



UNIVERSITÀ  
DEGLI STUDI  
FIRENZE

Scuola di Scienze Matematiche, Fisiche e Naturali  
Corso di Laurea Magistrale in Informatica  
Resilient and Secure Cyber-Physical System

UTILIZZO DI UN ALGORITMO SENSOR  
FUSION NELL'AMBITO DELLA  
LOCALIZZAZIONE FERROTRAMVIARIA

USE OF A SENSOR FUSION ALGORITHM IN  
THE AREA OF TRAMWAY LOCALIZATION

ALEX FOGLIA

ANDREA BONDAVALLI

Anno Accademico 2018-2019



---

## INDICE

---

1	Stato dell'Arte	7
1.1	Sistemi Ferroviari e Ferrotramviari	7
1.2	Il Problema del Posizionamento	8
1.2.1	Possibili Sviluppi	12
2	Sensor Fusion	15
2.1	Panoramica	15
2.1.1	Sistemi Dinamici	15
2.1.2	Misure e Rumore	16
2.2	I Filtri di Kalman	18
2.2.1	Premesse statistiche	18
2.2.2	Filtro di Kalman Lineare	19
2.2.3	Esempio applicativo	22
3	Applicazione di SFA: La Tramvia di Firenze	31
3.1	Architettura di Sistema	32
3.1.1	Architettura Hardware	32
3.1.2	Architettura Software	33
3.2	Gestione della trasmissione dei dati	35
3.2.1	Trasmissione in entrata	35
3.2.2	Trasmissione in uscita	37
3.3	Scenario di Esempio	39
3.4	Possibili sviluppi	42
3.4.1	Problematiche legate alla security	42
3.4.2	Miglioramenti al servizio fornito	45



---

## ELENCO DELLE TABELLE

---

Tabella 1	Segnalazioni semaforiche ferrotramviarie	12
Tabella 2	Misurazioni di esempio del corpo in caduta libera	24
Tabella 3	Risultati generali dell'algoritmo	29
Tabella 4	Errori a posteriori	29
Tabella 5	Confronto tra errore a posteriori sulla posizione, e distanza fra valori reali di posizione e misure di posizione	30
Tabella 6	Protocollo di comunicazione in entrata	36
Tabella 7	Significato del campo SENSOR_TYPE	37
Tabella 8	Protocollo di comunicazione in uscita	38
Tabella 9	Formato del pacchetto di <i>ack</i>	39
Tabella 10	Condizioni iniziali	39



---

## ELENCO DELLE FIGURE

---

Figura 1	Treno in arrivo alla stazione ferroviaria di Firenze Santa Maria Novella	8
Figura 2	Tramvia di Danhai, Taipan	8
Figura 3	Schema di un tipico scenario tramviario	9
Figura 4	UCS realizzato da Thales Italia SPA	10
Figura 5	Conta Assi	11
Figura 6	Esempio di <i>Point Machine</i> installata su una traccia ferrotramviaria	11
Figura 7	Schema SFA	13
Figura 8	Grafico dell' errore di stima della posizione con $\alpha = 10^0, \varepsilon = 10^{-3}$	17
Figura 9	Processo caratterizzato da <i>rumore</i>	18
Figura 10	Processo e misura caratterizzati da rumore	20
Figura 11	Schema di un KF lineare	22
Figura 12	Stima della velocità del corpo in caduta	27
Figura 13	Stima della posizione del corpo in caduta	28
Figura 14	Tramvia di Firenze - Linea T1	31
Figura 15	Architettura hardware bordo treno	34
Figura 16	Architettura software bordo treno	36





---

## STATO DELL'ARTE

---

### 1.1 SISTEMI FERROVIARI E FERROTRAMVIARI

Il concetto di *treno* come comunemente percepito nasce con l'inizio della Rivoluzione Industriale, avvenuta tra il *XVIII* e il *XIX* secolo, a seguito della quale l'avvento della macchina a vapore ha permesso all'umanità di disporre di fonti di energia sufficienti a fare evolvere i primi rudimentali trasporti su binario negli odierni sistemi ferroviari.

È possibile schematizzare un Sistema Ferroviario, o Ferrotramviario, come un veicolo, il treno, vincolato a muoversi attraverso una propulsione, elettrica o a combustibile, lungo una traccia fissa, il binario.

Queste caratteristiche accomunano qualsiasi sistema di trasporto ferroviario o ferrotramviario a prescindere dalla sua scala in termini di veicoli transitanti ed estensione geografica. Ciò che invece differenzia un Sistema Ferroviario da un Sistema Ferrotramviario sono:

- Le caratteristiche fisiche del treno, come lunghezza e massa;
- Le caratteristiche geografiche dell'ambiente operativo;
- Gli scopi del trasporto.

In generale, nel trasporto ferroviario si utilizzano treni caratterizzati da grandi dimensioni, che trasportano persone o merci su lunghe percorrenze (regionali, nazionali o internazionali), operando pertanto prevalentemente in ambienti extra urbani. Un esempio di treno operante in un sistema ferroviario classico è quello in figura 1.

