Delay Tolerant Networks for Disaster Scenarios

Andreea-Cristina PETRE[*], **Cristian CHILIPIREA**[*], **Ciprian DOBRE**[*1]

[*] University POLITEHNICA of Bucharest, Computer Science Department
Splaiul Independentei 313, Bucharest 060042, Romania
E-mails: {andreea.petre, cristian.chilipirea}@cti.pub.ro, ciprian.dobre@cs.pub.ro

Abstract. Disaster and emergency management refers to a range of activities designed to maintain control over crisis situations, providing the rescue and assistance equipment with a framework for helping victims and reducing its impact. The range of activities include prevention, advance warning, early detection, analysis of the problem and assessment of scope, notification of the public and appropriate authorities, mobilization of a response, containment of damage, and relief and medical care for those affected. One of the challenges in emergency scenarios is the fact that communications can be interrupted, cutting the information flow. This lack of communication infrastructure makes an appropriate response to the disaster more challenging, and leads to reduced quality of services experienced by vulnerable civilians. As an example, emergency scenarios with big agglomerations of people or traffic jams following accidents demand a unified communication infrastructure to optimize the response and decision making. This can be overcome using self-configured wireless networks, because they do not require any pre-existing infrastructure to be established, and are easy to deploy and fast to operate. The continuous use of modern smartphones facilitates the accessibility to wireless technologies. However, when incorporating mobile smartphones into disaster assisting networks, the biggest challenge is that such wireless networks need to be specifically designed and used for supporting victims, people and assistance equipment in crisis scenarios. Because of this, in future mobile networks designed for disaster management, there is a need for new architectures and protocols, capable to adapt existing and available wireless technologies for smart data capturing and decision making. This chapter analyses specific challenges and requirements related to supporting communication in such challenged situations. We present an extensive analysis of networking solutions designed to support situations such the ones described.

Keywords: Disaster Scenario, Networking, Delay Tolerant Networks, Mobile Devices, Communication and mobility support

[1] Corresponding author.

1. Introduction

In the past few years our dependency on technologies, such as the personal computer or the Internet, has grown to a point where we cannot sustain our normal day to day activities if we were to be denied access to such advancements. More and more businesses migrate part of their infrastructure to the Internet [1, 2], either to construct stronger business-to-client relations, or to simplify the process of acquiring new clients by having a more efficient infrastructure and communication process inside the company. Many e-commerce web sites, like Amazon, have managed to dominate the market by having their service available 24/7, with easy access to anyone interested in acquiring their products. The same can be said of many other e-commerce platforms that have managed to beat the competition, platforms which range from fast-food home delivery to electronics.

Social Networks, such as Facebook [3, 4], on the other hand, have become ubiquitous in the lives of many people. The number of users and time spent on such social networks increased with the emergence of new similar services, such as Google+ [5] and others dedicated to a certain activity (such as finding a job or sharing experience in programming). Furthermore, technologies such as Twitter [6], a micro-blogging platform, are used every day by millions of users, and have recently stood at the center of major political events, such as the ones in Libya [7].

The Internet is not only a tool represented by the various websites that are part of the web, but it is also an infrastructure that supports other services such as communication, like in the case of Skype [8], a Voice-over-IP service that only requires an Internet connection and is otherwise completely free that offers voice, text and video communication as well as file transfer.

Emerging technologies such as Internet of Things [9] or Smart Cities [10, 11, 12] will further increase our (already high) need for continuous Internet access. These emerging trends will connect more and more devices to the Internet, and will require high-availability connections to function correctly. An air conditioner will probably need to access a weather service to predetermine its usage and increase or lower the temperature of a room autonomously, before the user arrives home. Such technologies will probably be able to function without a permanent connection to the Internet, but their functionality and efficiency would dramatically be reduced if the connection is not available for longer periods of time.

This dependency continues with the centralization of user data, especially in the case of government centralized data. Considering the example of a hospital [13] that uses a government issued system to track patient confidential information; if an unconscious patient arrives at the hospital in a critical condition and the hospital does not have access to his data because of an Internet outage, mistakes can be made that can jeopardize his well-being. Such mistakes can be caused by the lack of patient history or the list of medication the patient is using.

To top all of these methods that the Internet is used in a day to day basis, cloud computing [14] (or, in a larger sense, utility computing) makes individual and businesses heavily dependent on good Internet connections. Without an Internet connection available, companies will not have access to data that would otherwise be always available on site. Most technologies, already available, or emerging ones, all increase our need for a stable Internet connection. Because of this, it is important to develop new technologies that guarantee Internet access for most people even in extreme scenarios. Furthermore we need to create technologies that give assurances that no one individual or organization can restrict access to a group of people.

The problem of managing access to communication resources becomes even more critical in case of disasters. The Great East Japan Earthquake in 2011 showed that disaster management services supported by communication between rescuers and victims are mandatory to be fast put in place to support efficient evacuation guidance procedures. Such services could use opportunistic communication. In recent years, as a practical use of Delay Tolerant Network and Mobile Opportunistic Network, researches on disaster evacuation guidance effective against situations of large-scale urban disasters have been undertaken. In such disaster evacuation guidance procedures based on opportunistic communication, evacuees collect location information of impassable and congested roads due to disaster in their smartphones by themselves, and share it with each other opportunistically by short-range wireless communication between nearby smartphones in order to not only navigate evacuating crowds to refuges, but also rapidly aggregate the disaster information.

In this paper we study existing and emerging technologies that provide an Internet connection or at least a communication method even in extreme circumstances such as natural disasters. In the following section we present why there is a need for such a technology and then we present the available networking technologies that try to solve this problem.

The rest of this chapter is structured as follows. We first present an analysis of extreme networking scenarios. Section 3 presents the set of requirements for networks in the case of disaster scenarios, and in Section 4 we present an analysis of current networking alternatives for disaster scenarios. This is followed in Section 5 by ad-hoc networking alternatives, and experimental results. Section 6 concludes and presents future work.

2. Extreme networking scenarios

High price/low availability – There are a number of regions in the world, such as sub-Saharan Africa [15], where the disparity between the price of an Internet connection and the income of most citizens is so high that most people cannot afford to own an Internet connection. This is not a problem that is confined to 3rd world countries like the ones in Africa, but are also common in rural area of more advanced countries.

This problem is introduced by the fact that the cheapest way to spread the Internet network is currently given by wired technology. Wired technology has severe disadvantages: the infrastructure needs to be deployed, usually requiring digging holes or raising posts; because of technologies such as fiber optic, it is usually enough to get one cable to a densely populated area and offer high speed bandwidth to a large number of users, this translates in lower prices only for densely populated areas; there are range-related limits for both fiber optic and cooper based networking, there is a need for repeaters which can dramatically raise price; usually deployment is not enough, there is need for administration and redundancy.

For sparse populated areas, or populated areas that are extremely far apart, like the case of cities separated by a desert, or villages built on top of mountains, the costs of constructing a wired networking infrastructure can be so high that it is not even worth considering. Furthermore because only a small number of people live in each of this villages, the price of constructing the initial infrastructure is split only by a small number, thus keeping price per person extremely high. This is opposite to a dense populated city, with huge buildings shared by several families, where the price per person to build the infrastructure can be extremely low.

