Ericsson white paper
GFMC-18:000199
May 2018

Ensuring critical communication with a secure national symbiotic network

Governments that want to deploy their own dedicated networks for mission-critical communication stand to gain substantial benefits by doing so using commercial cellular 3GPP technology. This approach enables the creation of a symbiotic network configuration that is capable of addressing all kinds of critical communication needs in a society, thereby supporting both public protection and disaster relief (PPDR) and the ongoing digitalization of society.

Introduction

The ability of a government to handle crises of various kinds requires technology that supports crisis management and facilitates cooperation between the various units involved. As communication becomes increasingly mobile, the growing desire of governments to take advantage of advancements in technology, such as augmented reality and drones, is increasing the need for more bandwidth and lower delays in communication. At the same time, the digitalization of society is dependent on robust and stable communication services, with requirements in this area rising to similar levels as those of governments.

Many countries already have national strategies in place to ensure that the evolution of critical-communication networks follows the evolution of technology. These strategies recognize the need for mobile communication services that provide outstanding availability, robustness, capacity and coverage at competitive cost levels.

We strongly recommend the use of standard cellular technology and spectrum (as specified by 3GPP) to any government that wants to deploy a modern and dedicated network for critical communications with ubiquitous coverage across the country. This approach enables a government to benefit from the 3GPP technology evolution and standardized products, as well as enabling the establishment of a symbiotic relationship with commercial networks.

What a critical communication network needs to deliver

Networks built for public protection and disaster relief (known as mission critical) must be able to conduct both voice and data communications under the most extreme circumstances. Mission-critical network users require secure and robust communication in all geographical areas with guaranteed capacity, performance and quality.

Mission-critical networks have high requirements on availability, coverage, capacity, security, and quality of service (QoS). This means that these networks always need to be available and operating within the terms of strict agreements between network users and network providers. Coverage and capacity need to be extendable for mission-critical users beyond what is typically available for normal commercial users. User data, such as end-user information and content, needs to be protected by securing authentication, authorization and integrity of all communication. In congestion situations, quality and priority control are needed to avoid congestion in the network and achieve the best possible availability, coverage and capacity.

As a baseline, mission-critical users need services similar to those delivered by existing land mobile radio systems, such as mission-critical push-to-talk and short data services. Cellular broadband communication technologies include mission-critical push-to-talk, video, and data services. In addition, proximity communication services allow two users to discover each other and communicate, even when they are out of network coverage. With isolated operations, users can maintain a level of local communication in the absence of backhaul communication between the radio base stations and the more centrally located communication control functions.

Mission-critical traffic needs to be able to connect across multiple networks. Emergency response agencies require secure integration of real-time collaboration, as well as management platforms for operations, planning, command, logistics, and incident management.

Investments made in mission-critical networks that provide communication services in the most extreme circumstances will serve a small but very important number of users. However, the same networks would be an excellent resource to enable a wider scope of crisis management for society. A symbiotic network solution made up of one or more commercial networks and a governmental network could provide the required flexibility to handle all types of extraordinary situations. Non-governmental users responsible for services such as a national power grid, banks or home care could then be temporarily allowed to use the governmental network for urgent needs.

One interesting example is the case of a major forest fire that has the potential to affect power distribution to the cellular network and thus the ability to support citizens in distress. While those in distress already have the ability to call emergency numbers outside of their own service provider's coverage area, this service would be of no use if there is no power in any of the networks. The resilience mechanisms in the governmental mission-critical network, however, are significantly higher than those in commercial networks, and have power backup and redundant transmission even after several days without power. A symbiotic network solution would extend these resilience mechanisms to benefit the users of commercial networks as well.

