A redundant tracking system for Public Safety and Emergency Response: Reporting past research, present findings and future directions

Jyri Rajamäki, Paresh Rathod and Pasi Kämppi

***Abstract*—** Tracking is playing very significant role in modern public safety and emergency response. There are many tracking technology available. Such as the geographic information systems (GIS) and global navigation satellite systems (GNSS) have transformed local, national and international emergencies and disasters response services. GIS/GNSS technologies offer great deal of assistance in public safety and emergency response enabling emergency management agencies to efficiently allocate resources, model risk and direct emergency response and recovery personnel. On the one hand, these technologies are bringing many innovative advantages to organizations responsible for public safety and emergency response. While on the other hand, it brings many challenges. For example, current GNSS-based tracking systems have serious technical flaws and vulnerabilities. This paper is reporting our research studies conducted in various projects and it also presents our finds including a detailed modular system-level description for a hybrid tracking system including control, space, tracking, communication, data processing, end-user and external applications segments. The paper further discusses and suggests how the technical vulnerabilities of GNSS-based tracking systems could be avoided considering hybrid tracking segment and multichannel communication paths. The paper is also exploring future possibilities to provide smooth tracking for public safety and emergency response.

***Keywords*—** Emergency management, Public Safety, Geographic information system, Security, Multichannel communications, Tracking.

I. Introduction

Emergency management needs geographic information for emergency response and planning operations. A geographic information system (GIS) can combine many layers of different information. GIS enables emergency managers to quickly access relevant data about an affected area during emergencies. GIS' objectives are to have a general view of the theatre of operations with its geographic characteristics, troop's location, roads and railways and fighting location [1]. Global navigation satellite systems (GNSS) -based tracking and navigation have gained broad popularity during past years. The primary focus of GNSS-based tracking systems within the GIS arena has traditionally been based around global positioning system (GPS) that collects, stores and transfers data from a field system to an office-based GIS [2].

Integration of information systems is a current trend in all businesses and organizations [3]. The trend is towards larger mobility and the Internet plays a major role in providing critical business and operational data, applications and services for mobile users. In this respect, service-level requirements play an important role in the process. However, service-level requirements are difficult to quantify during the project planning phase. The following intangible values could be used as guide lines for drawing up the operational constraints and goals required: 1) usability, 2) performance, 3) scalability, 4) reliability, 5) availability, 6) extensibility, 7) maintainability, 8) manageability and 9) trustworthiness and security. Only after deployment these attributes can be quantified. To meet pertinence requirements, the production (communication) system needs changing and tuning; if not possible, service-level requirements should be readjusted to conform the operational environment. The reason for the existence of any Internet based system is to support business and organizational needs. A shift of focus may be needed in any new project and Internet architecting activities should be given more effort, attention and seriousness. [4]

A GNSS-based tracking system combines navigation and telecommunication technologies. The system is relatively complicated and consists of many technical segments, including the control, space, tracking, communication, data processing, application interface for external applications and end-user segment [5]. The basic principle is that a tracked device is positioned by Global Navigation Satellite Systems (GNSS) and positioning data is delivered for post-processing via mobile networks, the Internet or a secure network. The end-user segment might be e.g. an office-based GIS for emergency response. The manner in which GNSS used with GIS is wide and varied allowing users to determine the way GIS and GNSS are used together to best meet their needs. However, with these impressive technologies come new and sometimes unforeseen challenges in implementation and coordination. For example, in the wake of the Space Shuttle Columbia disaster 2003, several lessons were learned about

Manuscript received November 9, 2013. This work has been partly founded by the Finnish project as component of the Eureka project Celtic-Plus MACICO (Multi-Agency Cooperation In Cross-border Operations) with 9 partners from Finland, France and Spain.

Jyri Rajamäki is with the Laurea University of Applied Sciences, Leppävaara, Espoo, Finland (e-mail: jyri.rajamaki@laurea.fi).

Paresh Rathod is with the Laurea University of Applied Sciences, Leppävaara, Espoo, Finland (e-mail: paresh.rathod@laurea.fi).

Pasi Kämppi is with the Laurea University of Applied Sciences, Leppävaara, Espoo, Finland (e-mail: pasi.kamppi@laurea.fi).

large-scale, multi-agency disaster response as it pertains to GIS and GPS [5].

GNSS-based tracking devices are able to calculate and deliver position information for post processing. Today many mobile phones (smart phones) include GPS receivers and phones are easy to turn into tracking devices by client software. For professional services like emergency response, TETRA clients and tracking-only clients without communications functionality are available. New positioning devices expected to support all four major systems (GPS, GLONASS, Compass and Galileo) so that several GNSS techniques can be used simultaneously to guarantee better positioning accuracy and availability. The accuracy and reliability of GNSS-based tracking can be improved by Satellite Based Augmentation Systems (SBAS) or dead reckoning capabilities. GNSS-based tracking is used in many applications, e.g. in agriculture [11], logistics, fleet management, road tolls, traffic signal management. Also, emergency response is using them e.g. for following troop's location.

