Secure and Redundant Public Safety Communication Network for Public Protection and Disaster Relief (PPDR) Organizations

Jari Ahokas, Jyri Rajamäki and Ilkka Tikanmäki

***Abstract*—** European Public Protection and Disaster Relief (PPDR) organizations have similar needs for communications. A common network for PPDR creates synergy and makes interoperability possible. This paper presents a new highly redundant and secure data communications network solution for Public Safety Communications (PCS). The solution is decentralized and communications paths are redundant. Even if the network layer is shared with different users or different use purposes all communications remains secured and access controlled. Distributed Systems intercommunication Protocol (DSiP) offers all of these features in a single solution. This enables building cyber-secure data network for PPDR organizations. Even though the communications channels are reliable and secured, there are still some issues to be considered. This paper introduces these issues and offers solutions for these challenges.

***Keywords*—**Cyber security, Disaster relief, Distributed Systems intercommunication Protocol, Multi organizational environment, Public safety communications.

I. Introduction

IN recent years, the capabilities of Public Protection and Disaster Relief (PPDR) organizations across Europe have been considerably improved with the deployment of new technologies including dedicated Terrestrial Trunked Radio (TETRA) and digital professional mobile radio (TETRAPOL) networks. Nevertheless, a number of events like the London bombing of 7th July 2005, the Schiphol airport disaster and the flooding disasters in 2010 and 2011 have highlighted a number of challenges that PPDR organizations face in their day-to-day work.

Secure and reliable wireless communication between first responders and between first responders and their Emergency Control Centre is vital for the successful handling of any emergency situation, whichever service (Police, Fire, Medical or Civil Protection) is involved.

Security organizations increasingly face interoperability issues at all levels (technical, operational and human) as they interact with other national, regional or international organizations. Not only assets and standards must be shared across Europe to empower joint responses to threats and crisis in an increasingly interconnected network, but also security organizations have to benefit from interoperability functionality in their day-to-day work.

On the one hand Europe is a patchwork of languages, laws, diverse cultures and habits that can change abruptly across borders. On the other hand, even in a same country, each security organization develops its own operational procedures even using incompatible technical solutions within the same country. For efficient operations, many significant challenges need to be addressed, including public safety communication systems (not compatible even when they use the same technology), differing procedures (legal issues) as well as inadequate language skills in cross-border cooperation.

This paper addresses not only the technical security and interoperability issue, but also the complete procedure to build a cyber-secure Public Safety Communication (PSC) system for a multi organizational environment enabling foreign users to cooperate keeping the intrinsic and vital cyber security mechanisms of such networks. Information of other requirements to communications networks and applications such as managing TCP vertical handoff challenges is also included. This paper also presents some of the other available technical solutions for partly producing the same functionality as with DSiP system.

II. Requirements for Public Safety Communication

This chapter identifies the generic requirements for Public Safety Communication (PSC). It addressed specifically the communication requirements that impact first responders.

PPDR field operations are increasingly dependent on ICT systems, especially on wireless and mobile communications. The generic PSC requirements are essentially the need for secure, bi-directional wireless voice communication, but with certain special features not available from the commercial mobile telecommunication network, such as the flexible formation of talk groups, broadcasting, fast call setup, the capability for team leaders to interrupt conversations, and direct-mode communication for cases where network service is either unavailable or disturbed due to the nature of the disaster [1].

Manuscript received May 19, 2012. This work was supported in part by Tekes – the Finnish Funding Agency for Technology and Innovation – as a part of the research project 40350/10 Mobile Object Bus Interaction (MOBI).

J. Ahokas, J. Rajamäki and I. Tikanmäki are with Laurea SID Leppävaara, Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, Finland (phone: +358-9-8868 7400; e-mail:jari.ahokas@laurea.fi, jyri.rajamaki@laurea.fi, ilkka.tikanmaki@laurea.fi).

The TETRA system satisfies a large extent of these requirements, as evidenced by its popularity for PSC in Europe and Asia and recent large sales to police forces in the UK and Germany. The equivalent system in the US is Project 25. Details of the TETRA services can be summarized as [2]:

Secure communications: not only to protect any personal data, but also to prevent eavesdropping or malicious intervention. The TETRA radio standard is defined by European Telecommunications Standards Institute (ETSI). TETRA is based on radio channels with a bandwidth of 25 kHz. Each channel is subdivided in 4 traffic channels using Time Division Multiple Access (TDMA).

