eit Knowledge & Innovation Community

EIT ICT Labs

Technical Foresight Report

Safety of Digital Cities

Manel Bourguiba, Khaldoun Al Agha

TDCT 2012

Technical Foresight Report on Safety of Digital Cities

Manel Bourguiba and Khaldoun Al Agha

2012-12-21

Executive summary

This report aims to identify trends, challenges and recommendations in regard of Safety of Digital Cities. This foresight will help expose future themes with high innovation and business potential based on a timeframe roughly 15 years ahead, or 2030! The purpose is to create a common outlook on the future of ICT and to establish a strong community across EIT ICT Labs nodes and partner organizations.

Trends

1. Widespread sensors in digital cities
2. Always connected citizens and smart phones acting as sensors
3. Powerful geo-localization applications
4. Security agents' intervention requires not only voice communications but also multimedia content exchange services
5. LTE is a promising technology for reliable and high bandwidth radio telecommunications

Challenges

1. Reluctant citizens may not be willing to participate in the sensing activity
2. A high performance network for mobile private communications is required for an efficient security forces intervention
3. Coverage and spectrum allocation issues in private mobile radio telecommunications

Recommendations

1. To exploit advances in LTE in order to enhance private mobile radio communications
2. To deploy new auto-adaptive spectrum allocation schemes
3. To use network coding technology in order to improve private mobile radio communications performance, robustness and security
4. To leverage ad-hoc networks to mitigate coverage problems
5. To incite citizens to cooperate and make them participate in the sensing activity in order to predict crisis

Citizens' cooperation and highly efficient and reliable radio telecommunications are keys to enabling safe digital cities. Security forces rely on information collected through sensors spread in the city or sent by collaborative citizens through their smart phones to predict security attacks. Furthermore, during their intervention, security agents make use of reliable and performant radio telecommunication systems to communicate and exchange data at high rates. Enhanced with recent advances in mobile communications through the LTE standard, private mobile communications represent a viable solution to enable security agents to communicate in order to efficiently coordinate their intervention.

Document Details

Action Line:	Digital Cities of the Future
KIC Activity Name:	Innovation Radar
KIC Activity Identifier:	TDCT 12185
Task:	T01
Catalyst:	Innovation Radar
Deliverable:	D6
Type:	Technical Foresight Report
Date:	2012-12-21
Status:	Final
Partner:	Paris-Sud University
Editor:	Manel Bourguiba and Khaldoun Al Agha

Contributors

Manel Bourguiba – Paris-Sud University
Hassan Noura – Paris-Sud University
Steven Martin – Paris-Sud University
Khaldoun Al Agha – Paris-Sud University

Table of Contents

Executive summary 2

Document Details 4

Contributors 5

Table of Contents 6

1 Introduction 7
- 1.1 Outline 7
- 1.2 Citizens safety in digital cities 7
- 1.3 A reliable radio communication system for a safe digital city 10
- 1.4 Scenarios 12
- 1.5 PMR enhancements: expected technological results 13

2 State-of-the-Art 14
- 2.1 Private mobile radio communications 14
- 2.2 LTE radio advances adaptation to PMR 16
- 2.3 An optimal frequency allocation for enhanced PMR 18
- 2.4 Network coding for robust and secure PMR 23

3 Foresight Results 32
- 3.1 Trends 32
- 3.2 Challenges 32
- 3.3 Recommendations 32

4 Conclusions 33

List of Acronyms 34

References 35

1 Introduction

This technical report is part of the EIT ICT Labs Foresight Study and Innovation Radar within the thematic action line of Digital Cities of the Future (TDCT).

The report aims to identify key scenarios, trends, challenges and recommendations in regard of Safety of Digital Cities. This foresight will help expose future themes with high innovation and business potential based on a timeframe at least 15 years ahead, or 2030! The purpose is to create a common outlook on the future of ICT and to establish a strong community across EIT ICT Labs nodes and partner organizations.

1.1 Outline

Chapter 1 gives an insight on the safety process in digital cities, highlights the necessity of an appropriate telecommunication system to guarantee citizens' safety and presents scenarios for safety services based on radio communications. Chapter 2 focuses on the security intervention process. It provides background information on private mobile telecommunications and their enhancement with technological advances achieved in LTE and network coding in order to meet the safety requirements. Chapter 3 presents trends, challenges and recommendations with a 2030 baseline in mind. Chapter 4 draws conclusions for future EIT ICT Labs activities.

1.2 Citizens safety in digital cities

1.2.1 Digital cities concept

The rapid growth of the cities yields new challenges spanning from the social to the technical point of view. Because the world becomes more and more urban [13], because the population density exceeds more than 5000 inhabitants per km^2, as the life today requires to be always connected to social networks, and as citizens safety is a crucial issue to improve the quality of life in cities, traditional safety processes and services should be redefined [19].

The concepts of Digital and Smart Cities are being constantly refined and expanded to describe the future of major developed cities in a world where a large majority of people live in urban areas. Many actors are innovating, exploiting ICT for improving our cities sustainability, efficiency and quality of life, as illustrated by the 2010 universal exposition in Shanghai ”Better City, Better Life” [14].

The general philosophy of Smart Cities [15, 16, 17] is a paradigm shift combining Internet of Things and Machine to Machine infrastructures with a User or Citizen

Centric model, all together leveraging massive data collected by sensors, connected devices, social applications, etc. Institutions, including European Union and NSF, therefore foster public initiatives, industrial development as well as research on finding breakthrough technologies for automatic and efficient management of energy networks, e.g. smart grids, regulated and sustainable mobility, real-time democracy and transparent government, added-value and citizens' safety, etc.
In the remainder of this report, we will focus on citizens' safety in digital cities.

1.2.2 Security process

Security forces refer to any governmental forces that are in charge of protecting people from any threat on their safety and of establishing the order in the city. Security forces can be the national police agents, the municipality policemen, firemen, etc. Their exact role and responsibilities and their organization may change from one country to another. Security forces are on the same side as the citizens but against other citizens that threaten the public safety. Although our report is largely inspired from the current French security forces model, we believe it can be quite easily generalized to other countries. From the security forces perspective, ensuring the citizens' safety is a continuous process that involves the operations detailed below. The same process will be used in the future digital cities. However, the means and the technologies that will be leveraged will evolve as detailed in the remainder of this report.

1) Prevention: security forces continuously try to predict any potential safety threat like terrorist attacks, robberies, violence, fire, etc. They collect relevant information that they analyze in order to estimate potential dangers. Collecting the information is nowadays mainly achieved through cameras spread in the city and connected to the police office that monitors in real time the activity reported in the videos. It can also be achieved through sensing the environment by spreading sensors in the city. The sensors offer the means to security forces to monitor people activity in the city in order to stay aware of any unusual behaviour. Sensors are nowadays mainly used for traffic monitoring in highways or downtown to give information about jam in some areas. In a future digital city, collecting the information can also be achieved through the participation of the citizens themselves. Equipped with smart phones that are enhanced by high geo-localization capabilities, citizens can be part of a participating sensing. In this case, they spontaneously inform the security agents of any feeling of vulnerability, any suspect behaviour or in opposite report that nothing unusual is happening in their area. Citizens can also participate in an opportunistic sensing, in which case the security forces exploit their smart phone as a sensor and extract information about their localization, their movement direction, or any other information that can be useful in determining the mobility patterns of people in the city, the density of some areas or in controlling special events, etc.

