Software-based Networking in Public Safety Networks

Daniela Santos Tinoco

Abstract—Public Safety Systems (PSSs) are an important part of each country's population protection and correspond to systems with which each country government worries about, but that does not always work in the best way. In times where technologies run our lives and changes the world, it seems that some of those vital systems for the society protection are being left behind and outdated. The Master Thesis described in this document intends to study the technologies, standards and solutions applicable to PSSs, with a focus on Software Defined Networking (SDN) and Network Function Virtualization (NFV) for the Public Safety Networks (PSNs), in order to present a viability study for the integration of those technologies in PSNs, and propose possible solutions for the "softwarization" of Public Protection and Disaster Relief (PPDR) communications systems.

Index Terms—Public Safety Network (PSN), Public Safety System (PSS), Emergency Networks, Public Protection and Disaster Relief (PPDR), Software Defined Networking (SDN), Network Function Virtualization (NFV)

1 Introduction

EVERY day, somewhere in the world, some catastrophe of every kind happens, fires, road accidents, earthquakes, tsunamis, events that put populations and infrastructures in risk. These populations and infrastructures need to be protected and rescued/evacuated every time that it is necessary. To do that, citizens must be capable of asking for help and rescue teams must be able to communicate with the citizens and with each other. For this purpose, each country has to have their own Public Safety Systems, in a way to protect their citizens in each accident and in each catastrophe that can happen.

The PPDR System of each country is composed by law enforcement, emergency medical services, firefighting corporations, among other important services and by a PSN that enables the emergency communications to allow to all of these forces just be able to communicate between them and with the population that they aim to protect. PPDR Systems are responsible for helping responding to emergency situations and because of that, they are a major part in Public Safety.

Communication technologies and Internet have been evolving significantly in the last few years and have remodeled our way of living and the way we see the world. So, keeping this in mind, why are many PSN still working with outdated technologies? With technology evolution, there are more and more solutions that can be applied in these kinds of systems, but due to research limitations and financial limitations of each country, the PSN are not updated as frequently as desirable.

1.1 Research Methodology

In order for the research process to be methodical and rigorous, we proposed to follow a Design Science Research Methodology (DSRM). This problem solving methodology, proposed in [1], is based on an iterative process composed of six phases, and requires the development and evaluation of an "artifact" designed to solve a problem in a given area. This artifact can be represented in several forms, but in this case it will be the viability

• *Daniela Santos Tinoco, nr. 82075,*
E-mail: danielatinoco@tecnico.ulisboa.pt,
Instituto Superior Técnico, Universidade de Lisboa.

Manuscript received September 15, 2020.

study that we carry out. The first phase of DSRM is Phase 1: problem identification and motivation. The problem of outdated Public Safety Networks is described and explained, justifying the importance that future solutions will have in preserving public safety. The second DSRM phase is Phase 2: Define the goals for the solution. As stated further, the goals for a possible solution are the modernization of Public Safety Networks using recent cellular/mobile technologies combined with other recent technologies. The third phase of DSRM is Phase 3: Design and development. In this phase the solution/artifact will be design and defined. The fourth phase of DSRM is Phase 4: Demonstration. In Demonstration phase will be described two case studies that will illustrate how the solution can be used in different emergency scenarios. The fifth DSRM phase is Phase 5: Evaluation. The solution's evaluation will be made by seeing and justifying how the architecture is able (or not) to respond to the scenarios different requirements. The sixth phase of DSRM is Phase 6: Communication. This phase corresponds to the elaboration of this document, what is the problem, how is it relevant, the artifact and its importance, relevance and effectiveness are described.

2 BACKGROUND

As described in [2], "A Public Safety Network is a communication network used by emergency services, such as police, fire brigades and medical emergency services, to prevent or respond to incidents that endanger people and/or property".

PSNs are not "mass networks" but are indeed dedicated networks and have with them a mission, usually critical, where human lives and/or important infrastructures depend on the success of information transmission.

