U.R.S.I. FRANCE JS 18

GEOLOCATION AND NAVIGATION IN SPACE AND TIME

Solution d'intégration de COTS offrant un service de navigation piéton collaboratif fiable, résilient et sécurisé

Integrating COTS to deliver secured and reliable navigation in a pedestrian collaborative radionavigation environment

Authors :

Dominique HEURGUIER (Thales TCS), Grégory GAILLIARD (Thales TCS), Frederique YWANNE (Thales TCS), Alain LEMER (Thales TCS), Goulven EYNARD (DGA MI).

Keywords :

GNSS ; RANGING ; RESILIENCE ; INTEGRITE ; COLLABORATIF

Résumé :

Cet article résume les leçons tirées de la conception d'un démonstrateur visant à prouver la faisabilité d'intégration de composants sur étagère bon marché, pour délivrer une navigation fiable et sécurisée. Destiné à un groupe de piétons interconnectés par un réseau radio MANET[1], ce démonstrateur repose notamment sur une approche de radiolocalisation collaborative. Celle-ci exploite des mesures de télémétries radio entre voisins en compléments des mesures GNSS[2] disponibles. Parallèlement à l'amélioration de disponibilité du service de navigation, ces travaux pointent la vulnérabilité d'une telle approche face à des malveillances par intrusion et démontrent l'intérêt de compléter les mesures de cyber protection par un contrôle d'intégrité efficace.

Abstract :

This paper sums up lessons learned from a demonstrator design, aiming to prove the integration feasibility of low cost COTS[3] components, to provide to the customer enhanced PNT[4] reliability and security. Intended for a group of pedestrians, interconnected by a MANET radio network, this demonstrator bases in particular on a collaborative radio localization approach. It exploits measures of radio telemetry between neighbors in complements to the available GNSS measures. Complementary to the improvement of availability of the navigation service, these works point out the vulnerability of such approach face of hostilities by intrusion and demonstrate the interest to complete the cyber protection by an efficient integrity monitoring.

1. Introduction

The concept of use of the demonstrator is a small set of collaborative pedestrian nodes, operating completely independently from any telecommunication infrastructures. This last point means no radio cellular network available, no fixed anchors deployed and finally no external GNSS alternative navigation system or dedicated augmentation system available.

It is assumed that certain nodes can be somehow corrupted and used - intentionally or not - to degrade the overall collaborative navigation of each nodes. It is also initially assumed that usual cyber protections, like authentication and cryptography, will not be part of the defense that the system will be able to deploy to protect himself against integrity attacks (in particular against stolen equipment). The objective is to examine the opportunities offered by civilian COTS for collaborative navigation, to identify the vulnerability points of such collaborative navigation, and to study and develop security solutions to protect it. The main degradation considered will be therefore intentional: false navigation data injection coming from one node or local denial of access (could be experienced for example when enduring GNSS jamming).

Precision of the collaborative PNT delivered by the system will not be the prime key performance indicator optimized. Indoor navigation is also deliberately out of the scope of the demonstrator's concept of use.

---

[1] Mobile Ad hoc NETworks

[2] Global Navigation Satellite System

[3] Commercial Off-The-Shelf

[4] Positioning, Navigation and Timing

Lastly but not least, GPS receivers based on military standards can be integrated in the mock up in order to take potentially into account high-integrity PNT, coming from an external secured and trusted source. Proof of concept of this integration has been done using Polaris receivers.

The paper structure is as follow: on the first part the overall architecture of the demonstrator, and then the overall architecture of each node is presented. The choices of the low cost sensors retained to provide information to the navigation filter are justified. On the second part of the paper, an integrity-based data fusion algorithm is presented. On the third part, the Human Machine Interface of the Android application, and the integration of all the sensors on one node, is presented. Finally, the abstract present some trials results obtained, exhibiting the added-value of integrity-oriented navigation algorithms.

2. Demonstrator architecture

The demonstrator consists of a network of 7 nodes: 5 collaborative "blue" nodes, one "red" node playing the role of an intruder, and one supervisor node, used to define scenario, supervise the situation in real time and record the results for potentially further analysis (Figure 1).

A blue node is made of Android smartphone, one GW5204 embedded board from Gateworks including WiFi card, one ranging module from Nanotron, battery, external antennas and optionally GPS watch and/or a GPS Polaris receiver from Rockwell & Collins (Figure 2).