The further we move from the large cities and the metropolises that many of us have grown accustomed to, the more we can feel the lack of stable Internet connections, or even their complete availability.

Because of this any networking technology that wants to provide Internet infrastructure to such areas should not have its price dependent on the number of users in an area that need to adopt it.

Unstable electricity – The same areas we presented earlier, in which the people have low income and the costs of infrastructure are extremely high, suffer from problems with stable, always available electricity. This areas usually have no or a small number of redundancies to their main line that provides electricity. If this main line fails for whatever reason it needs to be repaired before the electric service can again be available. The problem is further complicated by the fact that cables and infrastructure in these areas is not changed often enough and they are more likely to fail because of this.

To top all of this, repairs to any infrastructure, be it Internet, electrical or of any other type can take huge periods of time as access to such areas tends to be limited, or difficult.

To build a network that can provide high stability and functionality even in such environments it needs to require very little administration or change of infrastructure equipment and it needs to have a way to work even if there is no electricity through the use of batteries or alternative energy sources, like the use of solar panels.

Natural disasters – these represent problems that not only affect the regions presented earlier, but also affect densely populated regions. There are a number of natural disasters that can affect infrastructure, starting from earthquakes, volcanoes and all the way to tsunamis.

The problem with these is even greater if we consider the chaos they induce and the higher need for communication to save lives in such scenarios. People want to contact their loved ones and make sure they are safe and can overload even the remaining part of any infrastructure. Search and rescue teams need to communicate between themselves, to the central command and control and to the individuals they intend to rescue.

Search and rescue teams can also have huge benefits from any data that they have about a location. This data can be of multiple types, from recent maps to pictures from the area they are investigating to sensor data such as gas leakage detectors. There is an extremely high amount of data that can help search and rescue personnel to asses risk and to decide what the best course of action is.

Because of the potentially high number of people affected, the necessity of information, the potential to use data and communication to save life, and the reduction in stress in individuals given by the opportunity to communicate with close ones, we believe that this scenario is one of the most important one to take into account when considering developing technologies for extreme networking.

Building such technologies requires either a way to assure that the infrastructure will resist after the natural disaster event, which is really difficult, or the infrastructure can be replaced in a simple and fast manner. There is also the case where no infrastructure is required, this is the case of ad-hoc networks.

Oppression – after the incident in Libya, also known as the "Twitter Revolution" governments that oppress their citizens have tried to prevent the start of a revolution by limiting or stopping the access to Internet to its citizens. This was seen in January 2011 when Egyptian government [16] has shutdown Internet access in an attempt to stop civil unrest against President Mubarak.

There are other cases where the Internet is not stopped entirely but censored. This is the case of the "Great firewall of China" [17] which limit the access of Chinese citizens to the information on the Internet, both for in country websites and other countries.

Attempts of censorship have even crossed country borders in cases such as the one in which Pakistani government has tried to block access to YouTube [18], and in doing so has blocked access to the site for the entire world for several hours by adding a BGP route that sent all request to a server that dropped them. A mistake caused the route to spread in the entire Internet infrastructure with a claim that the shortest path to YouTube servers is through the Pakistani server.

Governments are not the only ones that try to censor its citizens, but various criminal organizations can be behind such activities. An attempt was recorded in March, 2013 when a group of Egyptian military has stopped several individuals in their attempt to cut an underwater cable [19]. The event would have caused the loss of Internet in 50% of the Egyptian infrastructure. This shows that Internet availability can be threatened by a targeted attack to the existing infrastructure. There are countries which only have a small number of connections with other countries and if this connections are disabled it can take large amounts of time for them to be rebuilt, thus cutting entire countries Internet access.

There are other forms of oppression present, like the modification of DNS entries by governments that have control of these servers. This types of oppression are common even in advanced and democratic countries such as the U.S.A..

Building the technology or the infrastructure in such a way that no one can block the access of a different individual to the Internet is extremely difficult. It requires a large number of redundancies and putting the control of the infrastructure in the hands of the citizens. This is usually not possible. However in the case of ad-hoc networks, this can be achieved on a smaller scale. Communication between devices can still be guaranteed, even if the infrastructure that provides access to the Internet is stopped.

To make sure the Internet is available, and accessible, at high quality rates, we need to consider technologies that take into account all the scenarios presented above. We need consider that probably no technology can bring 100% guarantees; even wireless connections can be jammed for instance, and all devices are currently dependent on electricity. To top all of this, we always need to consider the cost. A high cost directly translates in low adoption.

One would ask if the cost is really such a big problem, and argue that a person that cannot afford an Internet connection can probably also not afford a computer with which to utilize such a connection. This is not necessarily true, the cost of computing hardware has dropped dramatically in the past few years. Projects like the Rasberry Pi [20], have brought the size and the price of a computer down significantly. A unit is now not bigger than a credit card and it costs only 30$. This is an extremely small one time investment compared to the cost of an Internet connection that requires monthly recurring payments.

In the following Sections we will further present a discussion of the particular case of communication support for natural disasters. Such solutions could easily be adapted further to other cases (such as the ones presented here).

3. Requirements for networks in the case of disaster scenarios

In case of a disaster, a network needs to be able to operate effective even when parts or its entire infrastructure is no longer available. This requirement is the single most important one; the network could not be very fast, but it is this requirement which must hold in order to truly benefit the users. By users, we distinguish several categories. Also, we distinguish several periods after the disaster in which the network is used (which yields specific requirements on how the network needs to behave). The normal user wants to communicate with his close friends or family. This kind of usage is not as important as the communication between search and rescue teams. As such we can identify a few periods after a disaster in which we need to consider network needs separately.

The search and rescue phase – This is the main phase after any disaster. Search and rescue teams are deployed, and the wreckage is searched to find and identify survivors. This is a critical period. The communication between search and rescue teams is essential, as well as communication with a center responsible with the command and control of coordination between rescue teams. If we consider a network that is shared between search and rescue teams as well as individuals trying to communicate between themselves, there is a need for special protocols that would give priority to the traffic created by the search and rescue teams. We also need to consider the data that needs to pass over the network. For example, text takes a smaller amount of bandwidth. Building a network that can transfer small amounts of data is simpler and cheaper, but the majority of today's communication protocols insert an additional header which might prove to be inadequate for tomorrow's small data chunks needing to be transfer (and this is also true for machine-to-machine control communication, in a more generic sense). However, using voice and even video can help the search and rescue dramatically. But such data pose different requirements on the communication protocols. So, could both types of data co-exist efficiently over the communication channels in place for disaster management? Do we need separate solutions to route control / text messages (a control plane) completely separated from a multimedia plane? This is a question many researchers are trying to answer today.

Data availability is also important. Sending the teams in dangerous environments can be extremely risky, and everything needs to be considered when making such a decision. For instance: video feeds from individuals that require extraction, but are stuck, can help identify the priority targets; having sensors can help determine anything from stability of a building to gas or fire levels to other potential risks or hazards. There are two things to be considered here: first is how to acquire the data, usually networks of sensors need to be spread before the incident; second is how to sustain the flow and filtration of all available data. Filtering the data is important as multiple sensors can indicate the same thing and will only overload the network without providing any extra information.