2.1 Public Safety Networks Basic Requirements

The first requirement of a PSN is that this kind of network should never fail in a crisis, being always available and reliable. With the systems that are currently in use, this does not always happen.

Today's emergency communications mostly depend on voice communication, and in mission critical voice transfer, meaning that the time-related aspects of the voice transmission are crucial features of the emergency communications. PSSs should have the minimum delay the used technology allows. But with the evolution of communications technologies, there are other features that are becoming very useful, but that are not yet fully integrated in today's networks.

Situations where a PSN is necessary, usually have a huge diversity of people involved: citizens, rescue teams, medical staff, control center, among others. Teams with different objectives have different needs in terms of communication, so when planning and organizing a network like this, it is important to take into account all the necessary communication types. The most important types of communication in a PSN are: Multicast (and Group communications), that will allow rescue teams to communicate between them and to communicate with the control center; and Unicast, to make possible report events up in the hierarchy, being that these communications should have high priority in the network.

To make these different types of communication possible, the major PSN requirements are the geographic coverage, that should be very close to 100% in the affected area, robustness and reliability of the network, as well as resiliency of the network. In cases where it is not possible to ensure total geographic coverage it is necessary to have Device-to-Device Communication (D2D) mode, a communication type where the devices communicate directly with each other (not through the network infrastructure). Network resiliency can be affected by many external factors, such as the lack of energy, and so, another major PSN requirement is the electrical power source. A PSS cannot function without electrical power, so it is extremely necessary to ensure that the PSS power source is stable and as much as possible independent from the power distribution grid, so that power supply would not be affected by the catastrophe/disaster. It is also important to guarantee an efficient power utilization, because in some catastrophes, the

power supply can become a scarce resource without coming back prevision. To ensure the network robustness, reliability and resiliency, can be necessary to have more than the ideal devices in the network, so that the fault tolerance is secure and there are some redundancy methods (for example, having more sensors or more switches than the necessary) [3]–[5].

Due to the enormity of possible scenarios that a PSN can be used in, this kind of network must be capable to adapt itself to all the scenarios, and it has to be a pretty flexible and scalable network, because the user's number (more rescue teams and/or devices) can increase exponentially from one moment to the other. And networks have to be scalable at more than one level. PSNs have to be able to transfer diverse amounts of traffic, that can increase or diminish at any moment, have to be capable to cope with different quantities of active networked equipment and should be able to support different network protocols because different equipment may use different protocols [6], [7].

2.2 Today's Public Safety Networks

PSNs can be classified into two categories:

- **Traditional/legacy Land Mobile Radio System (LMRS) Networks:** they are based on wireless communication (specialized) systems and target terrestrial users (pedestrians or vehicles) who carry special mobile devices, such as digital radios or walkie-talkies. These types of systems use dedicated private networks that have been deployed for a specific purpose and also use a dedicated frequency spectrum, which provides more network control and high availability. These systems allow voice communication and small amounts of data transfer (but not broadband data) and have as their main objective the response to emergencies and critical communications, with the consequence of their main characteristics being: robustness, reliability and attempt at interoperability.
- **Evolved/future Long Term Evolution (LTE)-based Broadband Networks:** these systems have recently become the next technology to be used in PSSs. In addition to being more recent and with space to evolve technologically, nLTE-based networks allow very high data rates (which are not supported by any of the networks LMRS). They have as main benefits, comparing with LMRS networks, lower costs, lower latency, easy integration with other services, a fast evolution of the communication capacities and a better Quality Of Service (QoS). The main standardization project with LTE technologies is being developed by Third Generation Partnership Project (3GPP) and is described later in this document [5].

2.2.1 Long Term Evolution (LTE) Broadband

The majority of PSS today still use old and outdated technologies, but now the first efforts are being made to integrate new mobile/cellular technologies into PSS. Typically, systems like Terrestrial Trunked Radio (TETRA) use a dedicated private network to ensure the high availability and reliability of the network and the stagnation of PSS is due to the high cost of implementing an entirely new private and dedicated network for newer technologies like LTE, costs that cannot be borne by most national budgets.

