Integrity Monitoring of Navigation Systems using Repetitive Journeys

Clément Zinoune, Philippe Bonnifait, Javier Ibañez-Guzmán

▶ **To cite this version:**

Clément Zinoune, Philippe Bonnifait, Javier Ibañez-Guzmán. Integrity Monitoring of Navigation Systems using Repetitive Journeys. IEEE Intelligent Vehicles Symposium (IV 2014), Jun 2014, Dearborn, United States. pp.274-280. hal-01023069

HAL Id: hal-01023069
https://hal.science/hal-01023069

Submitted on 11 Jul 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Integrity Monitoring of Navigation Systems using Repetitive Journeys

Clément Zinoune[1,2], Philippe Bonnifait[1], Javier Ibañez-Guzmán[2]

***Abstract*— Currently, Advanced Driving Assistance Systems (ADAS) increasingly rely on information stored in vehicle on board digital maps. The vehicle position is projected onto the map to establish oncoming road context. However, errors might exist in the road geometry stored in the maps. The integrity of this map-matched estimate must be monitored in real-time to avoid errors that can lead to hazardous situations. This paper presents a monitoring system and fault detection, isolation and adaptation formalism which benefits of multiple vehicle journeys (e.g. commuting). We demonstrate that it is possible to assert correct navigation information within the first journey to a new area and to isolate areas where the road geometry is erroneous after the second journey. The approach takes into account errors that might occur on the estimation of the global vehicle position. The proposed formalism was experimentally validated using a passenger vehicle driven in different map and GNSS conditions.**

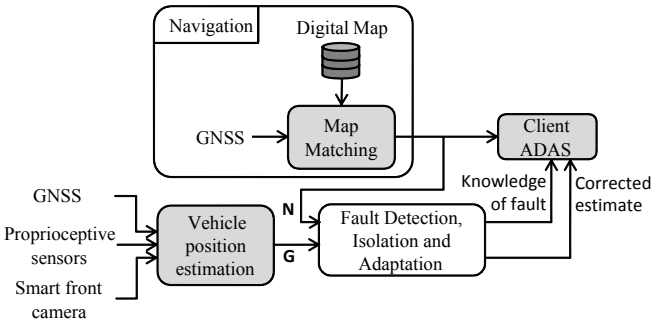


Fig. 1: Structure of fault detection isolation and adaptation in standard passenger vehicle.

I. Introduction

Digital maps are becoming an integral part of Advanced Driving Assistance Systems (ADAS) and Autonomous Driving as they provide contextual information to facilitate decision-making functions. However, experience has found that different types of errors exist in such maps. It can result in discomfort and hazardous situations which makes their use unsafe for critical applications.

A formalism applicable to the monitoring of errors in the description of road geometry embedded in digital maps is proposed. Errors on information provided by the vehicle navigation system may be due to several reasons: errors on the estimations of the localisation system, errors in the map itself or errors when projecting the location estimation onto the digital map (map-matching) [1]. For the purpose of this study, the monitoring of these errors is crucial for the Navigation System Integrity. The projected vehicle position on the navigation map is used as a source of information for ADAS and automated driving.

In this paper, it is assumed that the loss of integrity originates from road geometry error. Thus, our approach is concerned on identifying whether or not a road geometry error exists taking into account the likely existence of localisation errors. The first idea for reducing the ambiguity on the source of error is based on the use of repetitive paths of the subject vehicle. A second idea is to get an independent estimate of the vehicle position by combining an additional GNSS (Global Navigation Satellites System) receiver with vehicle proprioceptive data (speed and yaw rate) [2]. The latter is used to provide information with regard to the road to compensate lateral deviation. The principles are shown in Fig. 1.

The problem is addressed as a Fault Detection, Isolation and Adaptation (FDIA) task. Since both available estimates may be affected by faults, redundancy is provided by the use of position estimates of previous vehicle journey on the same road. We show how the knowledge of effects of faults on estimates makes isolation possible.

The contribution focuses on the mathematical framework necessary to reduce the ambiguity coming from the lack of redundancy and thus isolate faults. The paper is organised as follows. An overview of the theoretical tools used for FDIA together with the problem formulation is presented in Section II. It includes notations, and the underlying assumptions. The manner in which faulty estimates are inferred based on their pairwise comparison is presented in Section III. The conditions on these estimates that make fault isolation possible are included. Section IV presents and demonstrates the properties of the proposed formalism that make relevant its application to Intelligent Vehicles. Implementation of the formalism is detailed through two examples and its interest for monitoring integrity of navigation system for ADAS is given in Section V. This includes the results from experiments that apply the formalism to navigation functions using data acquired in real conditions. Section VI eventually concludes the paper.