The traffic channels can be used for both voice and data. The maximum bit rate is 28.8 kbps if all 4 traffic channels are joined together for one data connection. Average TETRA cells are remarkably larger than GSM cells. TETRA uses typically a frequency of 400 MHz, while GSM uses 900 or 1800MHz which provides much greater range for a single base station. Security is provided through the use of private frequencies and end-to-end encryption. Other features of the TETRA standard:

- Creation of teams (group call) and control hierarchy
- Prioritization (emergency call)
- Broadcasting (e.g. evacuation signal)
- Fast call setup (Push-To-Talk)
- Direct mode communication (no base station)
- Open channel
- Listen-in
- Access to the public network
- Short Data Service

However, today's immediate missing requirement is interoperability, not only between different services, but also within the same service if different systems are in operation between regions. This situation has arisen due to the fact that the different emergency services in each region, in each country had historically much autonomy in the way they developed their networks and the terminal devices they purchased [2].

A solution covering all regions regardless of the available communication technologies would be useful. For example if frontier guard is in the middle of a mission and the target moves to another country. Currently communications problems would make it technically impossible to continue following the target when the officials have entered the other country's territory only a few kilometers since communications to command and control center would be lost because most likely roaming would not work at a foreign territory.

Regarding the next generation of services for first responders, the ETSI MESA project [3] has examined what would be possible if wireless broadband capacity was available; i.e. if some of the technologies that have revolutionized the commercial transport of information (both wired and wireless) in recent years were applied in the PSC market. Fig 1 shows project MESA generic core network architecture picture for public services networks.

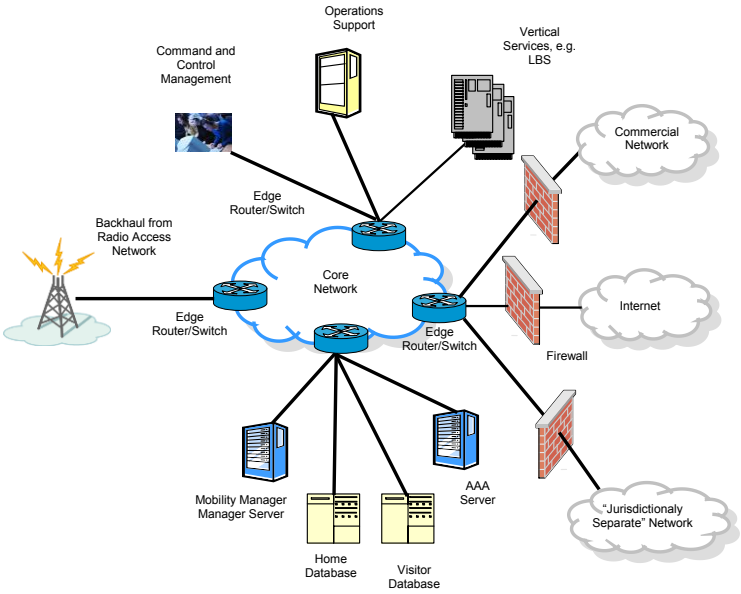

Fig. 1 Project MESA network architecture [3]

From the full list from [3], the ones selected below are considered as being common to all PPDR services:

- Interoperability
- Communication inside buildings
- Improvement in spectrum efficiencies (e.g. reducing channel spacing, using Software Defined Radio, or Cognitive Radio)
- Migration path from existing systems (TETRA, Project 25)
- The ability to remotely partition the network system or bandwidth at a particular site
- Simultaneous access to multiple networks or host computers by a single device, and simultaneous access from multiple user devices to a single host
- Pre-emption: the prioritization of access and routing and the ability to pre-empt non PPDR users (which implies the use of public or open (non-licensed) networks)
- A transaction and audit trail of the use of the network resources
- High-speed, error free transmission: at least 1.5 -> 2Mbps, end-to-end transmit time for data <400ms, end-to-end transmit time for voice <150ms (duplex), <250ms (half duplex) and <400ms if over satellite
- Seamless transparent transfer of devices across networks
- Inherent redundancy
- Typical data to be transported is identified as being:
  - o Voice
  - o Text
  - o Detailed graphical information (e.g. maps)
  - o Images
  - o Video
- Connectivity to local, national and international PPDR databases, and the dynamic updating of database entries from in-vehicle equipment and personal handheld devices
- Remote control of robotic devices
- Geographical position-locating capability

Lack of broadband connectivity of wireless communications for existing and future PPDR applications is a real problem [4]. The rationale behind many of the new services for PPDR actors is that having access to more information at the scene of the emergency, rather than having to request and retrieve it from the Emergency Control Centers, will improve the decision-making process at the scene of a crisis. Every first responder does not need a broadband terminal, but the commander of the mobile rescue team at the scene should have the broadband capability inside a fire engine, police car or ambulance [2].

