317–2346, Fou. 2015.

[17] H. Farhady, L. HyunYong, and N. Akihiro, "Software-defined networking: A survey," *Comput. Netw.*, vol. 81, pp. 79–95, Apr. 2015.

[18] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2456–2501, Aug. 2017.

[19] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software defined networks-based smart grid communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2637–2670, 3rd Quart., 2019.

[20] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-defined networking for smart grid resilience: Opportunities and challenges," in *Proc. 1st ACM Workshop Cyber-Phys. Syst. Secur.*, Apr. 2015, pp. 61–68.

[21] E. Molina and E. Jacob, "Software-defined networking in cyber-physical systems: A survey," *Comput. Electr. Eng.*, vol. 66, pp. 407–419, Feb. 2018.

[22] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, "Internet-of-Things-based smart environments: State of the art, taxonomy, and open research challenges," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 10–16, Oct. 2016.

[23] R. Du, P. Santi, M. Xiao, A. V. Vasilakos, and C. Fischione, ''The sensable city: A survey on the deployment and management for smart city monitoring,'' *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1533–1560, 2nd Quart., 2019.

[24] I. Jawhar, N. Mohamed, and J. Al-Jaroodi, ''Networking architectures and protocols for smart city systems,'' *J. Internet Services Appl.*, vol. 9, no. 1, p. 26, Dec. 2018.

[25] R. Petrolo, V. Loscrì, and N. Mitton, ''Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms,'' *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 1, p. e2931, Jan. 2017.

[26] S. Ijaz, M. Ali, A. Khan, and M. Ahmed, ''Smart cities: A survey on security concerns,'' *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 2, pp. 612–625, 2016.

[27] V. Glass, E. Woychik, and E. Glassa, ''Software defined network communications: The likely standard for smart grids,'' *Electr. J.*, vol. 32, no. 9, Nov. 2019, Art. no. 106639.

[28] S. Yi, C. Li, and Q. Li, ''A survey of fog computing: Concepts, applications and issues,'' in *Proc. Workshop Mobile Big Data*, Jun. 2015, pp. 37–42.

[29] S. Li, L. Da Xu, and S. Zhao, ''5G Internet of Things: A survey,'' *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018.

[30] N. Bizanis and F. A. Kuipers, ''SDN and virtualization solutions for the Internet of Things: A survey,'' *IEEE Access*, vol. 4, pp. 5591–5606, 2016.

[31] O. S. Oubbati, M. Atiquzzaman, T. A. Ahanger, and A. Ibrahim, ''Softwarization of UAV networks: A survey of applications and future trends,'' *IEEE Access*, vol. 8, pp. 98073–98125, 2020.

[32] T. Vu, B. Nguyen, Z. Cheng, M.-Y. Chow, and B. Zhang, ''Cyber-physical microgrids: Toward future resilient communities,'' 2019, *arXiv:1912.05682*. [Online]. Available: https://arxiv.org/abs/1912.05682

[33] T. M. Ho, T. D. Tran, T. T. Nguyen, S. M. A. Kazmi, L. B. Le, C. S. Hong, and L. Hanzo, ''Next-generation wireless solutions for the smart factory, smart vehicles, the smart grid and smart cities,'' 2019, *arXiv:1907.10102*. [Online]. Available: http://arxiv.org/abs/1907.10102

[34] O. Yurekten and M. Demirci, ''SDN-based cyber defense: A survey,'' *Future Gener. Comput. Syst.*, vol. 115, pp. 126–149, Feb. 2021.

[35] S. Bian, P. Zhang, and Z. Yan, ''A survey on software-defined networking security,'' in *Proc. 9th EAI Int. Conf. Mobile Multimedia Commun. (ICST)*. Brussels, Belgium: Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2016, pp. 190–198.

[36] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, ''SDN security: A survey,'' in *Proc. SDN Future Netw. Services (SDNFNS)*, 2013, pp. 1–7.

[37] Q. Li, Y. Chen, P. P. C. Lee, M. Xu, and K. Ren, ''Security policy violations in SDN data plane,'' *IEEE/ACM Trans. Netw.*, vol. 26, no. 4, pp. 1715–1727, Aug. 2018.

[38] *Floodlight Controller*. Accessed: Dec. 2020. [Online]. Available: http://www.projectfloodlight.org/floodlight/

[39] P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B. O'Connor, P. Radoslavov, W. Snow, and G. Parulkar, ''ONOS: Towards an open, distributed SDN OS,'' in *Proc. 3rd ACM Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, 2014, pp. 1–6.

[40] J. Medved, R. Varga, A. Tkacik, and K. Gray, ''OpenDaylight: Towards a model-driven SDN controller architecture,'' in *Proc. 15th IEEE Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2014, pp. 1–6.

[41] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker, ''NOX: Towards an operating system for networks,'' *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 3, pp. 105–110, 2008.

[42] *Ryu: SDN Framework*. Accessed: Dec. 2020. [Online]. Available: https://osrg.github.io/ryu/

[43] *OpenFlow Controller: SNAC, Simple Network Access Control*, Stanford Univ. Big Switch Netw., Santa Clara, CA, USA.

[44] A. Tootoonchian and Y. Ganjali, ''HyperFlow: A distributed control plane for OpenFlow,'' in *Proc. Internet Netw. Manage. Conf. Res. Enterprise Netw.*, 2010, p. 3.

[45] *OpenMUL Controller*. Accessed: Dec. 2020. [Online]. Available: http://www.openmul.org/

[46] S. H. Yeganeh and Y. Ganjali, ''Kandoo: A framework for efficient and scalable offloading of control applications,'' in *Proc. 1st Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, 2012, pp. 19–24.

[47] *Opencontrail*. Accessed: Dec. 2020. [Online]. Available: http://www.opencontrail.org

[48] *Trema: A Full-Stack OpenFlow Framework in Ruby and C*. Accessed: Dec. 2020. [Online]. Available: https://trema.github.io/trema/

[49] D. Erickson, ''The beacon openflow controller,'' in *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, 2013, pp. 13–18.

[50] S. Kaur, J. Singh, and N. S. Ghumman, ''Network programmability using pox controller,'' in *Proc. Int. Conf. Commun., Comput. Syst. (ICCCS)*, vol. 138, 2014, pp. 134–138.