II. Problem formulation

A. Background

Low level position integrity is performed in [3] with interval based methods. This kind of approach requires the

[1] Heudiasyc UMR CNRS 7253, Université de Technologie de Compiègne, France. philippe.bonnifait@hds.utc.fr, czinoune@hds.utc.fr
[2] Renault S.A.S, France. javier.ibanez-guzman@renault.com

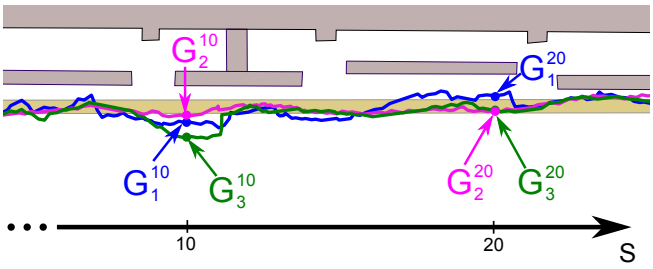


Fig. 2: Vehicle pose estimates for three vehicle journeys on the same road close to large buildings

use of raw sensor data. As shown in Fig. 1, all but FDIA function are black boxes. Access to internal variables is not permitted. For the same reason, approaches centred on direct access to the digital map data like [4] are not possible.

In [5], the authors propose a method to infer the digital map based on a large set of GNSS traces provided by probe vehicles. A server uses these data to update the digital map which is transmitted to the vehicles. However, in the proposed approach, it is assumed that there is no support of the infrastructure.

A high level Fault Detection and Isolation (FDI) approach is chosen, as presented in [6] and [7]. Both of these works employ a different lexicon but the introduced theoretical frameworks are similar. The knowledge about the system is represented by a basic model. Fault is detected when there is a conflict between the observations and the system. Isolation is performed if there is a unique explanation of the conflict.

In the proposed approach, integrity of the map matched estimate is spatially evaluated. Each location of the road network is considered as an operating point of the system to monitor. For a given location of the vehicle, the presence of fault is investigated using all the estimates recorded at this location during the previous vehicle journeys.

B. Problem statement

Let $K \in \mathbb{N}$ denote the total number of times the vehicle went on a given road. As shown in Fig. 2, the vehicle curvilinear abscissa on a given road along the carriageway with respect to its origin is written $s \in \mathbb{R}^+$. The true vehicle position at abscissa s of a given road and at the k^{th} journey is written P_k^s. This can be encoded as a vector that contains the vehicle's geographic coordinates (longitude, latitude and ellipsoidal height).

Using the same notation convention, G_k^s and N_k^s are estimates of the vehicle position P_k^s by the vehicle position and the map matched estimate respectively. Every time the vehicle is at abscissa s of a given road and for the k^{th} time, these two estimates are recorded. Fig. 2 shows some estimates recorded during three journeys in a difficult GNSS area.

Faults may affect the navigation system as well as the vehicle state estimator and cause their outputs to be significantly different from the ground truth (if a multipath affects a GNSS receiver for example). In this case, the estimates are said faulty. The notation $\nsim$ stands for two quantities which are significantly different. Let us define the faults as:

$$f_{N_k^s} \overset{\text{def}}{=} 1 \, if \; N_k^s \nsim P_k^s \text{ and } f_{G_k^s} \overset{\text{def}}{=} 1 \, if \; G_k^s \nsim P_k^s$$

In the following, the development of the method is done using classical equalities but the reader should bear in mind that equalities are true up to a threshold that is discussed in Section V:

$$f_{N_k^s} \overset{\text{def}}{=} \begin{cases} 1 & if \; N_k^s \neq P_k^s \\ 0 & otherwise \end{cases} \tag{1}$$

$$f_{G_k^s} \overset{\text{def}}{=} \begin{cases} 1 & if \; G_k^s \neq P_k^s \\ 0 & otherwise \end{cases} \tag{2}$$

Four realistic assumptions can be made on the errors that affect the estimates from one journey to the other:

- The perturbations cause random errors on vehicle pose estimate. Two faulty G estimates are then different from each other.
- Navigation faults are due to error on digital map which causes systematic errors on navigation estimates. Two faulty N are then equal.
- The method is spatially sampled with respect to the curvilinear abscissa s such that the true vehicle position at s is assumed to be discretised. FDIA at abscissa $s+1$ is performed independently of the FDIA at abscissa s.
- When travelling several times on a road, the vehicle follows the same path with small deviation. If the vehicle is equipped with a smart front camera, the lateral deviation can be automatically compensated.