2) Data analysis: the collected data will then feed a database located at the security office. The analysis of this data allows the security agents to determine whether

threats to citizens' safety exist. The analysis is performed on different types of data: video clips, audio sequences, or textual data. In a future digital city, textual data can be for example, tweets of citizens sent by people located in the same area and reporting on the same event. This provides useful information to security agents to control special events like strikes or important sportive events, etc. Complex processing might be performed on collected photos and videos like facing recognition, fingerprinting identification in order to identify people involved in security threats. Collected video clips can help the agents to rapidly react to catch people involved in violent attacks, robberies, etc.

3) Intervention: the analysis results will enable security agents to make decisions on whether an intervention is necessary or not. The intervention has to be fast and efficient. Hence a reliable and performant network is required so that the agents could coordinate their intervention. The coordination requires radio communications between the agents as well as communications with the security office to get information, perform data base inquiries, or to receive instructions from their hierarchy.

4) Evacuation: the intervention is followed by an evacuation of the citizens located in the crisis area. The security agents can use radio telecommunications to broadcast instructions in order to organize the evacuation. These instructions are built based on the information that the security agents get through the environment sensing (either opportunistic or participative sensing). The instructions are mainly intended to inform people about the direction they should follow in order to evacuate (emergency exit, load balanced gates, closest gate in a stadium, etc.).

1.2.3 Urban sensing for safety in digital cities

In future digital cities, guaranteeing safety of citizens is henceforth a collaborative task where both security forces and citizens cooperate in order to predict and prevent safety threats and facilitate the safety agents' intervention when necessary. The citizens can mainly help through participating in the data collecting process through urban sensing.

Besides dedicated and deployed sensors and actuators, still required for specific sensing operations such as the real-time monitoring of pollution levels, there is a wide range of relevant urban data that can be collected without the need for new communication infrastructures, leveraging instead on the pervasiveness of smart mobile terminals. With more than 80% of the population owning a mobile phone, the mobile market has a deeper penetration than electricity or safe drinking water [18]. Originally designed for voice transmitted over cellular networks, mobile phones are today complete computing, communication and sensing devices, offering in a handheld device multiple sensors and communication technologies.

Mobile devices such as smartphones or tablets are indeed able to gather a wealth of information through embedded cameras, GPS receivers, accelerometers, and cellular, WiFi and Bluetooth radio interfaces. When collected by a single device, such data may have small value per-se, however its fusion over large scales could prove critical for urban sensing to become an economically viable mainstream paradigm.
This is even more true when less traditional mobile terminals are taken into account: privately-owned cars, public transport means, commercial fleets, and even city bikes are starting to feature communication capabilities and the data they generate can bring a dramatic contribution to the cause of urban sensing. Beyond letting their own devices or vehicles autonomously harvest data from the environment through embedded or onboard sensors, mobile users can actively take part in the participatory sensing process because they can, in return, benefit from citizen-centric services which aim at improving their experience of the urban life.

The data generated from the urban sensing can be used by authorities to improve public safety services. However, in order to kindle this hidden information, important problems related to data gathering, aggregation, communication, data mining, or even energy efficiency need to be solved first.

This technical foresight report focuses on the intervention step in the security process and highlights the necessity to provide a reliable and performant network access to security agents in order to make the intervention successful. Private Mobile Radio telecommunications (PMR) represent a viable technology that offers telephony services and enables security agents upload and share data with pairs or with a remote office to make the adequate decisions of evacuation. However, PMR exhibit poor performance mainly in terms of uplink throughput. Next, we identify the challenging issues facing an efficient deployment of PMR. Then, we propose some solutions to adapt the recent advances achieved in radio technology to PMR context in order to optimize its capacity. The optimization is based on an adaptation LTE radio technology bricks, the use of network coding technology and the judicious allocation of the frequency spectrum.

1.3 A reliable radio communication system for a safe digital city

Security business is constantly increasing leveraging more and more sophisticated information systems and technologies. Radio telecommunications technologies leveraged by safety services like national police and fire brigade include dedicated mobile radio telecommunication systems called Private Mobile Radio telecommunications (PMR). These systems allow to safety agents to communicate either with each other or with a remote control center during their intervention.

PMR are networks that offer telephony services for security forces in a very limited spectrum. They fall into the narrow band networks category and are largely inspired

from the cellular networks concept (especially GSM). They offer a voice service and a very low bandwidth data transfer service of 4 kbps.

PMR share the spectrum with other private narrow band mobile networks and are deployed on a limited band of radio frequencies. This makes big volumes of data transfer impossible with this kind of networks. An adequate radio solution is hence necessary in order to efficiently make use of the scarce available radio frequencies and improve these networks' capacity, performance as well as robustness.

The future of PMR will definitely involve not only voice communication and text messaging but also multimedia services such as data, images, video, live feeds, face recognition and database queries [1] [2] [3]. The evolution of the security services from voice calls to more bandwidth greedy services has a straight impact on the requirements concerning the dedicated radio telecommunication systems. Traditional PMR exhibit a poor performance and do not meet the new services requirements in terms of bandwidth. A more efficient, reliable, high bandwidth network is then required in order to help security agents react more efficiently and rapidly in case of crisis like fire or accidents or when managing the security of special events like sport events or strikes, etc.

There are two possible actions in order to overcome this limitation. The first one is to struggle in order to get a non-shared spectrum by actively participating and lobbying in the frequency management organisms. The second one is rather based on technological innovation and aims at least at relaxing some constraints related to the spectrum usage in some scenarios. We indeed recommend the second solution, which is based on technological innovation.

Our recommendation is motivated by the capabilities offered through recent technological advances in the telecommunication field. In fact, technological advances achieved in civil mobile networks through LTE and LTE-Advanced are interesting and can be exploited to enhance PMR with new capabilities. Furthermore, network coding has recently emerged as the future technology that makes use of cheap processing power to increase the network efficacy. In fact, communication networks today share the same fundamental principle of operation. Whether it is packets over the Internet, or signals in a phone network, information is transported in the same way as cars share a highway or fluids share pipes. That is, independent data streams may share network resources, but the information itself is separate. Routing, data storage, error control, and generally all network functions are based on this assumption. Network coding [4] is a recent field in information theory that breaks with this assumption. Instead of simply forwarding data, nodes may recombine several input packets into one or several output packets.

Network coding is a new research area that may have interesting applications in practical networking systems. With network coding, intermediate nodes may send out packets that are linear combinations of previously received information. There are two main benefits of this approach:

- Throughput improvements
- High level of robustness.

Robustness translates into loss resilience and facilitates the design of simple distributed algorithms that perform well, even if the decisions are based only on partial information. In the next chapter, we will give an instant primer on network coding: we will explain what network coding does and how it does it.

The objective is then to make use of the existing radio standards such as LTE and to find solutions to the still open issues with PMR. The main problem is related to the sharing of the frequency spectrum with existing narrowband mobile networks. Another problem rises up especially because LTE was conceived for larger frequency bands than what is actually available. This makes the application of advances achieved with LTE not straightforward.

In the next chapter, we will highlight the challenges related to an efficient use of the frequency spectrum in the case of cohabitation between PMR and other mobile networks and the adaptation of technological advances of LTE to the requirements of PMR. Then we will detail our recommendations concerning the enhancement of PMR networks. These recommendations fall into three parts. The first one deals with the optimization of the frequency spectrum allocation within PMR. The second one is related to the adaptation of radio technologies bricks of LTE to the context of PMR. Finally, the third one is about the adoption of network coding technology.