Some new features can be deployed using the narrowband capabilities of the existing Private Mobile Radio (PMR) spectrum allocated for PSC. Examples are [2]: exploiting the use of sensors in tunnels (or sent into tunnels) to detect temperature, air quality, traffic flow, or built into the clothing of firemen (e.g. location detection, health monitoring), and the electronic tagging of accident victims at the scene and informing the hospital of his/her condition during the ambulance journey.

However, such solutions as the visualization of current traffic congestion on the route to an incident, or enabling remote access to critical information resources such as building plans, satellite photographs, crime databases, etc., depend upon the incorporation of multimedia services that are not feasible over today's PSC networks [2]. For example, descriptions of potential new services from the ETSI MESA group assume bandwidths of at least 1.5 -> 2 Mbps, which would require network infrastructure such as 2.5/3G (EDGE, WCDMA), IEEE802.x (WLAN, WiMAX, 4G/LTE) or satellite [3].

A Finnish study [5] notes that all PPDR actors have the same basic needs for the system, voice and data communication but they also have own distinct requirements. For finding mutual solutions and operation models, system integration is needed. This also enables coherent system design including improved activities, cost savings and improved multi-authority co-operation at the scene.

The roles of complementary technologies in the future are as follow [5]:

• GSM was initially designed as a pan-European mobile communication network. Shortly after the successful start of the first commercial networks in Europe, GSM systems were also deployed on other continents. In addition to GSM networks that operate in the 900 MHz frequency band, others so-called Personal Communications Networks (PCNs) and Personal Communication Systems (PCSs) are in operation. They use frequencies around 1800 MHz, or around 1900 MHz in North America. There are four main standards for 2G systems: Global Systems for Mobile (GSM) communication and its derivatives; digital AMPS (D-AMPS); code-division multiple access (CDMA) IS-95; and personal digital cellular (PDC). 2G/GPRS technologies are reaching the end of their life cycle.

• 3G technology has good coverage with 900 MHz band (better than 2G). However, there are problems on the availability/capacity of commercial networks during major accidents in crowded areas. The 3GPP Long-Term Evolution (LTE) is intended to be a mobile-communication system that is usable in the 2020s. The philosophy behind LTE standardization is that the competence of 3GPP in specifying mobile communication systems in general and radio interfaces in particular shall be used. The result shall not be restricted by previous work in 3GPP. Thus, LTE does not need to backward compatible with WCDMA and HSPA. The first 4G/LTE networks will be at 2.6 GHz, which is not suitable for rural coverage. In future, 800MHz LTE systems are anticipated.

• Wireless local area network (WLAN) technology has three use cases for data transfer: 1) from a vehicle to command and control room at the garage, 2) a local wireless network around the PPDR vehicle at the scene, and 3) from a vehicle to the Internet via a public WLAN; "WLAN fire plug". WLAN has limited range compared to other wireless technologies but bandwidth is generally good and network delay is lower than 3G networks are capable of. A future solution might be WiMAX which provides much larger coverage than WLAN networks are able to provide. Currently WiMAX availability is somewhat limited in Finland.

• Satellite technology has a complementary role when there is no terrestrial communications system coverage. This includes long term usage when no other systems are available and communication need for temporary sites. The telecommunication operator TeliaSonera has announced a start of EutelSat KA-SAT services in June 2011. The service may however be of limited use in PPDR communication applications due to the requirement of a relatively large-size satellite dish antenna, limiting the usability of the service in moving vehicles. A limiting factor is also the requirement of a clear view to a satellite, making it impossible to use satellite communications in an area where a clear view to the sky is unavailable such; as in tunnels or areas with dense forest. Also weather conditions affect satellite communications, heavy rain or snow can weaken the signal considerably. The cost of satellite communications fees (monthly and usage) can be considered an issue.

III. MULTI ORGANIZATIONAL ENVIRONMENT

According to [6] in major disasters no PPRD organization can work alone, but co-operation is needed between different actors. The operational parties should not merely trust on their own resources. Besides, a few organizations possess all the needed areas of expertise in a large-scale event, not to mention a large-scale disaster. Information sharing and training at organizational levels is required in order to achieve a working relationship between the actors. This means the actual and operational interoperability between the first responding organizations; also in reality and in the field – not only on "a paper level" in the form of an official agreement [6].