Dedicated, secure governmental networks

New dedicated governmental mission-critical networks will strongly benefit from the use of standard technology driven by commercial networks. The governmental networks could also leverage economies of scale and today's rapid technology evolution. 3GPP is the base for cellular technologies that provide the necessary characteristics for this solution, including a strong evolution path that also takes the installed technology into account. Prior to the introduction of 3GPP technology, mission-critical users have been locked into proprietary solutions that lack basic functionality like roaming to other networks. The ability to use mass-market technology provides a wide range of benefits.

The benefits of mass-market technology are not only applicable for the network equipment, but also for the devices connected to the network. A wide range of devices are interoperable and can be extended with application-specific software. The use of device certification and field-testing providers gives users and operators confidence that devices are compliant to standards. It is also important to note that the allocation of spectrum will have an effect on the cost of both the network and on the devices. The governmental mission-critical network can use the spectrum defined in standards, which is already implemented in chip-sets and devices. Thus, the governmental mission-critical networks benefit from the advantages of scale, interoperability testing and roaming that come from commercial networks.

A wide variety of emergency agencies, associations, organizations and committees all support 3GPP LTE (Long-Term Evolution) and 5G as the preferred technology for next-generation public safety networks. Work to enhance LTE capabilities with QoS priority and preemption features started in Release 8 (2009) of 3GPP [1] and are available in products. These enhanced features allow applications to prioritize communication and enable the secure transfer of significant amounts of data. 3GPP is currently introducing 5G into its specifications for further enhancements. These include more and wider frequency bands, enabling shorter latency and higher bandwidth.

Static infrastructure

The governmental network will contain a dedicated geo-redundant core network that provides the overall control of devices and traffic in the network, including functions like subscriber management, charging and policy control. Emergency agencies' platforms for operation, planning, command, logistics, and management can be integrated using standardized interfaces to middleware or applications. Radio access networks are built using base stations in a flat architecture and redundant transmission.

[1] The 3rd Generation Partnership Project (3GPP) unites "Seven" telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC). http://www.3gpp.org/

Dynamic infrastructure

Securing coverage and capacity is one key requirement for governmental mission-critical networks. The need to provide temporary coverage indoors or in remote geographical areas like mountains can be addressed by flexibly deploying one or several extra cells directly connected to the network. The alternative is to deploy cells through relay or chains.
It is also possible to deploy static and/or mobile command centers.

Mobile units (containing local access networks or autonomous networks) will be able to temporarily increase coverage and/or capacity for communication to support full coverage, or to increase capacity. Cell-on-wheels is a concept that refers to portable base stations that are connected to backhaul and use satellite or terrestrial radio links. This concept temporarily enables increased coverage and/or capacity for communication.

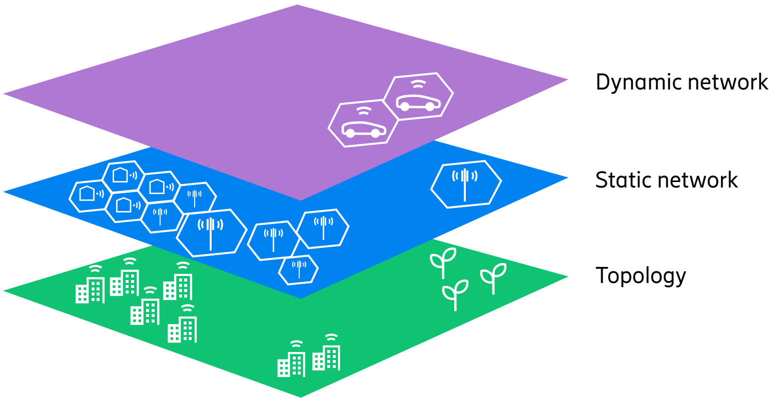

Figure 1: Governmental mission-critical network

Figure 1 illustrates the key components of a governmental mission-critical network and the relation between static and dynamic infrastructure, where the dynamic acts as a temporary fill-in of the static. A symbiotic evolution path and the sharing of infrastructure investment between governmental and commercial networks opens up the opportunity for possible technology and product reuse, site sharing and a symbiotic network model.