1.4 Scenarios

One can imagine multiple scenarios in a digital city where security forces can intervene in emergency and make use of ICT in order to successfully accomplish their mission. In order to understand the necessity of enhancing PMR for security forces communications, we consider the following scenarios:

1. In some cases, some information can be provided to mobile users so as to enforce their mobility: drivers can be alerted of the arrival of an emergency vehicle so that they leave the leftmost lane available, or participants leaving vast public events can be directed out of the event venue through diverse routes displayed on their smartphones so as to dynamically balance the pedestrian flows and reduce their waiting times. Enhanced PMR hence represents the radio telecommunication network that will vehicle the information to the mobile users.

2. A police agent uses a dedicated mobile network to upload the photo of a suspect and sends it to a remote police centre to be stored and processed. The processing aims at promptly identifying the person involved in the security attack. Getting this information as soon as possible enables the police officer to rapidly broadcast the photo and take the adequate decisions. There are multiple other scenarios where a rapid sharing of information like video clips or photos between security agents like firemen helps them achieve a better coordination and organization of their intervention. A fast sharing of this data with traditional PMR would not be possible due to the poor bandwidth offered by this type of technology. Therefore, reliable and optimized network access is a key to ensure safety in the digital cities.

1.5 PMR enhancements: expected technological results

The enhancements of PMR are expected to resolve issues related to coverage, spectrum efficiency and low bandwidth. Precisely, the proposed solutions and recommendations are expected to achieve the following improvements:

1) The opportunistic access to the radio resource with regard to the mobile requirements is expected to allow a capacity enhancement of 2.5 Mbps to 5 Mbps for a 5Mhz channel, depending on the considered scenario.

2) The adaptation of the wave based on filtering is expected to further improve the offered capacity by at least 2 Mbps within a 5Mhz channel, already shared with the existing narrow band technologies.

3) Leveraging MIMO/SIMO techniques in the band of 400 Mhz should allow a gain of 4 to 5 dB.

4) The joint optimization of physical and application layers for voice and video flows should allow freeing 30 to 50% of the initial spectrum.

5) Network coding is expected to improve networks security and robustness and throughput by at least 50%.

2 State-of-the-Art

2.1 Private mobile radio telecommunications

Private Mobile Radio telecommunications (PMR) are field radio communications systems, which use portable, mobile, base station, and dispatch console radios. Operation of PMR radio equipments is based on standards such as MPT-1327, TETRA and APCO 25, which are designed for dedicated use by specific organizations, or standards such as NXDN intended for general commercial use. Typical examples are the radio systems used by police forces and fire brigades. Key features of professional mobile radio systems can include:

1. Point to multi-point communications (as opposed to cell phones which are point to point communications)
2. Push-to-talk, release to listen: a single button press opens communication on a radio frequency channel
3. Large coverage areas
4. Closed user groups
5. Use of VHF or UHF frequency bands

When PMR first started, the systems simply consisted of a single base station with a number of mobiles that could communicate with this single base station. These systems are still in widespread use today with taxi firms and many others using them for communication. Because the antenna may be mounted on a high tower, coverage may extend up to distances of fifty kilometers; this is even helpful especially when there is no signal in a GSM mobile phone.

Licenses are allocated for operation on a particular channel or channels. The user can then make use of these channels to contact the mobile stations in their fleet. The base station may be run by the users themselves or it may be run by an operating company who will hire out channels to individual users. In this way a single base station with a number of different channels can be run by one operator for a number of different users and this makes efficient use of the base station equipment. The base station site can also be located at a position that will give optimum radio coverage, and private lines can be provided to connect the users' control office to the transmitter's site. As there is no incremental cost for the transmissions that are made, individual calls are not charged, but instead there is a rental for overall use of the system. For those users with their own licenses they naturally have to pay for the license and the cost of purchase and maintenance of that equipment.

The future of PMR involves not only voice communication and text messaging but also multimedia services such as data, images, video, live feeds, face recognition and database queries. All these services can be made available in a single pocket-size device like the Thales Every Talk smartphone. However, traditional PMR exhibit

a poor performance and do not meet the new services requirements in terms of bandwidth. Hence, in order to satisfy the evolution of the security agents' needs, these networks are required to offer higher throughputs that allow a high bit rate transfer of multimedia content. Uploading a video clip from the event location in order to be stored and processed at the remote decision making center. So PMR optimization is necessary to guarantee safety of the citizens in the digital cities of the future.

A good choice of the underlying radio technologies is determining of PMR efficiency. Recent advances achieved in radio mobile networks through LTE and LTE-Advanced technologies are promising since they allow a data transfer service at a high throughput. Enhanced by new techniques like Multiple Input Multiple Output (MIMO), and Hybrid Automatic Repeat reQuest (HARQ), these technologies are expected to enable throughputs reaching 300 Mbps and even 1Gbps. However, such throughput is only achievable on a wide spectrum of up to 20Mhz and 100 Mhz for LTE and LTE-Advanced respectively. Nevertheless, it is not possible to apply LTE and LTE-Advanced technologies as are in the context of PMR for the following reasons:

1) A lower carrier frequency for PMR: LTE and LTE-Advanced technologies operate at the high carrier frequencies of 900, 1800, 2000 and 2600 Mhz whereas PMR have been historically operating at the carrier frequency of 400Mhz. This band allows a better coverage. However, MIMO techniques, used with LTE are shown to be inefficient with this frequency. In fact, MIMO techniques cannot use more than two antennas in the transmission as well as the reception side. In order to achieve acceptable gains, a strong de-correlation between the antennas is required. Obviously, this de-correlation is achieved through the adjustment of the distance separating the antennas. But since the distance between the antennas is characterized in terms of wave length, which itself depends on the carrier frequency, it is quite impossible to use more than two antennas with PMR (at 400 Mhz).

2) A narrower band: PMR are also characterized by a very narrow located at a very busy part of the spectrum. Historically, PMR users' needs have been limited to voice services. Usually operated in a Frequency Division Duplex (FDD) mode, PMR use two bands of 5Mhz (one for the UpLink and one for the DownLink). Although LTE has been designed with multi-band in mind (1.4, 3, 5, 10, 15 and 20 Mhz), it is shown to exhibit poor performance with low frequencies. Some adjustments are then necessary in order to make it as efficient as with wide bands.

3) Higher transmission power: PMR systems usually use higher power transmitters than traditional mobile networks in order to increase the coverage area. This coverage is generally limited by the uplink. PMR equipments usually transmit at 2, 5, 10 and 20 W. LTE terminals power is limited to 250mW and hence are not appropriate. The terminals should then also be adapted.

4) Different operating modes: PMR and Public Land Mobile Networks (PLMN) based on LTE, UMTS or GSM operate in different modes: in PLMN, most of the communications fall into the point-to-point mode. Whereas in PMR, the point to multipoint mode is the most used. In this mode, only one resource is used and dedicated to the user that is talking and N resources are allocated in the downlink for the rest of the network users. A broadcasting system is then locally used in the cell. LTE does not deal with the point-to-multipoint mode. However, it is possible to exploit some features of the eMBMS (Multimedia Broadcast Multicast Service) system used with LTE for broadcast. These features should nevertheless be adapted to the context of Group Call in PMR since they have been designed especially with television broadcast issues in mind. Furthermore, PMR allow direct communications between terminals, which allows an ad-hoc communication, without any infrastructure. Such a mode allows participants to the same safety mission to communicate and exchange data directly even in the absence of the infrastructure. This feature is unfortunately not present with LTE.