The military (MIL), public protection and disaster relief (PPDR) as well as critical infrastructure protection (CIP) actors have multiple similar needs. Similarities in disaster relief mission scenarios include 1) serious disruptions in expected functionalities of critical infrastructures, e.g. transport, supplies, infrastructures, 2) operations in remote

areas without communication infrastructures, 3) cross border operations and multi-national teams, 4) high demand for interoperability, 5) no remaining communications infrastructure after a serious disaster, 6) congestion or otherwise not usable commercial networks, and 7) utilizing both AdHoc networks and permanent infrastructures [7]. Similarities in command and control communications involve 1) need to receive information on the operational environment, 2) need for the decision maker to watch operation (live video feed), 3) need to decide and emanate orders, and 4) need to assess the evolution of the operational situation after decision [7].

One possible use case for higher bandwidth and multichannel communications is use of an aircraft patrolling over a disaster area transmitting collected information to the command and control center or the rescue units already at the scene.

IV. CYBER SECURE PUBLIC SAFETY COMMUNICATIONS

Fig. 2 presents a new cyber secure data communications network structure for a multi organizational PPDR environment.

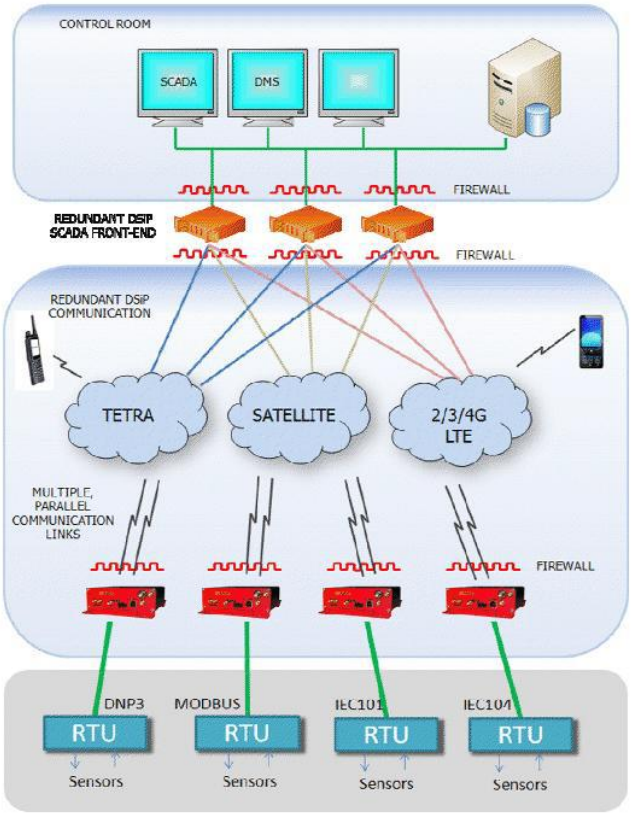

Fig. 2 Cyber secure data communications network structure [8]

The architecture is fully decentralized and all critical communication paths have redundancy. Although having common physical connections, all network actors and elements (multichannel routers, nodes) are identified as well as every organization's all user levels and their rights to different data sources are known.

The decentralized architecture based on the Distributed Systems intercommunication Protocol – DSiP (see e.g. [7], [9]-[10]) is highly fault-tolerant in normal conditions as well as in crises. The software-based approach is independent from different data transmission technologies, from IP core networks as well as from services of telecommunication operators. The solution enables to build a practical and timeless cyber secure data network for multi organizational environment, which being fully decentralized is hard to injure. The networks of different organizations are virtually fully separated, but if wanted they can exchange messages and other information which makes them interoperable.

The DSiP solution is able to offer several benefits:

- Better data security, integrity & priority
- Immunity towards virus infusion
- Immunity towards DoS network attacks
- Intrusion detection
- Authentication- and management tools
- Data-flow handshaking and flow-control
- Controllable data casting and compression
- Interfacing capabilities to equipment and software
- Transparent tunneling of any data
- Early detection of communication problems
- Automatic re-routing
- Cost-efficient network topology
- Insulation from Internet-system flaws
- Routing according to lowest cost and/or shortest hops
- LAN/WAN, TETRA, 2/3/4G, LTE(4G), WLAN, VHF, Satellite etc. communications channels can all be used simultaneously in parallel.

Critical networks and communication solutions require reliable and efficient management and monitoring tools which are easy to operate by command and control center employees. The DSiP solution contains several modules for support, maintenance and configuration of the system.

Authentication Server Software: The DSiP features centralized and mirrorable Authentication Server software. This software allows for maintaining passwords for DSiPnodes. The nodes may have passwords that expire after a specific time for security reasons. Nodes may be allowed in the DSiP routing system and they may be excluded from it at any given time.