Configuration of a symbiotic network

A symbiotic network is a configuration that allows a government mission-critical network to interact with commercial networks to the benefit of both governmental and commercial players. A symbiotic network can achieve additional flexibility for the commercial or governmental networks when, for example, they experience problems or need additional capacity.

The evolution of technology has made it possible to develop and deploy a symbiotic network without creating unmanageable complexity or long lead times. The commercial network can act as a capacity enhancer to maintain the important functions of the society, while the governmental network can act as a shared backup network for the commercial network. The overall network architecture is visualized in **Figure 2**.

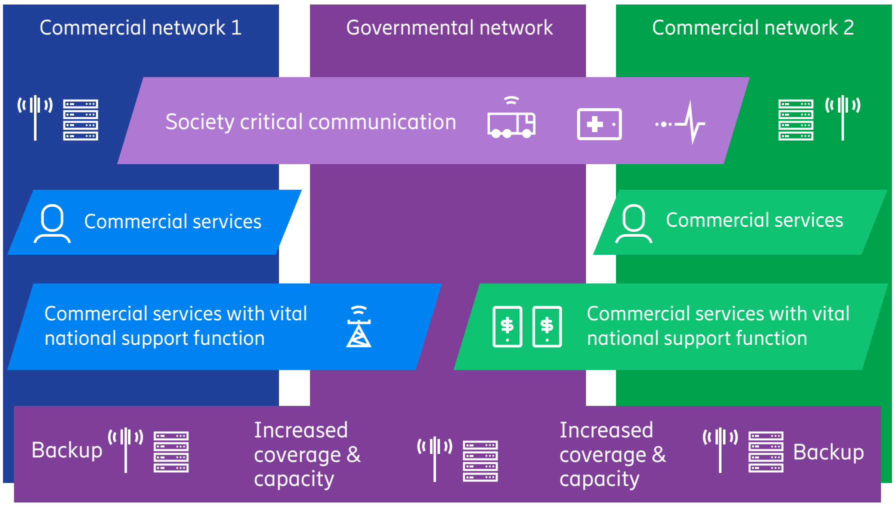
Commercial network 1
Governmental network
Commercial network 2
Society critical communication
Commercial services
Commercial services
Commercial services with vital national support function
Commercial services with vital national support function
$
$
Backup
Increased coverage & capacity
Increased coverage & capacity
Backup

Figure 2: Symbiotic network

Key capabilities

Roaming from a governmental network to commercial networks provides additional coverage and/or capacity to facilitate emergency communication. When this occurs, the symbiotic network ensures the separation and encryption of sensitive information and the prioritization of emergency cases. National roaming is particularly important when the governmental network is being deployed. The capacity boost makes it possible to meet peak traffic demands and thereby support advanced and bandwidth-hungry applications such as augmented reality, without heavy investments.

If a commercial network is experiencing an outage and is unavailable, it is important that a selected number of commercial services can be reached through the governmental network and/or that users are able to roam from commercial networks into the governmental network. This can be achieved through manual intervention or by allowing a pre-defined set of services. The services concerned can, for example, be controlled by the national power grid/plants or other vital national support functions. Another important use case that should be supported is the collaboration between mission-critical and commercial users to facilitate the formation of search and rescue groups, for example.

To increase coverage for these kinds of use cases, commercial operators could, if permitted, install equipment at government network sites. This would enable commercial operators to use the basic infrastructure, such as power supply, transmission and towers, with a high level of access and availability.

Techniques for supporting symbiotic networks

The following techniques/concepts will be useful to support both dedicated governmental networks and symbiotic networks. The techniques have been specified over the last few years and are commercially available now.

Roaming

The 3GPP standard describes several variants of roaming scenarios, with different service level agreements (SLAs) and arrangements between operators. These standards are in place and widely used to provide international roaming between partner operators, and if required, allow roaming between networks serving the same geographical region. Push-to-talk over LTE has been defined as a core service for Mission Critical Services 3GPP R13 (2016) [2]. This standard builds on the same architecture as other 3GPP roaming services, so that existing agreements and technical specifications can be leveraged.