Very often only the benefits of the satellite-based tracking solutions are advertised while the risks and weak points are forgotten. However, current GNSS-based tracking systems have serious vulnerabilities [5]. The systems are complex and open to several kinds of data delivery problems, data losses and cyber-attacks. The systems are GPS and GSM dependent for positioning and communications. GNSS systems operate in the IEEE L frequency band, located from 1 to 2 GHz [12] that is shared by several telecommunication systems, such as [13]: aeronautical navigation systems like civilian Distance Measuring Equipment (DME); air traffic control radars; military and government systems for terrestrial communication, navigation and identification; amateur radio communications; telemetry and telecommand services for aircraft and missiles; Digital Audio Broadcast; mobile satellite communication systems like Inmarsat and Iridium. They include no cross-over possibilities; positioning is not based on parallel satellite systems, known WLAN networks, mobile phone cell location, RF/DF etc. Also, intelligence is lacking from the systems; they can be commanded but they do not have the capability of self-reacting and alerting. Furthermore, available commercial products are vulnerable to jamming without jamming detection possibilities and their power consumption is not always optimized [5].

This paper studies current threats of satellite-based tracking systems in the field of emergency response. It also presents a detailed modular system-level description for a hybrid tracking system. This paper proposes how the vulnerabilities of satellite-based tracking systems could be avoided utilizing multi-GNSS (Galileo, GPS, CLONASS, Compass) capable equipment, taken a hybrid tracking segment and multichannel communication paths into account. Paper also discusses self-protection, counter measure protection, jamming detection as well as power consumption optimizing.

II. Satellite Based Tracking

The history of modern satellite navigation started in December 1973 when the Department of Defense (DoD) approved the Global Position System/NAVSTAR project. The target of the project was to combine the best practices of existing navigation projects 621B, TRANSIT and TIMATION. The existing projects were headed by the US Air Force or the Navy and they were competing with each other. The new navigation system was decided to be only for military use [xx].

The first Global Position System (GPS) satellite was launched in February 1978 and the constellation of the 24 satellites was achieved on 1988. In 1983 civilians were allowed to use GPS. The reason being that a Korean airplane had got lost over Soviet borders and been shot down. However, the accuracy of the civilian signal was limited by the selective availability (SA). GPS was allowed for global use free of charge in 1993 and SA was disabled on 2000 [xx].

A. Principle of Satellite Based Navigation

This section presents the basic principle of satellite based navigation. Information is based on GPS satellite navigation system but the principle is the same with other satellite based navigation systems too. Satellite based navigation is based on signals that are delivered by the satellites. The satellites orbit the earth at a height of 20200 km at a speed of 3.9 km per second. The orbit time is 12 hours. The satellites are powered by solar panels and the signal transmission power is about 50 watts. The estimated life time of the satellites is 4.5 – 7.5 years depending on the satellite model [xx] Fig. 1 presents satellites in their orbits.

The satellites deliver a signal that contains satellite identification, satellite position and the time when the signal was delivered. A GPS receiver compares the signal timestamp with the time when the signal was received and calculates the distance between receiver and satellite. The distance calculation is based on time difference between the sending and receiving time.

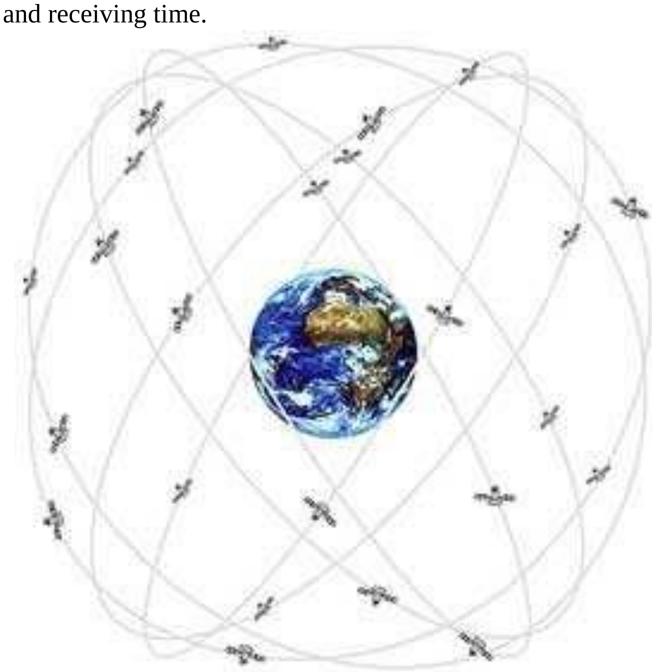

Fig. 1 GPS satellites in orbits

The satellites deliver a signal that contains satellite identification, satellite position and the time when the signal was delivered. A GPS receiver compares the signal timestamp with the time when the signal was received and calculates the distance between receiver and satellite. The distance calculation is based on time difference between the sending and receiving time.