According to the latter two assumptions, one can state that:

$$P_i^s = P_{i+1}^s, \; \forall i \in \{1, \ldots, K-1\} \tag{3}$$

III. Fault detection and isolation method

This section introduces the concepts of sets of faulty states and residuals that are fundamental for the proposed formalism. After having demonstrated how these concepts are linked, the fault detection and isolation method is presented.

A. Set of faulty states

Let e be the set of faulty states of all estimates available at a given abscissa s. It is composed of all $f_{G_k^s}$ and $f_{N_k^s}$ for the considered iterations K:

$$e \overset{\text{def}}{=} \left\{ f_{G_i^s} \, , \; f_{N_j^s} \right\} \, , \; \forall i, j \in \{1, \ldots, K\} \tag{4}$$

The cardinality of e is $2K$. Each term of e is a boolean value so there are 2^{2K} possible sets written e_n:

$$e_n \in \mathbb{B}^{2K} \, , \; \forall n = \left\{1, \ldots, 2^{2K}\right\} \tag{5}$$

Let us take an example with $K = 2$. There are $2^{2 \cdot 2} = 16$ different sets. The cardinality of each one is $2 \cdot 2 = 4$. For instance, $e_5 = \left\{ \begin{array}{cccc} 0 & 0 & 1 & 0 \end{array} \right\}$ means $\left\{ f_{G_2^s} = 0 \right.$ and $f_{N_2^s} = 0$ and $f_{G_1^s} = 1$ and $\left. f_{N_1^s} = 0 \right\}$.

B. Residuals processing

At a given abscissa s, every available estimate at the current iteration is compared to all the others and the result is stored in a residual vector R. R is therefore made of $C\left(2K, 2\right)$ boolean elements. $C\left(2K, 2\right) = K\left(2K - 1\right)$ stands for the number of 2-combinations from a given set of $2K$ elements.

The components of R are defined as:

$$r_{G_i^s G_j^s} \stackrel{\text{def}}{=} \left\{ \begin{array}{cc} 1 & if\ G_i^s \neq G_j^s \\ 0 & otherwise \end{array} \right. \forall i, j \in \{1, \ldots, K\}, i > j \tag{6}$$

$$r_{G_i^s N_j^s} \stackrel{\text{def}}{=} \left\{ \begin{array}{cc} 1 & if\ G_i^s \neq N_j^s \\ 0 & otherwise \end{array} \right. \forall i, j \in \{1, \ldots, K\} \tag{7}$$

$$r_{N_i^s N_j^s} \stackrel{\text{def}}{=} \left\{ \begin{array}{cc} 1 & if\ N_i^s \neq N_j^s \\ 0 & otherwise \end{array} \right. \forall i, j \in \{1, \ldots, K\}, i > j \tag{8}$$

For example, if at the second iteration, the estimates are such as $G_1^s \neq N_1^s = G_2^s = N_2^s$ then the residual vector contains $2 \cdot (2 \cdot 2 - 1) = 6$ elements:

$$R = \left[\begin{array}{cccccc} r_{N_2^s G_2^s} & r_{G_2^s G_1^s} & r_{N_1^s G_2^s} & r_{N_2^s G_1^s} & r_{N_1^s N_2^s} & r_{N_1^s G_1^s} \end{array} \right] \tag{9}$$

Here $R = \left[\begin{array}{cccccc} 0 & 1 & 0 & 1 & 0 & 1 \end{array} \right]$.

C. Relationships between faults and residuals

Let us show that the residual terms are actually the result of boolean operations between the faulty states of the estimates.

Proposition 1: Let $\vee$ and $\oplus$ denote boolean *or* and *exclusive or* operators respectively,

$$r_{G_i^s G_j^s} = f_{G_i^s} \vee f_{G_j^s}\ , \forall i, j \in \{1, \ldots, K\}\ ,\ i > j \tag{10}$$

$$r_{G_i^s N_j^s} = f_{G_i^s} \vee f_{N_j^s}\ , \forall i, j \in \{1, \ldots, K\} \tag{11}$$

$$r_{N_i^s N_j^s} = f_{N_i^s} \oplus f_{N_j^s}\ , \forall i, j \in \{1, \ldots, K\}\ ,\ i > j \tag{12}$$

Proof: Equation (10) is demonstrated first. Let i and j be such as $i, j \in \{1, \ldots, K\}$ and $i > j$. First of all, one can consider the case in which no fault affects the estimates. According to (2):

$$f_{G_i^s} = 0 \Longleftrightarrow G_i^s = P^s \tag{13}$$

$$f_{G_j^s} = 0 \Longleftrightarrow G_j^s = P^s \tag{14}$$

Then:

$$G_i^s = G_j^s \tag{15}$$

Secondly, the same reasoning is used if a fault affects one of the estimates: $f_{G_i^s} = 1$ and $f_{G_j^s} = 0$

$$f_{G_i^s} = 1\ and\ f_{G_j^s} = 0 \Longleftrightarrow G_i^s \neq G_j^s \tag{16}$$