The standards defined by 3GPP relate to the utilization of Fourth Generation (4G) LTE technology in Public Safety communications and in PSN. The 4G-LTE network uses a flexible air interface with low-latency and uses Frequency Division Duplex (FDD) and Time Division Duplex (TDD) as allocation methods in order to be able to support flexible channel bandwidth, which can vary between 1.4 MHz and 20 MHz (in both uplink and downlink communications). The difference between commercial LTE solutions and Public Safety LTE solutions is that LTE-based PSS should have greater availability and reliability, lower latency, different types of calls available, emergency calls, good quality communications, among other features and must meet the PSN requirements described above.

These standards advise the utilization of Orthogonal Frequency Division Multiplexing (OFDM) scheme, and control of multiple access

technologies to turn the transmissions more efficient, and also advises the use of Multiple-input Multiple-Output (MIMO) techniques in a way to improve the spectral efficiency.

Besides the LTE traditional features, 3GPP suggests some improvements specific for PSS, such as:

- Proximity Services (ProSe): LTE allows users to establish direct communication between two users using the D2D communication. The proximity services feature allows devices to discover who their neighbors are and allows them to establish optimized direct communication between them in three different ways: 1) Direct discovery, which allows the device to gather information about the surrounding devices and communicate directly with them; 2) Evolved Packet Core (EPC)-level discovery, where the device depends on the LTE network to discover it neighbours; and, 3) ProSe Relaying, service that allows to an User Equipment (UE) act as a relay between the E-UTRAN and one or more UE outside of the network coverage area, which will extend the coverage of the network.
- Group communication: allows an efficient exchange of voice and data between users of a certain group, in a controlled manner (similar to the normal Push To Talk (PTT) mode). For this, it was necessary to add a new resource to 4G LTE, Group Communication System Enabler for LTE (GCSE) LTE. This improvement includes a dedicated server in the architecture that decides which mode of data or voice transfer (unicast or broadcast) is indicated for a given situation;
- Mission critical PTT: a system that allows users to selectively and sequentially transmit messages between them, but when one of them is speaking, the only thing the others can do is listen, with permission to speak it is granted using priorities [8], [9].

The International Telecommunication Union (ITU) defined a standard spectrum allocation for PSS-LTE. The PSN-LTE should use frequencies in the 700 MHz range.

2.3 Software Defined Networking

SDN is a revolutionary way to manage and operate the traditional computer networks, i.e., the Internet infrastructure. This revolution is brought by the use of software to program all the network devices and by the centralized control of the network.

In traditional computer networks, the data plane and the control plane usually resTUde on the network device itself. The control plane is responsible for managing and updating the forwarding tables, tables that contain the necessary rules to deal with the packets forwarding. This plane is also responsible for processing various network protocols, which may have an influence on the forwarding table. The data plane is responsible for processing the incoming packets, and these packets can be buffered, scheduled, can see their header modified and can be forwarded. Using the forwarding table managed by the control plane, the data plane is able to handle most of the traffic autonomously, because for (almost) each packet, the data plane knows what action to take (this is called departure and action).

SDN has three fundamental characteristics: Plane separation, centralized control and network automation and virtualization. Plane separation consists of separating the data plane from the control plane on network devices, the data plane being maintained on each network device and the control plane being removed from those network devices. It is well known that most routing protocols used can take advantage of an overview of the network, so SDN suggests the use of centralized control. This control is done by a logically " centralized " controller, which hosts the control plan, which autonomously manages the entire network. The controller has a global view of the entire network and gives simple instructions (install rules for what is now called " Flow tables ") for network switches whenever necessary. When you remove the control plane from network devices, they become just high-speed network switches. Network Virtualization consists of the abstraction of routing details and specification details, that is, it must be possible to think about the final objective without thinking about

the physical details of the network. Network virtualization ends up reducing network costs and helps to reduce deployment time [10], [11].