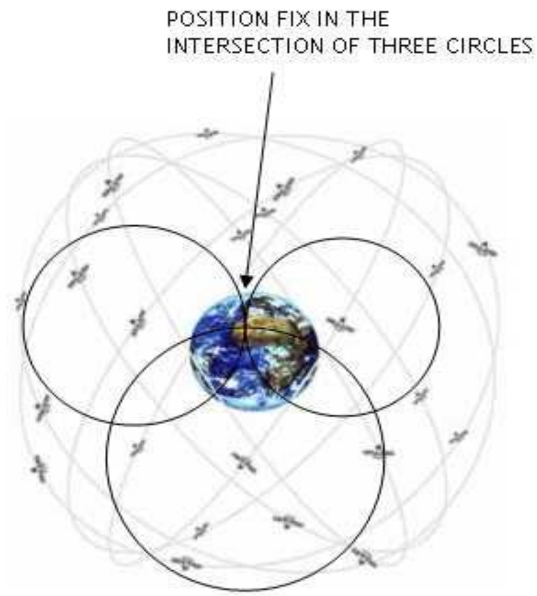

Fig. 2 Principle of 2D position calculation

When the GPS receiver knows the distance to the three satellites the position information is calculated by triangulation. A two dimensional position fix (2D), that includes latitude and longitude, requires signals from three satellites. The 2Dfix does not include altitude information. A three dimensional position fix (3D) with the altitude can be calculated when the signal from four satellites is available. The principle of calculation of the 2D position fix is presented in Fig. 2.

B. Technical System Description

A modern satellite-based tracking system combines navigation and telecommunications technologies. The system is complicated and it consists of many technical segments, including the control segment, space segment, tracking segment, communication segment, data processing segment, application interface for external applications and end-user segment. The basic principle is that a tracked device is positioned by Global Navigation Satellite Systems (GNSS), and positioning data is delivered for post-processing via mobile networks, the internet or a secure network. The sequence of the tracking: 1) Signals are delivered by the satellites, 2) GPS receiver calculates the position, 3) Position data is sent for post processing, 4) Position data is processed and stored, 5) End user access to position data

III. Current Treats to Satellite-Based Tracking Systems

Identifying threats of satellite-based tracking in order to avoid the problem of limited existing data or limited knowledge of the risk analysis team, it is necessary to investigate the requirements of the applications and operations/business. An application can have technical requirements that have not been levied on prior uses of the system. If the system cannot offer service with certain requirements, then it is a threat for the application. The requirements of the operations/business can create technical requirements, and the technical limitations of the system causes threats to those requirements being met. Using this approach, we were able to generate a model for identifying threats with regard to satellite-based tracking, shown in Fig. 3.

We started identifying threats by listing well known technical threats. The asset we chose to investigate was location data. First, we defined the segments of the system and then we group the threat according to the segments in which they occur. We discovered that a single technical threat can be the cause for some higher-level threat. For example, the cause of a tracking failure can be a technical problem in tracking device. The technical problem is the lower-level threat and the tracking failure is the higher-level threat. Also, we noticed that higher-level threats can help to find lower level threats. Data privacy threats are caused by certain technical reasons. The

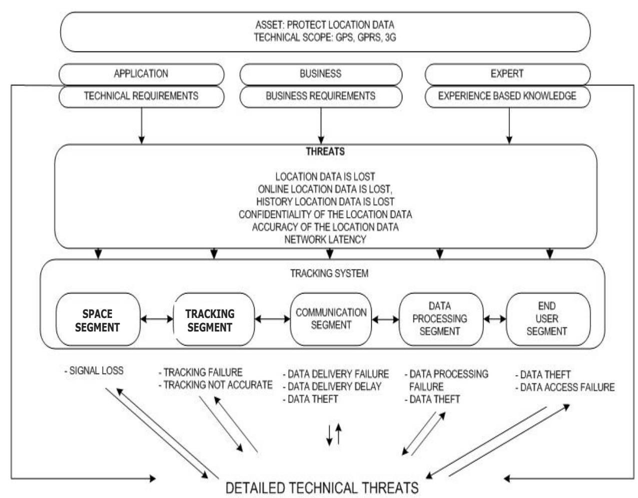

Fig. 3 Model for identifying technical threats of satellite-based tracking

data privacy is higher level threat and the technical reason is the lower level threat. Next, we investigated if higher-level threat could occur in the other segments of the system. For example, privacy threats can be caused by many technical reasons in many segments. This cycle generated relations between all threats and segments.

When we had sorted all well-known threats we added operational/business requirements. We have listed threats considering system segment including control, space, tracking, communication, data processing and end-use. Some of them can be technical bug or errors, natural disasters, hardware and software faults, capacity, coverage, corruption and many more. Table 1 on following page shows the threats resulting from this methodology grouped by system segments and categories. We have presented those as technical vulnerabilities in satellite-based tracking system.