Finally, if both estimates are faulty:

$$f_{G_i^s} = 1 \Longleftrightarrow G_i^s \neq P^s \tag{17}$$

and

$$f_{G_j^s} = 1 \Longleftrightarrow G_j^s \neq P^s \tag{18}$$

Due to the randomness of G errors, vehicle pose faults cannot compensate each other. Then:

$$G_i^s \neq G_j^s \tag{19}$$

One can conclude that if there is at least one fault on G_i^s or G_j^s, then $r_{G_i^s G_j^s}$ is equal to one. This proves (10).

Secondly, the same reasoning scheme is used to demonstrate (11).

A similar deduction is finally applied to justify (12). Equation (1) allows stating that:

$$f_{N_i^s} = 0\ and\ f_{N_j^s} = 0 \Longleftrightarrow N_i^s = N_j^s \tag{20}$$

Similarly, if a fault affects a navigation estimates:

$$f_{N_i^s} = 1\ and\ f_{N_j^s} = 0 \Longleftrightarrow N_i^s \neq N_j^s \tag{21}$$

Contrarily to the previous cases and due to the assumption made in Section II, two faulty N are equal, then:

$$f_{N_i^s} = 1\ and\ f_{N_j^s} = 1 \Longleftrightarrow N_i^s = N_j^s \tag{22}$$

Finally, $r_{N_i^s N_j^s}$ is equal to one if there is only one fault among $f_{N_i^s}$ and $f_{N_j^s}$. This proves (12). ■

Equations (10), (11) and (12) of Proposition 1 establish a link between available estimates (i.e. G and N) and the faults which affected them (i.e. f_G and f_M). The first two equations tell that if there is at least one fault on the considered estimates then the residual will be affected. In (12), the residual equals one if there is a unique fault among both estimates.

D. Fault detection and isolation

The fault detection and isolation strategy relies on listing all the possible sets of faulty states for a given K and calculating residual vectors with (10), (11) and (12). This forms the truth table for K. On the other hand, available estimates are used to compute the observed residual vector based on (6), (7) and (8). This vector, found in the truth table, allows determining the corresponding set of faulty states. Faults affecting each estimate can be finally deduced from this set.

By definition, the truth table is exhaustive; the observed residual vector does make part of it. However, some sets of faults induce the same residual vector. In this case, isolation is not possible. These are called adverse sets. At least one new system iteration is then required to perform isolation.

TABLE I: Truth table of fault detection and isolation for $K = 2$

	Sets of faults				Residuals					
	f_{G_2}	f_{N_2}	f_{G_1}	f_{N_1}	$r_{N_2G_2}$	$r_{G_2G_1}$	$r_{N_1G_2}$	$r_{N_2G_1}$	$r_{N_1N_2}$	$r_{N_1G_1}$
e_1	0	0	0	0	0	0	0	0	0	0
e_2	1	0	0	0	1	1	1	0	0	0
e_3	0	1	0	0	1	0	0	1	1	0
e_4	1	1	0	0	1	1	1	1	1	0
e_5	0	0	1	0	***0***	***1***	***0***	***1***	***0***	***1***
e_6	1	0	1	0	1	1	1	1	0	1
e_7	0	1	1	0	1	1	0	1	1	1
e_8	1	1	1	0	1	1	1	1	1	1
e_9	0	0	0	1	0	0	1	0	0	1
e_{10}	1	0	0	1	1	1	1	0	0	1
e_{11}	0	1	0	1	1	0	1	1	0	1
e_{12}	1	1	0	1	1	1	1	1	0	1
e_{13}	0	0	1	1	0	1	1	1	1	1
e_{14}	1	0	1	1	1	1	1	1	1	1
e_{15}	0	1	1	1	1	1	1	1	0	1
e_{16}	1	1	1	1	1	1	1	1	0	1

Being adverse depends on the number of faults affecting the estimates as stated in the following proposition.

Proposition 2: A set of faulty states is adverse if and only if it complies with one of the following rules:

1) $f_{N_i} = 1\ ,\ \forall i \in \{1, \ldots, K\}$ and $\exists! j \in \{1, \ldots, K\}$ such as $f_{G_j} = 0$
2) $f_{G_i} = 1\ ,\ \forall i \in \{1, \ldots, K\}$

In other words it is not possible to isolate faults if:

1) Every estimate N is faulty and there is a unique true G.
2) Every G is faulty.