5) Different dimensioning policies: both LTE and PMR require a set of techniques in order to optimize the resource allocation through a judicious frequency reutilization. However, this issue is much more challenging with PMR networks. In fact, scenarios with a high density of PMR users in a small part of the cell occur quite frequently because of special events. Then, a deeper study should be conducted in order to optimize resource allocation techniques. This optimization may be achieved through adding a supplementary base station either temporarily or permanently.

As a conclusion, with regard to the choice of radio solutions for PMR, LTE can be considered as an interesting orientation. Nevertheless, LTE Standard should first be adapted due to the multiple different characteristics of PMR that make the straightforward application of LTE impossible. In the next section, we provide further details on LTE radio technology bricks adaptation to PMR.

2.2 LTE radio advances adaptation to PMR

2.2.1 LTE radio technology

LTE Advanced has been defined by the 3GPP as an evolution of LTE in order to meet the ITU specifications for the 4th generation mobile communication systems. LTE Advanced is the subject of the Release 10 of 3GGP (The first release on LTE being the release 8). The initial specifications have been made available since March 2011. Several advances specified by R10 can bring solutions to issues related to the PMR as detailed before. These solutions are presented as follows:

1) Local IP access and Selected Internet IP Traffic Offload for HNB subsystem: this 3GPP activity studies the possibility of exchanging IP traffic between IP equipments within the same sub-network (could be an enterprise network), without passing through the operator network in order to reduce the traffic load in the core. This responds to the PMR need of performing communications in a security intervention area between different participants without necessarily passing through the core network.

2) Self Organizing Networks (SON): this activity within 3GPP consists in developing functionalities that enable the base stations to configure themselves autonomously. Specifically, the auto-configuration is performed in order to optimally manage the interferences and automatically handle the load balancing, mobility management, initial access, etc. Such functionalities are just as relevant in the context of PMR deployment.

3) Network based positioning for LTE: this activity aims to improve the estimation of the mobile position in the network, also valuable in PMR.

4) Carrier aggregation for LTE: this feature has been added in order to meet the ITU requirements. It allows optimizing the spectrum utilization. The R10 investigates the possibility of using multiple carrier frequencies that can be either adjacent or not. This feature is specifically relevant in the context of PMR since it would allow a better adaptation to the fragmented spectrum available to PMR due to the presence of other traditional radio systems.

5) Enhanced MIMO schemes: R10 investigates multi-antenna schemes in order to improve the spectral efficiency for the uplink as well as the downlink. Although it is very difficult to use a scheme of more than 2*2 antennas in the context of PMR (due to the UHF carrier frequencies), the possibilities offered by MIMO techniques in the uplink are very interesting since they allow balancing the link, usually limited by the uplink.

6) Relay for LTE: relays are leveraged in 3GPP in order to solve coverage problems. Although they are not a very successful solution with LTE, they can be considered as a very interesting one in the context of PMR to mitigate coverage issues.

7) Enhanced ICIC: Inter Cell Interference Control is a key feature that allows increasing the spectral efficiency of cellular systems. R10 proposes to study new advanced methods of interference control, which is relevant in PMR as well.

2.2.2 Radio technology bricks adaptation

It is interesting to further analyze the possibilities related to the enhancement of the radio physical layer in the context of PMR. These networks will operate in a bandwidth of 5Mhz, which offers less diversity than a 20 Mhz spectrum. The objective is then to reduce the spectral occupancy and improve the cohabitation capabilities with the existing narrow band PMR networks. This is possible through the following set of actions:

1) First, adapting the radio wave is crucial in order to reduce the spectral occupancy and hence facilitate cohabitation with existing narrow band PMR.

2) Second, a joint optimization technique of the physical and application layers allows freeing resources for video and voice flows.

3) Finally, MIMO/SIMO techniques are very interesting to investigate since they improve the spectral efficiency through the spatio-temporal diversity mechanisms they offer.

Future wide band PMR systems will be based on the existing communications standards. LTE seems to be a privileged candidate to be the base of these networks. Our recommendations are strongly based on optimizing and adapting LTE in order to support future wide band PMRs.

2.3 An optimal frequency allocation for enhanced PMR

A PMR network is characterized, in opposition to Public Land Mobile Networks by a low average users density and a very high local user density. The density and priority of users is considerably high in the area where the events happen. The event can be an accident, a terrorist attack, a strike or a sport event, etc.

In order to prevent network breakdown and throughput degradation, it is necessary to optimally allocate and reuse the available band of frequencies. Frequency reuse further improves the spectral efficiency.

The simplest frequency allocation scheme is the static frequency allocation, based on a network dimensioning in the worst case. Since this solution is very limited in terms of both performance and deployment flexibility, it is more judicious to deploy dynamic optimization mechanisms that offer a selective allocation of the services with regard to the current requirements and the opportunistic possibilities of

accessing the radio resource. Our recommendation falls precisely into this category of solution.

In this context, one important objective to determine the gain that could be achieved through a dynamic allocation of the carrier frequencies, compared to the static allocation. The dynamic allocation takes into consideration, at real time, the interference levels measured by the different terminals in the network and the requirements issued by each scenario.

2.3.1 Frequency allocation schemes with LTE

LTE standard has classified the spectrum allocation schemes into three use cases as follows:

1) Pure fractional: the spectrum is shared among the cells. The sharing can be either fair or not but must be established in advance. This basic scheme is the most used in traditional cellular networks.

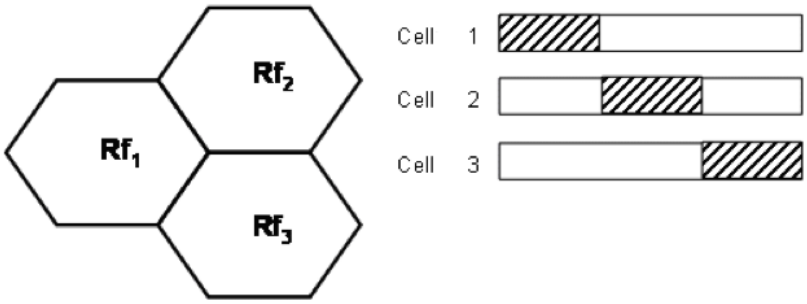

Figure 1: Pure fractional use case

2) Fractional reuse: all the cells use the same resource blocks in order to cover the center of the cell and share either fairly or not the rest of the resource blocks in order to cover the rest of the different cells. In this case also, the sharing has to be established in advance.

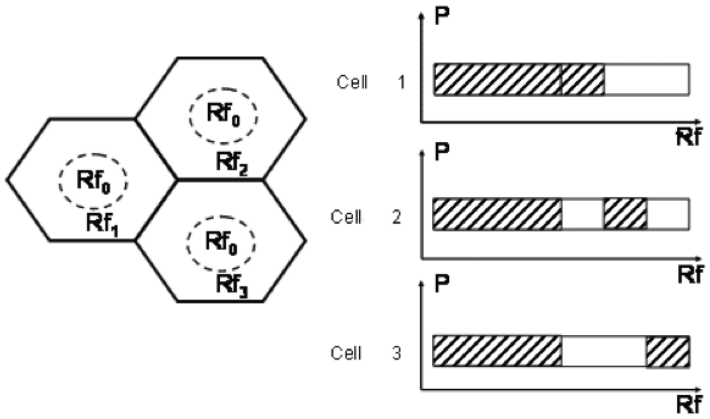

Figure 2: Fractional reuse use case

3) Soft frequency reuse: it represents a variant of the fractional reuse where all the cells use the totality of the resource blocks but do not transmit within the same resource block with the same power. The idea is to achieve a better frequency reutilization than in the last scenario (fractional reuse).

