On the Security of a Smart City SDN-Based Network

L Scripcariu¹*, P D Mătăsaru¹ and F Mocanu¹
¹ "Gheorghe Asachi" Technical University of Iași, 67 Prof. Dr. D. Mangeron Bd., Iași, Romania

*E-mail: lscripca@etti.tuiasi.ro

Abstract. Our research work focuses on the security techniques applied on a software-defined network (SDN), designed for a smart city. Information security is essential for the good functionality of the applications used in a smart city. Information should be correct and complete otherwise the ‘life’ of the city can be compromised by various cyberattacks targeting, for example, the public transportation system, the traffic information on highways or location services for emergency crews and many others. Securing all devices connected to the SDN, including end-user devices, wireless sensors, smart home equipment is essential because various cyberattacks may be launched and the smart city may be disturbed. This paper presents a risk analysis, the ways to choose the security solutions according to the smart city security policy and our proposal for the SDN security system. We compare different security techniques and present some recommended solutions.

1. Introduction

The smart city concept represents the future of the high-density urban areas [1]. It is the best way to offer many services to a lot of people and institutions, with real-time information and high-accuracy prediction. It implies using information technology all over the place, in order to collect data using large sensor network and to distribute information to interested users via different smart devices connected to a dense metropolitan network.

Nowadays, Intelligent Transportation System (ITS) is a real fact in some countries and it will be implemented all over the world [2]. This is only one application of smart cities. Many others can be developed for the economical field, health and emergency services, environmental monitoring, commerce, fashion, advertising campaigns, entertainment, sport events, smart homes, people safety, waste disposal services etc.

A high-density wide area network is needed to implement the smart city concept and a lot of energy is consumed to maintain functional all its components. Alternative energy sources must be installed in the city with backup energy solutions to sustain the entire system 24/7 without interruption. Planning a smart city is not an easy task because it has to deal with traditional city structures, historical sites, old buildings and maybe a low communication capacity [3].

A smart city needs a large number of devices connected to the metropolitan network by a lot of communication equipment. The amount of data is big so cloud storage is required and a high capacity of data processing in large data centers is needed. A traditional metropolitan area network (MAN) has a mesh physical topology and it is composed by many interconnected routers, grouped in the autonomous systems of different Internet service providers.

A lot of data is uploaded and downloaded in the same time so broadband communication systems are needed. Usually, the smart city network is created in a traditional city, with an existing
communication infrastructure and all existing networks are used. The communication infrastructure 
has to be extended systematically in order to offer the network services all over the city. All 
communication and network service providers are involved in developing the demanding cooperative 
project of a smart city. External services can also be used, for example cloud storage.

Software-Defined Networking (SDN) is a performant solution to centralize the control of MAN [4]. The 
network architecture is simplified by SDN and the network management is also improved. The 
routers are replaced by less complex and faster forwarding devices that are clients of the network 
controllers. The SDN concepts applied to a smart city are described in Section 2.

The overall network security and the security of data transferred over the network are critical 
because the risks are high and the consequences of lost or false information can be serious. Therefore 
the security risk analysis for the SDN of a smart city, presented in Section 3, is important in order to 
decide which security measures should be applied.

Section 4 describes the security techniques that must be adopted in order to design a robust 
communication network for a smart city.

2. Concepts of SDN

Software-Defined Networking (SDN) concepts separates the logical control plane responsible for 
decisions made in a network from the data transfer plane that includes all forwarding devices (FD) 
such as switches and routers (R). Above all of these is the management plane (MP) that includes 
different applications (A) for routing, network virtualization or security services like access control, 
network monitoring or attack detection.

The network controllers (NC), also named network operating systems (NOS), operate the 
forwarding devices by application programming interfaces (API) that are easy to reconfigure when it 
is needed. The network controller can be implemented in a centralized or a distributed way. The 
distributed NC avoid the collapse of the entire SDN layered structure produced by the centralized NC 
falling down. The software-defined network is more flexible and more reliable than the traditional 
network. The new way of networking is characterized by centralized control and management (Figure 1).

The traditional metropolitan network, with a mesh topology, is composed by a lot of routers and 
L3-switches that embed hardware and software capabilities. Routing, switching and forwarding are all 
embedded in one device with no separation between the control capability and the data transfer 
function. Routing information is transferred from each router to other routers by using routing 
protocols.

Network service providers (NSP) manage their routers grouped in autonomous systems (AS), 
eventually partitioned into areas of routers. Core routers from one area have Internet access through 
the boundary routers that communicates with each other by a network backbone connected to the 
public network through a border router. Such a packet transport network is complex and it is hard to 
configure and to secure.
The router processors do a lot of operational tasks producing high transmission delay. Each NSP has a lot of network servers for different network services (web, file transfer, e-mail, database management, DNS, logging history, authentication, etc.) that can be in-house servers or hosted in data centers with maintenance administration employees or external IT services. There are pros and cons for all these solutions regarding their effectiveness and security. It is a better choice to use cloud servers in order to reduce the costs of software license and computing devices purchasing, of maintenance and of IT services.