[51] J. H. Cox, S. Donovan, R. J. Clarky, and H. L. Owen, ''Ryuretic: A modular framework for Ryu,'' in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2016, pp. 1065–1070.

[52] M. Yu, J. Rexford, M. J. Freedman, and J. Wang, ''Scalable flow-based networking with DIFANE,'' *ACM SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 4, pp. 351–362, Aug. 2010.

[53] J. Reich, C. Monsanto, N. Foster, J. Rexford, and D. Walker, ''Modular SDN programming with pyretic,'' USENIX, Berkeley, CA, USA, Tech. Rep. USENIX, 2013.

[54] C. Price, S. Rivera, A. Peled, M. Wolpin, F. Brockners, P. Chinnakannan, A. Sardella, P. Hou, M. Young, P. Mehta, T. Nguyenphu, and D. Neary, ''OPNFV: An open platform to accelerate NFV,'' Linux Found., San Francisco, CA, USA, White Paper, 2012. [Online]. Available: https://networkbuilders.intel.com/docs/OPNFV_WhitePaper_Final.pdf

[55] K. Phemius, M. Bouet, and J. Leguay, ''DISCO: Distributed multi-domain SDN controllers,'' in *Proc. IEEE Netw. Oper. Manage. Symp. (NOMS)*, May 2014, pp. 1–4.

[56] *HP SDN Controller*. Accessed: Dec. 2020. [Online]. Available: https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c03967699

[57] T. Koponen, M. Casado, N. Gude, J. Stribling, L. Poutievski, M. Zhu, R. Ramanathan, Y. Iwata, H. Inoue, T. Hama, and S. Shenker, ''Onix: A distributed control platform for large-scale production networks,'' in *Proc. OSDI*, 2010, pp. 1–6.

[58] Z. Cai, A. L. Cox, and T. Ng, ''Maestro: A system for scalable openflow control,'' Rice Univ., Houston, TX, USA, Tech. Rep. 245, 2010.

[59] *UniFI SDN Controller*. Accessed: Dec. 2020. [Online]. Available: https://www.ui.com/software/

[60] *Ericsson Cloud SDN Controller*. Accessed: Dec. 2020. [Online]. Available: https://www.ericsson.com/en/portfolio/digital-services/cloud-infrastruc ture/cloud-sdn

[61] *Lumina SDN Controller*. Accessed: Dec. 2020. [Online]. Available: https://www.luminanetworks.com/

[62] *NEC Programmableflow Controller*. Accessed: Dec. 2020. [Online]. Available: https://www.necam.com/SDN/

[63] *Faucet Controller*. Accessed: Dec. 2020. [Online]. Available: https://faucet.nz/

[64] *Cisco Open SDN Controller*. Accessed: Dec. 2020. [Online]. Available: https://www.cisco.com/c/en/us/products/cloud-systems-management/open-sd n-controller/index.html

[65] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, ''OpenFlow: Enabling innovation in campus networks,'' *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Mar. 2008.

[66] S. J. Vaughan-Nichols, ''OpenFlow: The next generation of the network?'' *Computer*, vol. 44, no. 8, pp. 13–15, 2011.

[67] Y. Jarraya, T. Madi, and M. Debbabi, ''A survey and a layered taxonomy of software-defined networking,'' *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1955–1980, Apr. 2014.

[68] P. Pan and T. Nadeau, ''Software driven networks problem statement,'' *Netw. Work. Group Internet-Draft*, vol. 30, 2011.

[69] M. A. M. Vieira, M. S. Castanho, R. D. G. Pacífico, E. R. S. Santos, E. P. M. C. Júnior, and L. F. M. Vieira, ''Fast packet processing with eBPF and XDP: Concepts, code, challenges, and applications,'' *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–36, May 2020.

[70] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. P. C. Rodrigues, ''SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment,'' *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2629–2640, Jun. 2018.

[71] C. Levy-Bencheton, E. Darra, D. Bachlechner, and M. Friedewald, ''Cyber security for smart cities—An architecture model for public transport,'' Eur. Union Agency Netw. Inf. Secur., Heraklion, Greece, ENISA Rep., 2015, pp. 1–54. Accessed: Dec. 2020. [Online]. Available: http://www.enisa.europa.eu

[72] A. Akhunzada, E. Ahmed, A. Gani, M. K. Khan, M. Imran, and S. Guizani, ''Securing software defined networks: Taxonomy, requirements, and open issues,'' *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 36–44, Apr. 2015.