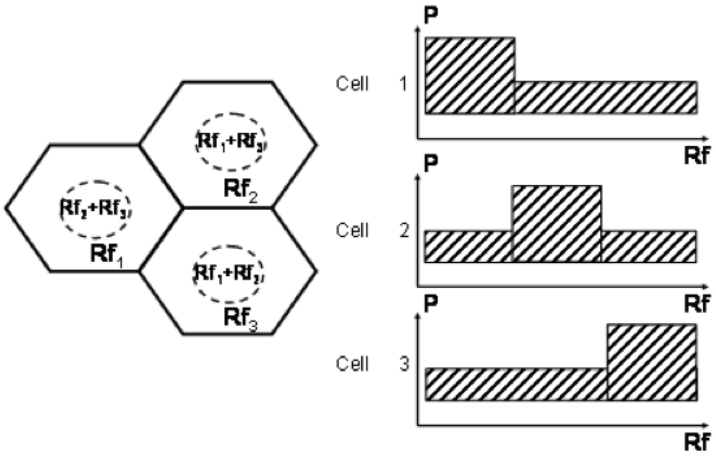

Figure 3: Soft Frequency Reuse use case

Obviously, the static allocation of some resource blocks to a set of cells beforehand can be advantageous to the resource and network management. However, it lacks flexibility in the case of a cell requiring instantaneously much more spectral resources to opportunistically attribute them to privileged users, if they are not in use by the neighboring cells. In order to illustrate this issue, let us consider the case of a

multi-cellular PMR network based on the LTE standard. Figure 4 illustrates the nominal scenario.

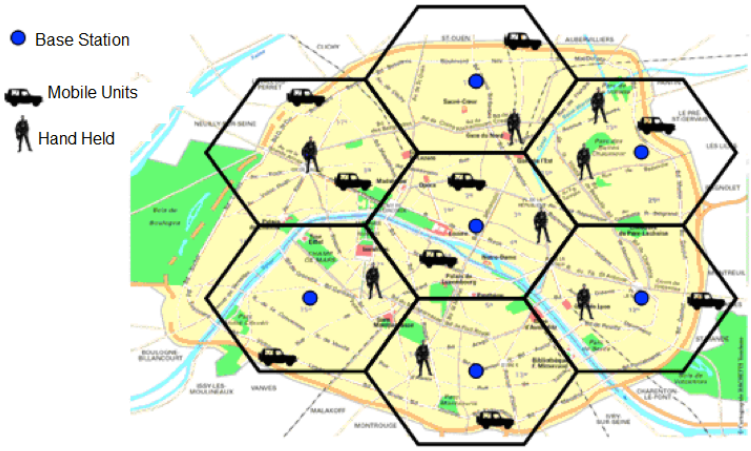

Figure 4: Nominal pattern of a PMR network in Paris

In this scenario, all the cells initially have the same resources, used based on the soft frequency reuse scheme. The spectral utilization in each cell is correct but not optimal. In fact, some cells may not use their available resources while other cells may require additional resources. Henceforth, it is necessary to study the benefits of auto-adaptive frequency reutilization techniques compared to this nominal scenario. The study should be conducted in the two following cases:

1) Pre-positioning or open loop: the objective is to evaluate the impact of the frequency re-utilization techniques in the case of a long loop where the reaction time is greater than a radio frame duration. In this case, we know in advance that an event will take place in a given area. We will then be able to evaluate the required resources and services accordingly. The scenario of a strike planned in the center of Paris can illustrate this situation. The security agents are informed about where and when the strike will take place. Based on this information, they estimate the necessary services and the required radio resources. The estimation takes into account the presence of multiple mobile communication systems' (GSM, 3G) users in the same area. The police agents will then have to predict the needs of the communications that will be used in order to control this strike. Then, we allocate to the cell where the event is happening the resources belonging to the neighboring cells if they are not in use as illustrated by figure 5. The mobility of the users should also be considered to continuously update the estimation during the event.

Figure 5: Pre-positioning PMR in Paris

2) Pure Adaptive or closed loop: the objective is to determine the impact of the frequency reutilization techniques in the case of a short loop where the reaction time is equal to a radio frame duration. In this case, the actors' mobility is a determinant factor. Let us consider the nominal case illustrated in figure 5. In the opposite of the first case, we do not know whether an event will occur or not. Hence, it is hard to estimate the needs in terms of resources and the required services in advance. In this case, we will be in a situation where resources will be taken from one cell to be attributed to another one rapidly. Furthermore, the resources utilization will also evolve dynamically with regard to the mobility of the actors. The case of a terrorist attack illustrates well this situation (Figure 6).

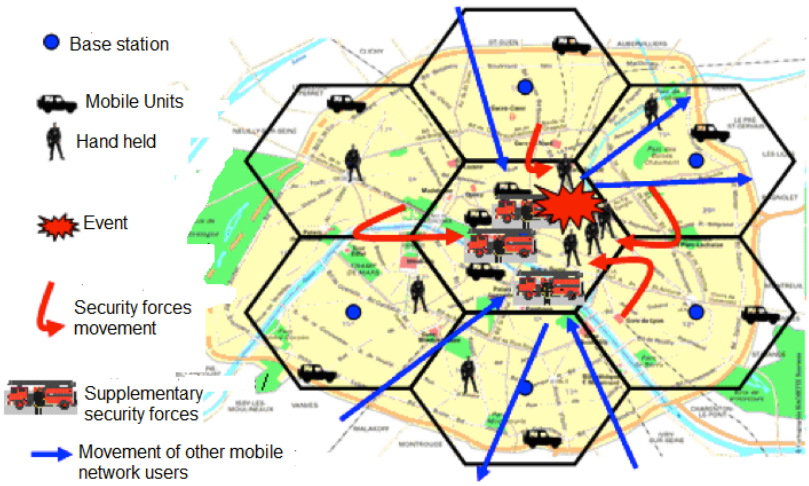

Figure 6: Adaptive PMR in Paris

2.3.2 Auto-adaptive radio frequency allocation

In a traditional multi-cellular PMR network, every cell has a base station to which every user or terminal moving within the cell will try to connect. The different base stations are connected together through a wired specific network. For example, the French national police network (ACROPOL) is different from the fire brigade one (ANTARES) which is different itself from the municipal police one, etc. However, gateways can be installed to interconnect these different networks.

LTE standards provide sensing mechanisms that allow to the mobile terminals to periodically sense their environment so that each base station could build its interference matrix. The idea is to make use of these mechanisms in order to end up with a global mechanism for the auto-adaptive frequency reutilization. Hence, each mobile will use its own sensing mechanism and provide this information to the base station it is attached to. This will enable the construction of the interference matrix in the base station as well as a database, distributed among the different base stations. Furthermore, this mechanism will also enable making decisions regarding the optimization of the network and the resources' management based on a set of parameters (QoS, policies, etc.).

The procedure is executed according to the following data exchange in a PMR network. First, the base station asks the mobile to sense the environment. Then, the mobile performs the sensing and sends the result to the base station. The base station collects the sensing measures from the different mobiles and builds its interference matrix. After that, the base station updates its database and exchanges it with the neighboring base stations. The other base stations do the same with their mobiles and databases. The decision making function allocates the resources based the different cells' requirements and the global allocation policy and informs the base stations of the decision. Finally, a scheduler executes the decision by informing the mobile stations.

2.4 Network coding for robust and secure PMR

Network coding is a new research area that has interesting applications in practical networking systems. With network coding, intermediate nodes may send out packets that are linear combinations of previously received information. There are two main benefits of this approach: throughput improvements and a high degree of robustness. Robustness translates into loss resilience and facilitates the design of simple distributed algorithms that perform well, even if decisions are based only on partial information.