Il trasporto ferrotramviario, di contro, vede l'utilizzo di treni dalle ridotte dimensioni, più leggeri di quelli usati nei sistemi ferroviari, e che hanno lo scopo di rappresentare un'alternativa per il cittadino all'utilizzo di mezzi privati durante i suoi spostamenti all'interno di un'area metropolitana. Quest'ultima caratteristica implica che l'ambiente operativo di un



Figura 1: Treno in arrivo alla stazione ferroviaria di Firenze Santa Maria Novella

sistema ferrotramviario sia radicalmente diverso da quello di un sistema ferroviario: i treni si muovono lungo rotaie installate su strade urbane, quindi il traffico ferrotramviario è fuso con il traffico automobilistico, motociclistico, ciclistico e pedonale che caratterizza l'ambiente urbano, come mostrato nelle figure 2 e 3.



Figura 2: Tramvia di Danhai, Taipan

## 1.2 IL PROBLEMA DEL POSIZIONAMENTO

Per posizionamento ferroviario, si intende la stima della posizione di un treno all'interno di una traccia ferroviaria. Esso esiste tanto nel contesto ferrotramviario quanto nel contesto ferroviario classico.

Sovente questa stima viene espressa come progressiva chilometrica rispetto all'origine della linea oppure, più raramente, come coordinata



Figura 3: Schema di un tipico scenario tramviario

geografica.

Il problema del posizionamento sorge nel momento in cui, per ragioni di rotta, un treno ha necessità di spostarsi da una sezione di binario, anche detta traccia, ad un'altra. Questa operazione di scambio è offerta dal sistema di *interlocking*. Tale sistema è detto *safety-critical*, in quanto offre una funzionalità che deve rispettare adeguati standard di sicurezza. Gli odierni sistemi di posizionamento si basano principalmente sull'utilizzo di strumenti installati a terra, che hanno lo scopo di rilevare il passaggio di un treno, e quindi di interagire con il sistema di *interlocking* della traccia al fine di garantire, con un elevato livello di confidenza, un transito sicuro dei mezzi.

#### *Odierna Tecniche di Posizionamento*

I sistemi di posizionamento attualmente in uso sono basati su un'architettura distribuita composta dai seguenti blocchi:

- Sottosistema di *interlocking*;
- Sottosistema di comunicazione treno-traccia;
- Sottosistema semaforico.

**SOTTOSISTEMA DI INTERLOCKING:** Il sottosistema di *interlocking* è la parte che si fa effettivamente carico di offrire al treno un attraversamento sicuro di una *Junction Area (JA)*. Una JA è un punto della linea ferroviaria in cui il treno può cambiare direzione, e occupare una nuova traccia di

binario.

La nuova traccia da occupare potrebbe avere particolari vincoli sul numero di treni contemporaneamente transitanti, ed in ogni caso lo scambio di rotaia deve essere corretto ed avvenire in sicurezza, in quanto occupare la traccia sbagliata potrebbe avere ripercussioni finanche catastrofiche.

Un sistema di *interlocking* è composto dai seguenti elementi:

- *Switch Control Unit (UCS):*

Piattaforma certificata SIL-3 che rappresenta il nucleo del sistema di *interlocking* e che implementa l'intera logica di gestione di una JA. Un UCS dispone di un'interfaccia di *Input/Output (I/O)* verso gli elementi di *interlocking* installati a terra che ne consente un controllo sicuro in accordo allo standard SIL-3.



Figura 4: UCS realizzato da Thales Italia SPA

- *Conta Assi:*

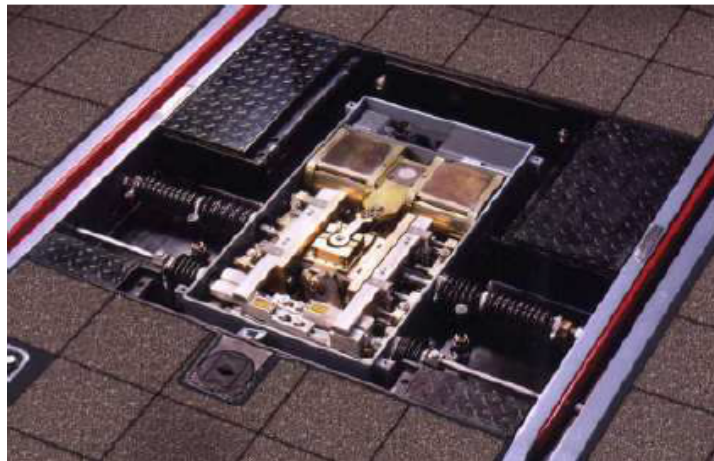
Il Conta Assi, o in inglese *Axle Counter (AC)*, è un sistema certificato SIL-3 che ha lo scopo di rilevare la presenza del treno e fornire quindi lo stato di occupazione della sezione di traccia in cui l'AC è installato.