To operate, SDN needs three basic components: SDN devices, controller and applications. The SDN devices have only one function, the forwarding function and also contain the data that allow the proper function of this forwarding function. This data is represented in the form of flow, flows that are defined by the controller, and each flow describes a set of packets transferred from one network endpoint (or specific set of endpoints) to another network endpoint (or set of specific endpoints). To store information for all flows, each SDN device has " flow tables ", where sets of flow entries and the actions associated with each flow entry are recorded. Thus, every time a packet arrives at a SDN device, the device searches the flow table for a match for the identified flow. If there is a match with the flow identified in the flow table, it takes the appropriate action, otherwise the SDN device sends the received packet to the controller. The communication between the SDN device and the controller is performed through the call Southbound Application Programming Interface (API). This API corresponds to an abstraction layer where the flow tables and packet processing functions reside, and these functions are different, depending on whether the network devices are virtual SDN switches or physical SDN switches [10].

The SDN controller has a real global view of the entire network, which allows to perform the best forwarding solutions. The controller is also responsible for abstracting the network from the applications. To help applications to respond to the packets that are forwarded to the controller by the SDN devices, the controller allows the applications in question to define flows that the controller will implement in the SDN devices. SDN applications communicate with the controller through the so called Northbound API, and they have as tasks to define the rules that SDN devices need in order to respond to the incoming packets, by setting and managing the necessary flows in the flow tables, managing traffic loads by the multiple possible paths and reacting to unexpected changes in the network topology.

2.4 Network Functions Virtualization

Without NFV, each time that a new network service was launched (for example a Firewall, a Network load/traffic Balancer), it was necessary to acquire new system (appliance, or server) dedicated to that new service. Besides the monetary cost of these new equipment, it also was necessary physical space and power sources capable of hosting the new equipment and it also was necessary to perform the integration capability with already existing equipment. Companies did not always have financial availability, space availability and technical skills to fulfill all those requirements.

With NFV, these problems can be addressed in a different way, because NFV allows to implement network functions and specific device functions in a virtual way, using software in non-dedicated hardware devices such as high-volume servers, switches, storage units, among others.

The NFV and SDN association can be advantageous, because they can complement each other, but no one depends on the other. NFV objectives can be reached by using traditional mechanisms, but the utilization of an SDN approach can improve the system performance, can simplify the process and it is a major help in terms of compatibility with existing systems, and the NFV can add more flexibility and can improve the SDN scalability [6], [10], [12].

3 SDN, NFV and Network Slicing

A concept that comes up when we talk about network sharing is the concept of Network Slicing. Network Slicing allows the deployment of multiple virtual logic end-to-end network, isolated from each other (Network Slices), with different requirements and different resource needs between them, over a shared common physical infrastructure. Since the Slice's intention is the creation of end-to-end networks, both the RAN and the core network can be sliced. This concept is closely connected to fifth generation networks, but is not exclusive to them. The implementation of Network Slicing

can be done based on SDN and NFV because the involvement of these two technologies brings greater flexibility and automation for the slice creation, operation and slice management.

[13] states that a possible Network Slice definition is something similar to "a set of network functions instantiated to form a complete logical network that meet the performance requirements of a service type(s)". In other words, in the end, a network slice is nothing more than a set of resources that work together to deliver the necessary features and to meet the established service requirements. One slice can be created to meet the specific necessities from a specific client or can be a more generic slice that is able to meet the requirements of multiple clients.

The necessary resources to the network slice creation and well function can be divided into two types:

1) Network Functions, that provide specific capabilities to the network so that the network can support and realize certain services and network functions are usually software instances running over physical infrastructures;
2) Infrastructure Resources, that are not more than generic hardware with the necessary software to accommodate and connect the network functions.

Virtualization is a process with major importance for slicing activity because after the available resource virtualization, is much simpler to share those resources among the existent slices.