Proof: Proposition 2 is demonstrated in [8]. ■

For example, let the observed residual vector calculated in Section III-B be $R = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$. This residual is found only once in the truth table for two iterations (in bold in Table I) and is caused by the set of faulty states $e_5 = \begin{Bmatrix} 0 & 0 & 1 & 0 \end{Bmatrix}$ meaning $\left\{ f_{G_2^s} = 0 \text{ and } f_{N_2^s} = 0 \text{ and } f_{G_1^s} = 1 \text{ and } f_{N_1^s} = 0 \right\}$.

IV. Noteworthy method properties

Properties are deduced from the proposed FDI formalism. They are detailed as follows.

A. Guaranteed fault detection

The formalism always detects the presence of faulty estimates. In other words, as soon as there is a faulty estimate, the formalism detects it (but may not be able to isolate the faulty estimates).

This is demonstrated by showing that the formalism is always able to isolate the only set that contains no fault. The Proposition 2 indeed shows that this set (for which $f_{N_i} = f_{G_j} = 0\ ,\ \forall i, j \in \{1, \ldots, K\}$) is not adverse.

B. Isolation convergence

The ratio between the number of adverse sets of faulty states and the total number of sets goes to zero when the number of iterations increases. This means that increasing K improves fault isolation capabilities.

To justify this, let $A(K)$ stand for the number of adverse sets of faulty states for K iterations. $A\,(K)$ is the sum of the number of sets induced by the two rules of Proposition 2:

$$A(K) = C\,(K, 1) + \sum_{j=0}^{K} C\,(K, j) \tag{23}$$

The binomial formula applied for coefficients 1 and 1 gives:

$$A(K) = K + 2^K \tag{24}$$

The ratio $q(K)$ between $A(K)$ and the total number of possible sets is:

$$q(K) = \frac{K + 2^K}{2^{2K}} \tag{25}$$

The limit of $q(K)$ as K goes to infinity is 0.

C. Conservation of isolability

Once fault isolation is performed, fault isolation will be performed at any new iteration.

Let I_k be the set of isolable e at $K = k$. Reciprocally, let I_k^c be the complement of I_k, i.e. the set of adverse sets of faulty states. To prove the property, let us demonstrate its contrapositive:

$$e \in I_{k+1}^c \implies e \in I_k^c \tag{26}$$

Let e be an adverse at iteration $k + 1$ such as $e \in I_{k+1}^c$. Then e complies with one of the rules stated in proposition 2. On the one hand, if e is adverse due to rule 1, this may be caused by two reasons:

1.a. $f_{N_i} = 1\ ,\ \forall i \in \{1, \ldots, k+1\}$ and $\exists! j \in \{1, \ldots, k+1\}$ such as $f_{G_j} = 0$ and $j \neq k+1$, or

1.b. $f_{N_i} = 1\ ,\ \forall i \in \{1, \ldots, k+1\}$ and $\exists! j \in \{1, \ldots, k+1\}$ such as $f_{G_j} = 0$ and $j = k+1$.

If e complies to rule 1.a, then:

$$\implies f_{N_i} = 1\ ,\ \forall i \in \{1,\dots,k\}\,,$$

$$\text{and } \exists! j \in \{1,\dots,k\}\,|f_{G_j} = 0 \tag{27}$$

$$\implies e \in I_k^c \tag{28}$$

due to rule 1. If e complies to rule 1.b, then:

$$\implies f_{G_i} = 1\ ,\ \forall i \in \{1,\dots,k\} \tag{29}$$

$$\implies e \in I_k^c \tag{30}$$

because of the rule 2. This shows that, if e is adverse due to rule 1, then (26) is satisfied.

On the other hand, let us consider the case for which e is adverse due to rule 2.

$$f_{G_i} = 1\ ,\ \forall i \in \{1,\dots,k+1\} \tag{31}$$

$$\implies f_{G_i} = 1\ ,\ \forall i \in \{1,\dots,k\} \tag{32}$$

$$\implies e \in I_k^c \tag{33}$$

This finally fulfils the demonstration of (26) and proves the conservation of isolability property.

D. Adaptation

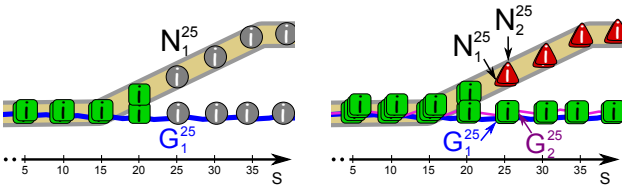
If fault detection and isolation are performed, then adaptation is possible. Adaptation is understood here as a mechanism that consists in determining a fault-free estimate once detection and isolation have been performed.