[73] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 623–654, 1st Quart., 2016.
[74] J. Spooner and S. Y. Zhu, "A review of solutions for SDN-exclusive security issues," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 8, pp. 1–11, 2016.
[75] F. Bannour, S. Souihi, and A. Mellouk, "Distributed SDN control: Survey, taxonomy, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 333–354, 1st Quart., 2018.
[76] N. Mohamed, J. Al-Jaroodi, I. Jawhar, S. Lazarova-Molnar, and S. Mahmoud, "SmartCityWare: A service-oriented middleware for cloud and fog enabled smart city services," *IEEE Access*, vol. 5, pp. 17576–17588, 2017.
[77] J. Wu, S. Luo, S. Wang, and H. Wang, "NLES: A novel lifetime extension scheme for safety-critical cyber-physical systems using SDN and NFV," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2463–2475, Apr. 2019.
[78] M. S. Munir, S. F. Abedin, M. G. R. Alam, N. H. Tran, and C. S. Hong, "Intelligent service fulfillment for software defined networks in smart city," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2018, pp. 516–521.
[79] C. R. Taylor, T. Guo, C. A. Shue, and M. E. Najd, "On the feasibility of cloud-based SDN controllers for residential networks," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Nov. 2017, pp. 1–6.
[80] A. Chowdhary, A. Alshamrani, and D. Huang, "SUPC: SDN enabled universal policy checking in cloud network," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2019, pp. 572–576.
[81] M. Condoluci, F. Sardis, and T. Mahmoodi, "Softwarization and virtualization in 5G networks for smart cities," in *Proc. Int. Internet Things Summit*. Cham, Switzerland: Springer, 2015, pp. 179–186.
[82] M. J. Islam, M. Mahin, S. Roy, B. C. Debnath, and A. Khatun, "DistBlackNet: A distributed secure black SDN-IoT architecture with NFV implementation for smart cities," in *Proc. Int. Conf. Electr., Comput. Commun. Eng. (ECCE)*, Feb. 2019, pp. 1–6.
[83] C. Xu, H. Lin, Y. Wu, X. Guo, and W. Lin, "An SDNFV-based DDoS defense technology for smart cities," *IEEE Access*, vol. 7, pp. 137856–137874, 2019.
[84] A. Guerrero-Pérez, A. Huerta, F. González, and D. López, "Network architecture based on virtualized networks for smart cities," White Papers From Smart Cities Future Kickoff Event, White Paper, 2013.
[85] A. A. Abbasi, A. Abbasi, S. Shamshirband, A. T. Chronopoulos, V. Persico, and A. Pescape, "Software-defined cloud computing: A systematic review on latest trends and developments," *IEEE Access*, vol. 7, pp. 93294–93314, 2019.
[86] A. Manzalini and A. Stavdas, "The network is the robot," *Commun. Strategies*, vol. 96, no. 96, p. 73, 2014.
[87] *Network Functions Virtualisation (NFV); Use Cases*, document G. ETSI 001, Group Specification, 2013.
[88] M. Barcelo, A. Correa, J. Llorca, A. M. Tulino, J. L. Vicario, and A. Morell, "IoT-cloud service optimization in next generation smart environments," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 4077–4090, Dec. 2016.
[89] A. Corici, R. Steinke, T. Magedanz, L. Coetzee, D. Oosthuizen, B. Mkhize, M. Catalan, J. C. Fontelles, J. Paradells, R. Shrestha, D. Nehls, and B. Riemer, "Towards programmable and scalable IoT infrastructures for smart cities," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2016, pp. 1–6.
[90] A. Gember-Jacobson, R. Viswanathan, C. Prakash, R. Grandl, J. Khalid, S. Das, and A. Akella, "OpenNF: Enabling innovation in network function control," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 4, pp. 163–174, 2014.
[91] A. Gember, S. S. J. A. Krishnamurthy, R. Grandl, X. Gao, A. Anand, T. Benson, A. Akella, and V. Sekar, "Stratos: A network-aware orchestration layer for middleboxes in the cloud. Corr (2013)," Tech. Rep., 2013.
[92] Z. A. Qazi, C.-C. Tu, L. Chiang, R. Miao, V. Sekar, and M. Yu, "Simple-fying middlebox policy enforcement using SDN," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 27–38, 2013.
[93] S. K. Fayazbakhsh, L. Chiang, V. Sekar, M. Yu, and J. C. Mogul, "Enforcing network-wide policies in the presence of dynamic middlebox actions using flowtags," in *Proc. 11th USENIX Symp. Netw. Syst. Design Implement. (NSDI)*, 2014, pp. 543–546.
[94] J.-M. Kang, H. Bannazadeh, H. Rahimi, T. Lin, M. Faraji, and A. Leon-Garcia, "Software-defined infrastructure and the future central office," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2013, pp. 225–229.
[95] J. M. Schleicher, M. Vogler, S. Dustdar, and C. Inzinger, "Enabling a smart city application ecosystem: Requirements and architectural aspects," *IEEE Internet Comput.*, vol. 20, no. 2, pp. 58–65, Mar. 2016.
[96] P. Neves, R. Calé, M. R. Costa, C. Parada, B. Parreira, J. Alcaraz-Calero, Q. Wang, J. Nightingale, E. Chirivella-Perez, W. Jiang, H. D. Schotten, K. Koutsopoulos, A. Gavras, and M. J. Barros, "The SELFNET approach for autonomic management in an NFV/SDN networking paradigm," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 2, Feb. 2016, Art. no. 2897479.
[97] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A survey on software-defined wireless sensor networks: Challenges and design requirements," *IEEE Access*, vol. 5, pp. 1872–1899, 2017.
[98] D. Artmann and R. Khondoker, "Security analysis of SDN WiFi applications," in *SDN and NFV Security*. Cham, Switzerland: Springer, 2018, pp. 57–71.
[99] E. J. Kitindi, S. Fu, Y. Jia, A. Kabir, and Y. Wang, "Wireless network virtualization with SDN and C-RAN for 5G networks: Requirements, opportunities, and challenges," *IEEE Access*, vol. 5, pp. 19099–19115, 2017.
[100] A. Hakiri and P. Berthou, "Leveraging SDN for the 5G networks: Trends, prospects and challenges," 2015, *arXiv:1506.02876*. [Online]. Available: http://arxiv.org/abs/1506.02876
[101] S. Sun, M. Kadoch, L. Gong, and B. Rong, "Integrating network function virtualization with SDR and SDN for 4G/5G networks," *IEEE Netw.*, vol. 29, no. 3, pp. 54–59, May 2015.
[102] P. Bellavista, C. Giannelli, T. Lagkas, and P. Sarigiannidis, "Multi-domain SDN controller federation in hybrid FiWi-MANET networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, p. 103, Dec. 2018.
[103] P. Gallo, K. Kosek-Szott, S. Szott, and I. Tinnirello, "SDN@home: A method for controlling future wireless home networks," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 123–131, May 2016.
[104] K. Akkaya, A. S. Uluagac, and A. Aydeger, "Software defined networking for wireless local networks in smart grid," in *Proc. IEEE 40th Local Comput. Netw. Conf. Workshops (LCN Workshops)*, Oct. 2015, pp. 826–831.
[105] P. Bellavista, C. Giannelli, S. Lanzone, G. Riberto, C. Stefanelli, and M. Tortonesi, "A middleware solution for wireless IoT applications in sparse smart cities," *Sensors*, vol. 17, no. 11, p. 2525, Nov. 2017.
[106] L. Zhou, D. Wu, Z. Dong, and X. Li, "When collaboration hugs intelligence: Content delivery over ultra-dense networks," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 91–95, Dec. 2017.
[107] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and challenges of software-defined mobile networks in network security," *IEEE Secur. Privacy*, vol. 14, no. 4, pp. 34–44, Jul. 2016.
[108] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.
[109] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.
[110] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Software-defined mobile networks security," *Mobile Netw. Appl.*, vol. 21, no. 5, pp. 729–743, Oct. 2016.
[111] Q. Yan, Q. Gong, and F.-A. Deng, "Detection of DDoS attacks against wireless SDN controllers based on the fuzzy synthetic evaluation decision-making model," *Adhoc Sensor Wireless Netw.*, vol. 33, pp. 275–299, Jul. 2016.
[112] M. Sweatha and S. Vijayalakshmi, "A security framework for distributed denial of service attacks (DDoS) detection on wireless sensor networks in smart cities," *Int. J. Innov. Res. Sci., Eng. Technol.*, vol. 6, no. 4, Apr. 2017.
[113] J. H. Cox, R. Clark, and H. Owen, "Leveraging SDN and WebRTC for rogue access point security," *IEEE Trans. Netw. Service Manage.*, vol. 14, no. 3, pp. 756–770, Sep. 2017.
[114] M. Huang, B. Yu, and S. Li, "PUF-assisted group key distribution scheme for software-defined wireless sensor networks," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 404–407, Feb. 2018.
[115] J. Zhou, H. Jiang, J. Wu, L. Wu, C. Zhu, and W. Li, "SDN-based application framework for wireless sensor and actor networks," *IEEE Access*, vol. 4, pp. 1583–1594, 2016.
[116] A. Y. Ding, J. Crowcroft, S. Tarkoma, and H. Flinck, "Software defined networking for security enhancement in wireless mobile networks," *Comput. Netw.*, vol. 66, pp. 94–101, Jun. 2014.
[117] J. Wu, K. Ota, M. Dong, and C. Li, "A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities," *IEEE Access*, vol. 4, pp. 416–424, 2016.