- *Point Machines:*

Le *Point Machines* infine, sono degli strumenti certificati SIL-3 che hanno lo scopo di direzionare le rotaie verso una determinata sezione di traccia.



Figura 5: Conta Assi

Figura 6: Esempio di *Point Machine* installata su una traccia ferrotramviaria

L'intero sistema di *interlocking* viene attivato dai *Track Circuit*. Questi apparati sono installati a terra prima di ciascuna JA, e segnalano al sistema di *interlocking* l'avvicinamento di un treno alla successiva JA.

**SOTTOSISTEMA DI COMUNICAZIONE TRENO-TRACCIA:** Il sottosistema di comunicazione treno-traccia è gestito da un computer installato bordo treno, chiamato *On Board Control Unit* (OBCU), ed ha lo scopo di fornire funzionalità non legate alla *safety* e pertanto poco interessanti. OBCU viene principalmente utilizzato per monitorare lo stato del traffico ferrotramviario in una architettura di *monitoring* centralizzata. Il monitoring si basa su comunicazioni *wireless*. In alcune applicazioni può comprendere una comunicazione più o meno diretta con il sistema di *interlocking* allo scopo di segnalare l'avvicinamento del treno a una JA.

**SOTTOSISTEMA SEMAFORICO:** Il sottosistema semaforico prende in ingresso informazioni dal sistema di *interlocking* ed eventualmente, da OBCU, e gestisce i segnali luminosi da mostrare sui semafori a un mac-





Segnale	Descrizione	Significato
	Barra bianca orizzontale	Fermarsi
	Barra bianca verticale	Procedere avanti
	Barra bianca ruotata di 45 gradi	Procedere solo a destra
	Barra bianca ruotata di -45 gradi	Procedere solo a sinistra

Tabella 1: Segnalazioni semaforiche ferrotramviarie

chinista che si appresta a superare una JA.

In tabella 1 viene riportata la lista dei segnali semaforici utilizzati nel contesto ferrotramviario.

### 1.2.1 Possibili Sviluppi

Le attuali tecniche di posizionamento richiedono un intervento trascurabile di computer installati a bordo e una grande quantità di apparati installati a terra. Mentre i computer di bordo non forniscono in generale funzionalità legate alla *safety*, gli apparati installati a terra sono costosi e hanno un impatto ambientale non trascurabile.

È possibile considerare il treno e il computer di bordo come un unico sistema, ossia il treno viene modellato come un *Cyber-Physical System*.

Un *Cyber-Physical System* (CPS) è un sistema composto da una parte *fisica* e da una parte *cyber*. Il sottosistema fisico è composto da sensori e attuatori che hanno rispettivamente lo scopo di rilevare lo stato dell'ambiente circostante e di alterarlo se necessario. Il sottosistema *cyber* è essenzialmente un elaboratore, che dispone di processore, memoria, e interfacce I/O verso i sensori gli attuatori, ed eventuali operatori umani. Una tale

architettura di sistema, permette di sfruttare le capacità di calcolo dei moderni processori per implementare algoritmi anche molto complessi per il *processing* di grandi quantità di dati provenienti dai sensori.

Lo scopo della Tesi è quello di mostrare come può un CPS sostituire il complesso e costoso sistema di posizionamento tuttora operante, attraverso l'uso combinato di un insieme di sensori i cui dati rilevati vengono processati da un algoritmo noto come *Sensor Fusion Algorithm* (SFA).

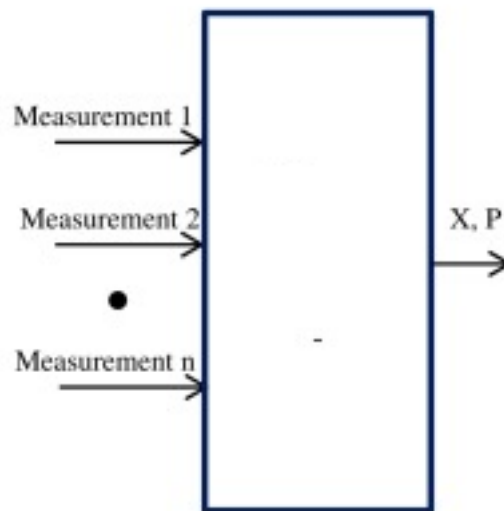


Figura 7: Schema SFA

Tale algoritmo è schematizzabile come una *black-box*: le misurazioni dei sensori sono l'ingresso, mentre l'uscita è la misura cercata, nella fattispecie, la posizione del treno lungo la traccia. Utilizzando SFA, il treno è in grado di auto-posizionarsi, capacità che minimizza la necessità di installare apparati di terra.

Un algoritmo che tiene conto delle misurazioni di un *set* di sensori, usato in luogo di un semplice *processing* di insiemi di misure provenienti da sorgenti omologhe, permette al sistema di correggere il rumore che disturba le singole misurazioni, realizzando così una nuova misura più accurata di quella che si avrebbe considerando i sensori in maniera mutuamente esclusiva.