User capabilities and service access are governed by the user's home network subscriber database. Nevertheless, the network accessed by the user can still in some detail, control and limit what the users are allowed to do. This setup is based on a trust relationship between the visited network's operator and the home network's databases. The visited network can block individual services or limit data volumes.

On the network level, exchanging information between the visited and the home network requires connectivity for both the actual user traffic, but also for network signaling. Due to the sensitive nature of a dedicated mission-critical network, any roaming between it and commercial cellular networks requires special care when setting up the connections. In addition to standard IT technologies, such as firewalls, protection against distributed denial of service, or IPsec virtual private network technologies, firewall vendors have developed special features to provide application-level supervision of diameter or SS7 signaling connections. Additionally, telecom applications provide enhanced security features directly on the application level, such as peer IP address validation or topology hiding. Combining all these provides a sufficient security level to the control layer of these networks.

Network slicing and user management

Additional needs can be addressed by extending roaming capabilities with network slicing. Wireless standards and networks have long included mechanisms that logically partition the network and share a network between multiple providers, which is often referred to as "network sharing". Such mechanisms can also be used in the creation of symbiotic networks. Recent technology advancements such as virtualization, software defined networking (SDN) and automation have allowed network-sharing concepts to evolve, adding more flexibility and versatility. The resulting architectural paradigm is referred to as "network slicing", in which a set of logical networks known as "network slices" are realized on top of a shared network infrastructure.

Each network slice is designed to fulfil its requirements, which means they can be differentiated to support different transmission characteristics (such as bandwidth and latency), different levels of isolation from other network slices (such as different degrees of sharing of resources between the slices), different levels of robustness and operational isolation, and so on.

As network slices are logical, they are not limited physically, and can therefore be realized on top of an infrastructure layer that encompasses several parties. In the case of a symbiotic network, network slices can consequently extend over the commercial infrastructure and the governmental infrastructure, as illustrated by **Figure 3**.

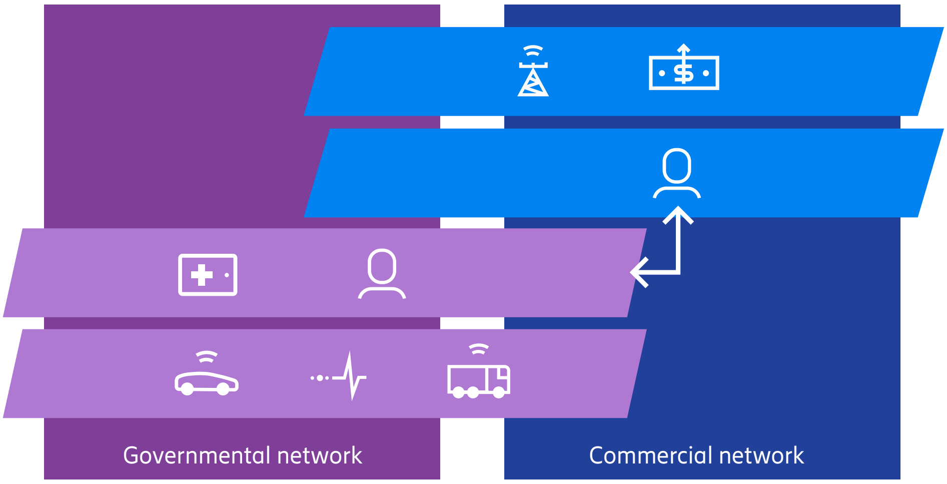

Figure 3: Network slicing for symbiotic networks

In the context of symbiotic networks, network slicing enables the following example scenarios:

- A network slice operated by a commercial provider may use resources that are provided by the governmental network. For example, the governmental network may have resource partitions that are associated with the commercial provider and may have selection mechanisms that allow access to the commercial network slice through the governmental network. An example of this can be the control of electricity distribution.