In this phase any infrastructure is most likely to be down. There are a number of reasons for this to happen. Wired connections can be broken. Repeaters or any devices that help extend the network can be down because of lack of electricity or even destroyed by electrical spikes. We can also consider a lack of available personnel to manage the infrastructure or to do any repairs.

It is also important to consider the destruction of Internet Service Providers server centers. These are probably the most expensive and hardest parts to replace. This process might also take a high amount of time.

The reconstruction phase – after the search and rescue phase, there is another period in which infrastructure is not yet available. The reconstruction of critical infrastructure is under way, but it can take a large period of time until everything becomes fully operational. The search and rescue teams have mostly finished their tasks and communication between them is not as big a priority as it was.

In recent years, as a practical use of Delay Tolerant Network and Mobile Opportunistic Network, disaster evacuation guidance effective against situations of large-scale urban disasters have been studied. In disaster situations, this navigation becomes disaster evacuation guidance navigating crowds of evacuees to the nearest refuges. Also, disaster information sharing is also available by opportunistic communication. For example, authors of [52, 53] have previously proposed the use of opnets for autonomously navigating crowds of evacuees to refuges, but also rapidly aggregating real-time disaster information. They propose the opportunistic collaboration between individual mobile nodes, using wireless communication, to assist with the reconstruction phase through guidance: evacuees naturally collect location information of impassable and congested roads in their smartphones by themselves and share it with nearby smartphones by opportunistic communication. Using the collected information, the guidance proposes an effective shortest-path based evacuation route to the nearest refuge avoiding known impassable and congested roads beforehand. By simulating a simple mathematical model of urban disaster scenarios, authors have actually shown numerically that the guidance reduces the average and maximum evacuation times even when the effects of congestion by evacuees is applied.

However, in the reconstruction phase there are several issues remaining to be solved as well. Everyone needs to communicate and reach as many other individuals as they can, make assurances to families and friends that everything is alright and start rebuilding what they lost. In this phase, hospitals and other centers can be overcrowded (network in such locations can be overused).

These are several places where, with a higher priority, the infrastructure needs to be restored fast. As infrastructure is restored, offering higher bandwidth, most people will try to use it to share whatever information they can, be it text, video or voice.

Finally, after this phase is completed, the infrastructure should be completely restored and the entire area struck by the disaster should go back to its standard functionality.

It is however important to minimize the time an area stays in reconstruction phase. The faster a network can be rebuilt the more content will the individuals using it be.

In summary, there should be a way to classify traffic and to offer QoS assurances to a number of individuals, like the search and rescue teams; the network should work with 0 or very little infrastructure and be easily extendable; reconstructing the original network should be as simple and as time and cost effective as possible.

To add to the above mentioned features we should also add that security can prove to be a huge concern. Individuals can try and disable the remaining network. Individuals can use information they gather on the network to do more harm. A network should be able to withstand any cyber-attack that can be used against it. This means the use of a number of security protocols and security considerations. The ability to remotely remove malicious individuals from the network could prove a huge benefit.

It is important to add that some individuals can create a high load on the network without even realizing they are doing a great decrement to everyone else. Take for instance a network with very low band-width and an individual that streams video that he considers is relevant for a search and rescue. This individual needs to be stopped without permanently blocking his access to the network.

4. Current networking alternatives for disaster scenarios

Wired networking solutions are the most popular to support disaster management operations at the moment, because of the high bandwidth they provide. Also, the security is higher, because the medium provides low direct access (it is more difficult to connect to the network simply because the access requires a physical connection). Furthermore, wired networking gives certain assurances to the user. Once connected, it is difficult for instance to lose connection, like the case with a

Wi-Fi network in which movement inside a house can affect the performance of the connection and there can even be a complete loss of signal.

The price of a wired network is a complicated topic however. Deploying a temporary small area (inside a house or a room) network is extremely cheap because the devices and technology used have their price lowered by the popularity of the medium. However, deploying such a network on a large scale requires taking certain assurances that the cables used to form the connections are always secure and safe, regardless of changes in the location in which they have been deployed. Cables need to be put up on posts or underground to assure no one has direct access to them. Some need even more extensive protection against rodents or other such animals that can damage the cable.

We have to keep in mind that most wireless connection requires a wired backbone. If such a backbone is not available the price for a large scale wireless network rises because the technology to support large distance or to position directed antennas is nor as widely used. Wireless networks also have signals that overlap each other, for instance Wi-Fi 802.11b has only 4 non-overlapping frequencies available. This means that an entire Wi-Fi 802.11b network can only support 4 distinct connections before suffering a loss of performance. This means that building a large scale Wi-Fi Network requires either a strong wired backbone or special technology that can sustain high bandwidth connection between the center devices.

If bandwidth is not a strict requirement the deployment of a wireless only network is possible, this is proved by projects such as Loon [36]. Project Loon plans to put a fleet of balloons in the sky with wireless equipment and solar panels to provide power. Each balloon has a theoretical area limit of 40 km's. Deploying a large number of these devices can provide a cheap networking alternative even in places with sparse population. However these devices do not offer high bandwidth or low latency and require specialized equipment for every connecting node on the ground.

Further on, we will not discuss wired networks as they do not provide a cost effective way of deployment in the scenarios we are interested in. Furthermore, deployment can take a lot of time. We do mention these networks as they stand as backbone for most of the wireless alternatives we present.

The Public Safety/Security (PSS) sector currently relies on Professional Mobile Radio (PMR)/TETRA networks due to its benefits on high security and resilience. As a result, PSS organizations lack advanced communication functionality because TETRA is currently lagging behind the commercially available networks (3G, LTE, WIMAX etc.) in terms of data rate, speed, and coverage (see Table 1). According to Gartner, the trend towards a more data centric set of operational services in PSS services (e.g. image/video communication) will follow that of the wider commercial market, where data traffic has increased significantly. However, the current TETRA network is unsuitable to host most data centric applications and services [21] and would need to adopt wireless and mobile broadband networks.

Moreover, with more industries becoming reliant on mobile communications (as part of their operations and/or service offerings), there will be an increased demand for more complex mobile device functionality and application (e.g. GPS and other remote sensing applications). Apart from increased pressure on the network providers (as mentioned above), this will also put more pressure on the processing/energy resource of the mobile device which has a memory capacity and processing power limitation. This increases the need to intelligently manage mobile device resources and ensure resources are available when needed.

There is a need for a future communication network to cope with the projected industry growth of mobile and fixed connected devices and satisfy the needs and requirements across all industry sectors (including PSS). This need is in line with the Digital Agenda Europe (DAE) [22], which aims to help Europe's citizens and businesses to get the most out of digital technologies. It particularly aligns with pillars II (Interoperability & Standards), IV (Fast and ultra-fast Internet access), and VII (ICT-enabled benefits for EU society); address the specific actions around telecoms and the Internet [23]. Hence, this future network will need to be:

- High-speed and secure, with high quality-of-service (QoS) and quality-of-experience (QoE) for users.
- Resilient, robust, flexible across spectrum and always available.
- Energy-efficient and capable of managing mobile device and network resource intelligently.

Public Safety and Security (PSS) organizations, such as law enforcement, ambulance services, fire services, and other civil emergency/disaster management services, are tasked with providing public safety and security service. Due to the nature of the services, mobile communication is a main requirement and Professional Mobile Radio (PMR) communication systems are extensively relied on to conduct critical operations.