Table 1. Technical vulnerabilities in satellite-based tracking systems

System segment	Threats
Control segment	Error in monitoring data, Error in adjustment commands
Space segment	Natural disasters (e.g. solar storms, ash cloud from volcano eruption), Collisions in the orbit, Unintended interface, Intentional interface, Atmospheric conditions, Multipath propagation, Selective availability, Total signal loss
Tracking segment	HW fault, SW fault, Power feed break-down, Clock drift, Signal attenuation, Information security diminution
Communication segment	Capacity, Radio coverage, Roaming, Latency, Information security diminution
Data processing segment	HW fault, SW fault, Power feed break-down, Capacity, Information security diminution, Database corruption
End-user segment	HW fault, SW fault, Power feed break-down, Capacity, Information security diminution

IV. Improved Tacking System for Public Safety and Emergency Response

Previous section investigates the main threats of today's satellite-based tracking systems. These systems have no cross-over possibilities for positioning and communications as the tools are GPS and GSM dependent. In emergency situations, some of these threats (e.g. power feed breakdown) are more probable to realize. For this reason, we propose an improved tracking system for emergency response, shown in Fig. 4. The improved tracking system for emergency response includes three main segments: (1) Integrated tracking segment where the location could be calculated based on several satellite systems, known WLAN-networks, mobile phone cell location, etc.; (2) multichannel communication segment which could utilize the best available communication path or several parallel paths; and (3) GIS integrated data processing, API and end-user segments.

A. Integrated Tracking Segment

New tracking devices should support multiple GNSS systems (GPS, GLONASS, Compass and Galileo) so that several systems can be used simultaneously to guarantee better positioning accuracy and availability. For robustness reasons, relying on only one technology (GNSS) is not enough. For example, electromagnetic interference might interrupt all GNSS operations in a certain area [14].

The accuracy, integrity, continuity and availability of GNSS can be improved by using Satellite-Based Augmentation Systems (SBAS). SBAS system is based on delivering differential correction and integrity messages by geostationary satellites. There are several SBAS-systems implemented in larger scale including Geostationary Navigation Overlay Service (EGNOS) covers Europe, Wide Area Augmentation System (WAAS) covers North America, Multi-functional Satellite Augmentation System (MSAS) covers Japan and GPS and GEO Augmented Navigation (GAGAN) covers India. The STARFIRE service covers whole globe.

In case of not receiving satellite signals there can be alternative methods used. Mobile networks have support to locate mobiles by triangulation or cell location when the GNSS service is not available. It is also possible to utilize known WLAN networks or dead reckoning. Dead reckoning uses external sensors for calculating position. In automotive navigation the system calculates position by data from the CAN bus like speed, steering directions, and so on. Portable devices can have advantage for using Micro-Electro-Mechanical Systems (MEMS) sensors. MEMS sensors add capabilities to calculate position by gyroscopes or geomagnetic sensors.

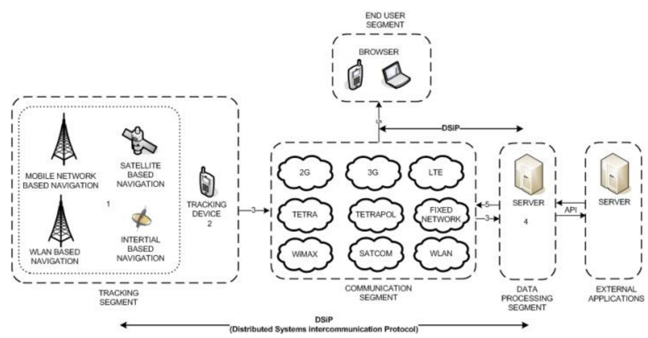

Fig. 4 Modular system-level description of improved tracking system for emergency response

In emergency situations, the power consumption of the tracking device could be a critical factor. Combining device's power consumption optimization with utilizing energy harvesting from ambient vibrations, wind, heat or light and new high energy rechargeable battery technologies, a multiply running time could be achieved. Outfitting the tracking device with jamming detection ability requires access to GNSS chips Automatic Gain Control (AGC) software and comparing the chances in gain and signal to noise ratio. Furthermore, the devices could have artificial intelligence for self-reacting and/or alerting when certain abnormalities occur.

B. Multichannel Communications Segment

A multichannel data communication concept provides a uniform way to communicate over virtually any type of communications media in such a way that multiple, sometimes parallel communication paths appear as a single robust, uninterruptable, secure and reliable communication link between communicating peers [9]. For example, a solution named DSiP (Distributed Systems intercommunication Protocol) makes it possible to distribute all telecommunication among several operators and methods, resulting in a true multichannel communication system. The DSiP telemetry system increases reliability, security and integrity in telecommunication and allows regular communication methods to be used in mission critical telemetry systems. This is achieved by (1) splitting risks between operators and communication channels, (2) better routing and priority capabilities that takes security and intrusion risks into account and (3) adding modularity [7]. The DSiP is entirely a software protocol solution. There are fundamentally two types of software elements in the solution: DSiP-routers and DSiP-nodes. Fig. 3 depicts the blueprint of DSiP solutions.

The nodes constitute interface points (peers) to the DSiP routing solution, and the DSiP-routers drive traffic engineering and transport in the network. DSiP routers establish multiple authenticated and encrypted, sometimes parallel connections according to configuration parameters, between each other (item #10) and nodes establish multiple simultaneous connections to one or more routers in the system. All connections may be strongly encrypted and trustworthy based upon usage of certificates effectively meaning that all elements in the DSiP routing solution are known. As routers may use multiple parallel connections (10) between each other and as nodes may make multiple parallel connections (6) between themselves and one or more routers, the solution results in a true mesh-like structure between the network peers (nodes).