After virtualization and separation of available resources, it is necessary to use a process that allows to manage and coordinate these resources. This process is called orchestration and as stated in [14] an orchestrator is software necessary to coordinate the various network processes used to create, manage and deliver the requested services. Open Network Foundation (ONF) [15] defines orchestration as the continuous process of collecting resources that meet customer requirements (policies and Service Level Agreements (SLAs)) in the best possible way. The orchestration function is from controller's responsibility. In network slice definition, isolation is referred as an important requirement for slicing. This isolation will allow the correct operation for parallel slices sharing a common infrastructure and isolation can be divided into three sub-types:

1)Performance isolation, being that each slice has its own specific requirements that should be achieved, regardless what is going on in other slices; 2)Security and privacy isolation, because if security treats or security failures occur in one slice, that should not transpire nor affect the remaining slices and each slice security functions should be independent; 3)Management isolation, because each slice management should be done in a independent way, as if each slice represents a different network, and the management of one slice should not affect the management of the remaining slices [14].

While there is already a lot of knowledge and research on network slicing, there is little knowledge about Radio Access Network (RAN) slicing, especially about network radio aspects managing. In the traditional SDN, the separation of the data plane and the control plane allows each equipment to make its own decisions, but this cannot be applied directly to the management of radio resources because the proximity between base stations can imply in interference if spectrum allocation is not well managed. There are some entities and work groups such as European Telecommunications Standards Institute (ETSI), International Telecommunication Union - Telecommunication (ITU-T), 3GPP and ONF working on defining standards for 5G slicing and some of those standards will be approached next. In [15], ONF elaborates a SDN-based architecture that can be applied to 5G slicing, have been ONF one of the first entities to develop a possible slicing architecture. There exist two main contexts:

1) Client context, that allows a complete resource abstraction and supports the control logic that constitutes a network slice. Inside this context exists the Resource Group that contains the necessary resource set to slice's activity and these resources are managed by the controller;
2) Server context, that is similar to the previous context mas contains everything that is necessary to interact with the available underlying resources.

The Administrator entity is responsible for the controller and for configuring the policies that will be applied by the controller. The controller is responsible for managing all available resources, for managing the existing network slices and for implementing the policies transmitted to it by the administrator. In the architecture presented, the slices are represented as an analogy to the client's context [14]–[16].

ITU-T developed the IMT-2020 Project [17] that it is dedicated to the definition of standards for the services offered by Fifth Generation (5G) networks. One of the most relevant services addressed in the document is the network slicing and it was also suggested a Framework for the slice management and orchestration. This framework can be divided into two sub-levels,

1))network slice life-cycle management level, where are included the functions used to create and manage the network slice instances, and,
2) network slice instances level, containing the functions instantiated in the actual network slices.

Of the few projects that exist on RAN softwarization, two are playing a more prominent role. A relevant one is FlexRAN [18], a platform responsible for separating the RAN data plane from the RAN control plane, through a southbound API (similar to traditional SDN). FlexRAN objective is to give a flexible control plane through the utilization of virtualization, following SDN/NFV principles. This project has two main components, the FlexRAN controller and the FlexRAN agent. The controller is connected to the agent present in each eNodeB of the network and these agents can act as local controllers because in addition to the limited view of the network they have, they deal with the control that the master controller can delegate to it. FlexRAN also uses a specific FlexRAN protocol that allows communication in both directions, so that the agent can send the status of eNodeB and relevant messages about the status of the network to the controller and for the controller to be able to transmit commands necessary for the best behavior of the agent. From the user's point of view, FlexRAN is irrelevant because it is transparent.