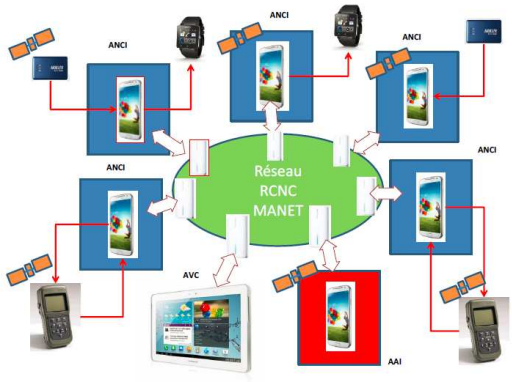

Figure 1: Functional diagram of the collaborative radio navigation mock-up

Figure 2: Sensor integration of one node in the collaborative radio navigation

1.1 Embedded navigation sensors

1.1.1 Inertial sensors

The basic use of smartphone embedded MEMS[5] accelerometer with double integration is not realistic due to the drift of these current sensors. The zero update velocity, usually used with rigid mobile structure or with Inertial Motion Unit (IMU) mounted foot for pedestrian, to reset the drift on zero velocity (i.e. zero when the foot is on the ground), cannot be performed with a smartphone used in the usual way. Nevertheless, trials have confirmed that it is possible to offer a continuity of navigation service to a walking pedestrian for some time, using accelerometer and gyroscope from an accurate initial position and orientation, requiring an initial smartphone calibration phase and an estimate of the stride length of the user. This approach has not been implemented due to the IMU using constraints which are not compatible with usual operational missions (any kind of pedestrian motion, like running, crawling, etc.).

1.1.2 Barometer

It has been experimentally shown that smartphone embedded barometer could be very useful to contribute to differential measurement of altitude. But this has not been implemented due to the focus on 2D only navigation. Nevertheless, this sensor, when present in the smartphone, is used for the integrity monitoring. An abnormal difference of pressure between two nodes, meaning in outdoor an abnormal difference of altitude, is used as a coherence criteria. Abnormal differential pressure leads to alert and data possible rejection.

[5] MicroElectroMechanical Systems

1.1.3 Inter-node ranging module

Low cost COTS performing inter-node radio ranging now exists and can be integrated into a collaborative navigation system. A promising COTS is the module from Nanotron performing ranging in ISM[6] band on Chirp Spread Spectrum (CSS) waveform with Symmetric Double-Sided TWR[7] (SDS_TWR) protocol. First trials have proven that accuracy of about 1 or 2 meters is achievable in outdoor environments. This module may be used in an autonomous way thanks to the swarm mode. It is embedded in the router board and connected to the router in order to deliver ranging measurements to the collaborative navigation data fusion algorithm.

1.2 Mobile Ad-hoc NETwork (MANET)

Existing open source projects developing Android applications for wireless networking in MANETs like SPAN [1] and SERVAL [2] use rooted devices to address this issue. This solution was not retained for the demonstrator design, in order to keep a requirements guarantee regarding the application portability and modularity, as well as a protection against malware provided by an always up-to-date operating system.

Ad hoc and mesh networking modes are however not natively supported for 802.11 WLAN on non-rooted Android OS. User requests to support Wi-Fi ad hoc networking and mesh networking protocols) on the Android open source project issue tracker were classified as obsolete and respectively closed in April 2015 and December 2014.

Departing from these statements, the chosen solution relies on an external Linux COTS router that supports ad hoc/mesh modes and MANET routing protocols. The module retained is the GW5204 embedded board from Gateworks company. Smartphone and its accompanying router forming a wireless ad-hoc routing node may be connected either by an USB wire interface or by Wi-Fi. No porting or integration with Android is required compared to SPAN and Serval applications on rooted smartphones.

Figure 3: Gateworks router

Figure 4: inter-Ranging Nanotron Module

1.3 Integration of the navigation sensors / communications device on each node

The demonstrator has been integrated in a tactical gilet. Smartphone, Router board and optional Polaris GPS receiver are integrated in dedicated front pockets. Antennas (WiFi, Nanotron, GNSS L1 band for router receiver and GPS for optional Polaris) are positioned on the shoulders. Batteries are placed in the back of the gilet and wires are fully integrated in the vest. A general interrupter is available in the router board pocket.

Figure 5: Integration of a node on a tactical gilet

[6] Bande « Industriel, Scientifique et Médical”

[7] Two Way Ranging

1.4 Hybridization and sensor fusion for a non-centralized collaborative navigation

The fusion algorithm developed for the demonstrator is completely decentralized and is implemented on each node. It uses positioning measurements delivered by the local GNSS receiver when available, ranging measurement of local node on nearby nodes, ranging measurement of friends and positions of friends when available (resulting of the fusion algorithm). This fusion algorithm delivers periodic navigation solution (each 2 s) thanks a two steps process:

- Geolocalisation process using local GNSS measurement (when available), ranging measurement and position of friends (when available) to elaborate an estimation of local position by minimizing a Less Mean Square criteria thanks to a Gauss-newton algorithm. Due to strong non linearity of the criteria, an efficient initialization is implemented.
- Tracking process based on Extend Kalman Filter with a Nearly Constant Position motion model, suitable for pedestrian nodes.