DSiP-routers in routing network are typically distributed to different physical locations. The nodes are typically located at, for example, but not limited to, public safety vehicles and control rooms. The connection establishment is always constructed from the node towards the router element and one router to another router in a preconfigured manner. The system features a third element named configuration server software from where nodes may read new configuration data should the underlying physical transport layer request changes or configurations needed to be done.

The nodes and routers maintain multiple parallel physical connections between each element in the DSiP routing solution. That removes this complex burden from external equipment and software that use the system as routing. Consider, for example, a vehicle computer in a public safety vehicle; this computer either contains a DSiP-node which uses multiple wireless modems, or it connects to a vehicle router-hardware containing the DSiP-node and multiple modems. The DSiP-node is performing tunneling of the users applications IP-traffic from the vehicle to the control room and vice versa, thus mitigating complex issues routing in between network peers. The DSiP solution is capable of transparently maintaining the connections and communications between users systems or applications or hardware without having to program this functionality into the applications – DSiP is fully transparent to its users. For example, a user may run VPN client software in his laptop computer. The nature of the VPN demands that it must establish its connections over a single physical communication line. If this line has a problem or breaks up, the user must re-authenticate his or her VPN session over another physical media. When DSiP is used, the user may use his or her VPN client or server to establish a VPN session over multiple physical connections – should one or more have problems, the VPN session remain intact as the DSiP is tunnels the session through itself. This feature is of utmost importance in critical applications [10].

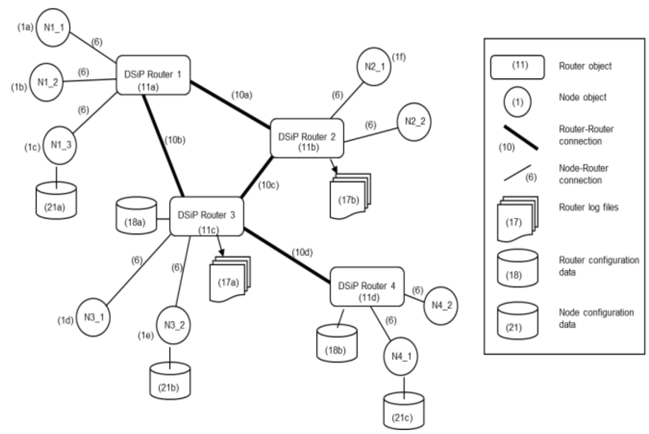

Fig. 5 Blueprint of DSiP network solution [10]

The nature of a crisis event affects the usable media. During a panic event, public cellular technology is useless. The public cellular data is highly loaded during minor event with a large crowd, but dispersed communication may get through. In a case of the oil disaster within large geographic area, cellular technology is operative and interoperability required. TETRA works in all circumstances, but the data capacity is limited. TEDS will bring some improvement, however, may fall short to future needs. Satellite communication can be considered pretty advantageous. The comprehensive answer can be found with parallel use of several communications networks, and DSiP realizes this demand. Furthermore, it is possible to interconnect any device or network segment using any media in DSiP. IPv4, IPv6 or non-IP supported in DSiP, while on the other hand, it supports redundant and secure way of communication. DSiP may be regarded as a multi-point to multi-point mesh-structured VPN network with good control over priority, security and reliability. Applications and devices will see the multiple connections as they would be a single connection channel; thus eliminate the modification of any application or device.

C. *End-user Segment*

There are many ways that GIS and tracking technologies can and already do work well together. From complete commercially available data collection and data maintenance systems, to help with the management of spatial features and attribute data, through to very flexible software development kits, to assist in the creation of unique and sophisticated field applications [2]. In the future, office-based command and control rooms will more and more be replaced by mobile and field command systems.

The end-user segment could also take advantage of DSIP-based communication system to guarantee reliable access to location data. DSIP-based communication can be implemented e.g. in vehicles by separate equipment or it could be integrated into handheld devices by software.

V. Discussion and Conclusion

The Geographic information systems can combine many layers of different information, creating products that are more sophisticated than flat maps. GIS can map and access data — from flood zones and local infrastructure to population density and road closures — before, during, and after an emergency. By linking maps to databases GIS enables users to visualize, manipulate, analyze, and display spatial data. The primary focus of satellite-based tracking systems within the GIS arena has traditionally been to collect, store and transfer data from a field system to an office-based GIS. All the time, satellite-based systems are becoming more popular and positioning information becomes more important in managing field operations. However, there is no interoperability standard to exchange location information and simple GIS information.