One must notice that the only set in which every estimate is faulty is adverse (the faults are not isolable because of the second rule of Proposition 2). The consequence is that every isolable fault configuration contains at least one true estimate. As isolation is performed, the true estimate is perfectly identified within the set. Then this true estimate can replace the faulty one.

E. Conservation of Adaptation

If fault isolation is achieved at the K^{th} iteration, whatever happens at the $(K+1)^{th}$ iteration in terms of faults, the proposed formalism allows performing adaptation.

Indeed, the conservation of isolability property states that, if fault isolation is performed at iteration K, isolation will also be performed at $K+1$. Moreover, the adaptation property shows that adaptation is always possible as soon as faults are isolated. Then, if faults are isolated at iteration K, adaptation will be possible at $K+1$.



(a) First journey (blue line) (b) Second journey (purple line)

Fig. 3: A faulty map area. Circular grey marks are for estimate for which the method has detected but not isolated a fault. Green squares are for true estimates and red triangles are the faulty estimates.

V. Application to Navigation Integrity Monitoring

The formalism presented in Section III is applied to the integrity monitoring of the navigation vehicle position estimate. The experimental framework is presented before detailing each step of the FDIA through two simple examples. A more complete set of results finally demonstrates the consistency of the proposed formalism for intelligent vehicles.

All data employed in the following were acquired from a standard GPS receiver on board a passenger vehicle. The map matching function uses an editable digital map. The stored road geometries were locally changed to represent errors found in such digital maps. All algorithms were coded in the C++ language.

The vehicle travels several times to the same new destination using the same roads. The proposed method is run at 5 metres intervals which provides a good spatial sampling of the road geometry. For implementation purposes, estimates separated by a distance lower than 1.5 metres are considered as equal. Map road geometric errors less than this threshold are not significant for most ADAS applications.

For all the experiments, two estimates are used for the analysis: the estimation of the vehicle position G and the projection of the vehicle position onto the road network of the digital map provided by the navigation function N (as defined in Fig. 1). During the experiments, the subject vehicle travels several times over the same roads, thus several estimates of the observed variables are available.

A. Illustrative examples

In the first example, the map contains an error and we show how the method performs fault detection, isolation and adaptation. Each step of the proposed method is detailed and the properties introduced in Section IV are illustrated. In the second example, the map geometry is perfect but a large building may cause errors on vehicle state estimation. This shows how the method rejects faulty estimates.

TABLE II: Truth table for $K = 1$

Sets of faulty states			Residuals
	f_{G_1}	f_{N_1}	$r_{G_1N_1} = f_{G_1} \vee f_{N_1}$
e_1	0	0	0
e_2	1	0	1
e_3	0	1	1
e_4	1	1	1

1) Map road geometric error: In this example (Fig. 3), the true road goes straight whilst there is an error in the representation of the road in the map. The first vehicle journey is shown in Fig. 3a. Let us detail the proposed formalism at abscissa 25m of the first journey.

The first time the vehicle is at abscissa $s = 25$, position estimates are provided by the vehicle state (G_1^{25}) and by the navigation (N_1^{25}) functions (see Fig. 3a). One can compute the observed residual (7):

$$G_1^{25} \neq N_1^{25} \implies r_{G_1^{25}N_1^{25}} = 1$$

This residual is found three times in the truth table for one journey FDI (Table II): the sets of faulty states e_2, e_3 and e_4 give $r_{G_1N_1} = 1$. The proposed method then detects a faulty estimate among G_1^{25} and N_1^{25} but is not able to isolate it. The integrity monitoring system cannot state on the faultiness of N_1^{25}, it sends *unknown* to ADAS which is represented by circular grey marks on Fig. 3a.

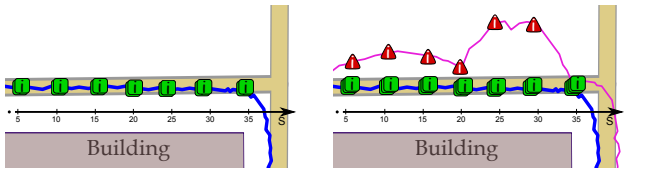
The second time the vehicle crosses abscissa $s = 25$ of the same road (Fig. 3b), a new pair of position estimates becomes available: G_2^{25} and N_2^{25}. The residual vector dimension increases to 6. The elements are calculated using (6), (7) and (8):

$$\begin{aligned}
N_2^{25} \neq G_2^{25} &\implies r_{N_2^{25}G_2^{25}} = 1 \\
G_2^{25} = G_1^{25} &\implies r_{G_2^{25}G_1^{25}} = 0 \\
N_1^{25} \neq G_2^{25} &\implies r_{N_1^{25}G_2^{25}} = 1 \\
N_2^{25} \neq G_1^{25} &\implies r_{N_2^{25}G_1^{25}} = 1 \\
N_1^{25} = N_2^{25} &\implies r_{N_1^{25}N_2^{25}} = 0 \\
G_1^{25} \neq N_1^{25} &\implies r_{G_1^{25}N_1^{25}} = 1
\end{aligned}$$

Then $R = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$.