---

## SENSOR FUSION

---

Nei sistemi in cui è richiesta un'alta *reliability* delle misure, l'informazione fornita dai singoli sensori non è sufficiente. In questi casi è raccomandato l'utilizzo di un insieme di sensori in contemporanea.

### 2.1 PANORAMICA

In generale, un algoritmo SFA viene utilizzato per stimare lo stato di un sistema dinamico in un ambiente caratterizzato da *rumore*.

#### 2.1.1 Sistemi Dinamici

Un sistema dinamico è una modellazione matematica di un processo che evolve nel tempo, la cui evoluzione è descritta attraverso un sistema di equazioni differenziali o alle differenze, nel caso esso si evolva rispettivamente a tempo continuo o a tempo discreto.

Sia  $S$  l'insieme dei possibili stati che il sistema può assumere, e sia  $m = |S|$  la dimensione dello spazio degli stati.

Senza perdere in generalità, si possono formalizzare questi due tipi di sistemi dinamici come:

$$y'(t) = f(t, y(t)), \quad t \geq 0 \quad (1)$$

Con  $y(0) \in \mathbb{R}^m$  condizione iniziale nota, e:

$$y_{n+1} = f(n, y_n), \quad n = 0, 1, \dots \quad (2)$$

con al solito  $y_0 \in \mathbb{R}^m$  condizione iniziale nota.

Ricavare lo stato del sistema dinamico per un certo istante  $t$ , o  $n$ , equivale a risolvere le equazioni cui sopra e valutarne la traiettoria soluzione in  $t$

o in  $n$ .

Un semplice sistema dinamico è rappresentato da un punto materiale che si muove con una accelerazione costante

$$\mathbf{a} = a\mathbf{k}$$

dove  $\mathbf{k}$  è un qualunque versore della base canonica di  $\mathbb{R}^3$ .

Supponendo che il punto si muova con velocità iniziale  $\mathbf{z}'(0) = v_0\mathbf{k}$  nota e inizi il moto da una coordinata  $\mathbf{z}(0) = z_0\mathbf{k}$  nota, si ha:

$$z''(t) = a \quad (3)$$

$$z'(t) = \int a dt = at + v_0$$

$$z(t) = \int (at + v_0) dt = \frac{1}{2}at^2 + v_0t + z_0$$

L'equazione  $z(t)$  descrive completamente la traiettoria di moto del punto materiale, mentre  $z'(t)$  descrive completamente la traiettoria della velocità del punto durante il suo moto.

### 2.1.2 Misure e Rumore

In questo semplice esempio, viene fatta l'assunzione di conoscere a priori il valore esatto di  $a$ , di  $v_0$  e di  $z_0$ .

Nella pratica, per misurare l'accelerazione  $a$  è necessario uno strumento denominato *accelerometro*, il quale produrrà delle misure giocoforza affette da errori casuali. Si supponga di sostituire  $a$  nell'equazione  $z(t)$  con una sua perturbazione  $\tilde{a} = a + \varepsilon$  dove  $\varepsilon$  è una variazione casuale della misura data dal *rumore* che caratterizza qualsiasi processo di misura. Si può supporre  $\text{Var}(\varepsilon) = 0$  e considerare, ai fini di questa trattazione,  $\varepsilon$  come un valore costante; in realtà  $\varepsilon$  è una variabile casuale a varianza generalmente non nulla. Si suppongano inoltre  $v_0 = z_0 = 0$  per comodità di calcolo:

$$z(t) = \frac{1}{2}\tilde{a}t^2 = \frac{1}{2}(a + \varepsilon)t^2 = \frac{1}{2}(at^2 + \varepsilon t^2)$$

Si nota immediatamente che la variazione della misura  $z(t)$  data da  $\varepsilon$  aumenta con il quadrato del tempo.