A satellite-based tracking system integrates satellite-based positioning, mobile and fixed telecommunication networks as well as data processing and administration. Most western European satellite-based tracking systems are based on GPS operated by the United States Air Force who, however, cannot guarantee to maintain global uninterrupted service. If GPS signals were switched off in Europe tomorrow, emergency response efficiency would suffer heavily jeopardizing the public safety. European Public Protection and Disaster Relief (PPDR) operators can only be self-dependent if their tracking is based on Galileo, the only European global navigation satellite – supported by other GNSS systems. And for example in northern Scandinavia, GLONASS gives better service accuracy than GPS. Galileo will allow positions to be determined accurately even in high-rise cities, where buildings obscure signals from today's satellites. Galileo will also offer several signal enhancements making the signal more easy to track and acquire and more resistant against interferences and reflections. In the future, European GNSS will deliver much more precise and much more reliable services than the American and Russian systems. By placing satellites in orbits at a greater inclination to the equatorial plane, Galileo will also achieve better coverage at high latitudes, making it particularly suitable for operation over northern Europe, an area not well covered by GPS. However, presuming on only one technology (GNSS) is not enough and utilizing SBAS, mobile network location services, known WLAN-networks or dead reckoning could give notable additional value for location data availability.

The power consumption of the tracking device could be a critical factor, especially during emergencies. Combining device’s power consumption optimization with utilizing energy harvesting from ambient vibrations, wind, heat or light and new high energy rechargeable battery technologies, a multiplied running time could be achieved.

There is a lack of interoperability between different technical systems in use by emergency services. When managing troops during emergencies, communications is critical. Mobile devices make use of different networks. In general, they are legacy systems without a homogeneous and/or secured configuration and their default encryption is weak and very easy to hack. Often, even one single point attack can compromise the complete network connection and bring the network down. At present, the roaming features of TETRA/TETRAPOL networks are inadequate to apply them in cross-border PPRD operations. Therefore, the need for secure multichannel communication is global and exploding. DSiP is a commercial solution allowing regular communication methods to be used in mission critical communication systems. It also enables a combination of all kinds of telecommunication resources: IP traffic and non-IP traffic over TETRA, radio links, satellite communications, serial connections etc. can all co-exist forming a single uniform and maintainable system.

In the future interoperability between different telecommunications systems could be improved because 3GPP, ETSI TC TETRA, TCCA and NIST agreed to integrate public safety related features into 3GPP LTE-standards. Future networks will also have Self-Optimizing Network (SON) support and that will integrate inbuilt health state awareness in mobile radio networks.

This article presents a modular system-level description of improved tracking system for emergency response. Within GNSS systems a tracking device calculates its location itself and sends this information for post-processing. In most other system, location of the tracking device - ‘tag’ - will be calculated by the system and the tag sends no location data. However, with current knowledge the integration of these different technologies is realizable.

Acknowledgment

Authors are thanking our sponsored and funding agency for providing full support for our research studies, experiments and field studies. This work has been partly founded by the Finnish project as component of the Eureka project Celtic-Plus MACICO (Multi-Agency Cooperation In Cross-border Operations) with 9 partners from Finland, France and Spain. Some of research results also compiled from our previous research project including:

1) MOBI (Mobile Object Bus Interaction): It is a joint project together with Laurea University of Applied Sciences, Ajeco Insta, Cassidian, Sunit, the Finnish Police and Tekes. Mobi is about communication infra for public safety vehicles.

2) Saterisk project: It is a joint project of Laurea university of applied sciences and theUniversity of Lapland. The main funder of the project is Tekes. The project also involves several companies and other partners using satellite navigation systems. The Saterisk-project has been started in 2008 and it ended in august 2011.

REFERENCES

[1] S. Sauvagnargues-Lesage and P. A Ayral, "Using GIS for emergency management: a case study during the 2002 and 2003 flooding in south-east France". *International Journal of Emergency Management*, 2007. Vol. 4, No. 4, pp. 682 – 703.

[2] A. Harrington, "GPS/GIS Integration: GPS Can Play a Major Role in GIS Data Maintenance?" *GeoWorld, Daneilson, Todd (ed.)*, Vol.12 No.10, Arlington Heights: Adams Business Media, 1999.

[3] D. Litan and A-M. Mocanu, "Information systems integration, a new trend in business", in *Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11)*, 2011.

[4] S. Tumin and S. Encheva, "A brief look at Web architecting", in *Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11)*, Meloneras, Gran Canaria, Canary Islands Spain, March, pp. 245-249, 2011

[5] J. Rajamäki, "Cross-border Satellite-based Tracking: Needs, Approach, Benefits and Competition", In proceedings of *2nd International Conference on Ubiquitous Positioning, Indoor Navigation and Location-Based Service, UPINLBS2012*, Helsinki, October 3-4, 2012.

[6] S. Brown, S. Crum and V. Foote, "GIS and GPS Emergency Response Lessons Learned from the Space Shuttle Columbia Disaster", *Journal of Extension*, Num. 4, Vol. 41, 2003. Available at: http://www.joe.org/joe/2003august/iw1.php

[7] J. Holmstrom, J. Rajamäki and T. Hult, "The future solutions and technologies of public safety communications - DSiP traffic engineering solution for secure multichannel communication", *International Journal of Communications*, World Scientific and Engineering Academy and Society (WSEAS), USA, Issue 3, Vol. 5, 2011. pp.115-122.

[8] J. Lento, J. Rajamäki and P. Rathod, "Conceptualized view on can cloud computing improve the rescue services in Finland?", In Proceedings of the *11th WSEAS international conference on Applied Computer and Applied Computational Science(ACACOS'12)*, World Scientific and Engineering Academy and Society (WSEAS) Press, Stevens Point, USA, 2012. pp65-70.