4 Proposed Architecture

A possible solution that respects everything that was described until this point is the utilization of an LTE network, with a simplified architecture close to the one described below. This architecture is based on the one described in [19]. This is an LTE network that can fit in different sharing situations such as: a service provider network shared with the PSS with dynamic resource allocation; a network that belongs to a private company and is shared with a PSS or a network dedicated to the many agencies part of a PSS. This network contains, beside the normal LTE elements, a SDN controller, a Software Defined RAN (SD-RAN) controller and an orchestrator. These additional elements allow a higher network programmability and flexibility, allowing the utilization of slicing. As was stated before, network slicing allows the creation and management of network slices, flexible and created on demand, with the necessary requirements for each "sub network" and isolated between them. A network with these features can respond to a variety of scenarios, with different requirements while minimizing the waste of network resources or, on the opposite hand, the lack of resources in a dedicated network. The idea is to have a shared network, possibly with one of the solutions indicated above and use network slicing to manage and allocate network resources according to the needs, So, this flexible resource management will allow a great response to PSN need in any situation and almost on demand, knowing that other network(s) who share the infrastructure with the PSN can suffer some service breaks or service quality issues in extreme situations, but this will be rare and punctual situations.

As previously mentioned, the main focus of coverage for the commercial service provider is in areas with a high population density, therefore, they will focus most of the infrastructure and ensure network coverage in those areas. This can be translated into a lack of coverage in rural and remote areas, especially in dense forests, mountains and similar places. These locations still need coverage from PSN as these

locations are at risk from some catastrophes such as fires, missing persons, overthrown, etc. For this reason, it may be necessary, in case of network infrastructure sharing, to add some Public Safety Network (PSN) exclusive eNodeb in these areas. In addition, it may be important for network redundancy to add a satellite communication link to PSN in order to guarantee communication in case of failure of other redundancy mechanisms. For the allocation of resources, the use of LTE and 5G allows the use of priorities so that the slice(s) corresponding to PSN can have more priority than other slice(s). In the remaining slices it is also possible to assign priority to certain communications. The suggested network can be divided into two parts. The core network contains the traditional LTE core network elements along generic programmable switches, controlled by a regular SDN controller. [19] suggests the use of OpenDaylight, because of its flexibility and great integration with multiple protocols.

The E-UTRAN part contains an SD-RAN controller. The most used one is FlexRAN [18], that is a platform that encompass as a controller and an agent placed in each eNodeB. This platform allows separating RAN's control and data planes through a new southbound API (such as in traditional SDN). Assisted by NFV, FlexRAN is able to manage and coordinate the various RAN entities through the new and flexible control plane.

On top of the network exists an orchestrator, responsible for coordinate both controllers, coordinate both parts of the slices and guarantee a good network function as stated before.

5 DEMONSTRATION

The first scenario corresponds to an Earthquake in an urban area scenario defined by ETSI in [20]. A scenario like this one can or can not be predicted, has a short incident time (seconds or few minutes), the response to it can last days or weeks and the actors involved in the scene belong to many different teams and organizations.

The main characteristics of a scenario like this one are the high casualties number, the damage to infrastructures that can cause access limitation to get to the victims and, due to the fact that urban areas are highly populated areas, the need of emergency services is higher than the available resources. The communications can be affected by possible damage to infrastructure (power supply disruption, destroyed Base Station (BS), among other factors) and by the high service demand of people trying to ask for help and trying to contact family and friends.

From the communications point of view, an earthquake scenario will probably be characterized by the high demand of service due to a high concentration of people in an urban area. This scenario has the advantage of being in an urban area so is probable that area has, supposedly, a good network coverage. But in an earthquake, there is a high probability of damage to the network infrastructure.

The second scenario corresponds to an Mass Transportation Accident (MTA) in a rural environment defined by ETSI in [21]. In this scenario a train collided with a road vehicle. These accidents can not be predicted, have a considerable number of victims in different states of need, the actors involved in the scene belong to many different teams and organizations, the action is limited to a confined geographic area what, joined with the state of the access, can be translated in access limitations. Communications in rural environments can present sparse communications coverage.

From the communications point of view, a scenario like this may gather more people than usual in a small area. This, in an urban environment would not be a problem, but in a rural environment it can be one because the network infrastructure is not prepared to serve many people at the same time in remote areas like the one described in this scenario. Here it will be needed to add some solution to the network to increase network serving capability for specific communications, such has the public safety agencies communications.