[118] A. Irfan, N. Taj, and S. A. Mahmud, "A novel secure SDN/LTE based architecture for smart grid security," in *Proc. IEEE Int. Conf. Comput. Inf. Technol., Ubiquitous Comput. Commun., Dependable, Autonomic Secure Comput., Pervas. Intell. Comput.*, Oct. 2015, pp. 762–769.
[119] X. Liang and X. Qiu, "A software defined security architecture for SDN-based 5G network," in *Proc. IEEE Int. Conf. Netw. Infrastruct. Digit. Content (IC-NIDC)*, Sep. 2016, pp. 17–21.
[120] M. S. Siddiqui, E. Escalona, E. Trouva, M. A. Kourtis, D. Kritharidis, K. Katsaros, S. Spirou, C. Canales, and M. Lorenzo, "Policy based virtualised security architecture for SDN/NFV enabled 5G access networks," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Nov. 2016, pp. 44–49.
[121] M. Liyanage, I. Ahmad, M. Ylianttila, A. Gurtov, A. B. Abro, and E. M. de Oca, "Leveraging LTE security with SDN and NFV," in *Proc. IEEE 10th Int. Conf. Ind. Inf. Syst. (ICIIS)*, Dec. 2015, pp. 220–225.
[122] D. Hyun, J. Kim, J. P. Jeong, H. Kim, J. Park, and T. Ahn, "SDN-based network security functions for VoIP and VoLTE services," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2016, pp. 298–302.
[123] M. Usman, A. A. Gebremariam, U. Raza, and F. Granelli, "A software-defined device-to-device communication architecture for public safety applications in 5G networks," *IEEE Access*, vol. 3, pp. 1649–1654, 2015.
[124] U. Ghosh, P. Chatterjee, and S. Shetty, "A security framework for SDN-enabled smart power grids," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, Jun. 2017, pp. 113–118.
[125] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. P. C. Rodrigues, "SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2629–2640, Jun. 2018.
[126] C. Gonzalez, S. M. Charfadine, O. Flauzac, and F. Nolot, "SDN-based security framework for the IoT in distributed grid," in *Proc. Int. Multidisciplinary Conf. Comput. Energy Sci. (SpliTech)*, Jul. 2016, pp. 1–5.
[127] R. Chaudhary, G. S. Aujla, N. Kumar, A. K. Das, N. Saxena, and J. J. P. C. Rodrigues, "LaCSys: Lattice-based cryptosystem for secure communication in smart grid environment," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
[128] D. Antonioli and N. O. Tippenhauer, "MiniCPS: A toolkit for security research on CPS networks," in *Proc. 1st ACM Workshop Cyber-Phys. Syst.-Secur. PrivaCy (CPS-SPC)*, 2015, pp. 91–100.
[129] A. Zaballos, J. Navarro, and R. M. De Pozuelo, "A custom approach for a flexible, real-time and reliable software defined utility," *Sensors*, vol. 18, no. 3, p. 718, Feb. 2018.
[130] H. Maziku and S. Shetty, "Software defined networking enabled resilience for IEC 61850-based substation communication systems," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Jan. 2017, pp. 690–694.
[131] S. Wang, J. Wu, S. Zhang, and K. Wang, "SSDS: A smart software-defined security mechanism for vehicle-to-grid using transfer learning," *IEEE Access*, vol. 6, pp. 63967–63975, 2018.
[132] M. H. Rehmani, F. Akhtar, A. Davy, and B. Jennings, "Achieving resilience in SDN-based smart grid: A multi-armed bandit approach," in *Proc. 4th IEEE Conf. Netw. Softwarization Workshops (NetSoft)*, Jun. 2018, pp. 366–371.
[133] O. Jung, P. Smith, J. Magin, and L. Reuter, "Anomaly detection in smart grids based on software defined networks," in *Proc. 8th Int. Conf. Smart Cities Green ICT Syst.*, 2019, pp. 157–164.
[134] A. Aydeger, N. Saputro, K. Akkaya, and S. Uluagac, "SDN-enabled recovery for smart grid teleprotection applications in post-disaster scenarios," *J. Netw. Comput. Appl.*, vol. 138, pp. 39–50, Jul. 2019.
[135] B. J. Liu, P. Yu, Q. Xue-song, and L. Shi, "Survivability-aware routing restoration mechanism for smart grid communication network in large-scale failures," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, pp. 1–21, Dec. 2020.
[136] F. von Tüllenburg, P. Dorfinger, A. Veichtlbauer, U. Pache, O. Langthaler, H. Kapoun, C. Bischof, and F. Kupzog, "Virtualising redundancy of power equipment controllers using software-defined networking," *Energy Informat.*, vol. 2, no. S1, pp. 1–20, Sep. 2019.
[137] J. Zhao, L. Pang, and B. Lin, "SDNVD-SCADA: A formalized vulnerability detection platform in SDN-enabled SCADA system," in *Proc. Conf. Adv. Comput. Archit.* Singapore: Springer, 2020, pp. 3–15.
[138] A. Leal and J. F. Botero, "Defining a reliable network topology in software-defined power substations," *IEEE Access*, vol. 7, pp. 14323–14339, 2019.
[139] K. Geisler, "The relationship between smart grids and smart cities," *IEEE Smart Grid Newslett.*, 2013.
[140] J. Kim, F. Filali, and Y.-B. Ko, "Trends and potentials of the smart grid infrastructure: From ICT sub-system to SDN-enabled smart grid architecture," *Appl. Sci.*, vol. 5, no. 4, pp. 706–727, Oct. 2015.
[141] R. Martín de Pozuelo, A. Zaballos, J. Navarro, and G. Corral, "Prototyping a software defined utility," *Energies*, vol. 10, no. 6, p. 818, Jun. 2017.
[142] Z. Zhou, J. Gong, Y. He, and Y. Zhang, "Software defined machine-to-machine communication for smart energy management," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 52–60, Oct. 2017.
[143] B. Genge, F. Graur, and P. Haller, "Experimental assessment of network design approaches for protecting industrial control systems," *Int. J. Crit. Infrastruct. Protection*, vol. 11, pp. 24–38, Dec. 2015.
[144] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, Jun. 2015.
[145] K. Kalkan and S. Zeadally, "Securing Internet of Things with software defined networking," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 186–192, Sep. 2018.
[146] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, "An information framework for creating a smart city through Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 2, pp. 112–121, Apr. 2014.
[147] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 812–837, 1st Quart., 2019.
[148] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2016, pp. 1109–1111.
[149] M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow," in *Proc. 11th Int. Conf. Availability, Rel. Secur. (ARES)*, Aug. 2016, pp. 147–156.
[150] S. Chakrabarty, D. W. Engels, and S. Thathapudi, "Black SDN for the Internet of Things," in *Proc. IEEE 12th Int. Conf. Mobile Ad Hoc Sensor Syst.*, Oct. 2015, pp. 190–198.
[151] T. Chin, K. Xiong, and M. Rahouti, "SDN-based kernel modular countermeasure for intrusion detection," in *Proc. 13th EAI Int. Conf. Secur. Privacy Commun. Netw. (SecureComm)*. Cham, Switzerland: Springer, 2017, pp. 270–290.
[152] P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson, "Flow based security for IoT devices using an SDN gateway," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2016, pp. 157–163.
[153] O. Flauzac, C. Gonzalez, A. Hachani, and F. Nolot, "SDN based architecture for IoT and improvement of the security," in *Proc. IEEE 29th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, Mar. 2015, pp. 688–693.
[154] C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN security for IoT-related deployments through blockchain," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Nov. 2017, pp. 303–308.
[155] M. M. Mazhar, M. A. Jamil, A. Mazhar, A. Ellahi, M. S. Jamil, and T. Mahmood, "Conceptualization of software defined network layers over Internet of Things for future smart cities applications," in *Proc. IEEE Int. Conf. Wireless Space Extreme Environ. (WiSEE)*, Dec. 2015, pp. 1–4.
[156] P. K. Sharma, B. W. Kwon, and J. H. Park, "DSS-SL: Dynamic signage system based on SDN with LiFi communication for smart buildings," in *Advances in Computer Science and Ubiquitous Computing*. Singapore: Springer, 2017, pp. 805–810.
[157] Y. Liu, Y. Kuang, Y. Xiao, and G. Xu, "SDN-based data transfer security for Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 257–268, Feb. 2018.
[158] K. K. Karmakar, V. Varadharajan, S. Nepal, and U. K. Tupakula, "SDN enabled secure IoT architecture," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, Apr. 2019, pp. 581–585.
[159] P. K. Sharma, J. H. Park, Y.-S. Jeong, and J. H. Park, "SHSec: SDN based secure smart home network architecture for Internet of Things," *Mobile Netw. Appl.*, vol. 24, no. 3, pp. 913–924, Jun. 2019.
[160] M. Gheisari, G. Wang, S. Chen, and H. Ghorbani, "IOT-SDNPP: A method for privacy-preserving in smart city with software defined networking," in *Proc. Int. Conf. Algorithms Archit. Parallel Process.* Cham, Switzerland: Springer, 2018, pp. 303–312.
[161] C. Gonzalez, O. Flauzac, F. Nolot, and A. Jara, "A novel distributed SDN-secured architecture for the IoT," in *Proc. Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2016, pp. 244–249.