[9] J. Rajamäki, J. Holmström and J. Knuuttila, "Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities", Proc. of the *17th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT) and IEEE Xplore*, Twente, The Netherlands Nov. 24-25, 2010.

[10] J. Rajamäki, P. Rathod, J. Holmström, "Decentralized Fully Redundant Cyber Secure Governmental Communications Concept", In Proceedings of the *2013 European Intelligence and Security Informatics Conference (EISIC '13)*. IEEE Computer Society, USA, 2013

[11] G. Bãdescu1, R. Bãdescu, M. Ortelecan, O. Stefan and M. Dirja, "Some aspects of using modern GNSS-RTK type technology in agriculture", In RECENT RESEARCHES in APPLIED ECONOMICS and MANAGEMENT. Economic Aspects of Environment, Development, Tourism and Cultural Heritage, Volume 2: Proceedings of *the 5th International Conference on Applied Economics, Business and Development (AEBD '13),)*, World Scientific and Engineering Academy and Society (WSEAS) Press, USA, 2013, pp- 252-258.

[12] The European GNSS (Galileo) Open Service Signal in Space Interface Control Document, Issue 1.1, September 2010.

[13] E. D. Kaplan and C.J. Hegarthy, *Understanding GPS Principles and application*, Artech House, Boston, 2006, pp. 244-247.

[14] A. Rusu-Casandra, E-S. Lohan, G. Seco-Granados, I. Marghescu, "Investigation of Narrowband Interference Filtering Algorithms for Galileo CBOC Signals" in RECENT ADVANCES in COMMUNICATIONS, CIRCUITS and TECHNOLOGICAL INNOVATION, Ed. A. Pisarchik, Y. Shang and C. Bulucea, World Scientific and Engineering Academy and Society (WSEAS) Press, USA, 2012, pp. 274-279.

[15] MACICO project information. Available: http://www.celticplus.eu/Projects/Celtic-projects/Call8/MACICO/macico-default.asp

[16] J. Eberspächer, H. J. Vögel, C. Bettstetter and S. Hartmann, "GSM architecture protocol and services", Third Edition. John Wiley & Sons Ltd. Great Britain. 2011.

[17] 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.

[18] A. Daneels and W. Salter, "What is SCADA?", *International Conference on Accelerator and Large Experimental Physics Control Systems*, Trieste, Italy, 1999.

[19] SCADA. Available: http://www.scadasystems.net/, http://www.controlmicrosystems.com/resources-2/faqs/scada11/

[20] G. Clarke and D. Reynders, "Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems", Elsewier, Great Britain, pp. 15-16, 19, 163, 2004.

[21] United States General Accounting Office, "CRITICAL INFRASTRUCTURE PROTECTION Challenges and Efforts to Secure Control Systems", 2004. Available: http://www.gao.gov/new.items/

[22] D. Kieran, J. Weir & W. Yan, "A Framework For An Event Driven Video Surveillance System", *Journal of Multimedia*, Volume 6, Number 1, February, pp. 3-13, 2011.

[23] M. Adámek, Z. Tvrdý, M. Matýsek and P. Neumann, "The Use of Camera Systems in Municipalities", 2nd International Conference on Information Technology and Computer Networks (ITCN '13), Antalya, Turkey, pp 160-166, 2013.

[24] A. Dziech, J. Derkacz and M. Leszczuk "INDECT and TAPAS projects – research objectives and chosen solutions", 2nd International Conference on Information Technology and Computer Networks (ITCN '13), Antalya, Turkey, pp 119-124, 2013.

[25] J. Korhonen, "Introduction to 3G Mobile Communications", Second Edition. Artech House. Norwood, MA. 3, 14, 2003.

[26] E. Dahlman, S. Parkval, J. Sköld and P. Beming, "3G Evolution: HSP and LTE for mobile Broadband", Second Edition. Academic Press. Burlington, MA, pp. 9, 22, 2008.

[27] P. Stavroulakis, "Signals and communication technology, Terrestrial Trunked Radio- TETRA, A Global Security Tool", Springer, Heidelberg, pp. 2, 27, 51, 170, 2007.

[28] E. Knapp, "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems", Elsevier Inc, USA, 2011.

[29] J. Ahokas, J. Rajamäki and I. Tikanmäki, "Secure and Redundant Public Safety Communication Network for Public Protection and Disaster Relief (PPDR) Organizations", *International Journal of Communications*, Issue 1, Volume 6, 2012, pp. 120-127.

[30] Office of Emergency Communications, "Nationwide Public Safety Broadband Network", USA, 2012, The U.S. Department of Homeland Security (DHS), Available: http://www.dhs.gov/

[31] M. Zafirovic-Vukotic, R. Moore, M. Leslie, R. Midence and M. Pozzuoli, "Securing SCADA Communications following NERC CIP Requirements", Asia Energy Week 2008, Kuala Lumpur, Malaysia, May, 2008.