Specification	Frequency	Spectrum	Coverage (Urban - Rural)	Data rate	Latency
TETRA	400, 800 MHz	5 - 20 MHz	5 - 15 Km	13 Kbps	250 ms
TEDS	400, 800 MHz	20 MHz	2 - 7 Km	20 - 80 Kbps	200 ms
GSM	900 MHz	35 MHz	40 - 100 Km	11.4 - 22.8 Kbps	800- 3000 ms
WI-FI	2.4, 5 GHz	20 - 40 MHz	5-20m (indoor) to 2 Km (Outdoor)	50 Mbps - 1 Gbps	5 - 20 ms
3G/UMTS	900, 1800, 2100 MHz	30 - 50 MHz	1.5 – 4 Km	64 - 384 Kbps	170 ms
HSDPA	1800, 2100 MHz	10 - 15 MHz	500m - 1.5 Km	1.8 - 7.2 Mbps	60 ms
WIMAX	700 MHz, (2.4, 3.5, 5.8) GHz	200 MHz	400m - 1Km	4 - 20 Mbps	30 ms
LTE	700, 1800, 2100 MHz	18 - 60 MHz	300 - 800 m	10 - 100 Mbps	10 ms

Table Error! No text of specified style in document.**: Characteristics of the various Communication Standards.**

TETRA is the widely accepted communication network choice in Europe. PSS organizations cannot afford the risk of failures in their ‘mission critical' communications (voice, data or video), hence they require: resilient and highly available infrastructure; reliable and secure communication; point-to-multipoint communication; large geographical coverage; and (recently) interoperability between different PSS organizations locally and across borders. This can only be ensured by a robust, secure and resilient mobile and fixed communication network infrastructure. Also, for these organizations to be adequately prepared to tackle any future event like those previously witnessed (September 11th World Trade Centre attack, the Atocha (Madrid) bombing, the London underground attack, the major earthquake in Van, Turkey), they need to be properly equipped.

There are needs for new advanced applications envisioned in the next generation PSS communication such as:

- Remote sensor networks (personnel monitoring, forest fire tracking or water/flood level monitoring).
- Multi-functional mobile terminals (real-time video, biometric data, ID verification, image transfer).
- Remote database access, device control, etc.

However, with the growing demand for resilient, reliable and secure high-speed data communication, the current capacity for PSS communication network (i.e. TETRA) will be exceeded. It is considered likely that an upgrade or replacement in current network will be required across Europe in the next 5-10 years. TETRA is constantly being evolved by ETSI (European Telecommunications Standards Institute) and new features are being introduced to fulfill the growing PSS requirements. Like GSM moving to GPRS, EDGE, 3G/UMTS, and now LTE, TETRA attempted to evolve to satisfy increasing user demand for new data services by upgrading the original TETRA standard (TETRA 1, which had less emphasis on data) to TETRA 2 (TETRA Enhanced Date Service - TEDS). However, demand growth for frequencies and more data intensive applications is likely to go beyond TEDS’s capacity and will not satisfy future needs for the essential services highlighted.

After TETRA 2, an attempt has been made to continue working on TETRA 3 (also called TETRA Broadband, DAWS and MESA), but the development of this standard has officially been cancelled [24]. This is because PSS network manufacturers and operators cannot afford the several billion euro research and development budgets to develop next generation PMR mobile radio network in parallel to or even ahead of commercial networks. Even if they could, it may take as long as 10 years to plan and deploy such network [25]. Hence, there is the need to extend the capabilities of PSS communication by interfacing with commercial communication networks.

A new ETSI working group has started working on the standardization of mission-critical broadband communications, whereby LTE has been opted for as the basis for this standard. This is because of the increasingly rapid progress in the capability of communication technologies deployed in the commercial network, particularly with regard to over-the-air data rates and the spectrum efficiency that can be achieved. This has seen the rise of an increasing gulf between the capabilities of commercial networks and dedicated PSS networks. However, replacing TETRA with LTE is not a short term option, for many reasons. First of all, LTE does not yet support the voice communication features of TETRA and secondly, there is a huge TETRA infrastructure that cannot be replaced rapidly. This infrastructure needs to be used effectively.

There has been strong research effort in the last decade on the development and integration of new wireless access technologies for mobile Internet access. This is considered by many experts to be the de-facto direction for future researches to support disaster management, as mobile phones and tabletPCs become more commonly encountered everywhere, and their communication capabilities could be used to sustain mobile wireless networks in support for rescue procedures. But, still, such wireless network will need to work with wired backbones, so researchers investigate various means to create next-generation heterogeneous networks. Among the main research concepts for taking advantage of the availability of various heterogeneous networking technologies in place, Always Best Connected (ABC) and Quality of Experience (QoE) Bandwidth Aggregation concepts have been at the center of attention.

- *Always Best Connected* implies that end-users expect to be able to connect anytime, anywhere – also when on the move – by their terminal of choice. End-users also expect to be able to specify in each situation whether "best" is defined by price or capability. However, the current state-of-the-art solutions, such as IETF Mobile IPv6 (MIP) or the emerging Host Identity Protocol (HIP), mainly focus on mobility management, instead of considering additional user-related issues, such as user preferences, associated cost, access-network operator reputation, and trust and mainly application-related issues like (Quality of Service) QoS and failure recovery in conjunction with mobility.
- *Quality of Experience (QoE)* reflects the collective effect of service performances that determines the degree of satisfaction of the end-user, e.g. what the user really perceives in terms of usability, accessibility, retain-ability and integrity of the service. Seamless communications is mostly based on technical Network QoS parameters so far, but a true end-user view of QoS is needed to link between QoS and QoE. While existing 3GPP or IETF specifications describe procedures for QoS negotiation, signalling and resource reservation for multimedia applications (such as audio/video communication and multimedia messaging, support for more advanced services, involving interactive applications with diverse and interdependent media components) is not specifically addressed. Additionally, although the QoS parameters required by multimedia applications are well known, there is no standard QoS specification enabling to deploy the underlying mechanisms in accordance with the application QoS needs.

One of the early attempts to provide all-IP architecture and integrate different access technologies for public safety communications was by the project MESA (Mobility for Emergency and Safety Applications), an international partnership project by ETSI and TIA dating back to 2000 [26]. A.K. Salkintzis proposed a solution for integrating WLAN and TETRA networks that fits to the all-IP architecture of MESA and allows TETRA terminals to interface the TETRA infrastructure over a broadband WLAN radio access network instead of the conventional narrowband TETRA radio network, while remaining fully interoperable with conventional TETRA terminals and services. Chiti et al. [27] proposed a wireless network that aims to interconnect several heterogeneous systems and provide multimedia access to groups of people for disaster management. The authors address the issues of heterogeneous network interconnection, full and fault tolerant coverage of the disaster area, localization to enable an efficient coordination of the rescue operations, and security. The focus of this work is on the use of WiMAX-based wireless network as a backbone to provide reliable and secure multimedia communications to operators during the disaster management. Also, Durantini et al. [28] present a solution for interoperability and integration among Professional Mobile Radio systems (TETRA and Simulcast), public systems (GSM/GPRS/UMTS), and broadband wireless technologies, such as WiMAX, with the aim of enabling distributed service provisioning while guaranteeing always best connection to bandwidth demanding applications provided by an IP-based core network. Furthermore, the authors address the issue of optimizing the quality of service management in a multi-network environment, and propose a QoS mapping between WiMAX QoS classes and TETRA service typologies.