Configuration Server Software: The Configuration Server software is an entity for providing routing instructions and firmware updates to nodes. Nodes may be instructed to contact the Configuration Server at any time.

Network Management Server Software: The Network Management Server software constantly monitors the connections in the DSiP system. A graphical tool called DSiPView enables the user to get a visual feedback over the current network function. Nodes marked green are working as normal, yellow indicates anomalies in the functionality and red fatal errors. Users may select a node and query its status. DSiP-Graph is a browser tool presenting various graphs over node latencies, volume of transferred data in a given time etc. [8].

A. *MOBI -Project*

Laurea University of applied sciences (LUAS) has ongoing project called Mobile Object Bus Interaction (MOBI), funded by the Finnish Funding Agency for Technology and Innovation (Tekes). Project's aims are to create a basis for export-striving emergency vehicle concept and to initiate standardization development with like-minded-countries and possible with EUROPOL. There are also three corporate projects exploiting data which are launched alongside with the project. Project has eight work packages; 1) Coordination, 2) User needs, 3) Vehicle infrastructure and power generation, 4) Data communication, 5) Software infrastructure, 6) Applications, 7) Demonstration on police vehicle and 8) Business model development [11].

In MOBI project will be tested a demo vehicle, where among other things is tested similar data communications solution that Fig. 3 illustrates. Demo vehicle is equipped with multi-channel router which is connected satellite-, TETRA, and 3G data networks. Data Communications solution is tested by field tests with the authentic police vehicle, which the Finnish Police Technical Centre has provided for LUAS to enable tests. Fig 3 shows a concept used in demo vehicle.

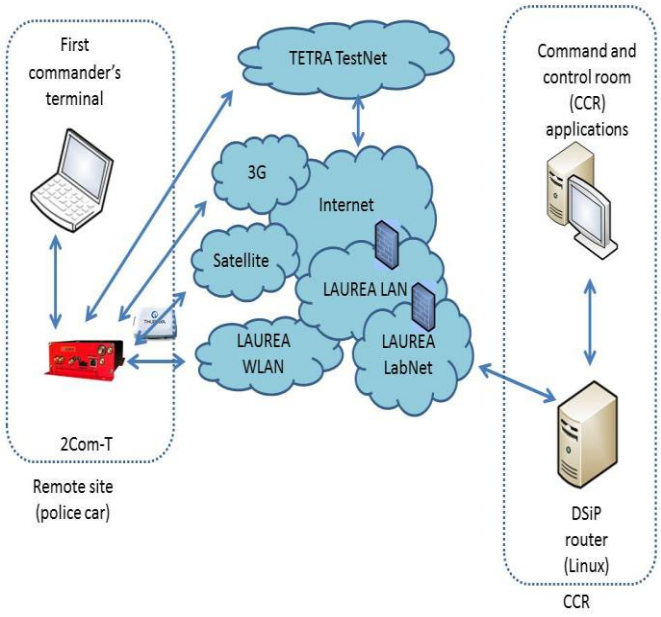

Fig. 3 data communication network structure: case demo vehicle

As shown in Fig. 2, TETRA communication is done by a TETRA test network, which is suitable for this kind of demonstration. There are multiple 3G operators normally used in police cars because of their different coverage in different locations. In this demo we use only one operator's 3G networks. For a satellite communication in this demo is used Spacecom Vehicle Antenna for ThurayaIP and ThurayaIP satellite modem.

Although the TETRA radio network is available, the signal quality may be poor, and system is in practice inoperable. Even if TETRA network is not available, it is not intended to exclude other networks to be used [12].

A multichannel router gives a solution for a problem where is needed duplicated, more than one functional data communication channel for data transmission. The router has opportunities to use several parallel communication paths instead of particular one [8]. In this demonstration is used Ajeco Inc's manufactured 2Com-T Multichannel Router with 3G, TETRA, and Satellite communication channels to vehicle's external communications.

All connection methods do not work in all areas, so several connection methods improve access in the public authorities' information systems (IS) availability. If one of the communication channels, such as 3G network is not available, multichannel router changes the connection automatically for an available network. Multi-Channel Router's Quality of Service (QoS) option sets the desired order of the network access by desired Cost of Service (CoS) value. Therefore, when operating in areas where the network availability and signal strength vary widely, the network exchange should proceed without user noticing it and without breaking the connection.

The user organization will choose in advance whether to use neither the strongest signal nor the cheapest cost network. This selection is done by setting the value of the CoS.