A simple example in a wireless context is a three-node topology, as shown in Figure 7. Linear network coding, in general, is similar to this example, with the difference that the xor operation is replaced by a linear combination of the data, interpreted as numbers over some finite field. This allows for a much larger degree of flexibility in the way packets can be combined.

In addition to the throughput benefits evidenced in this example, network coding is also very well suited for environments where only partial or uncertain information is available for decision making.

Similar to erasure coding, the successful reception of information does not depend on receiving a specific packet content but rather on receiving a sufficient number of independent packets. Linear combining requires enhanced computational capabilities at the nodes of the network. However, according to Moore's law, processing is becoming less and less expensive. Since the bottleneck has shifted to network bandwidth to support the ever-growing demand in applications and QoS guarantees over large unreliable networks, network coding utilizes cheap computational power to increase network efficacy. The goal of this background section is to make the basic concepts of network coding available to the networking community.

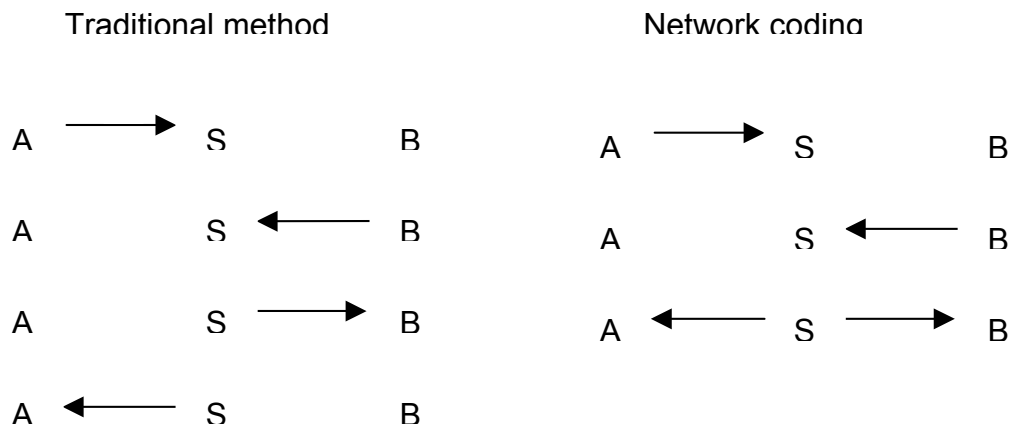

Figure 7: A simple network coding example. Nodes *A* and *B* want to exchange packets via an intermediate node *S* (wireless base station). *A* [resp. *B*] sends a packet *a* [resp. *b*] to *B*, which then broadcasts *a* xor *b* instead of *a* and *b* in sequence. Both *A* and *B* can recover the packet of interest, while the number of transmissions is reduced.

2.4.1 Network coding principles

Consider a system that acts as an information relay, such as a router, a node in an ad-hoc network, or a node in a peer-to-peer distribution network. Traditionally, when forwarding an information packet destined to some other node, it simply repeats it. With network coding, we allow the node to combine a number of packets it has received or created into one or several outgoing packets.

Assume that each packet consists of L bits. When the packets to be combined do not have the same size, the shorter ones are padded with trailing 0s. We can interpret s consecutive bits of a packet as a symbol over the field $F2s$, with each packet consisting of a vector of L/s symbols. With linear network coding [5], outgoing packets are linear combinations of the original packets, where addition and multiplication are performed over the field $F2s$. The reason for choosing a linear framework is that the algorithms for coding and decoding are well understood.

Linear combination is not concatenation: if we linearly combine packets of length L, the resulting encoded packet also has size L. In contrast to concatenation, each encoded packet contains only a fraction of the information contained in original packets. One can think of linear network coding as a form of information spreading, which has benefits in several cases (as in Figure 7).

1) Encoding: Assume that a number of original packets $M1,..., Mn$ are generated by one or several sources. In linear network coding, each packet through the network is associated with a sequence of coefficients $g1,..., gn$ in $F2s$ and is equal to $X = i=1n\ gi \cdot Mi$. The summation has to occur for every symbol position, i.e., $Xk = i=1n\ giMki$, where ki and Xk is the kth symbol of Mi and X respectively.

In the example of Figure 7, the field is $F2$ = 0, 1, a symbol is a bit, and the linear combination sent by S after receiving $M1 = a$ and $M2 = b$ is $M1+ M2$ (the + sign here is addition in $F2$, i.e. bitwise xor).

For simplicity, we assume that a packet contains both the coefficients $g = (g1,..., gn)$, called encoding vector, and the encoded data $X = i=1n\ g1 \cdot Mi$, called information vector [6]. The encoding vector is used by recipients to decode the data, as explained later. For example, the encoding vector ei = 0,…, 0, 1, 0,…0, where the 1 is at the ith position means that the information vector is equal to Mi (i.e., is not encoded).

Encoding can be performed recursively, namely, to already encoded packets. Consider a node that has received and stored a set $g1$, $X1$,…, gm, Xm, of encoded packets, where gj [resp. Xj] is the encoding [resp. information] vector of the jth packet. This node may generate a new encoded packet g', X' by picking a set of coefficients $h1$, …, hm and computing the linear combination X'=j=1m $hj \cdot Xj$.

The corresponding encoding vector g is not simply equal to h, since the coefficients are with respect to the original packets $M1$, …, Mn ; in contrast, straightforward algebra shows that it is given by gi'=j=1m $hj \cdot gji$. This operation may be repeated at several nodes in the network.

2) Decoding: decoding requires solving a set of linear equations. In practice, this can be done as follows. A node stores the encoded vectors it receives as well as its own original packets, row by row, in a so-called decoding matrix. Initially, it contains only the non-encoded packets issued by this node with the corresponding encoding vectors (if any, else it is empty). When an encoded packet is received, it is inserted as last row into the decoding matrix. The matrix is transformed to triangular matrix using Gaussian elimination. A received packet is called innovative if it increases the rank of the matrix. If a packet is non-innovative, it is reduced to a row of 0s by Gaussian elimination and is ignored. As soon as the matrix contains a row of the form ei, this node knows that x is equal to the original packet Mi. This occurs at the latest when n linearly independent encoded vectors are received. Note that decoding does not need to be performed at all nodes of the network, but only at the receivers.

3) How to select the linear combinations: the problem of network code design is to select what linear combinations each node of the network performs. A simple algorithm is to have each node in the network select uniformly at random the coefficients over the field $F2s$, in a completely independent and decentralized manner [7]. With random network coding there is a certain probability of selecting linearly dependent combinations. This probability is related to the field size 2s. Simulation results indicate that even for small field sizes (for example, s = 8). This probability becomes negligible [7].

4) Generations: for all practical purposes, the size of the matrices with which network coding operates has to be limited. This is straightforward to achieve for deterministic network codes but more difficult with random network coding. For the latter, packets are usually grouped into so called generations, and only packets of the same generation can be combined [6]. The size and composition of the generations may have significant impact on the performance of network coding. Similar considerations hold for the size of the finite field.

Both parameters allow to trade off performance for lower memory requirements and reduced computational complexity.

- Delay: the fact that packets need to be decoded has a minor impact on delay. It is usually not necessary to receive all encoded packets before some of the packets can be decoded (i.e., whenever Gaussian elimination leads to a row in the form $ei,i)$. Together with a reduction in the number of required transmissions, the overall end-to end delay with network coding is usually not larger than the normal end-to-end delay in realistic settings.