Using cloud services is an improvement but the packet-switching network topology is still complicated and difficult to manage, to extent and to reconfigure. Therefore, SDN must be considered as a good solution for the network sustaining a smart city.

In order to design the network of a smart city, a macro-map has to be created. This macro-map contains different small networks interconnected by the city transport network. These small networks can be sensor networks, vehicular networks, wireless communication networks, private networks, etc. The cooperation between these networks is essential for the success of the project but it is critical regarding the security. Securing the borders of each network as part of the smart city network is very important.

Implementing the smart city network based on SDN concepts is a good strategy because the network control is centralized. An SDN controller can be programmed for each component network, all these controllers being supervised by the city management stations from the Network Operating Center (NOC). The centralized control is the key for a unitary robust wide-spread system.

3. Security Risk Analysis for a Smart City Network

The smart city network is vulnerable to a lot of attacks intended to block the communication, to steel information, to insert false data, to take control on a service or on the entire network.

The smart city offers a lot of services in many fields such as traffic control, health, emergency services, environmental monitoring, commerce, event advertising, smart homes, people safety, etc. All these services need large databases to manage the customers and a wide high-density network to communicate with them. These databases must secure personnel information. Public information must also be secured in order to avoid misinformation of people by the city network. Database applications have to be developed to manage people, devices, institutes, locations, events, facts, and all data transferred by the smart city network. Cloud servers can be used in order to have access to services from any location, on all the devices connected to the SDN-enabled smart city network (Figure 2).

Figure 2. Smart City Network.
Web applications must be developed to send information to people, on their personal smart devices or on public devices located throughout the city. Large public displays can offer visual information to people, on the street. Audio information can also be delivered on different places from the city.

Many sensors and cameras installed in the city send data to the city servers using the SDN-enabled metropolitan network [5].

All devices can get information from the network, for example, emergency applications can shut down energy or natural gas sources when an earthquake occurs.

The actuator network that is a component of the smart city network is used to turn off or on different equipment from the city area.

Traffic lights can be configured to keep opened the traffic on one street, without stopping for a period of time, when congestion is imminent or emergency vehicles have to pass.

The risks of malfunction exists in any point of the network, on all the layers of the ‘onion’ security model: physical access, logical access, service access, application and information layers (Figure 3).

![Figure 3. ‘Onion’ Security Model.](image)

Protection of people, institutions, devices, applications, information and of the entire city is the goal of the security system designed for the smart city network.

Physical risks are numerous and can involve power outage, communication link failure, equipment failure or steel, including personal devices with authorized access to restricted ‘areas’ of the network, such as access cards, smart phones, notebooks, etc.

Logical risks concern the steel of authorized user account or devices credentials. Attackers get access to various network equipment and devices and can produce many damages in the city, like traffic events, energy supply interruption, surveillance cameras shut down, servers blocking, disrupting of normal operation of a smart house or of different institutions.

Network services vulnerabilities can be exploited by attackers in order to steal information, to use them without authorization and to misinform people or officials in order to create disorder in the city, traffic congestion, false emergency calls and so on.

Financial consequences can occur by attacking the automatic toll collection network of the city. On the one hand, payment is not made and the service is used free of charge or toll collection can be redirected to other bank accounts, but on the other hand users’ banking information can be stolen if this data is not protected.

Application servers can be attacked in various ways by web attacks, SQL insert attacks, Denial-of-Service (DoS), DNS attacks, etc.

People can be targeted by cyberattacks based on social engineering methods, like phishing, that exploits the human nature weaknesses and its lack of awareness or knowledge about cybersecurity.
The real problem is that the smart city network is accessible to so many people and devices, with more or less computing resources and various security mechanisms, that it is very difficult to manage and secure all of them. Attackers will always exploit the weakest link of the system chain and thus they can get access to other more important components of the network and produce serious damages in the system.

All people connected to the network and using network services should be aware of the risk they are exposed and apply all recommended security measures with high responsability.

4. Security Measures for a Smart City Network

Risk analysis leads to a systematic security plan that includes security measures for all the components of the network [7], including in terms of Quality of Service, as the principles of trade-off between different levels for security and QoS go hand in hand [8].

An overall view of the network security shows its complexity. The division of tasks between all actors acting on the smart city ‘scene’ is a crucial choice for security efficiency.

A smart city network includes many users that access home, public or private enterprise networks. Personal device security is usually the responsibility of the owner. It is important to update periodically the device in order to run the best security software modules, antivirus, anti-spyware and anti-malware defense programs and keep it safe from today’s cybersecurity threats.

The software developers should provide updates to their application programs in order to offer the strongest security options. Automatic software update must be compulsory and not optional for all devices connected to the smart city network. Devices that do not run the latest software and have not enabled all security options should not gain access to the network. Devices must be certified in order to access a network service. Messages sent via this network should be digitally signed and message authentication codes must be used to check their authenticity by the destination node.