Table I is the truth table for two journeys. According to the first journey observation, one knows that $f_{G_1^{25}}$ and $f_{N_1^{25}}$ are not both null. The first four rows of Table I could be ignored. The observed residual is finally found only once in this table (caused by the set of faulty states e_{11}), one can then conclude that $f_{G_2^{25}} = 0$, $f_{N_2^{25}} = 1$, $f_{G_1^{25}} = 0$ and $f_{N_1^{25}} = 1$.

The integrity monitoring system returns the instruction *don't use the navigation position estimate* (N_2^{25}). Estimates found faulty (resp. true) by the method are represented by red triangles (resp. green squares) on Fig. 3b. Since error-free estimates have been identified (G_2^{25} and G_1^{25}), adaptation is possible by providing either G_2^{25} or G_1^{25} to client systems. Due to the property detailed in Section IV-E, the integrity monitoring system will be able to provide an error-free pose estimate for all future vehicle journeys on this road.



(a) First journey (blue line) (b) Second journey (purple line)

Fig. 4: A correct map area close to a large building. Red triangles (resp. green squares) are for estimates which the method has isolated as faulty (resp. true).

2) Isolation of GNSS faults: In the second example, shown in Fig. 4, there is no error in the map but the road is close to a large building that may cause GNSS faults. No fault affects vehicle position estimate the first time the vehicle goes in this area (Fig. 4a). The method states with certainty that there is no fault for the seven evaluation points of this example. According to the properties detailed in Sections IV-C to IV-E, one knows that fault isolation and adaptation will be performed at any future journey on this road whatever the faults encountered. Fig. 4b illustrates this with the second journey which is perturbed by the buildings. The method directly isolates the faulty vehicle position estimates and keeps confidence in current and past navigation estimates.

Two opposite cases have been shown by these examples: one erroneous map area in good GNSS conditions and one correct map area in poor GNSS conditions. The method works properly even if faults affect both estimates. In such a situation, fault detection is directly made but isolation and adaptation require more journeys.

B. Experiments

A larger dataset is employed to validate the proposed formalism. A digital map that contains geometrical errors feeds the navigation function. The rural area of this digital map was designed to represent the road network as it was before large road works a few years ago. In the urban area, the map errors were generated to show that, even in poor GNSS conditions, fault detection and isolation of navigation position estimates is possible. As the method generates a large amount of data, Fig. 5 and 6 are synthetic views of the results.

In the rural environment, no fault affects the GNSS receiver. Faulty areas are detected at the first journey. As shown by Fig. 5, the second journey allows the method incriminating the navigation in these areas.

In the urban environment, due to the fault affecting some GNSS estimates, three journeys are required to fully perform isolation on all the roads (Fig. 6).

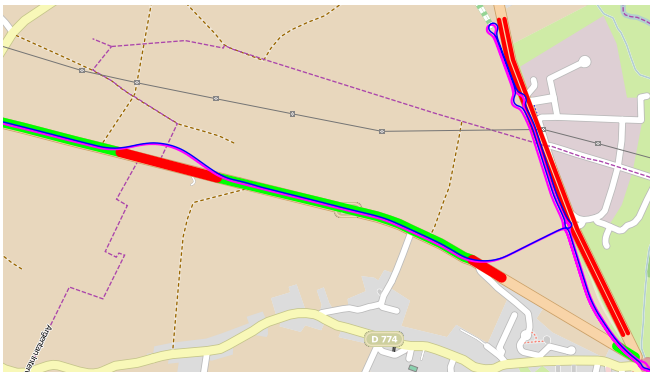


Fig. 5: Results of FDI in rural environment after two journeys (blue and purple lines). In green, navigation estimates that have been identified as correct (during the first journey), in red faulty ones (during the second one).