[162] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, 2017.

[163] L. Shif, F. Wang, and C.-H. Lung, "Improvement of security and scalability for IoT network using SD-VPN," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Apr. 2018, pp. 1–5.

[164] D. P. Abreu, K. Velasquez, M. Curado, and E. Monteiro, "A resilient Internet of Things architecture for smart cities," *Ann. Telecommun.*, vol. 72, nos. 1–2, pp. 19–30, Feb. 2017.

[165] A. Hamza, H. H. Gharakheili, and V. Sivaraman, "Combining MUD policies with SDN for IoT intrusion detection," in *Proc. Workshop IoT Secur. Privacy*, Aug. 2018, pp. 1–7.

[166] A. Volkov, A. Khakimov, A. Muthanna, R. Kirichek, A. Vladyko, and A. Koucheryavy, "Interaction of the IoT traffic generated by a smart city segment with SDN core network," in *Proc. Int. Conf. Wired/Wireless Internet Commun.* Cham, Switzerland: Springer, 2017, pp. 115–126.

[167] A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M. A. Ferrag, M. Mukherjee, and F. A. Khan, "Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security," *Sensors*, vol. 19, no. 14, p. 3119, 2019.

[168] S. Wang, K. M. Gomez, K. Sithamparanathan, and P. Zanna, "Software defined network security framework for IoT based smart home and city applications," in *Proc. 13th Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Dec. 2019, pp. 1–8.

[169] C. Lin, G. Han, J. Du, T. Xu, L. Shu, and Z. Lv, "Spatiotemporal congestion-aware path planning toward intelligent transportation systems in software-defined smart city IoT," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8012–8024, Sep. 2020.