- Finite field operations: network coding requires operations in F2, i.e., operations on strings of s bits. Addition is the standard bitwise xor. For multiplication, one interprets a sequence $b0,\ldots, bs-1$ of s bits as the polynomial $B0+b1X+\ldots+bs-1Xs-1$. Then one picks a polynomial of degree s that is irreducible over F2 (there are several of them and each gives a different representation of $F2s$; for example, Rijndael's representation of $F28$ uses $1+X+X3+X4+X8$). Multiplication is obtained by first computing the usual product of two polynomials (which gives a polynomial of degree possibly larger than s−1), and then computing the remainder modulo the chosen irreducible polynomial. Division is computed by the Euclidian algorithm. Both multiplication and division can be implemented efficiently with s shifts and additions.

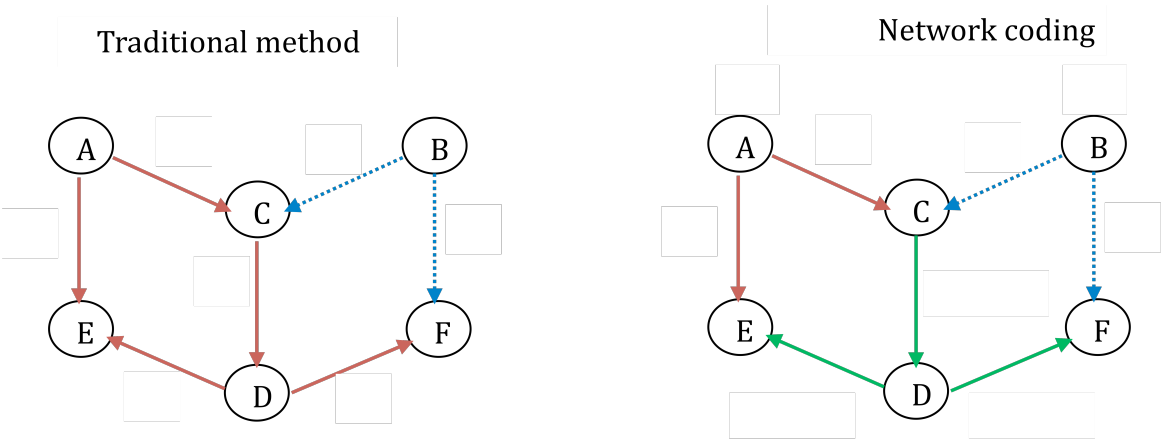

Figure 8: (Butterfly Network) S_1 and S_2 multicast to both R_1 and R_2. All links have capacity 1. With network coding (by xoring the data on link CD), the achievable rates are 2 for each source, the same as if every destination were using the network for its sole use. Without network coding, the achievable rates are less (for example if both rates are equal, the maximum rate is 1.5).

2.4.2 Network Coding benefits for wireless networks

Theoretically proven results about network coding mainly concern performance improvements in static settings. We first review these and then discuss random distributed settings.

1) Throughput gain in a static environment

A primary result that sparked the interest in network coding is that it can increase the capacity of a network for multicast flows. More specifically, consider a network that can be represented as a directed graph. The vertices of the graph correspond to terminals, and the edges of the graph correspond to channels. Assume that we have M sources, each sending information at some given rate, and N receivers. All receivers are interested in receiving all sources. Assume that the source rates are such that, without network coding, the network can support each receiver in isolation (i.e. each receiver can decode all sources when it is the only receiver in the network). With an appropriate choice of linear coding coefficients, the network can support all receivers simultaneously. In other words, when the N receivers share the network resources, each of them can receive the maximum rate it could hope to receive, even if it was using all the network resources by itself. Thus, network coding can help to better share the available network resources (Figure 8). Network coding may offer throughput benefits not only for multicast flows, but also for other traffic patterns, such as unicast. Consider again Figure 7 but assume now that source S1 transmits to destination R2 and S2 to R1. With network coding we can send rate 1 to each receiver, while without, we can only send rate 1/2 to each receiver.

2) Robustness and Adaptability

The most compelling benefits of network coding might be in terms of robustness and adaptability. Intuitively, we can think that network coding, similarly to traditional coding, takes information packets and produces encoded packets, where each encoded packet is “equally important”. Provided we receive a sufficient number of encoded packets, no matter which, we are able to decode. The new twist that network coding brings, is that the linear combining is performed opportunistically over the network, not only at the source node, and thus it is well suited for the (typical) cases where nodes only have incomplete information about the global network state.

Consider again Figure 7 and assume that A and B may go into sleep mode (or may move out of range) at random and without notifying the base station S. If the base

station S broadcasts a (or b), the transmission might be completely wasted, since the intended destination might not be able to receive. However, if the base station broadcasts a xor b, or more generally, random linear combinations of the information packets, the transmission will bring new information to all active nodes. This argument is the basis for the significant performance improvements achieved with network coding.

2.4.3 Where can network coding be used?

In the following, we list a number of applications of network coding and discuss how the benefits mentioned before can improve performance in concrete settings.

1) Bidirectional traffic in a wireless network

As shown in Figure 7, network coding can improve throughput when two wireless nodes communicate via a common base-station. Given a scheduler that alternates between adjacent routers, after a few initial steps, all intermediate routers have packets buffered for transmission in both directions of the path. Whenever a transmission opportunity arises, a router combines two packets, one for each direction, with a simple xor and broadcasts it to its neighbours. Both receiving routers already know one of the packets of the broadcast is coded over, while the other packet is new. Thus, each broadcast allows two routers to receive a new packet, effectively doubling the capacity of the path.

Overhearing a packet of a neighbour that is coded over information previously forwarded to the neighbour serves as a passive acknowledgment. This allows making a better use of the transmission opportunities at routers that only have new packets buffered for a single direction. In this case, one of the new packets is combined with an old packet for the reverse direction for which no passive acknowledgment has been received.

2) Residential wireless mesh networks

Even a limited form of network coding which only uses xor to combine packets may significantly improve network performance in wireless mesh networks [8]. All transmissions are broadcast and are overheard by the neighbours. Packets are annotated with summary information about all other packets a node already heard. This way, information about which nodes hold which packets is distributed within the neighbourhood. A node can xor multiple packets for different neighbours and send them in a single transmission, if each neighbour already has the remaining information to decode the packet. In experiments with 802.11 hardware, it has been shown that network coding almost doubles network throughput.

3) Many-to-many broadcast

Network-wide broadcast is used for a number of purposes in ad-hoc networks (e.g., route discovery) and can be implemented much more efficiently with network coding [5]. Already a simple distributed algorithm for random network coding reduces the number of transmission by a factor of 2 or more, leading to significant energy savings. In such a setting, a larger transmit power directly translates into a reduction in the number of required transmissions, which allows for interesting energy tradeoffs. Energy expenditure is either evenly distributed among the nodes or covered by only a few nodes (maybe with longer battery life). There is a larger flexibility in the distribution the energy requirements compared to conventional algorithms.

2.4.4 Network coding for secure communications

In [10], the authors investigate the problem of designing secure network codes for wiretap networks, where attackers can access certain links. They assume that it is known which links are tapped. The source combines the original data with random information and designs a network code in a way that only the receivers are able to decode the original packets. Furthermore, the mutual information between the packets obtained by the eavesdroppers and the original packets is zero (security in the information theoretic sense).

The fact that with network coding nodes can only decode packets if they have received a sufficient number of linearly independent information vectors allows for a weaker form of security [11]. Such codes are more efficient, but an attacker who has $n-1$ out of n linear combinations only has to guess the content of a single packet to be able to decode all n packets (hence the name “weak security”).