The requirements for emergency communications defined by ETSI are: Good quality (sufficient for good understanding) speech, short setup times for the calls and end to end delay below 400 ms and some specific services such as group communications, status monitoring

to transmit data such as vital signs, location services, data services for a diverse number of data applications that have in common the need of throughput, the need of the information arrive to the destination in a certain time frame and the preservation of data integrity.

So, how the architecture suggested above in the document is able to respond to the needs and requirements of a scenario like this one?

- As stated before, it is possible that network infrastructure fails and it can be possible lack of coverage. To address this situation, it is necessary to add one or more post-disaster network recovery solutions, like the ones described before. A good solution in a case like this one is the usage of some type of Unmanned Aerial Vehicle (UAV) immediately after the disaster to recover the network, until it is possible to place some Cell On Wheels (COW) on the ground, which can take some time due to possible access limitations.
- An architecture using recent technologies brings the opportunity of more services than the traditional ones such as real-time image and video. In this scenario, the UAVs can play other roles besides the network recovery. UAVs can be equipped with cameras and transmit live images from the air that will offer a different scenario vision to rescue teams. The images can be very useful in human resource organization, victim identification, scenario state, organizing escape routes, etc.
- The use of SDN and NFV can be very useful in a situation that involves UAVs because it the devices are able to form a network between them and this technologies are very useful in managing and controlling a network in an autonomous way. Such as in the example [22], SDN can help managing and controlling the UAV Network by giving the controller a global view of the network and take the appropriated decisions having this view in mind. This can be extremely important in matters of coverage, to adapt the UAVs position so that the main goal of providing additional coverage and allowing the network to recover from some failure can be better fulfilled.
- Network slicing will allow the allocation of resources necessary to Public Safety Network (PSN), even if that allocation implicates general population communication service break, if the network infrastructure is shared with a commercial network. Emergency communications are more relevant and priority in this scenario than the general population ones. The slice(s) correspondent to the PSN will have a higher priority than the remaining slices. This will ensure that all the communications deriving from PSN slice(s) will have priority over all other communications. Inside emergency communications slices is also possible to attribute priorities to the different types of communications that exist. The distress call from the general population can be assured by the use of communication priorities in the remaining communications inside commercial/general slices.
- The choice of LTE as the elected technology allows to positively respond to ETSI emergency communication requirements because LTE allows the usage of Mission-Critical PTT, group communications, proximity and location services and data and multimedia services, and is able to respond to setup call time and delay requirements as it was stated until now on the description and analysis of the many technologies involved. Besides that, the infrastructure that exists for LTE networks nowadays can be considered resilient and redundant and is always possible to add some mechanism such as some of the described before to add redundancy and resiliency to the network.

6 Conclusion

After analyzing the PSSs standards and technologies that are used these days, it is possible to understand that the systems utilized to protect the population still depend on outdated technologies and still have many undesirable flaws such has lack of adequate resiliency and interoperability. Public Safety Technology is an area with much room for evolution, specially

with the utilization and integration of the recent technologies. With the intensive study realized on the many technologies available in the market and the ones emerging now, it is clear that it is possible to create new and better systems to protect population.

Legacy systems like TETRA are capable of serving the basic communication needs in Public Safety matters but not much more. Recent technologies like LTE secure the basic PSN requirements, offer better network performance (latency, call establishment times, delays, data speed, ...) and offer new relevant services (geolocation, real-time image and video, ...) than legacy systems.

Besides that, recent technologies like Software Defined Networking (SDN) and Network Function Virtualization (NFV) also described in this document are a great addition to the mobile technologies because it allows the flexibility and programability of the network, what bring new opportunities in sharing networks and reducing costs.

Fortunately, some research efforts started to appear, with proposals and projects using new technologies in Public Protection and Disaster Relief (PPDR), but there is still plenty of room for innovation in this area.

ACKNOWLEDGMENTS

I would like to thank to Professor Rui dos Santos Cruz for all the guidance, help and patience during the realization of this work.

REFERENCES

[1] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 12 2007.

[2] D. Câmara and N. Nikaein, Eds., *Wireless Public Safety Networks 1*. ISTE Press Ltd and Elsevier Ltd, 2015.