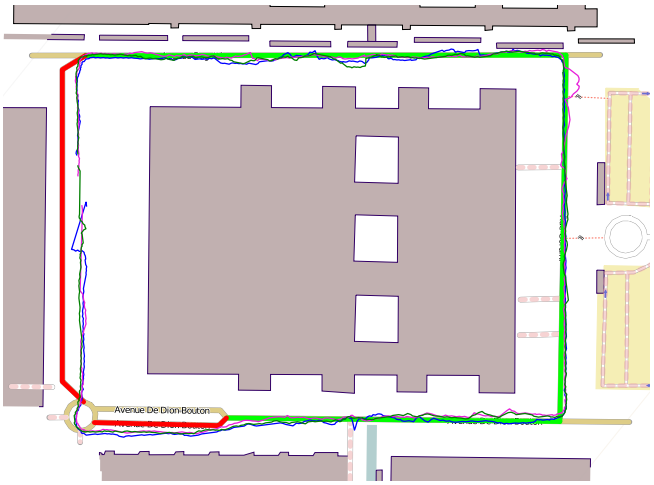


Fig. 6: Results of FDI in a urban environment after three journeys. The red links correspond to map errors that have been fully isolated during the third journey.

As stated in Section V, the method is spatially triggered with a distance of 5 metres in these experiments. The GNSS receivers (the one of the navigation and the one of the monitoring system shown in Fig. 1) used in these experiments are timely synchronised and their maximum frequency is 10 Hz. The navigation fixes are rejected unless they correspond to a sampled abscissa with a 1 m tolerance. Due to the velocity of the vehicle in real traffic conditions, especially in the rural environment, some sampled abscissa can't be evaluated. We define the availability rate of method as the ratio between the total number of sampling points of the vehicle path and the actual number of times the method is run. In these experiments, the availability rate is 80% on the urban scenario and 75% on the rural scenario. Availability would be improved either by using a navigation GNSS receiver triggered on vehicle odometer or by interpolating points at required abscissa.

During the first two journeys, the method states *unknown* every time the situation is theoretically not isolable (according to the rules stated in Proposition 2). We have noticed for these experiments that three journeys are sufficient to isolate every faulty estimate. In the rural scenario, there are 3% of wrong isolations (i.e. some map errors samples have been declared correct and some correct vehicle estimates have been isolated as faulty).

VI. Conclusion

This paper described a fault detection, isolation and adaptation formalism based on the use of multiple iteration of a system. Residuals were defined and the FDI strategy was detailed. A set of properties deduced from this formalism showed its interest for the intelligent vehicles application. Integrity of the navigation position estimate was monitored taking benefit of the repetitive vehicle journeys.

This application allowed detailing first every step of the method through two simple examples. The method performance was then evaluated based on real data in rural and urban environments and it shows a good relevance for the monitoring of the navigation system since it detects misleading information at the first journey and performs isolation from the second journey on the same road.

Current work aims at triggering sensors on spatial vehicle position to improve the availability rate. Moreover, a combination of the method presented here and the spatial approach of [2] is being developed.

References

[1] M. A. Quddus, W. Y. Ochieng, and R. B. Noland, "Current map-matching algorithms for transport applications: State-of-the art and future research directions," *Transportation Research Part C: Emerging Technologies*, vol. 15, no. 5, pp. 312 – 328, 2007.

[2] C. Zinoune, P. Bonnifait, and J. Ibanez-Guzman, "A sequential test for autonomous localisation of map errors for driving assistance systems," in *Intelligent Transportation Systems (ITSC), 2012 15th International IEEE Conference on*, 2012, pp. 1377–1382.

[3] L. Jaulin, M. Kieffer, I. Braems, and E. Walter, "Guaranteed nonlinear estimation using constraint propagation on sets," *International Journal of Control*, vol. 74, no. 18, pp. 1772–1782, 2001.

[4] D. Betaille and R. Toledo-Moreo, "Creating enhanced maps for lane-level vehicle navigation," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 11, no. 4, pp. 786 –798, dec. 2010.

[5] G. Agamennoni, J. Nieto, and E. Nebot, "Robust and accurate road map inference," in *Robotics and Automation (ICRA)*, may 2010, pp. 3946 –3953.

[6] R. Reiter, "A theory of diagnosis from first principles," *Artificial intelligence*, vol. 32, no. 1, pp. 57–95, 1987.

[7] J. De Kleer and B. C. Williams, "Diagnosing multiple faults," *Artificial intelligence*, vol. 32, no. 1, pp. 97–130, 1987.

[8] A. Monteil and C. Zinoune, "Demonstration of the rules non isolability of sets of faulty states," University of Technology of Compiegne, http://bibliotheque.utc.fr/medias/doc/EXPLOITATION/IFD/IFD_REFDOC_0002463/demonstration-of-the-rules-non-isolability-of-sets-of-faulty-states, Tech. Rep., 2014.