This algorithm provides a localization solution of the current node even in lack of GNSS signal, under availability of a sufficient number of ranging measurements (node positioning observability condition).

1.5 Integrity monitoring for secured collaborative navigation

If an intruder is able to disseminate corrupted data in the collaborative navigation network without been detected by the passive security protections of the navigation system (case for example of stolen equipment), the only way to detect it consists to analyze navigation data to find abnormal data or behavior in the current navigation context. That is performed first, by detecting abnormal data compare to a priori knowledge and secondly, by searching potential incoherencies between data themselves (if there is enough redundancy). Some algorithms have been developed to check data likelihood by comparing navigation data to some reference models (thanks to a priori knowledge database) and to detect incoherence in different subsets of data using statistic tests (chi2 typically). If there is enough redundancy between data, these algorithms allow detect integrity problem, identifying corrupted data, corrupted sources or nodes. This process lead finally to detect attack and raise integrity alerts, identify attacking node and reject data coming from corrupted node, offering so reliable collaborative navigation with a good guaranty of the integrity of the localization. An operator may also decide to exclude temporary or permanently a node (if he is for example systematically alerted about corruption of a particular node by the integrity monitoring process). In this case, the navigation data and measurement coming from the excluded node will not be used by the navigation process, neither by the integrity monitoring process.

1.6 Human Machine Interface (Android application)

The Android smartphone is used for its embedded sensors and, mainly, as a Human Machine Interface. Firstly, a local Geographical Information System supports map used by the android application to display Blue Force Tracking data and main characteristics of the different member node of the collaborative network.

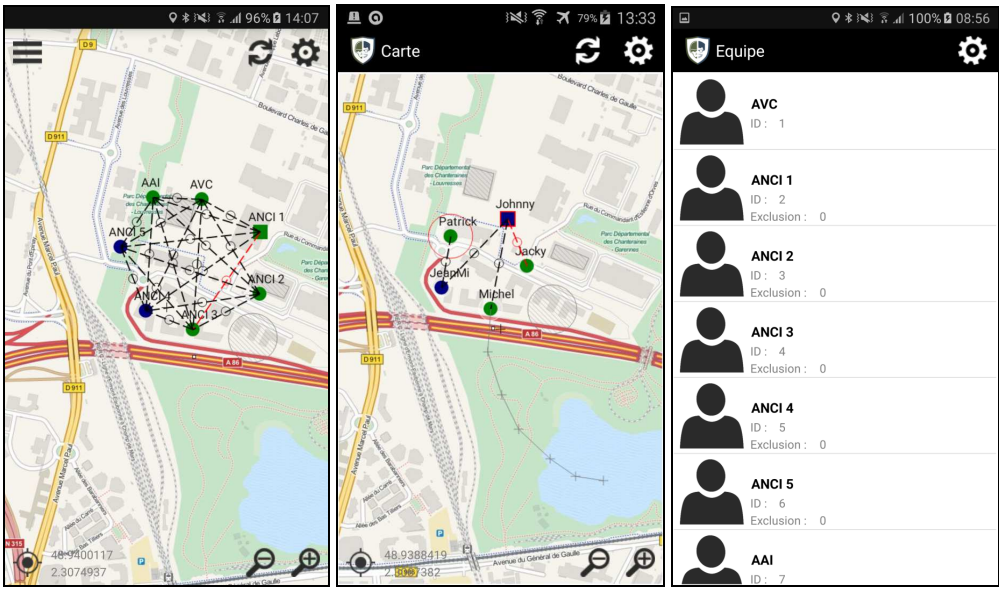

Figure 6: Smartphone HMI

The Human Machine Interface (HMI) of the Android application allows also displaying the measurements: local GNSS data (PVT, NMEA frame and satellite card), ranging and barometer measurements.

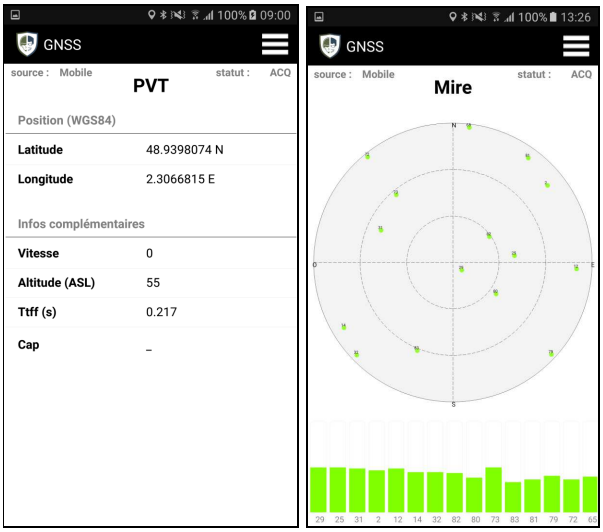

Figure 7: Smartphone HMI for sensors

The Android Human Machine Interface allows also to display status of radio links and the alerts related to the state of the radio network (in blue), the state of GNSS receiver (in green), the integrity monitoring (in orange) and the node exclusion by operators (in red). The operator may also give orders, typically to exclude a node or change the display parameters.