B. *Related Other Public Safety Projects*

There is also another project currently going on which is relying on the same techniques as used in this project. This other project is about securing Supervisory Control and Data Acquisition (SCADA) program communication to power stations and providing enough bandwidth for delivering live video stream from the power stations to the control room. The communications solution is also based on DSiP system using same communications channels and techniques as in PPDR, see Fig 4. Power station control and surveillance communications do not have the same need for mobility as with PPDR units but many of the power stations are located in remote locations thus requiring communications methods like satellite communications. Securing the power distribution network has similar requirements as PPDR and uninterrupted power distribution is equally important to the modern society [13].

DSiP is not the only possibility to solve secure and reliable network requirement. One solution would be the integration of the Crossed crypto-scheme to the SCADA system in Smart Grid environment [14]. It solves the problem of securing communications channels but does not handle the problem of managing several communications channels.

However using only this solution does not answer the question of how to deliver several reliable communications channels seamless to the application. That is; communications without requiring that the application, SCADA in this use case, has complete knowledge of all possible communications channels.

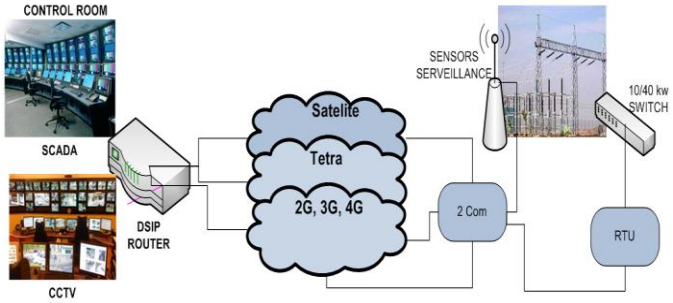

Fig. 4 secure communications for multinational electricity supply deployment [14]

Also tracking of the sea traffic can benefit from the same communications solution as PPDR does. Several sensor nodes collect information of vessels at the sea and transmit this information to the command and control center. This information, such as pictures of the vessel and tracking of the voyage of vessel, is processed at the command and control center and a threat assessment can be made from the collected information. All of these nodes require communications channels and some of the nodes require faster and more reliable connection than the others. DSiP technology is suitable also for this use case when reliability and security is required [15].

C. Other Communications Solutions

As an example it is possible to communicate between communications nodes without supporting infrastructure as ad-hoc basis. This is required when the supporting infrastructure has failed completely because of a natural phenomenon or an act of terrorism or similar event. One solution when using ad-hoc networks is the Ad hoc On-Demand Distance Vector (AODV) algorithm [16]. The AODV algorithm makes communications more efficient by enhancing the routing protocol and guaranteeing level of QoS. In this case DSiP solution security measures and seamless roaming from network to network would be temporarily unavailable until connectivity is restored.

In theory it would be possible to transfer data in such a situation where all network communications to the backbone network are completely lost. This technique is called Intermittently Connected Networks (ICN). In practice a data collecting device can collect data and travel to another location where network connectivity is again available and connect to the backbone network and transfer the data the device carried from other cells to the backbone network. Such a device could be data collecting and transmitting unmanned airplane. PPDR organizations could benefit from this kind of technology because of PPDRs could collect data from the disaster area and transfer it to the control room relatively easily compared to other possible solutions such as transferring data with an external memory device manually from the disaster area to a location with functioning network connection.

A more common usage example would involve communications between military groups in a hostile area where normal communications networks are unavailable, unreliable or unsecure for transferring data. Continuous network connection is not required for exchanging situation information and receiving orders from unit commanders.

A modified back-pressure routing algorithm that can separate the two time scales of ICNs is presented in study of [16] ICN. These algorithms are required to make ICNs usable with TCP protocol. This algorithm improves communications performance in demanding environments. On top of this algorithm a rate control protocol implemented for transmissions in order to control the speed of the data transfer when connectivity is available [17].

D. TCP Protocol Challenges with DSiP

The DSiP device and software solution can hide the complexity of the network architecture from the applications and especially form the end users. But a problem with TCP network convergence still exists. When the charcteristics of the unrelaying physical network change rapidly, often and/or considerably, the currently used TCP congestion protocols are unable to follow the change in a timely manner. To mitigate this problem various solutions are available. One possible solution is to modify the senders TCP/IP stack to make it adjust itself faster when the network changes by using techniques improving vertical handoff. The ability to quickly adapt to network changes is essential to VOIP communications and also streaming technologies like live video feed could have issues with rapidly changing network characteristics.