[170] J. Li, J. Cai, F. Khan, A. U. Rehman, V. Balasubramaniam, J. Sun, and P. Venu, "A secured framework for SDN-based edge computing in IoT-enabled healthcare system," *IEEE Access*, vol. 8, pp. 135479–135490, 2020.

[171] I. Yaqoob, I. Ahmad, E. Ahmed, A. Gani, M. Imran, and N. Guizani, "Overcoming the key challenges to establishing vehicular communication: Is SDN the answer?" *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 128–134, 2017.

[172] I. Ku, Y. Lu, M. Gerla, R. L. Gomes, F. Ongaro, and E. Cerqueira, "Towards software-defined VANET: Architecture and services," in *Proc. Med-Hoc-Net*, 2014, pp. 103–110.

[173] Z. He, J. Cao, and X. Liu, "SDVN: Enabling rapid network innovation for heterogeneous vehicular communication," *IEEE Netw.*, vol. 30, no. 4, pp. 10–15, Jul. 2016.

[174] K.-K. Yap, M. Kobayashi, R. Sherwood, T.-Y. Huang, M. Chan, N. Handigol, and N. McKeown, "OpenRoads: Empowering research in mobile networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 1, pp. 125–126, Jan. 2010.

[175] J. Schulz-Zander, C. Mayer, B. Ciobotaru, S. Schmid, and A. Feldmann, "OpenSDWN: Programmatic control over home and enterprise WiFi," in *Proc. 1st ACM SIGCOMM Symp. Softw. Defined Netw. Res.*, Jun. 2015, p. 16.

[176] L. Mendiboure, M. A. Chalouf, and F. Krief, "Towards a blockchain-based SD-IoV for applications authentication and trust management," in *Proc. Int. Conf. Internet Vehicles*. Cham, Switzerland: Springer, 2018, pp. 265–277.

[177] X. Wang, C. Wang, J. Zhang, M. Zhou, and C. Jiang, "Improved rule installation for real-time query service in software-defined Internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 2, pp. 225–235, Feb. 2017.

[178] A. Di Maio, M. Palattella, R. Soua, L. Lamorte, X. Vilajosana, J. Alonso-Zarate, and T. Engel, "Enabling SDN in VANETs: What is the impact on security?" *Sensors*, vol. 16, no. 12, p. 2077, Dec. 2016.

[179] S. Rinaldi, F. Bonafini, P. Ferrari, A. Flammini, and M. Rizzi, "Evaluating low-cost bridges for time sensitive software defined networking in smart cities," in *Proc. IEEE Int. Symp. Precis. Clock Synchronization Meas., Control, Commun. (ISPCS)*, Aug. 2017, pp. 1–6.

[180] G. K. Ndonda and R. Sadre, "A low-delay SDN-based countermeasure to eavesdropping attacks in industrial control systems," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Nov. 2017, pp. 1–7.

[181] S. K. Tarai and S. Shailendra, "Optimal and secure controller placement in SDN based smart city network," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2019, pp. 254–261.

[182] C. Rametta, G. Baldoni, A. Lombardo, S. Micalizzi, and A. Vassallo, "S6: A smart, social and SDN-based surveillance system for smart-cities," *Procedia Comput. Sci.*, vol. 110, pp. 361–368, Jan. 2017.

[183] M. Boussard, F. Santoro, D. T. Bui, L. Ciavaglia, R. Douville, M. L. Pallec, N. L. Sauze, L. Noirie, S. Papillon, and P. Peloso, "Software-defined LANs for interconnected smart environment," in *Proc. 27th Int. Teletraffic Congr.*, Sep. 2015, pp. 219–227.

[184] Y. Bi, C. Lin, H. Zhou, P. Yang, X. Shen, and H. Zhao, "Time-constrained big data transfer for SDN-enabled smart city," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 44–50, Dec. 2017.

[185] R. Abhishek, S. Zhao, D. Tipper, and D. Medhi, "SeSAMe: Software defined smart home alert management system for smart communities," in *Proc. IEEE Int. Symp. Local Metrop. Area Netw. (LANMAN)*, Jun. 2017, pp. 1–6.

[186] Y. He, F. R. Yu, N. Zhao, V. C. M. Leung, and H. Yin, "Software-defined networks with mobile edge computing and caching for smart cities: A big data deep reinforcement learning approach," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 31–37, Dec. 2017.

[187] L. M. R. Arbiza, L. M. R. Tarouco, L. M. Bertholdo, and L. Z. Granville, "Sdn-based service delivery in smart environments," in *Intelligent Distributed Computing IX*. Cham, Switzerland: Springer, 2016, pp. 475–484.

[188] M. Rahouti, K. Xiong, T. Chin, and P. Hu, "SDN-ERS: A timely software defined networking framework for emergency response systems," in *Proc. IEEE Int. Sci. Smart City Oper. Platforms Eng. Partnership With Global City Teams Challenge (SCOPE-GCTC)*, Apr. 2018, pp. 18–23.

[189] Q. Xiaofeng, L. Wenmao, G. Teng, H. Xinxin, W. Xutao, and C. Pengcheng, "WoT/SDN: Web of things architecture using SDN," *China Commun.*, vol. 12, no. 11, pp. 1–11, Nov. 2015.

[190] G. Baldoni, M. Melita, S. Micalizzi, C. Rametta, G. Schembra, and A. Vassallo, "A dynamic, plug-and-play and efficient video surveillance platform for smart cities," in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2017, pp. 611–612.

[191] N. Zhang, S. Zhang, P. Yang, O. Alhussein, W. Zhuang, and X. S. Shen, "Software defined space-air-ground integrated vehicular networks: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 101–109, 2017.

[192] F. Tao, Y. Zuo, L. Da Xu, and L. Zhang, "IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1547–1557, May 2014.

[193] G. S. Aujla, A. Jindal, N. Kumar, and M. Singh, "SDN-based data center energy management system using RES and electric vehicles," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

[194] G. S. Aujla and N. Kumar, "MEnSuS: An efficient scheme for energy management with sustainability of cloud data centers in edge–cloud environment," *Future Gener. Comput. Syst.*, vol. 86, pp. 1279–1300, Sep. 2018.