Alcatel-Lucent recently demonstrated at TETRA World Congress a very interesting use case for TETRA communications over an LTE network. A Standardized Digital Professional Mobile Radio systems user with a TETRA client application running on an LTE rugged terminal, can communicate with other TETRA users over an LTE network, while using all of the TETRA services. This option opens the way to TETRA/LTE hybrid solutions combining the best features of the two technologies to provide broadband overlay services to existing TETRA networks. There is a multitude of other similar work focusing on the integration of various network technologies in and out of the scope of public safety communications. However, solutions available to date are fragmented and each considers only a subset of the ideal QoE-aware and autonomous connectivity solution that can also simultaneously exploit all available network interfaces. During large scale emergencies and disasters, it is crucial to aggregate the scarce communication resources of multiple technologies and be able to use simultaneously, since the leftover capacity of a single technology may suffer due to infrastructural damages.

An alternative consists in the incorporation of Multipath TCP into the wireless communication world. The transmission control protocol (TCP), which serves as the data transport basis of many telecommunication services of today, was designed to work on single links and does not cope well with the simultaneous use of multiple links at the same time. A survey of TCP performance in heterogeneous networks [29] shows the existing solutions to date and their problems. Magalhaes et al. present a solution for channel aggregation at the transport layer, called R-MTP (Reliable Multiplexing Transport Protocol), which multiplexes data from a single application data stream across multiple network interfaces [30]. The recent EU-funded ‘Trilogy’ project introduced the Multipath TCP (MPTCP) solution, towards enabling the simultaneous use of several paths by a modification of TCP that presents a normal TCP interface to applications, while in fact spreading data across several subflows [31]. An IETF working group has been formed to develop the MPTCP protocol, which is an on-going effort. However, through extensive evaluation studies over MPTCP, some authors [32] report that heterogeneous network environment (Ethernet, Wi-Fi and 3G) has a great impact on MPTCP throughput and reveals the need of an intelligent algorithm for interface selection in MPTCP.

In terms of security, the Terrestrial Trunked Radio (TETRA) supports two types of security: air-interface security and end-to-end security. Air-interface security [33] protects user's identity, signaling, voice and data between mobile station (MS) and base station (BS). It specifies air-interface encryption, (mutual) authentication, key management (OTAR: over-the-air-rekeying) and enable/disable functionality. End-to-end security [34] encrypts the voice from MS to MS. Current candidates as encryption algorithms are IDEA (owned by MediaCrypt AG) and AES as the encryption schemes.

One of the main challenge for multi-technology communication is the compatibility problem between the security mechanisms (encryption, authentication, integrity and key management) supported by these technologies. Wireless LAN supports various security mechanisms, uses of which are mostly optional. MAC address filtering and hidden service set identifier (SSID) are the simplest techniques. Today very few access points use Wired Equivalent Privacy (WEP) because many cracking tools are publicly available on Internet. Wi-Fi Protected Access (WPA and WPA2 based on 802.11i) are introduced to overcome this problem but weak passwords are still a problem. 802.1x defines the encapsulation of the Extensible Authentication Protocol (EAP), and enables authentication through third party authentication servers such as Radius and Diameter. End-to-end security can be provided by use of Internet Protocol Security (IPSEC), Transport Layer Security (TLS), Secure Sockets Layer (SSL), Secure Shell (SSH), pretty Good Privacy (PGP), etc. Security of GSM and 3G suffers from similar compatibility problems with TETRA. GSM security defines Subscriber Identity Module (SIM), the MS, and the GSM network. SIM hosts subscribe authentication key (K), Personal Identification Number (PIN), key generation algorithm (A8) and authentication algorithm (A3). MS contains the encryption algorithm (A5) for air interface. Encryption is only provided for the air-interface. 3G security builds upon the security of GSM. It addresses the weaknesses in 2G systems with integrity and enhanced authentication as well as with enhanced encryption using longer keys and stronger algorithms.

Another challenge in multi-technology communication is that most of the security mechanisms are optional, and they are maintained based on the policies of different administrative domains. An end-to-end connection between two MS may go through an unsecure public network which may permit in variety of attacks including denial-of-service and man-in-the-middle. Cost of mitigating these attacks on MS side may be higher than the benefit of the connection in terms of Quality of Service (QoS) and Quality of Experience (QoE) metrics. Therefore, QoS and QoE mechanisms must involve related metrics to provide predictable security service levels to the end users [35].

5. Ad-hoc Networking alternatives

Worldwide communication networks are growing exponentially, with close to 80 per cent of the world's population now enjoying access to a mobile phone [37]. And with more mobile devices than people in 97 countries around the world, the mobile communication industry in particular is constantly evolving and growing at a rapid pace. This is due to the impact made by exciting new devices including iPhone, Android, Windows phone and tablets [38]. Besides the volume of devices in the market, the data consumption is also surging, with a recent Ericsson Mobility Report [39] estimating that *mobile data traffic doubled in just one year between 2011 and 2012*. It also estimated that *by 2018, demand for mobile data will increase by a factor of 12*.While this exceptional pace of growth is exciting, it also presents a whole new set of challenges as network service providers need to invest in improving network speed, flexibility, availability, utilization and efficiency.

From mobile phones, tablets, laptops and devices such as smart appliances/meters, it is predicted that *more than 50 billion devices will be connected to the web by 2020* [40] as the 'Internet of Things' concept develops further. It is estimated that there are currently approximately 14 billion devices connected to the Internet. Hence, the forecast is predicting this number to almost quadruple by 2020 with *social network, commerce, transport, public safety/security, entertainment and utilities industries being dependent on wireless and mobile broadband services and having increased data usage* [41].

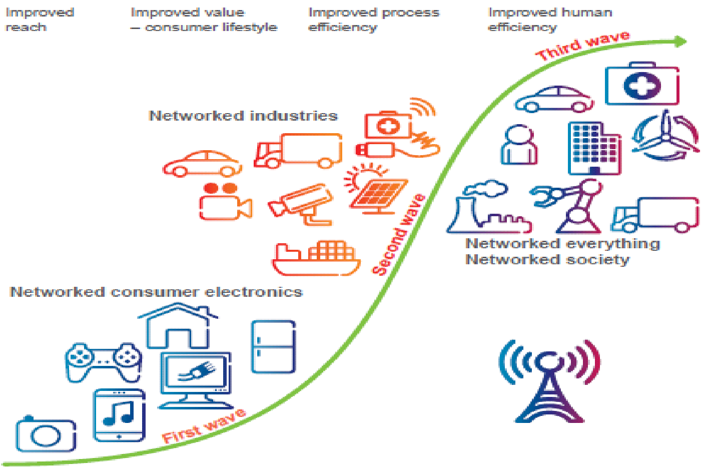
Improved reach
Improved value – consumer lifestyle
Improved process efficiency
Improved human efficiency
Third wave
Networked industries
Second wave
Networked everything
Networked society
Networked consumer electronics
First wave

Figure 1. The Development Waves of Connected Devices

Mobile Ad Hoc Networks are multi hop networks where nodes can be stationary or mobile and they are formed on a dynamic basis. They allow people to perform tasks efficiently by offering unprecedented levels of access to information. In mobile ad-hoc networks, topology is highly dynamic and random and in addition, the distribution of nodes and their capability of self-organizing play an important role. Their main characteristics can be summarized as follows:

- Topology is highly dynamic and frequent changes in the topology may be hard to predict.
- Based on wireless links, this may have a lower capacity than their wired counterparts.
- Physical security is limited due to the wireless transmission.
- Affected by higher loss rates and can present higher delays/jitter than fixed networks due to wireless links.
- Nodes rely on batteries or other exhaustible means for their energy. As a result, energy savings are an important system design criterion.
- Furthermore, nodes have to be power-aware: the set of functions offered by a node depends on its available power (CPU, memory, etc.).