General TCP algorithms for vertical handoffs include Duplicate Selective Acknowledgement (DSACK) which is an extension of TCP SACK in which the receiver reports to the sender that duplicate segment has been received. TCP-Eifel detection algorithm uses TCP timestamps option to detect spurious retransmissions. The Eifel detection provides a faster detection of spurious retransmission timeouts (RTO) compared to DSACK algorithm. Forward RTO-Recovery is a TCP sender-only implemented algorithm that helps detecting spurious RTOs. This doesn't require any TCP options to operate.

The TCP protocol congestion control algorithms have been designed to enable TCP protocol to adapt to the fluctuating bandwidth available on its end-to-end path. TCP connection itself remains fairly stable over the lifetime of the connection. A mobile node can quite easily obtain detailed information regarding the occurrence of a vertical handoff and the status of the wireless link: IEEE 802.21 standard can provide event notifications such as link-up or link quality is degrading.

Proposed enhancements are implemented in the TCP SACK algorithm and they are invoked when a cross-layer notification arrives from the mobile node to the TCP sender. This information contains occurrence of a handoff and rough estimate of the bandwidth and delay for the old and the new access links. Algorithms are incremental in nature and are also conservative it the sense that they are designed not be counter-productive in any situation. Experiments conducted in Linux kernel version 2.6.18 show that performance of the proposed algorithms is quite close to the results obtained in the

simulation experiments. In the absence of the cross-layer information, the proposed enhancements don't affect the normal behavior of the TCP algorithm [18].

E. Quality of Service (QoS)

For communication to be successful it is also important to focus on network traffic prioritizes for different types of communication streams. When Voice Over IP (VOIP) traffic does not have the highest possible priority in the network it would quite easily become impossible to use any IP based network for reliable voice communications. VOIP traffic is unable to handle jitter, delay or packet loss in a decent manner. To solve this issue a suitable QoS mechanism must be utilized. Using a suitable Differentiated Services (DiffServ) scheme helps solving this prioritization problem. This can be achieved by using a suitable QoS management module for controlling traffic prioritization. Centralized management for DiffServ schemes helps managing all the possible QoS parameters since there are many services and several communications channels available and this cumulates to numerous combinations for QoS classes and service levels [19].

V. DISCUSSION

The public safety communication and information management services market is relatively small (in the year 2008 approximately 2 million users in the US, and similar amounts in Europe and Asia) compared with the 3.4 billion mobile phone users in the commercial telephone network [2]. The PSC and information management systems have different needs (reliability, robustness, security and simplicity) from the regular consumer ITC business. Furthermore, different PPDR services in each region had much autonomy, how they developed their networks. This has caused inadequate interoperability. PSC systems (networks, devices, services) also have a long lifespan; the systems being sold today have changed little over the past 25 years [2]. The aforementioned matters present the need for different business models than in the regular consumer ITC services which have a lifecycle of couple of years for support and maintenance.

The two main challenges in European PPDR field operations are the lack of interoperability and the lack of broadband connectivity [4]. Lack of interoperability limits the effectiveness of PPDR practitioners in actual operations, and an evident lack of understanding as to whether these limitations arose from technology, operational procedures, and gaps in procurement or research. Lack of broadband connectivity of wireless communications limits especially the work of the commander of the mobile rescue team at the scene. At least every fire engine, police car and ambulance should have the broadband capability.

Fault tolerant and highly secure network with seamless roaming capabilities alone does not provide a complete solution for authorities in Europe. Even in Finland there is a lack of communication between different authorities like the police and the border guard. Legislation might permit accessing data cross authorities but there is no technical solution to enable access across authorities automatically. Authorities must have a common framework for transferring data between systems and accessing data in all databases available for different actors. One possible solution to improve data sharing between authorities is systems architecture based on cloud computing [20]. This could also increase availability of the systems since it enables faster capacity additions and provides possibilities to host the services at many different locations for disaster recovery purposes. If cloud computing is designed and deployed thoroughly it can help lowering the TCO of IT systems required by PPDR organizations. This also increases the need for reliable and fast communications system such presented in this paper.

DSiP solution is likely to be more expensive than a regular single channel solution. The reason for this is the required more sophisticated hardware & software than earlier and use of several simultaneous communications channels. But this cost can be considered insignificant if it can save human lives in a disaster scenario. Or even preventing illegal activity in the border zone justifies the cost of the DSiP solution.

If other users also implement the DSiP solution, like power station controlling and monitoring, the cost of the system will be lower per organization when implementing the solution.

Today, all new cars have dual brake systems; if one fails, the brakes can still be used for stopping the car in a safe way. Commercial passenger aircraft have two or more engines; if one engine fails, the plane is still able to fly safely. How it is possible that critical communication systems are based only on a single communication channel? Distributed Systems intercommunication Protocol (DSiP) offers multichannel communication software forming multiple parallel communication paths between the remote end and the command and control room. All this is achieved in a safe manner from network security point of view. Should one of the communication channels be unavailable for use, the other channels can still continue transmitting data without interruption to applications or end users.