The network administrators have to secure all devices, users’ accounts and communication links. Basic principles of cybersecurity must be applied to users’ account configuration [6]. Principle of Least Privilege (POLP) is essential in avoiding potential damages produced by people with or without intention. Account configuration should be based on roles, seniority, place and time of the day criteria. The risk analysis conducts to a particular risk grade associated to a user or a device that is also a criterion of granting or revoking privileges. Mutual authentication is recommended in order to avoid the masquerade attack and to protect users’ credentials.

Public information and periodical training of the employed staff is very important for them to be aware of the risks to which the entire network is exposed. Public users and employees should be aware of the risk of social engineering based-attacks like phishing and to be trained to have a responsible attitude that counteracts these malicious actions.

Backup solution must be created for each component of the network like connections, forwarding devices, SDN controllers, servers, databases and human personnel.

For the energy supply sources of the city, backup solutions, including alternative energy sources, must be ready at any moment to become active in order to avoid service interruption.

Virtualization is an option for the network security. Configuring Virtual Private Networks (VPN) is a good security solution for enterprises to keep their network traffic secure, with data encryption and authorized access only [9]. VPNs can be offered as a service by the network providers.

Information protection can be ensured applying the CIA principle that means Confidentiality-Integrity-Availability. Different encryption protocols can be applied but it depends on the device’s resources and the importance of data [10]. Information redundancy can be ensured by sending it on multiple path and check its integrity after the transmission.

Servers can be ‘separated’ by installing Virtual Machines (VM) and configuring multiple virtual servers. Virtual containers can be configured to share the virtual space to many services and users.

Using cloud servers, the security of them is the responsibility of the cloud service provider. Robust security can be offered by a third part authority as a professional service with some financial costs but with the guaranty of no security incidents.
SDN allows centralizing the security measures. In this case, the number of nodes that requires higher security levels is reduced and these are the network controllers and the servers. Service orchestration is supervised by the city security staff. Network monitoring and logging history analysis is important to identify possible attacks, to detect intrusion and prevent them. For such a large network, this must be done automatically, using specialized software.

A Security Incident and Event Management (SIEM) system should be used to monitor the security of the smart city network as a whole. Being such a complex task, Machine Learning (ML) based security mechanisms can be used to secure all network components by the mean of the SDN controllers. Artificial intelligence (AI) algorithms could create behavior patterns for all the entities involved in the communication process that can be used to do automatic recognition of security events. Security scripts run by the SDN controllers can be written in different programming languages. Network programmers are responsible for the applications developed by them for software-defined networking with guarantee of security. A monitoring, alert and interventional security system have to be designed for the smart city SDN-based network in order to launch automatic countermeasures against imminent or ongoing network attacks, to quarantine risky objects from the network, to block access of intruders and to alert network administration staff to act properly on each situation.

5. Conclusions
The design of a smart city communication network is a very complex task with a lot of responsibility regarding the possible consequences of malfunction or disruption. SDN-networking is a good option for the metropolitan network design with a centralized topology. Cyberattacks are a reality of nowadays Internet and various security solutions must be adopted in order to avoid or to minimize the effects of any possible attack. A security risk analysis for the smart city network is presented. The security has to be ensured on all levels, starting with the physical one, continuing with the logical access control, users’ accounts, devices’ certificates, network services usage and, finally, ensuring the information integrity. The availability of services is an overall task of network administration that can be accomplished by continuously monitoring the network, real-time alerts, prevention mechanisms and interventional techniques. Different security techniques are recommended in order to ensure the security of the SDN-based network for a smart city.

6. References
[1] Albino V, Berardi U, Dangelico R 2015 Journal of Urban Technology 22(1) 3-21
[2] Stawiarska E and Sobczak P 2018 Sustainability 10(1318) 1-32
[3] Greco I, Cresta A 2015 International Conference on Computational Science and Its Applications Proceedings Book 563-576
[4] Kreutz D, Ramos F M V, Verisimo P E, Rothenberg C E, Azodolmolky S and Uhlig S 2015 Proceedings of the IEEE 103(1) 14-76
[5] Ceken C and Al-Hubaishi M 2019 Integrating SDN – Enabled Wireless Sensor Networks into the Internet, 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 18-21 September 2019, Metz, France Proceedings Book 1090-1094
[6] Craigen D, Diakun-Thibault N and Purse R 2014 Management Review 13-21
[7] Diaconeasca V D, Scripcariu L, Matasaru P D, Diaconeasca M R, Ignat C A 2018 IOP Conference Series: Materials Science and Engineering 374 1-10
[8] Matășaru P D, Scripcariu L and Diaconu F 2017 An up-to-date overview on QoS for Satellite IP networks Proceedings of the International Symposium on Signals, Circuits and Systems Iasi, Romania (ISSCS 2017)
[9] Scripcariu L and Bogdan I 2009 Revista de Telecomunicatii, Bucuresti 2 32-37
[10] Scripcariu L 2015 International Symposium on Signals, Circuits and Systems, Iasi Proceedings Book 1-4