Finally, network coding simplifies the protection against modified packets in a network [12]. At a normal network (and no additional protection), an intermediate attacker may make arbitrary modifications to a packet to achieve a certain reaction at the attacked destination. However, in the case of network coding, an attacker cannot control the outcome of the decoding process at the destination, without knowing all other coded packets the destination will receive. Given that packets are routed along many different paths, this makes controlled man-in-the-middle-attacks more difficult.

Network coding may have an impact on the design of new networking and information dissemination protocols. By allowing to better spread the information content in the network environment, it can simplify distributed algorithms.

Reliable multicast is an example where the existing solutions need to be re-thought; we have shown in our review that emerging areas such as ad-hoc networks, overlay infrastructures and sensor networks are starting to benefit of network coding. More such applications are expected to emerge.

3 Foresight Results

3.1 Trends

- Citizens in digital cities are always connected to mobile networks. Smart phones are powerful tools that can act as a sensor and provide useful information to security forces.
- Geo-localization applications are a powerful capability that helps security forces to predict and prevent safety problems
- Sensors are widespread in digital cities. They feed the security forces' database with useful information in preventing safety attacks
- The security services are evolving from voice calls to multimedia services such as data, images, video, live feeds, face recognition and database queries.

3.2 Challenges

- Citizens' behavior: reluctant citizens may not accept to participate to the sensing activity for privacy issues.
- Some citizens are not yet comfortable with using very sophisticated communications systems
- With radio communications systems challenges are mainly related to the co-existence of PMR with other systems using the same spectrum. This rises frequency allocation issues
- Coverage problems
- PMR do not meet the new multimedia services requirements during the security services intervention

3.3 Recommendations

- Sensing the environment is very important and requires the participation of citizens themselves
- An efficient PMR should be based on LTE radio technology
- Frequency allocation optimization: dynamic optimization mechanisms that allow a selective allocation of the services with regard to the current requirements and the opportunistic possibilities of accessing the radio resource
- Network coding should be adopted to further improve PMR performance, robustness and security and offer higher potentials for security business
- Deploying ad-hoc networks to mitigate coverage issues

4 Conclusions

The rapid growth of the cities yields new challenges spanning from the social to the technical point of view. Many actors are innovating, exploiting ICT for improving our cities efficiency, quality of life and safety.

The advances in technology and the resulting change in the citizens' behaviour have an important impact on the way safety is perceived and guaranteed in the digital cities. Specifically, the growth of the use of smartphones as well as the recent advances achieved with mobile networks have changed the way people interact, disseminate and share the information. With a permanent connection to the social networks, people exchange at real time information about events, news, and any activity in a precise area and time. Such high level of connectivity should be exploited by security forces in order to enhance their database with information that might be useful in predicting security threats.

Furthermore, in case of emergency, security forces need to efficiently coordinate their intervention and rapidly evacuate people in a crisis area. This requires reliable, high performant radio communications systems. Enhanced with recent technological advances in mobile networks like LTE radio access technology and network coding, private mobile radio telecommunication (PMR) networks are a viable solution. PMR enable the security forces to efficiently coordinate their intervention and rapidly communicate with victims in order to perform a successful evacuation.

Safety in digital cities is definitely one the of the fields where the new shape of cities is perceptible since it involves both the technological advances and the changes we are witnessing in the citizens behaviour due to the penetration of those technologies. This will further impact the behaviour of the citizens as well as the security industry.

List of Acronyms

EIT	European Institute of Innovation and Technology
ICT	Information and Communications Technology
LTE	Long Term Evolution
NSF	National Science Foundation
GPS	Global Positioning System
PMR	Private Mobile Radio telecommunications
GSM	Global System for Mobile communications
MIMO	Multiple Input Multiple Output
SIMO	Single Input Multiple Output
VHF	Very High Frequencies
UHF	Ultra High Frequencies
HARQ	Hybrid Automatic Repeat reQuest
FDD	Frequency Division Duplex
PLMN	Public Land Mobile Network
UMTS	Universal Mobile Telecommunications Systems
eMBMS	evolved Multimedia Broadcast Multicast Service
3GPP	3rd Generation Partnership Project
ITU	International Telecommunication Union
HNB	Home Node B
SON	Self Organizing Networks
ICIC	Inter Cell Interference Control
3G	Third Generation
QoS	Quality of Service
kbps	kilo bit per second
mbps	Mega bit per second

References

[1] ETSI TR 102 628 V1.1.1 (2010-08) Electromagnetic compatibility and Radio Spectrum Matters (ERM) ; System Reference document; Land Mobile Service; Additional Spectrum Requirements for Future Public Safety & Security (PSS) wireless communications systems in the UHF Frequency range

[2] CEPT/ECC document: FM 38 (10) 36-Developments of BroadBand PPDR (Public Protection Disaster Relief) possible future spectrum use, 1st November 2010

[3] http://www.arcep.fr/uploads/tx_gspublication/contrib-divnum-EADS-Secure-Networks.pdf

[4] R. Ahlswede, N. Cai, S. R. Li, and R. W. Yeung. Network information flow. IEEE Transactions on Information Theory, July 2000.

[5] S-Y. R. Li, R. W. Yeung, and N. Cai. Linear network coding. IEEE Trans. Inform. Theory, 49:371–381, Feb.2003.

[6] P. A. Chou, Y. Wu, and K. Jain. Practical network coding. In Proc. Allerton, Oct. 2003.

[7] T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, A random linear network coding approach to multicast. IEEE Transactions on Information Theory, Oct. 2006.

[8] S. Katti, D. Katabi, W. Hu, H. Rahul, and M. Medard. The importance of being opportunistic: Practical network coding for wireless environments. In Allerton, 2005.

[9] C. Fragouli, J. Widmer, and J.-Y. L. Boudec. A network coding approach to energy efficient broadcasting: from theory to practice. Technical Report LCA-REPORT-2005-009, accepted at Infocom 2006, EPFL, July 2005.

[10] N. Cai and R. W. Yeung. Secure network coding. In International Symposium on Information Theory (ISIT), 2002.

[11] K. Bhattad and K. R. Nayayanan. Weakly secure network coding. In Proc. First Workshop on Network Coding, Theory, and Applications (NetCod), Apr. 2005.

[12] T. Ho, B. Leong, R. Koetter, M. Mdard, M. Effros, and D. R. Karger. Byzantine modification detection in multicast networks using randomized network coding.In International Symposium on Information Theory (ISIT), 2004.

[13] UNO Economic and Social Affairs. World Urbanization Prospects The 2009 Revision. Technical report, United Nations, 2010.

[14] Expo 2010 Shanghai, China. http://en.expo2010.cn

[15] European Smart Cities project, http://www.smart-cities.eu.

[16] ICT Lab Digital Cities of the Future, European Institute of Innovation & Technology http://www.eitictlabs.eu/action-lines/ digital-cities-of-the-future

[17] City Science, MIT Media Lab, http://cities.media.mit.edu.

[18] C. Sharma, Global Mobile Market Update, available online http://www.chetansharma.com/GlobalMobileMarketUpdate2012.htm

[19] I. Augé-Blum, K.Boussetta, H. Rivano, R. Stanica, F. Valois, "Capillary networks, a Novel paradigm for urban environments", UrbaNe'12, Nice, France, December 2012

Imprint:
EIT ICT Labs IVZW
22 Rue d'Arlon, 1050 Brussels
BELGIUM

ISBN 978-91-87253-15-7

Innovation Radar