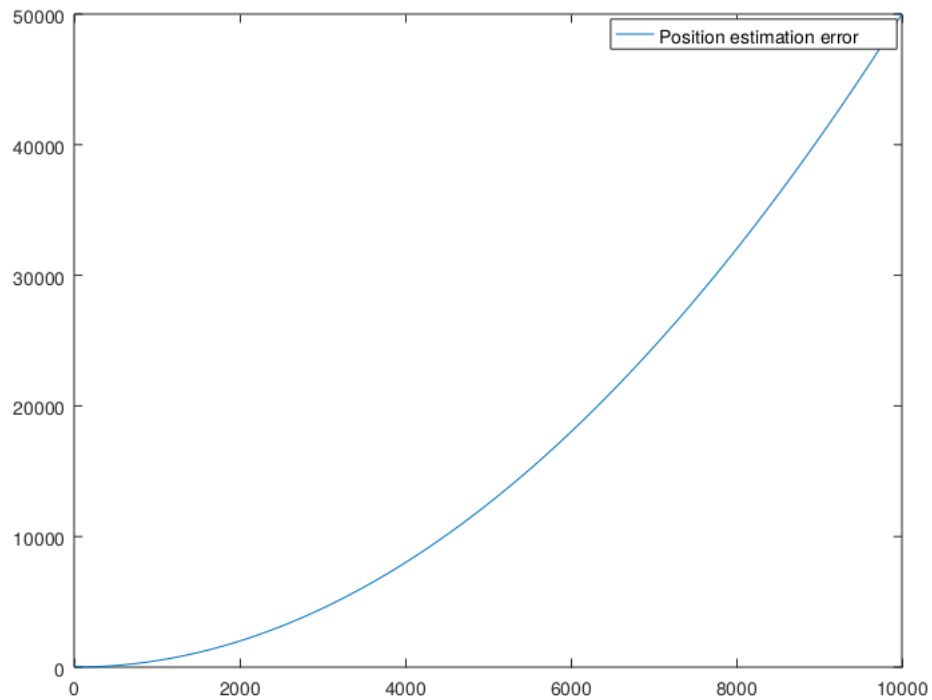
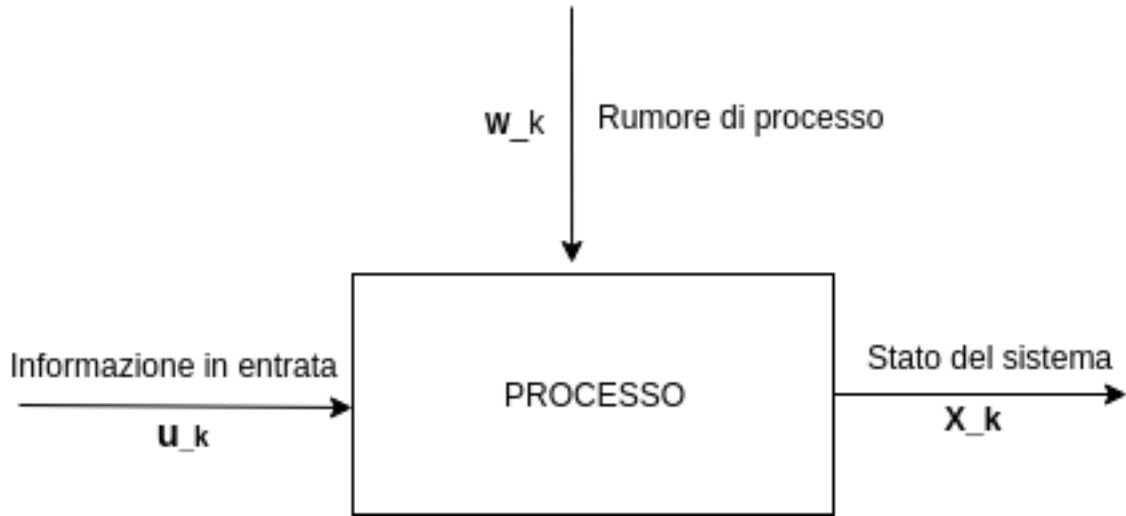


Figura 8: Grafico dell' errore di stima della posizione con  $\alpha = 10^0$ ,  $\varepsilon = 10^{-3}$

Il sistema dinamico individuato in (3), è una tipologia di sistema dinamico caratterizzato da assenza di *rumore di processo*: fatta assunzione di conoscere esattamente il valore di  $\alpha$ , la doppia integrazione di (3) rispetto al tempo fornisce una descrizione esatta e deterministica della dinamica del sistema: la traiettoria sarà *esattamente* quella individuata dalla soluzione.

Alcuni processi tuttavia evolvono in parte stocasticamente per loro natura, e questa natura stocastica insita nel processo viene chiamata *rumore di processo*. Si conclude pertanto che non solamente le misurazioni sono affette da rumore, ma anche il processo evolutivo stesso può essere affetto da rumore stocastico intrinseco. La conseguenza è che la forma esplicita delle equazioni (1) e (2) contiene un termine casuale individuato da una variabile aleatoria.

Uno schema di un processo caratterizzato da *rumore* è mostrato in figura 9.

Figura 9: Processo caratterizzato da *rumore*

## 2.2 I FILTRI DI KALMAN

Un Filtro di Kalman, o in inglese *Kalman Filter* (KF), è, da un punto di vista statistico, uno *stimatore* dello stato di un sistema dinamico caratterizzato da rumore. L'algoritmo individuato dalla formulazione matematica di un KF è un caso particolare di SFA.

### 2.2.1 Premesse statistiche

Un insieme di  $N$  sorgenti di misurazioni viene modellato come un insieme di  $N$  variabili casuali.

Siano  $X_1, \dots, X_N$   $N$  variabili casuali a valori in un insieme finito non vuoto  $\mathbb{X}$ , e sia  $X, Y$  una qualsiasi coppia presa tra le  $N$  variabili casuali.