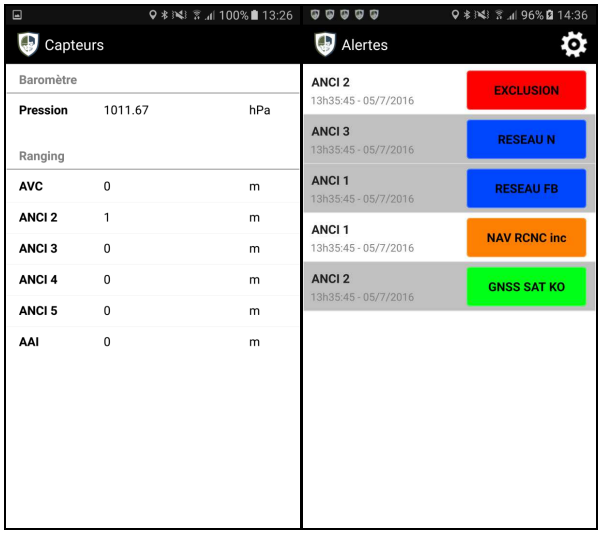

Figure 8: Smartphone HMI for alerts

3. Experimentations and results

Different trials has been performed in an open outdoor area in order to :

- Evaluate the benefit of the collaborative navigation in jamming GNSS context in comparison to the classical autonomous GNSS navigation,
- Evaluate the benefit of the integrity monitoring against integrity attacks in comparison to collaborative navigation without integrity monitoring.

Several fixed point trials have shown the negative effect of a hostile intruder in the collaborative navigation but they have also shown the capability to detect, identify and reject the intruder when the collaborative navigation is coupled to an integrity monitoring.

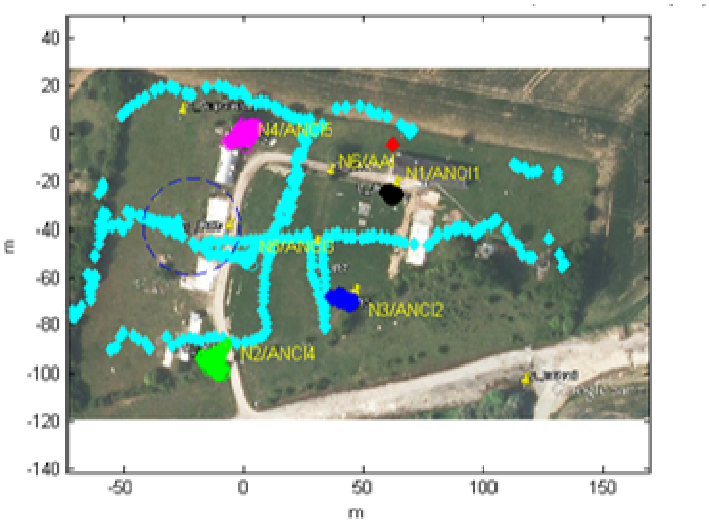

Figure 9: Free run trial

This free-run trial, with a moving GNSS jammed node, has clearly shown the capability to maintain a positioning and navigation with the hybridization and sensor fusion of the collaborative approach.

4. Conclusions

Experience gained during the design of the collaborative navigation demonstrator shows that generic non-rooted Android smartphones have today some limitations for an implementation relying on a non-centralized collaborative outdoor pedestrian navigation.

Some of these limitation rose during the design of the demonstrator was the absence of modular MANET chipset, the limited precision of the possible Wi-Fi ranging, or of the incorporated GNSS sensor. These limitations can however be overcome by the use of additional external COTS. At the end, it appears that today the smartphone mainly constitutes a very good Man-Machine Interface, and that secured navigation has to be delivered by auxiliary components.

Trials made with the demonstrator shows that potential vulnerability of collaborative navigation against integrity attacks could be efficiently treated by integrity monitoring algorithms. The demonstrator provides a first example of a possible implementation of a secured non centralized collaborative navigation.

References

[1] Thomas J. and Robble J, "Off-Grid Communication with Android – Meshing the mobile world", The MITRE Corporation, 2012

[2] Gardner-Stephen, P.; Challans, R.; Lakeman, J.; Bettison, A.; Gardner-Stephen, D.; Lloyd, M., "The serval mesh: A platform for resilient communications in disaster & crisis," IEEE Global Humanitarian Technology Conference (GHTC), 2013, pp.162,166, 20-23 Oct. 2013