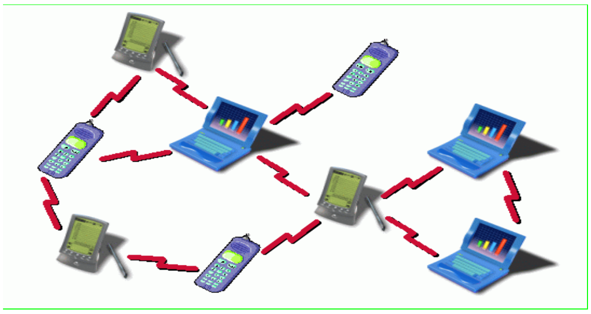

Figure 2. Mobile Ad-Hoc Network

A well-designed architecture for mobile ad-hoc networks involves all networking layers, ranging from the physical to the application layer. Power management is of paramount importance and general strategies for saving power need to be addressed, as well as adaptation to the specifics of nodes of general channel and source coding methods of radio resource management and multiple accesses. In mobile ad-hoc networks, with the unique characteristic of being totally independent from any authority and infrastructure, there is a great potential for a user-centric network (users in control). Two or more users can become a mobile ad-hoc network simply by being close enough to meet the radio constraints, without any external intervention.

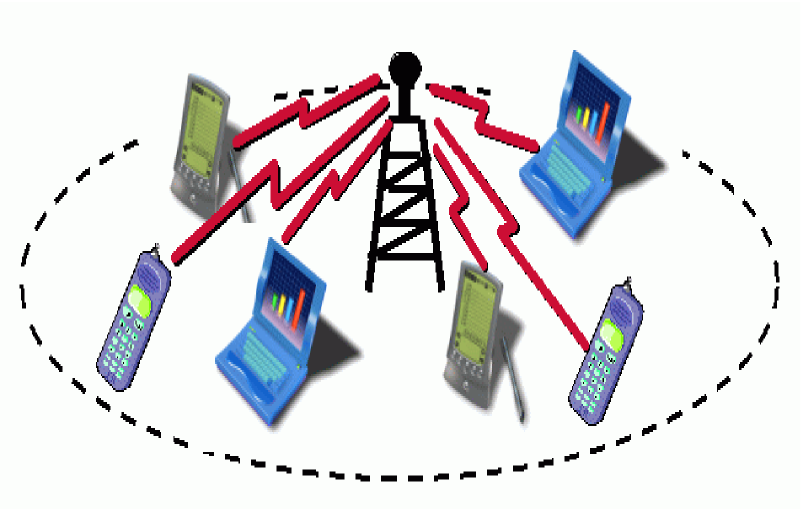

Figure 3. Infrastructure Based Wireless Network

Delay Tolerant Networks also known as DTNs are an important branch of Ad-Hoc Networks. These networks work on the assumption that nodes in the network are sparse and very mobile. Here we use nodes based on a probability that the other node will be able to transmit the package, without any assurances. As such a store-and-forward policy is needed.

A node stores messages that do not have itself as a destination and collects messages for the destinations it has a high probability to encounter in the near future. When a destination or a node with a bigger probability of success is reached the packages are forwarded to this other node.

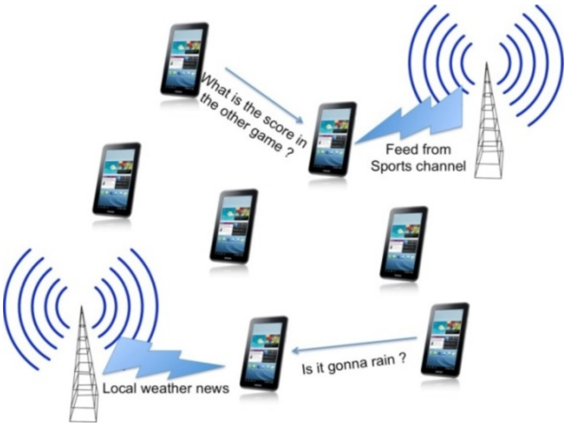

Figure 4. Delay Tolerant Network

It is important to not see DTN networks as a standalone network. At any point in the process a node can choose to forward the packets to an existing backbone.

This is usually done on a node by node basis, as the cost of forwarding to a backbone can vary greatly. Because of this property a DTN network can even be used to join two or more distinct pieces of Network that have lost connection between them because of a natural disaster or a similar incident.

A DTN has also an extremely important property of being very low cost. Being based on devices that are already ubiquitous in most areas and having the possibility to be deployed using inexpensive computers like the Raspberry Pi the network can function without any other infrastructure. There are papers like the case of TRIAGE [49] that try to offer a delay tolerant solution specifically for disaster scenarios. Furthermore DTN networks can be used to deliver important sensor data in case of a disaster scenario [51] even if the infrastructure normally used to gather this data is down.

There are already a large number of proposals for algorithms that work in this manner and studying the complex requirements of each of them is beyond the scope of this paper. **Epidemic** [42] tries to get the biggest number of packets to their destination, to achieve this it sends each packet to all the nodes that it encounters if the node has not yet received that packet. This assures that Epidemic has the highest cost and delivery rate from all the DTN algorithms. **Wait** [43] does the complete opposite of Epidemic, it sends packets only to the destination. As such the cost of delivering all packets is equal to the delivery ratio and they are both low. Both Epidemic and Wait are algorithms that are not meant to be used in real life scenarios: Epidemic has a very high cost and assumes that devices have unlimited memory resources while Wait has a delivery ratio that is unacceptably low in most scenarios.

Multiple-Copy-multiple-hoP [44] is a version of Epidemic in which the packets are sent only for a number of hops and only a limited number of copies are created every time. This algorithm can provide a well enough comparison for any others as its performance is acceptable for real-life scenarios.

dLife [45] assumes a pattern in the way nodes encounter each other. Using this assumption daily statistics are calculated and nodes receive a social weight. **Rank** [44] makes the assumption that some nodes are more popular than others and packets are forwarded to these nodes in hope that it has a higher chance of meeting the destination. In our experience Rank has extremely good results in both delivery ratio and cost.

Label [46] assumes that nodes are grouped in communities and to forward a packet it is first important to have it reach the community of the destination. Label does require a way to determine the community, before the packets are forwarded, this can be done in a static manner or calculated while the network is being used. **BUBBLE Rap** [44] makes a merger between rank and label and tries to forward packets so that they both reach the community they are intended for and the most popular nodes in each community. There are 2 versions the initial one, A, and the modified version, B, that removes a packet after it was forwarded.