Si chiama *covarianza* di  $X, Y$  la seguente quantità:

$$\text{cov}(X, Y) = \mathbb{E}\{[X - \mathbb{E}(X)][Y - \mathbb{E}(Y)]\} = \sigma_{XY}$$

Si osservi che :

$$\text{cov}(X, X) = \mathbb{E}\{[X - \mathbb{E}(X)][X - \mathbb{E}(X)]\} = \mathbb{E}[X - \mathbb{E}(X)]^2 = \sigma_X^2$$

Per un vettore di  $N$  variabili aleatorie  $X_1, \dots, X_N$ , si definisce la matrice di *varianza-covarianza*, o semplicemente matrice di *covarianza*, la seguente matrice quadrata  $N \times N$ :

$$\begin{aligned} \Sigma &= \begin{pmatrix} \text{cov}(X_1, X_1) & \text{cov}(X_1, X_2) & \dots & \text{cov}(X_1, X_N) \\ \vdots & \vdots & \ddots & \vdots \\ \text{cov}(X_N, X_1) & \text{cov}(X_N, X_2) & \dots & \text{cov}(X_N, X_N) \end{pmatrix} \\ &= \begin{pmatrix} \sigma_{X_1}^2 & \sigma_{X_1, X_2} & \dots & \sigma_{X_1, X_N} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{X_N, X_1} & \sigma_{X_N, X_2} & \dots & \sigma_{X_N}^2 \end{pmatrix} \end{aligned}$$

Un vettore di  $N$  variabili casuali si dice congiuntamente *gaussiano*, ossia distribuito secondo una distribuzione di probabilità *normale multivariata*, quando qualunque combinazione lineare non banale:

$$Y = \sum_{i=1}^N \alpha_i X_i \quad \alpha_i \in \mathbb{R}$$

Ha distribuzione di probabilità *gaussiana*.

### 2.2.2 Filtro di Kalman Lineare

I KF sono comunemente basati su sistemi dinamici *lineari* a tempo discreto, tuttavia i fenomeni reali sono raramente lineari. Un modello lineare è spesso un'approssimazione di un modello più complesso.

Nel dominio applicativo in cui si colloca la Tesi, ossia quello del posizionamento ferroviario, occorre utilizzare una generalizzazione al caso non-lineare dei Filtri di Kalman standard: il Filtro di Kalman Esteso (CITARE PAPER QUA). Per ragioni di semplicità, in questo capitolo viene esposto il principio base del funzionamento di un semplice KF lineare.

#### Definizione del problema

Si consideri il seguente sistema dinamico lineare discreto:

$$\begin{cases} \mathbf{x}_k = \mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}\mathbf{u}_k + \mathbf{w}_k \\ \mathbf{y}_k = \mathbf{C}\mathbf{x}_k + \mathbf{v}_k \end{cases} \quad (4)$$

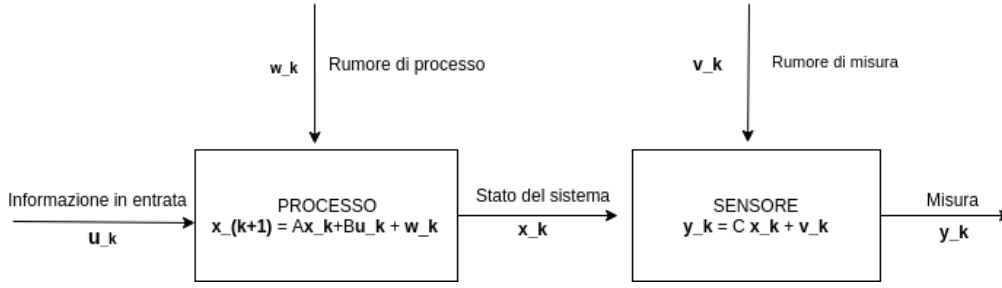


Figura 10: Processo e misura caratterizzati da rumore

In cui i vettori  $w_k$  e  $v_k$  rappresentano rispettivamente il rumore di processo e il rumore di misura. Si assumono *congiuntamente gaussiani*, indipendenti e con matrici di covarianza  $Q, R$  rispettivamente.

Il vettore  $y_k$  rappresenta il vettore di misurazioni campionate all'istante  $k$ , mentre il vettore  $x_k$  rappresenta lo stato del sistema all'istante  $k$ .

Le matrici  $A$  e  $B$  descrivono la dinamica del modello e si assumono note a priori, pena l'introduzione di errori sistematici, mentre la matrice  $C$  descrive la dinamica del processo di misura. Il vettore  $u_k$  rappresenta l'informazione data in ingresso al sistema al tempo  $k$ .

Uno schema della (4) ad ogni istante di tempo  $k$  è riportato in figura 10.

Dal momento che non è possibile individuare una soluzione analitica di (4), il problema da risolvere è *stimare* lo stato del sistema  $x_k$  per qualunque istante di tempo  $k$ .

### Soluzione

Si definiscono i vettori:

- $\hat{x}_k^-$  come la stima *a priori* dello stato del sistema all'istante  $k$ , sulla base della conoscenza del processo all'istante  $k - 1$ ;
- $\hat{x}_k$  come la stima *a posteriori* dello stato del sistema all'istante  $k$ , data dalle misurazioni  $y_k$  allo stesso istante.