[32] NERC Standard CIP-002-3 through -009-4, Cyber Security, 2009-2012 Retrieved November 10, 2012, North American Electric Reliability Council (NERC), Critical Infrastructure

[33] B. Zhu, A. Joseph and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems", *Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*, 19-22 Oct,. pp. 380-388, 2011.

[34] J. Rajamäki, "The MOBI project: Designing the future emergency service vehicle", *IEEE Vehicular Technology Magazine*, June 2013 [In Press].

[35] L. Daniela, "Cross-layer Assisted TCP Algorithms for Vertical Handoff", Department of Computer Science Series of Publications Report A-2010-6, University of Helsinki Finland, 2010.

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

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

[38] H. G. Park, B. Shin, H. K. Park, J. Park, C. Yoon, S. Rho, C. Lee, J. Jang, H. Jung and 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.

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

[40] A. Delfosse, J. Fanton, T. Floriani, V. Malguy, N. Marine and C. Tavernier, Cloud Data security and privacy in IAAS model", 2nd International Conference on Information Technology and Computer Networks (ITCN '13), Antalya, Turkey, pp 54-67, 2013.

Jyri Rajamäki received his M.Sc. (Tech.) degree in electrical engineering from Helsinki University of Technology, Finland in 1991, and Lic.Sc. (Tech.) and D.Sc. (Tech.) degrees in electrical and communications engineering from Helsinki University of Technology in 2000 and 2002, respectively.

From 1986 to 1996 he works for Telecom Finland being Development Manager since 1995. From 1996 to 2006 he acted as Senior Safety Engineer and Chief Engineer for the Safety Technology Authority of Finland where his main assignment was to make the Finnish market ready for the European EMC Directive. Since 2006 he has been a Principal Lecturer at Laurea University of Applied Sciences, Espoo, Finland, where he also serves as a Head of Laurea's Data Networks Laboratory ´SIDLabs Networks´. His research interests are electromagnetic compatibility (EMC) as well as ICT systems for private and public safety and security services. He has authored about 90 scientific publications.

Dr. Rajamäki has been an active actor in the field of electro technical standardization. He was 17 years the secretary or a member of Finnish national committee NC 77 on EMC, ten years a member of NC CISPR and he represented 15 years Finland at IEC, CISPR, CENELEC and ETSI EMC meetings. He was also the Chairman of Finnish Advisory Committee on EMC from 1996 to 2006. Dr. Rajamäki has been the scientist in charge for several research projects funded by Tekes – the Finnish Funding Agency for Technology and Innovation, industry and EURESCOM. He is currently the scientific supervisor and director of one ITEA2 and one Tekes project.

Paresh Rathod is born in India and settled in Finland. He has received his Masters of Computer Application (MCA) from Bhavnagar University, India in year 2000. Paresh is also holding Post Graduates in Advanced Computer Systems Development (ACSD) from University of The West of Scotland, UK in year 2006. Paresh has also achieved his NSA sanctioned CNSS information security professional certification from MIS Department of University of Arizona, USA in year 2010. Paresh is also an Oracle Certified Professional since year 2004.

He is a technocrat, educator and researcher. He has many years' experience in an International business and ICT fields, as a consultant, project leader, database administrator, application programmer, quality assurance professional and researcher. Currently, he is working as a Senior Lecture and Degree Programme Coordinator (BIT) at Laurea University of Applied Science, Espoo city, Finland. His current research interests in the area of information assurance and cyber security, service innovation and service-oriented architecture (SOA), cloud computing and cutting-edge technologies. He has published scientific articles in refereed international conferences and journals.

Mr. Rathod is a professional member of many professional bodies including ACM, IEEE, IEEE Computer Society, ISACA, ASIS and Finnish Information Security Association (FISA). Mr. Rathod also a member of Special Interest Group on Security, Audit and Control (SIGSAC) and Special Interest Group on Information Technology Education (SIGITE). He is a member of scientific committees of international conferences and organizations. Mr. Rathod is active reviewer in international journals, publications and conferences. He is also volunteering in many causes.

Pasi P. Kämppi was born in Varkaus, Finland on 11th December 1973. His educational background is presented in chronological order: B.Sc. in telecommunications, University of Applied Sciences, Kotka, Finland, 1996; Sergeant in signal corps, The Finnish Defense Forces, 1997; MBA (BIT), Laurea University of Applied Sciences, Espoo, Finland, 2011. Currently he is studying in HAMK University of Applied Sciences in Professional Teacher Education Unit. He also holds Juniper JNCIA-EX certification on year 2009.

He has been working with telecommunications since 1997. He started his career on 1997 in Nokia Networks as Testing Engineer and he had several positions like Senior Testing Engineer, System Specialist and Senior System Specialist in Nokia Siemens Networks. His responsibility was packet switched mobile networks and IP networking. He has deployed many technologies for field testing including 3G, UMA, WiMAX and LTE. On 2011-2012 he worked as network consultant in Qentinel. Since 2012 he has been working as project manager, researcher and lecturer in Laurea University of Applied Sciences. Currently he is in active role in MOBI- and MACICO-projects. He has also authored many ICT, telecommunications and public safety related scientific publications.