- A network slice operated by the government could use resources that are provided by commercial networks. In this case, the commercial network is set up with resource partitions that serve the governmental network slice and allows them to be "selected". The purpose of this is to enhance the governmental network with additional capacity and/or coverage.

- Users and devices are associated with and allowed access to network slices. This is made possible through mechanisms of "slice selection" that are built into the network, as are provisioning subscriber databases. A search and rescue operation is one example of when this can be useful.

A network slice is, in its nature, isolated from other network slices. As a result, it can be set up with a higher level of security (separate VPNs, stronger firewall protection, and so on) compared to other network slices. This is an improvement compared to a more monolithic network where tradeoffs must be made to match the varying needs of different services. When required for highly sensitive services, network slices can be assigned dedicated resources (such as data center resources).

On the user/device level, it is possible to let a device/user that normally uses a commercial network slice and service to gain temporary access to one of the governmental network slices. This can be handled by dynamically changing the policies for how user sessions are directed and authorized in the network. New network mechanisms associated with network slicing simplify this.

While some of these scenarios would have been possible in the past using PLMN selection mechanisms, network slicing technologies add a much higher degree of flexibility as well as enabling new scenarios. The ability to orchestrate and automate across commercial and governmental actors is crucial. In the past, it would have been almost impossible to execute these services – the use cases quickly became too complex, costly or impractical, due to the large need for manual operations (to set up new services, move subscribers, and so on).

Capacity and coverage

Today's LTE networks offer a broad range of network capacity with reliable and proven geographical coverage. Future 5G radio access technology will address high traffic growth and increasing demand for high-bandwidth connectivity. It will also support massive numbers of connected devices and meet the real-time, high-reliability communication needs of mission-critical applications. This will be realized through the development of LTE in combination with new radio access technologies (such as 5G NR and narrowband IoT) and existing ones (such as Wi-Fi).

In general, 5G networks will not be based on one specific radio access technology. Key technology components include the use of higher frequency bands (e.g. millimeter-wave), flexible spectrum usage (such as multi-band operation, spectrum sharing and the use of unlicensed spectrum), multi-antenna transmission (such as transmit beamforming and beam tracking to increase spectral efficiency and reduce interference) and ultra-lean design to reduce protocol overhead.

These high capacities and beamforming can also help increase the coverage of the mission-critical network in case of disaster or emergency situations. Ad-hoc base stations can be deployed quickly and can reuse existing LTE or 5G capacity on site, to be relayed back to existing base stations. Advanced auto-integration features currently being rolled out in both baseband and transport equipment support the quick addition of these ad-hoc stations.

On top of the quick addition of ad-hoc base stations, 3GPP also specifies Proximity Services, which are services that relay network connectivity. For example, Proximity Services can relay network connectivity from a device in an emergency vehicle located in front of a building to devices with bad coverage inside that building, effectively extending the reach of a public safety network.

Positioning

In public safety, positioning capabilities are vital for locating mobile emergency callers, communication devices of rescue personnel, or specific resources or equipment connected to the network. Today's mobile broadband devices and networks support a large variety of indoor and outdoor positioning techniques that can be leveraged for both emergency callers and rescue personnel to achieve network positioning accuracies in the sub-10m range, depending on satellite visibility and device capabilities.

Positioning accuracies in the range of 100-200m can be reached using low-cost devices that do not contain functionality, such as satellite receivers. When more modern technologies are deployed, they can typically deliver a positioning accuracy of approximately 10-50m without the use of device-level satellite navigation.

Greater availability of low-cost sensors and communication equipment in the near future will allow additional use cases, such as the distribution of sensor devices by plane into geographic areas impacted by radioactive contamination, flooding or fires. The assessment of the geographical spread of such disasters will then be based on measurements sent by the sensors and their position given by the network.

