

PLEASE NOTE! THIS IS SELF-ARCHIVED VERSION OF THE ORIGINAL ARTICLE

To cite this Article: Rajamäki, J. ; Rathod, P. & Kämppe, P. (2013) Hybrid Multi-channel and Redundant Tracking System in Emergency Response. In Sergio Lopes (Editor) Recent Advances in Computer Science and Networking. 2nd International Conference on Information Technology and Computer Networks (ITCN '13), October 8-10, 2013, Antalya, Turkey, 177-182.

URL: <http://www.wseas.us/e-library/conferences/2013/Antalya/ITCN/ITCN-24.pdf>

Hybrid Multi-channel and Redundant Tracking System in Emergency Response

JYRI RAJAMÄKI, PARESH RATHOD and PASI KÄMPPI

Laurea SID Leppavaara

Laurea University of Applied Sciences

Espoo

FINLAND

{jyri.rajamaki, paresh.rathod, pasi.kamppi}@laurea.fi <http://www.laurea.fi/en>

Abstract: - 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. However, current GNSS-based tracking systems have serious technical flaws and vulnerabilities. This paper presents 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.

Key-Words: *Emergency management, Public Safety, Geographic information system, Security, Multichannel communications, Tracking.*

1 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 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. GNSS-based tracking is used in many applications, e.g. in 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. 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.

2 Threats of Current Satellite-Based Tracking Systems

Utility 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. 1.

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

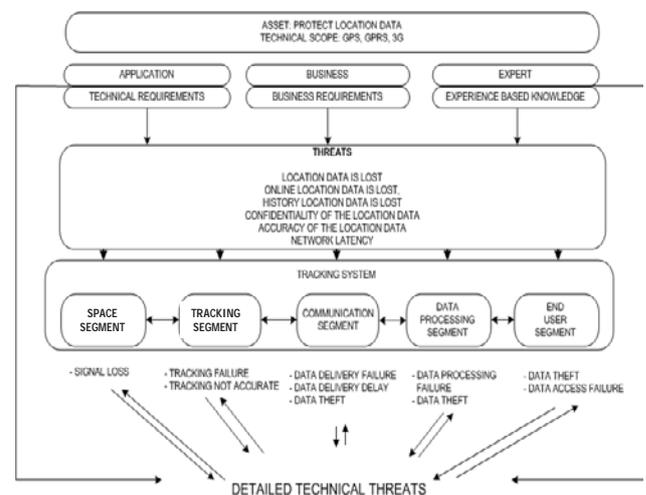


Fig. 1 Model for identifying technical threats of satellite-based tracking

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 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. Table 1 shows the threats resulting from this methodology grouped by system segments and categories.

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 breakdown, 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 breakdown, Capacity, Information security diminution, Database corruption
End-user segment	HW fault, SW fault, Power feed breakdown, Capacity, Information security diminution

3 Improved Tracking System for Public Safety and Emergency Response

Previous chapter 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 Figure 2. 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.

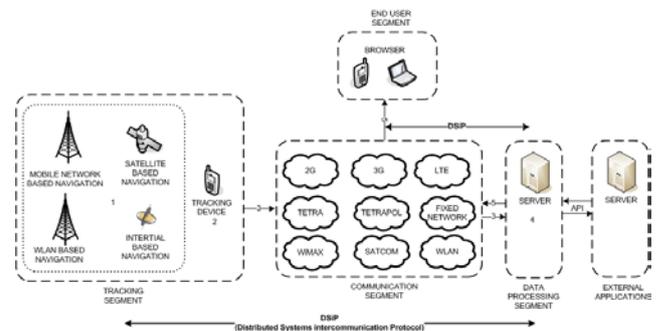


Fig. 2 Modular system-level description of improved tracking system for emergency response

3.1 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. Utilizing known WLAN-networks, mobile phone and TETRA/TETRAPOL cell location, etc. information could give notable additional value for calculation of the location. 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.

3.2 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, uninterrupted, 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 tunnelling 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].

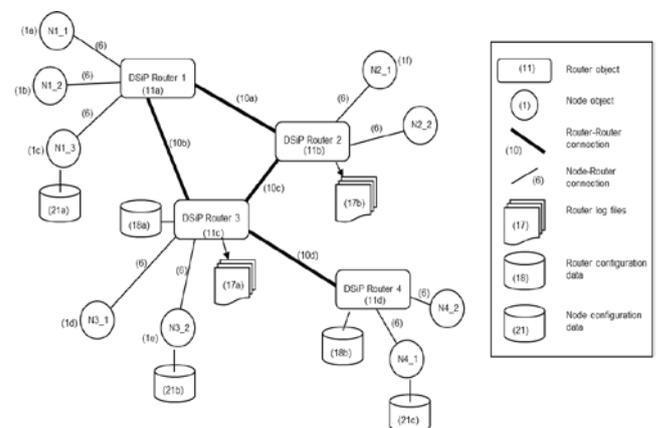


Fig. 3 Blueprint of DSiP network solution [10]

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.

3.3 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.

4 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 known WLAN-networks, mobile phone and TETRA/TETRAPOL cell location, etc. information 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.

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

References:

- [1] Sauvagnargues-Lesage, S and Ayrat, P-A. "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] Harrington, A. "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] Litan, D. and Mocanu, A-M. "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] Tumin, S. and Encheva, S. "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] Rajamäki, J., "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] Brown, S., Crum, S. and Foote, V. "GIS and GPS Emergency Response Lessons Learned from the Space Shuttle Columbia Disaster", *Journal of Extension*, Num. 4, Vol. 41, 2003.
- [7] Holmstrom, J., Rajamäki, J. and Hult, T. "The future solutions and technologies of public safety communications - DSIP traffic engineering solution for secure multichannel communication", *International Journal of Communications*, Issue 3, Vol. 5, 2011. pp.115-122.
- [8] Lehto, J., Rajamäki, J., and Rathod, P., "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), Stevens Point, USA, 2012. pp65-70.
- [9] Rajamäki, J. Holmström, J and Knuuttila, J. "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] Rajamäki, J., Rathod, P., Holmström, J. "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 (in print)

Available at:
<http://www.joe.org/joe/2003august/iw1.php>