PRoPHET [47] uses contact history to compute the probability of encountering another node. This metric is called delivery predictability and one such value should exist for any 2 node combination in the network, although not all values need to be stored. This value is then used to send a packet on an increasing probability path to the destination.

PROPICMAN and **CiPRO** [48] use context information to determine the path, any data is useful like information of where an individual carrying a node lives or where he works. This information is not always available and people might be reluctant to share it.

To evaluate the feasibility of such opportunistic routing algorithms, for disaster management, we developed the CCPAC simulator (http://ccpac.hpc.pub.ro/). Furthermore, we used the simulator in a series of realistic experiments, where we compared all previously mentioned algorithms.

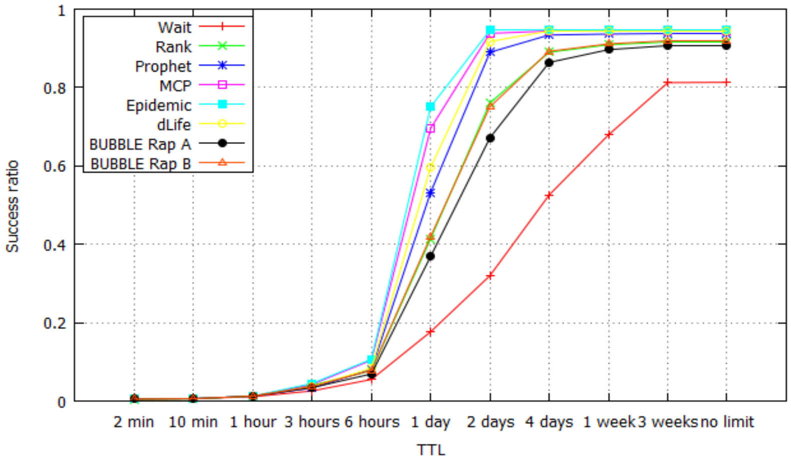

Figure 5. Random Waypoint Delivery Ratio

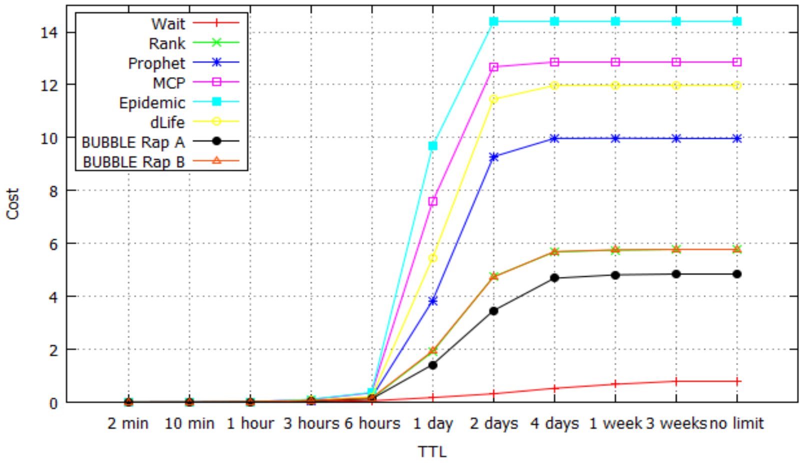

Figure 6 Random Waypoint Cost

The experimental scenario used for this case was a Random waypoint simulation, in which nodes where moving randomly. We have conducted similar tests on real life traces and the results are very similar, with only small variations in algorithms performance.

These figures should offer a comparison view of the presented algorithms, they all have their individual stats and performance issues and choosing one of them should take into account the scenario in which they should be used.

6. Conclusion

In this paper we have presented a number of scenarios in which building and sustaining networking infrastructure can be a complex matter. We have presented the existing types of networking solutions available at the moment and we have discussed their advantages/disadvantages in these scenarios.

We strongly believe that the best way to insure functionality in extreme scenarios and especially after natural disasters technologies that assure operability between different networking systems [51] are needed. This is probably the best way to assure simple, fast and efficient deployment of an infrastructure.

DTNs have proven to be an emerging trend that is stimulated by the mass usage of mobile devices such as smart phones. These networks are extremely resilient because they do not require any infrastructure. Furthermore one can use a DTN network to insure connection between different networks that, during a disaster, or from some other cause have lost connectivity.

One can envision many scenarios in which these networks and interoperability between them can lead to a safer world.

References

1. Chen, Lei-da, et al. "Small business Internet commerce: a case study." *Information Resources Management Journal (IRMJ)* 16.3 (2003): 17-41.
2. Chen, Kuanchin, J. Michael Tarn, and Bernard T. Han. "Internet dependency: its impact on online behavioral patterns in e-commerce." *Human Systems Management* 23.1 (2004): 49-58.
3. Böhmer, Matthias, et al. "*Falling asleep with angry birds, facebook and kindle: a large scale study on mobile application usage*." Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services. ACM, 2011.
4. Ulusu, Yesim. "Determinant factors of time spent on Facebook: brand community engagement and usage types." *Journal of Yasar University* 18.5 (2010): 2949-2957.
5. Curran, Kevin, Scott Morrison, and Stephen Mc Cauley. "Google+ v Facebook: The Comparison." *TELKOMNIKA* (Telecommunication, Computing, Electronics and Control) 10.2 (2012): 379-388.

6. Java, Akshay, et al. "*Why we twitter: understanding microblogging usage and communities*." Proceedings of the 9th WebKDD and 1st SNA-KDD 2007 workshop on Web mining and social network analysis. ACM, 2007.
7. Duncombe, Constance. "*The twitter revolution? Social media, representation and crisis in Iran and Libya*." Australian Political Science Association Conference (APSA) 2011. School of Politics & International Relations, 2011.
8. Guha, Saikat, and Neil Daswani. "*An experimental study of the skype peer-to-peer voip system*". Cornell University, 2005.
9. Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The Internet of things: A survey." *Computer Networks* 54.15 (2010): 2787-2805.
10. Shapiro, Jesse M. "Smart cities: quality of life, productivity, and the growth effects of human capital." *The review of economics and statistics* 88.2 (2006): 324-335.
11. Caragliu, Andrea, Chiara Del Bo, and Peter Nijkamp. "*Smart cities in Europe*". Vrije Universiteit, Faculty of Economics and Business Administration, 2009.
12. Mahizhnan, Arun. "Smart cities: the Singapore case." *Cities* 16.1 (1999): 13-18.
13. Fuller, Sherrilynne S. "Internet connectivity for hospitals and hospital libraries: strategies." *Bulletin of the Medical Library Association* 83.1 (1995): 32.
14. Armbrust, Michael, et al. "A view of cloud computing." *Communications of the ACM* 53.4 (2010): 50-58.
15. Oyelaran-Oyeyinka, Banji, and Kaushalesh Lal. "Internet diffusion in sub-Saharan Africa: A cross-country analysis." *Telecommunications policy* 29.7 (2005): 507-527.
16. Woodcock, Bill, and Packet Clearing House. "*Overview of the Egyptian Internet Shutdown*." (2011).
17. Clayton, Richard, Steven J. Murdoch, and Robert NM Watson. "*Ignoring the great firewall of china*." Privacy Enhancing Technologies. Springer Berlin Heidelberg, 2006.
18. Bailey, Michael, and Craig Labovitz. "Censorship and Co-option of the Internet Infrastructure." *Ann Arbor* 1001 (2011): 48104.
19. http://english.ahram.org.eg/NewsContent/1/64/67894/Egypt/Politics-/Egypts-military-stops-attempt-to-cut-Internet-cabl.aspx (21-06-2013), last accessed June 20, 2013.
20. Upton, Eben, and Gareth Halfacree. "*Meet the Raspberry Pi*". Wiley, 2012.
21. Feature: Airwave 'Could Be Replaced', Police Oracle, http://www.policeoracle.com/news/Police+IT+and+Technology/2013/Feb/19/Feature-Airwave-Could-Be-Replaced_61319.html (February 19th, 2013), last accessed June 20, 2013.
22. Digital Agenda Europe, http://ec.europa.eu/digital-agenda/digital-agenda-europe, last accessed June 20, 2013.
23. Telecoms Internet, Europe, http://ec.europa.eu/digital-agenda/telecoms-Internet-0, last accessed June 20, 2013.
24. TETRA standard and applications, http://www.tetra-applications.com/item.html&objID=15774, last accessed June 20, 2013.
25. The evolution of TETRA, white paper, http://www.p3-group.com/downloads/4/1/7/5/P3_-_Evolution_of_TETRA_-_White_Paper_-_v1.0.pdf, last accessed June 20, 2013.
26. The MESA project, http://www.projectmesa.org, last accessed June 20, 2013.