[195] Z. Shu, J. Wan, D. Li, J. Lin, A. Vasilakos, and M. Imran, "Security in software-defined networking: Threats and countermeasures," *Mobile Netw. Appl.*, vol. 21, no. 5, pp. 764–776, 2016.

[196] L. M. L. Oliveira, J. J. P. C. Rodrigues, A. F. de Sousa, and J. Lloret, "Denial of service mitigation approach for IPv6-enabled smart object networks," *Concurrency Comput., Pract. Exper.*, vol. 25, no. 1, pp. 129–142, Jan. 2013.

[197] K. Phemius, M. Bouet, and J. Leguay, "DISCO: Distributed SDN controllers in a multi-domain environment," in *Proc. IEEE Netw. Operations Manage. Symp. (NOMS)*, May 2014, pp. 1–2.

[198] A. Voellmy and J. Wang, "Scalable software defined network controllers," in *Proc. ACM SIGCOMM Conf. Appl., Technol., Archit., Protocols Comput. Commun. (SIGCOMM)*, 2012, pp. 289–290.

[199] M. P. Fernandez, "Comparing OpenFlow controller paradigms scalability: Reactive and proactive," in *Proc. IEEE 27th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Mar. 2013, pp. 1009–1016.

[200] Z. Cai, A. L. Cox, and T. Ng. (2010). *Maestro: A System for Scalable OpenFlow Control*. Accessed: Dec. 2020 [Online]. Available: https://www.cs.rice.edu/~eugeneng/papers/TR10-11.pdf

[201] M. Wang, J. Liu, J. Chen, X. Liu, and J. Mao, "PERM-GUARD: Authenticating the validity of flow rules in software defined networking," *J. Signal Process. Syst.*, vol. 86, nos. 2–3, pp. 157–173, Mar. 2017.

[202] S. Shin, P. A. Porras, V. Yegneswaran, M. W. Fong, G. Gu, and M. Tyson, "FRESCO: Modular composable security services for software-defined networks," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2013, pp. 1–16.

[203] T. Hinrichs, N. Gude, M. Casado, J. Mitchell, and S. Shenker, "Expressing and enforcing flow-based network security policies," Univ. Chicago, Chicago, IL, USA, Tech. Rep., 2008, vol. 9. Accessed: Dec. 2020. [Online]. Available: https://pdfs.semanticscholar.org/8d86/97a07c3bd824f9d60d0fed189948e3506135.pdf

[204] A. K. Nayak, A. Reimers, N. Feamster, and R. Clark, "Resonance: Dynamic access control for enterprise networks," in *Proc. 1st ACM Workshop Res. Enterprise Netw. (WREN)*, 2009, pp. 11–18.

[205] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: Transparent moving target defense using software defined networking," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, 2012, pp. 127–132.

[206] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, "A security enforcement kernel for OpenFlow networks," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, 2012, pp. 121–126.

[207] M. A. S. Santos, B. T. de Oliveira, C. B. Margi, B. A. A. Nunes, T. Turletti, and K. Obraczka, "Software-defined networking based capacity sharing in hybrid networks," in *Proc. 21st IEEE Int. Conf. Netw. Protocols (ICNP)*, Oct. 2013, pp. 1–6.

[208] T. Dierks, *The Transport Layer Security (TLS) Protocol Version 1.2*, document RFC 5246, 2008.

[209] C. YuHunag, T. MinChi, C. YaoTing, C. YuChieh, and C. YanRen, "A novel design for future on-demand service and security," in *Proc. IEEE 12th Int. Conf. Commun. Technol.*, Nov. 2010, pp. 385–388.

[210] S. Namal, I. Ahmad, A. Gurtov, and M. Ylianttila, "Enabling secure mobility with OpenFlow," in *Proc. IEEE SDN for Future Netw. Services (SDN4FNS)*, Nov. 2013, pp. 1–5.

[211] G. Yao, J. Bi, and P. Xiao, "Source address validation solution with OpenFlow/NOX architecture," in *Proc. 19th IEEE Int. Conf. Netw. Protocols (ICNP)*, Oct. 2011, pp. 7–12.

[212] S. Gutz, A. Story, C. Schlesinger, and N. Foster, "Splendid isolation: A slice abstraction for software-defined networks," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, 2012, pp. 79–84.

[213] A. Khurshid, W. Zhou, M. Caesar, and P. Godfrey, "VeriFlow: Verifying network-wide invariants in real time," in *Proc. 1st ACM Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, 2012, pp. 49–54.

[214] *The International Telecommunication Union (ITU)*. Accessed: Dec. 2020. [Online]. Available: https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx

[215] (2002). *ITU-T Recommendation: Security Architecture for Systems Providing End-to-End Communications*. [Online]. Available: https://www.itu.int/rec/T-REC-X.805-200310-I/en

[216] Z. Faigl, J. Pellikka, L. Bokor, and A. Gurtov, "Performance evaluation of current and emerging authentication schemes for future 3GPP network architectures," *Comput. Netw.*, vol. 60, pp. 60–74, Feb. 2014.

[217] D. Farinacci, D. Lewis, D. Meyer, and V. Fuller, *The Locator/ID Separation Protocol (LISP)*, document RFC 6830, 2013.

[218] A. Gurtov, *Host Identity Protocol (HIP): Towards the Secure Mobile Internet*, vol. 21. Hoboken, NJ, USA: Wiley, 2008.

[219] *NOX: The Original OpenFlow Controller*. Accessed: Dec. 2020. [Online]. Available: https://github.com/noxrepo/nox

[220] J. C. Mogul, J. Tourrilhes, P. Yalagandula, P. Sharma, A. R. Curtis, and S. Banerjee, "DevoFlow: Cost-effective flow management for high performance enterprise networks," in *Proc. 9th ACM SIGCOMM Workshop Hot Topics Netw. (Hotnets)*, 2010, p. 1.

[221] S. Sharma, D. Staessens, D. Colle, M. Pickavet, and P. Demeester, "Enabling fast failure recovery in OpenFlow networks," in *Proc. 8th Int. Workshop Design Reliable Commun. Netw. (DRCN)*, Oct. 2011, pp. 164–171.