REFERENCES

[1] ETSI EMTEL Technical Reports TS 102 181: Requirements for communication between authorities/ organisations during emergencies.
[2] Public Safety Communication Europe, WP1: Users requirements, Report on the definition of the generic users requirements, D1.2, 2009.
[3] ETSI Project MESA: Services and Applications SoR - TS 170.001 V3.3.1.
[4] G. Baldini, Report of the workshop on "Interoperable communications for Safety and Security", Publications Office of the European Union, 2010.
[5] M. Rantama, Pelastustoimen langattoman tiedonsiirron tarpeet ja toteutusmahdollisuudet tulevaisuudessa, Pelastusopiston julkaisu, B-sarja. Tutkimusraportit 2/2011.
[6] Investigation Commission of Jokela School Shootings, Ministry of Justice Publications 2009:2, Helsinki. G. Lapierre, "Synergies and challenges between Defence and Security (PPDR) applications. What implication for the EU?", PSC Europe Conference, 7-8 June 2011, Brussels.
[7] M. Nordman, M. Lehtonen, J. Holmström, K. Ramstedt and P. Hämäläinen, "A TCP/IP communication architecture for distribution network operation and control", in Proc. of the 17th Internal Conference on Electricity Distribution, Barcelona, Spain, May 12-15, 2003.
[8] Ajeco Oy. Available: http://www.ajeco.fi/

[9] J. Rajamäki, J. Holmström and J. Knuuttila, Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities, Proc. of the 17th Symposium on Communications and Vehicular Technology in the Benelux, Twente, The Netherlands, 2010. IEEE Xplore.

[10] J. Holmstrom, J. Rajamaki and T. Hult, "The Future Solutions and Technologies of Public Safety Communications - DSiP Traffic Engineering Solution for Secure Multichannel Communication", International Journal of Communications, Issue 3, Volume 5, 2011, pp.115-122.

[11] T. Hult and J. Rajamäki. "ICT Integration of Public Protection and Disaster Relief (PPDR): Mobile Object Bus Interaction (MOBI) Research and Development Project", 10th WSEAS International Conference on Applications of Computer Engineering, Playa Meloneras, Gran Canaria, Spain, March 22-26, 2011.

[12] A. Durantini, M. Petracca, F. Vatalaro, A. Civardi, and F. Ananasso, "Integration of Broadband Wireless Technologies and PMR Systems for Professional Communications", Fourth International Conference on Networking and Services, ICNS 2008, Gosier, Guadeloupe, March 16-21, 2008.

[13] J. Ahokas, T. Guday, T. Lyytinen and J. Rajamäki, "Secure Data Communications for Controlling Electric Power Stations and Distribution Systems", Proceedings of the 3rd International Conference on Energy, Environment, Devices, Systems, Communications, Computers (INEEE '12), Rovaniemi, Finland, April 18-20, 2012.

[14] R. Robles & T. Kim, "Communication Security for SCADA in Smart Grid Environment", WSEAS Conference in Advances in Data Networks, Communications, Computers, 2010.

[15] M. Morel and S. Claisse, "Integrated System for Interoperable sensors & Information sources for Common abnormal vessel behavior detection, & Collaborative Identification of threat (I2C)", IEEE Conference publishing, 2010

[16] H. G. Park, B. Shin, H. K. Park, J. Park, C. Yoon, S. Rho, C. Lee, J. Jang, H. Jung & Y. Lee, "Development of Ad hoc Network for Emergency Communication Service in Disaster Areas", Proceedings of the 9th WSEAS International Conference on Applications of Computer Engineering, 2010.

[17] J. Ryu,"Congestion Control and Routing over Challenged Networks", The University of Texas at Austin, USA, 2011.

[18] L. Daniel, "Cross-layer Assisted TCP Algorithms for Vertical Handoff", University of Helsinki, Finland, 2010.

[19] J P. Orefice, L. Paura & A. Scarpiello, "Inter-vehicle communication QoS management for disaster recovery", The Internet of Things, 20th Tyrrhenian Workshop on Digital Communications, Springer New York 2010.

[20] J. Lehto, J. Rajamäki and P. Rathod," Conceptualised View on: Can Cloud Computing Improve the Rescue Services in Finland?", 11th WSEAS International Conference on Applied Computer and Applied Computational Science, Rovaniemi, Finland, April 18-20, 2012.