27. Chiti, F.; Fantacci, R.; Maccari, L.; Marabissi, D.; Tarchi, D.;, "A broadband wireless communications system for emergency management," *Wireless Communications*, IEEE , vol.15, no.3, pp.8-14, June 2008.

28. Durantini, A.; Petracca, M.; Vatalaro, F.; Civardi, A.; Ananasso, F.;, "*Integration of Broadband Wireless Technologies and PMR Systems for Professional Communications*," Networking and Services, 2008. ICNS 2008. Fourth International Conference on , vol., no., pp.84-89, 16-21 March 2008.

29. Barakat, C.; Altman, E.; Dabbous, W.;, "On TCP performance in a heterogeneous network: a survey," *Communications Magazine*, IEEE , vol.38, no.1, pp.40-46, Jan 2000.

30. Magalhaes, L.; Kravets, R.; , "*Transport level mechanisms for bandwidth aggregation on mobile hosts*," Network Protocols, 2001. Ninth International Conference on , vol., no., pp. 165- 171, 11-14 Nov. 2001.

31. Barré S.; Paasch C.; Bonaventure O.; "*MultiPath TCP: From Theory to Practice*," Proceedings of the IFIP Networking Conference, 2011.

32. Nguyen, Sinh Chung; Nguyen, Thi Mai Trang; , "*Evaluation of multipath TCP load sharing with coupled congestion control option in heterogeneous networks*," Global Information Infrastructure Symposium (GIIS), 2011 , vol., no., pp.1-5, 4-6 Aug. 2011.

33. Terrestrial Trunked Radio (TETRA), Voice plus Data (V+D), Part 7: Security, ETSI EN 300 392-7 V3.2.1 (2010-06).

34. Terrestrial Trunked Radio (TETRA), Direct Mode Operation (DMO), Part 6: Security, ETSI EN 300 396-6 V1.4.1 (2010-07).

35. Evdoxia Spyropoulou, Chris Agar, Timothy Levin, Cynthia Irvine, "*IPsec Modulation for Quality of Security Service*", Proceedings of the International Systems Security Engineering Conference, 2002.

36. The Loon project, http://www.google.com/loon (24-06-2013) , last accessed June 20, 2013.

37. International Telecommunication Union, October 2010.

38. The new mobile world order, http://www.cisco.com/web/about/ac79/docs/sp/New-Mobile-World-Order.pdf, last accessed June 20, 2013.

39. Erricson, Mobility report, http://www.ericsson.com/res/docs/2012/ericsson-mobility-report-november-2012.pdf, last accessed June 20, 2013.

40. 50 billion devices online by 2020, The Telegraph, http://www.telegraph.co.uk/technology/Internet/9051590/50-billion-devices-online-by-2020.html, last accessed June 20 (January 31, 2012), 2013.

41. Erricson, http://www.ericsson.com/res/docs/whitepapers/wp-50-billions.pdf, last accessed June 20, 2013.

42. A. Vahdat, D. Becker. "*Epidemic routing for partially connected ad hoc networks*". Technical Report CS-200006, Duke University, 2000.

43. T. Spyropoulos, K. Psounis, C.S. Raghavendra. "*Single-copy routing in intermittently connected mobile networks*". In Proc. Of First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON 2004), pp.235-244, Oct. 2004.

44. P. Hui, J. Crowcroft. "BUBBLE Rap: Social-Based Forwarding in Delay-Tolerant Networks". *IEEE Transactions on Mobile Computing*, vol. 10, no.11, pp. 1576–1589, 2011.

45. W. Moreira, P. Mendes, S. Sargento. “*Opportunistic routing based on daily routines*”. In Proc. of IEEE Int. Symp. World of Wireless, Mobile and Multimedia Networks (WoWMoM 2012), pp. 1-6, June 2012.

46. P. Hui, J. Crowcroft. “*How Small Labels Create Big Improvements*”. In Proc. of the 5th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW '07). Washington, DC, USA, pp. 65-70, 2007.

47. A. Lindgren, A. Doria, O. Schelen. “Probabilistic Routing in Intermittently Connected Networks”. *SIGMOBILE Mob. Comput. Commun. Rev.* 7(3), pp. 19-20, July 2003.

48. H. Anh Nguyen, S. Giordano, A. Puiatti. “*Probabilistic Routing Protocol for Intermittently Connected Mobile Ad hoc Network (PROPICMAN)*”. In Proc. of IEEE Int. Symp. on World of Wireless, Mobile and Multimedia Networks (WoWMoM 2007), pp. 1-6, June 2007.

49. Luqman, F., "*TRIAGE: Applying context to improve timely delivery of critical data in mobile ad hoc networks for disaster response*," Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on , vol., no., pp.407,408, 21-25 March 2011

50. Yu, F.R.; Jie Zhang; Tang, H.; Chan, H. C B; Leung, V.C.M., "Enhancing interoperability in heterogeneous mobile wireless networks for disaster response," *Wireless Communications, IEEE Transactions on* , vol.8, no.5, pp.2424,2433, May 2009

51. E. Cayirci, T. Coplu , “SENDROM: sensor networks for disaster relief operations management”, *Wireless Networks*, Vol. 13, No. 3. (2007), pp. 409-423.

52. A. Fujihara and H. Miwa, “Real-time Disaster Evacuation Guidance using Opportunistic Communications,” The 2012 IEEE/IPSJ International Symposium on Applications and the Internet (SAINT2012), pp. 326-331, 2012.

53. A. Fujihara and H. Miwa, “Effect of Traffic Volume in Real-time Disaster Evacuation Guidance using Opportunistic Communications,” Third International Conference on Intelligent Networking and Collaborative Systems (INCoS2012), pp. 457-462, 2012.