[222] L. Vanbever, J. Reich, T. Benson, N. Foster, and J. Rexford, "HotSwap: Correct and efficient controller upgrades for software-defined networks," in *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, 2013, pp. 133–138.

[223] R. AlZoman and M. J. F. Alenazi, "Exploiting SDN to improve QoS of smart city networks against link failures," in *Proc. 7th Int. Conf. Softw. Defined Syst. (SDS)*, Apr. 2020, pp. 100–106.

[224] K. Wrona, M. Amanowicz, S. Szwaczyk, and K. Gierlowski, "SDN testbed for validation of cross-layer data-centric security policies," in *Proc. Int. Conf. Mil. Commun. Inf. Syst. (ICMCIS)*, May 2017, pp. 1–6.

[225] C. Yoon, S. Lee, H. Kang, T. Park, S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "Flow wars: Systemizing the attack surface and defenses in software-defined networks," *IEEE/ACM Trans. Netw.*, vol. 25, no. 6, pp. 3514–3530, Dec. 2017.

[226] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2013, pp. 413–424.

[227] S. Shin and G. Gu, "Attacking software-defined networks: A first feasibility study," in *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, 2013, pp. 165–166.

[228] G. Yao, J. Bi, and L. Guo, "On the cascading failures of multi-controllers in software defined networks," in *Proc. 21st IEEE Int. Conf. Netw. Protocols (ICNP)*, Oct. 2013, pp. 1–2.

[229] S. Sezer, S. Scott-Hayward, P. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Commun. Mag.*, vol. 51, no. 7, pp. 36–43, Jul. 2013.

[230] A. Tootoonchian, S. Gorbunov, Y. Ganjali, M. Casado, and R. Sherwood, "On controller performance in software-defined networks," in *Proc. USENIX Workshop Hot Topics Manage. Internet, Cloud, Enterprise Netw. Services (Hot-ICE)*, vol. 12, 2012, pp. 1–6.

[231] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *Proc. IEEE Local Comput. Netw. Conf. (LCN)*, Oct. 2010, pp. 408–415.

[232] H. Wang, L. Xu, and G. Gu, "FloodGuard: A DoS attack prevention extension in software-defined networks," in *Proc. 45th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2015, pp. 239–250.

[233] H. Kim and N. Feamster, "Improving network management with software defined networking," *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 114–119, Feb. 2013.

[234] G. P. Tank, A. Dixit, A. Vellanki, and D. Annapurna, "Software-defined networking: The new norm for networks," Open Netw. Found., ONF White Paper, vol. 2, 2012, pp. 2–6.

[235] A. Voellmy, H. Kim, and N. Feamster, "Procera: A language for high-level reactive network control," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, 2012, pp. 43–48.

[236] D. M. Mattos, N. C. Fernandes, V. T. Da Costa, L. P. Cardoso, M. E. M. Campista, L. H. M. Costa, and O. C. M. Duarte, "OMNI: OpenFlow management infrastructure," in *Proc. Int. Conf. Netw. Future (NOF)*, 2011, pp. 52–56.

[237] R. Cohen, L. Lewin-Eytan, J. S. Naor, and D. Raz, "On the effect of forwarding table size on SDN network utilization," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2014, pp. 1734–1742.

[238] H. Maziku, S. Shetty, D. Jin, C. Kamhoua, L. Njilla, and K. Kwiat, "Diversity modeling to evaluate security of multiple SDN controllers," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Mar. 2018, pp. 344–348.

[239] L. Fawcett, S. Scott-Hayward, M. Broadbent, A. Wright, and N. Race, "Tennison: A distributed SDN framework for scalable network security," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 12, pp. 2805–2818, Dec. 2018.

[240] T. Park, Y. Kim, V. Yegneswaran, P. Porras, Z. Xu, K. Park, and S. Shin, "Dpx: Data-plane extensions for sdn security service instantiation," in *Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment*. Cham, Switzerland: Springer, 2019, pp. 415–437.

[241] A. F. Murillo, S. J. Rueda, L. V. Morales, and A. A. Cárdenas, "SDN and NFV security: Challenges for integrated solutions," in *Guide to Security in SDN and NFV*. Cham, Switzerland: Springer, 2017, pp. 75–101.

[242] A. Grusho, N. Grusho, M. Zabezhailo, A. Zatsarinny, and E. Timonina, "Information security of SDN on the basis of meta data," in *Proc. Int. Conf. Math. Methods, Models, Archit. Comput. Netw. Secur.* Cham, Switzerland: Springer, 2017, pp. 339–347.

[243] G. S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han, and R. Buyya, "BlockSDN: Blockchain-as-a-service for software defined networking in smart city applications," *IEEE Netw.*, vol. 34, no. 2, pp. 83–91, Mar. 2020.

MOHAMED RAHOUTI received the M.S. and Ph.D. degrees from the Department of Mathematics and the Department of Electrical Engineering, University of South Florida, Tampa, FL, USA, in 2016 and 2020, respectively. He is currently an Assistant Professor with the Department of Computer and Information Sciences, Fordham University, Bronx, NY, USA. He holds numerous academic achievements. His current research focuses on computer networking, software-defined networking (SDN), and network security with applications to smart cities.

KAIQI XIONG (Senior Member, IEEE) received the Ph.D. degree in computer science from North Carolina State University. Before returning to academia, he was with IT industry for several years. He is currently a Professor with the Intelligent Computer Networking and Security Laboratory, the Florida Center for Cybersecurity, the Department of Mathematics and Statistics, and the Department of Electrical Engineering, University of South Florida. His research was supported by the National Science Foundation (NSF), NSF/BBN, the Air Force Research Laboratory, Amazon AWS, the Florida Center for Cybersecurity, and the Office of Naval Research. His research interests include security, networking, and data analytics, with applications such as cyber-physical systems, cloud computing, sensor networks, and the Internet of Things. He received the Best Demo Award at the 22nd GENI Engineering Conference and the U.S. Ignite Application Summit with his team in 2015 and received the best paper award at several conferences.

YUFENG XIN received the Ph.D. degree in operations research and computer science from North Carolina State University, Raleigh, NC, USA, in 2002. He is currently a Senior Researcher with the Renaissance Computing Institute, University of North Carolina at Chapel Hill. His research interests include networking, cloud computing, and cyber-physical systems.