Conclusion

The idea of using commercial technology for mission-critical, emergency services has not been successful in the past because commercial technology lacked a number of important capabilities. Today, however, all the necessary technology is in place, namely: high-capacity radio (LTE), an evolution path to even more capable radio (5G), virtualization, software defined networking, automation, network slicing, positioning, proximity communication, the ability to prioritize communication and secure data transfer.

In light of this, Ericsson recommends that any government that wants to deploy a dedicated network for mission-critical communications use commercial mainstream technology (3GPP 4G/5G) to do so. The main benefits of using standard cellular technology to build mission-critical networks is that doing so makes it possible for governments to use well proven products, take advantage of the ongoing evolution in the telecom technology area, and gain a cost advantage. Commercial and governmental networks also stand to mutually benefit from their respective investments by deploying a symbiotic network configuration.

Glossary

3GPP	Third Generation Partnership Project
5G	Fifth Generation Cellular System
IoT	Internet of Things
LTE	Long Term Evolution
NR	New Radio
PLMN	Public Land Mobile Network
PPDR	Public Protection and Disaster Relief
QoS	Quality of Service
SDN	Software Defined Networking
SLA	Service Level Agreement
SS7	Signaling System Number 7
VPN	Virtual Private Network

References

1. 3GPP, Mission Critical Services in 3GPP, available at: http://www.3gpp.org/news-events/3gpp-news/1875-mc_services

2. 3GPP, SA6 – Mission-critical applications, available at: http://www.3gpp.org/specifications-groups/sa-plenary/sa6-mission-critical-applications

Further reading

1. Ericsson, Mission-critical and private networks, available at: https://www.ericsson.com/ourportfolio/networks-solutions/mission-critical-and-private-networks

2. Ericsson, Response redefined – ICT and the future of public safety, white paper (2016), available at: https://www.ericsson.com/en/white-papers/response-redefined--ict-and-the-future-of-public-safety/white-paper--response-redefined

Contributors

The contributors to Ericsson's opinion on this topic are Håkan Djuphammar, Nicklas Spångberg, Christoph Meyer and Henrik Basilier.

Håkan Djuphammar
Håkan Djuphammar has held a variety of positions within Ericsson since 1991, both in Sweden and abroad, and currently serves as Head of Special Projects at the company's CTO office. He holds a number of patents and played a key role in the establishment of the 3G standard. Before joining Ericsson he was co-founder and President of Abstract Electronics AB. He has an M.Sc. in Telecommunications from Imperial College in London and an electrical engineering degree from Chalmers University in Gothenburg, Sweden.

Nicklas Spångberg
Nicklas Spångberg is a senior solution architect with more than 12 years of experience in mission-critical communications. Over the years, his responsibilities have ranged from complex technical assignments delivering architecture and functional requirements, through to business and solution development, targeting the transition from today's narrowband to next-generation broadband networks for mission-critical communications. Prior to joining Ericsson, Spångberg was the technical solution manager for a major system vendor delivering the Swedish national digital communication system for emergency services.

Christoph Meyer
Christoph Meyer holds a Dr. rer. nat. in Physics from RWTH Aachen University in Germany and currently works as a networking expert within Ericson's development unit Networks. Since joining Ericsson in 2000, he has focused on IP networking and end-to-end solutions in the areas of mobile core connectivity and mobile broadband. His current work focuses to a large degree on technology trends and their relevance for the Ericsson product portfolio, most notably in the areas of cloud, NFV and SDN. Meyer holds six patents and seven patent applications.

Henrik Basilier
Henrik Basilier holds an M.Sc. in Computer Science and Technology from Linköping University in Sweden. He has 25+ years of experience in the telecom industry, with experience spanning a wide range of technology areas and positions, including packet core networks, cloud technologies and OSS. He currently works as an expert on network architecture evolution, focusing on 5G networks and applications, and how network slicing can act as a key enabler for these new opportunities.