[3] C. M. Machuca, S. Secci, P. Vizarreta, F. Kuipers, A. Gouglidis, D. Hutchison, S. Jouet, D. Pezaros, A. Elmokashfi, P. Heegaard, S. Ristov, and M. Gusev, "Technology-related disasters: A survey towards disaster-resilient Software Defined Networks," in *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*, 2016, pp. 35–42.

[4] V. Y. Kishorbhai and N. N. Vasantbhai, "AON: A Survey on Emergency Communication Systems during a Catastrophic Disaster," *Procedia Computer Science*, vol. 115, pp. 838–845, 1 2017.

[5] L. Borenovic and M. Simic, "Test measurements considerations for LTE as future public safety communication technology," in *55th International Symposium ELMAR-2013*, 2013, pp. 243–246.

[6] M. Wetterwald, D. Saucez, X.-n. Nguyen, and T. Turletti, "SDN for Public Safety Networks," Tech. Rep., 2016.

[7] M. Mihailescu, H. Nguyen, and M. R. Webb, "Enhancing wireless communications with software defined networking," in *2015 Military Communications and Information Systems Conference (MilCIS)*, 11 2015, pp. 1–6.

[8] A. Jarwan, A. Sabbah, M. Ibnkahla, and O. Issa, "LTE-Based Public Safety Networks: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1165–1187, 2019.

[9] B. Bertenyi, "LTE Standards for Public Safety–3GPP view," in *Critical Communications World, 21st-24th May 2013*, no. May, 2013. [Online]. Available: http://www.3gpp.org/IMG/pdf/2013_05_3gpp_ccw.pdf

[10] C. Black, P. Goransson, and T. Culver, *Software Defined Networks*. Elsevier.

[11] M. S. Olimjonovich, "Software Defined Networking: Management of network resources and data flow," in *2016 International Conference on Information Science and Communications Technologies, ICISCT 2016*. IEEE, 2016, pp. 1–3.

[12] ETSI, "Network Functions Virtualisation,An Introduction, Benefits, Enablers, Challenges & Call for Action," in *SDN and OpenFlow World Congress*, no. 1, 2012, pp. 1–16.

[13] G. Brown, "4G & 5G-Ready Network Slicing," Tech. Rep.

[14] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 80–87, 2017.

[15] Open Networking Foundation, "TR-526 "Applying SDN Architecture to 5G Slicing"," Tech. Rep. 1, 2016.

[16] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Computer Networks*, vol. 167, 2020.

[17] ITU-T, "IMT-2020," Tech. Rep., 2017.

[18] X. Foukas, N. Nikaein, M. M. Kassem, M. K. Marina, and K. Kontovasilis, "FlexRAN: A flexible and programmable platform for software-defined radio access networks," *CoNEXT 2016 - Proceedings of the 12th International Conference on Emerging Networking EXperiments and Technologies*, pp. 427–441, 2016.

[19] K. Ramantas, E. Kartsakli, M. Irazabal, A. Antonopoulos, and C. Verikoukis, "Implementation of an SDN-enabled 5G experimental platform for core and radio access network support," *Advances in Intelligent Systems and Computing*, vol. 725, pp. 791–796, 2018.

[20] ETSI, "Satellite Earth Stations and Systems (SES); Reference scenario for the deployment of emergency communications; Part 1: Earthquake," European Telecommunications Standards Institute, Tech. Rep. TS 103 260-1, 2015.

[21] ——, "Satellite Earth Stations and Systems (SES); Reference scenario for the deployment of emergency communications; Part 2: Mass casualty incident in public transportation," European Telecommunications Standards Institute, Tech. Rep. TS 103 260-2, 2015.

[22] Z. Zhao, P. Cumino, A. Souza, D. Rosário, T. Braun, E. Cerqueira, and M. Gerla, "Software-defined unmanned aerial vehicles networking for video dissemination services," *Ad Hoc Networks*, vol. 83, pp. 68–77, 2019.