Si ha che ciascun  $\hat{x}_k^-$  e ciascun  $\hat{x}_k$  è in effetti un vettore di variabili aleatorie.

Siano  $e_k^- = (x_k - \hat{x}_k^-)$ ,  $e_k = (x_k - \hat{x}_k)$  rispettivamente l'errore a priori e l'errore a posteriori di stima, e siano  $P_k^-$  e  $P_k$  rispettivamente le matrici di covarianza di  $e_k^-$  e di  $e_k$ .

Un KF lineare è una quintupla di equazioni:

1.  $\hat{x}_k^- = A\hat{x}_{k-1}^- + Bu_k$

2.  $P_k^- = AP_{k-1}^- A^T + Q$
3.  $L_k = P_k^- C^T (CP_k^- C^T + R)^{-1}$
4.  $\hat{x}_k = \hat{x}_k^- + L_k(y_k - C\hat{x}_k^-)$
5.  $P_k = (I - L_k C)P_k^-$

In cui le equazioni 1 e 2 vengono dette *equazioni di predizione* e proiettano lo stato e la covarianza dell'errore di stima a priori all'istante temporale  $k - 1$ , in avanti all'istante  $k$ ; mentre le equazioni 3, 4, 5, vengono dette *equazioni di aggiornamento*:

- Viene prima calcolata  $L_k$ , ossia la *matrice dei guadagni di Kalman*;
- Le misure  $y_k$  vengono usate per determinare una *stima a posteriori* dello stato del sistema all'istante  $k$ ;
- Infine viene calcolata una stima della covarianza dell'errore a posteriori  $P_k$ .

In figura 11, è riportato uno schema del funzionamento logico di un KF collegato a un sistema dinamico lineare a tempo discreto.

KF è un *filtro ricorsivo*, in quanto la stima  $\hat{x}_k$  dello stato del sistema all'istante  $k$  viene determinata combinando le informazioni date dal vettore di misurazioni  $y_k$  campionate all'istante  $k$  con la stima dello stato del sistema all'istante  $k - 1$ <sup>1</sup>.

KF è uno *stimatore ottimo*, dove ottimo significa che minimizza la covarianza dell'errore di stima a posteriori, se tutti i rumori hanno distribuzione normale multivariata.

---

<sup>1</sup> Supposto noto lo stato iniziale  $x_0$ .

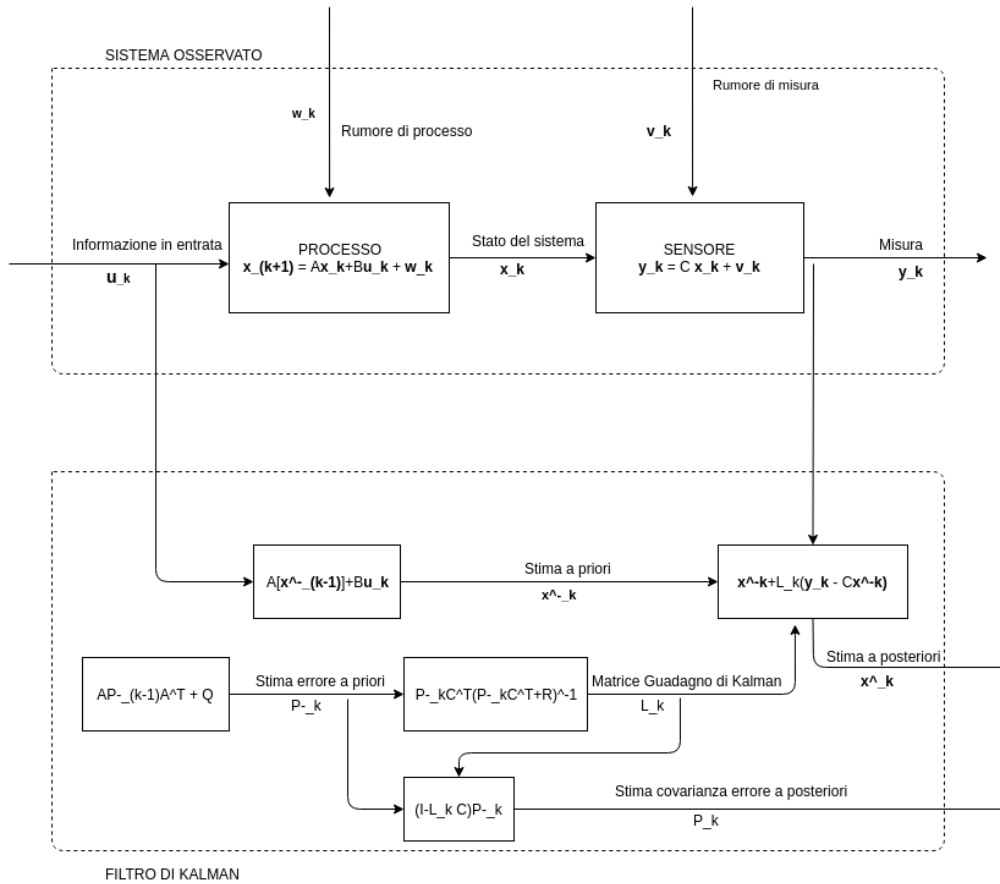


Figura 11: Schema di un KF lineare

### 2.2.3 Esempio applicativo

Si supponga di voler determinare posizione e velocità nel sistema dinamico individuato dalla (3). Valgono le seguenti ipotesi:

- Il corpo, modellato come puntiforme, viene lasciato cadere da una quota  $z(0) = z_0$  assegnata, con velocità iniziale  $v_0$ ;
- La sola accelerazione a cui è soggetto il corpo è l'accelerazione gravitazionale  $-g$ ;
- Il sistema non è caratterizzato da rumore di processo;
- Un osservatore è in grado di misurare la quota dell'oggetto mediante uno strumento di misura  $X$  distribuito come una normale univariata con varianza  $R$ ;



- Il sistema viene osservato ogni secondo per un intervallo di tempo lungo  $t_M$  s

Valori numerici:

- $z_0 = 100$  m
- $v_0 = 0 \frac{\text{m}}{\text{s}}$
- $g = 1 \frac{\text{m}}{\text{s}^2}$
- $R = 1 \text{ m}^2$
- $t_M = 10$  s

Si scrivono le equazioni (4) modellanti la dinamica del processo evolutivo e la dinamica del processo di misurazione:

$$\begin{aligned} \begin{cases} \mathbf{x}_k = A\mathbf{x}_{k-1} + B\mathbf{u}_k + \mathbf{w}_k \\ \mathbf{y}_k = C\mathbf{x}_k + \mathbf{v}_k \end{cases} &= \begin{cases} \mathbf{x}_k = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mathbf{x}_{k-1} + \begin{pmatrix} \frac{1}{2} \\ 1 \end{pmatrix} - g + \underline{0} \\ \mathbf{y}_k = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mathbf{x}_k + \mathbf{v}_k \end{cases} = \\ &= \begin{cases} \mathbf{x}_k = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mathbf{x}_{k-1} - \begin{pmatrix} \frac{1}{2} \\ 1 \end{pmatrix} \\ \mathbf{y}_k = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mathbf{x}_k + \mathbf{v}_k \end{cases} \end{aligned}$$

Il Filtro di Kalman è dato dalle seguenti equazioni:

- 1.  $\hat{\mathbf{x}}_k^- = A\hat{\mathbf{x}}_{k-1}^- + B\mathbf{u}_k =$   
 $= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \hat{\mathbf{x}}_{k-1}^- - \begin{pmatrix} \frac{1}{2} \\ 1 \end{pmatrix}$
- 2.  $P_k^- = AP_{k-1}^-A^T + Q =$ <sup>2</sup>  
 $= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} P_{k-1}^- \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^T + 0$

<sup>2</sup> Non essendoci rumore di processo, la matrice Q di covarianza di tale quantità è la matrice nulla.

- 3.  $L_k = P_k^- C^T (C P_k^- C^T + R)^{-1} =$   

$$= P_k^- \begin{pmatrix} 1 \\ 0 \end{pmatrix}^T \left[ \begin{pmatrix} 1 \\ 0 \end{pmatrix} P_k^- \begin{pmatrix} 1 \\ 0 \end{pmatrix}^T + 1 \right]^{-1} =$$
- 4.  $\hat{\mathbf{x}}_k = \hat{\mathbf{x}}_k^- + L_k (\mathbf{y}_k - C \hat{\mathbf{x}}_k^-) =$   

$$= \hat{\mathbf{x}}_k^- + L_k \left[ \mathbf{y}_k - \begin{pmatrix} 1 \\ 0 \end{pmatrix} \hat{\mathbf{x}}_k^- \right]$$
- 5.  $P_k = (I - L_k C) P_k^- =$   

$$= \left[ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - L_k \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right] P_k^-$$

Assegnato lo stato iniziale:

$$\mathbf{x}_0 = (z_0, v_0) = (100, 0)$$

Si ha che la stima a priori dello stato del sistema all'istante 0 vale esattamente lo stato iniziale noto del sistema:

$$\hat{\mathbf{x}}_0^- = \mathbf{x}_0 = (z_0, v_0) = (100, 0)$$

Mentre la matrice di covarianza dell'errore a priori viene inizializzata come la matrice di covarianza della sorgente delle misurazioni:

$$P_0^- = R = 1$$

Supponendo di effettuare, attraverso lo strumento X, le misure riportate in tabella 2, un esempio di implementazione in linguaggio MATLAB<sup>3</sup> del KF descritto è mostrato di seguito.

$t$ (s)	1	2	3	4	5	6	7	8	9	10
$y_t$ (m)	100	97.9	94.9	92.7	87.3	81.3	75.8	67.5	59.17	51.1

Tabella 2: Misurazioni di esempio del corpo in caduta libera

<sup>3</sup> Le motivazioni della scelta di MATLAB sono da ricercarsi nella natura del linguaggio: esso è fortemente orientato al calcolo numerico e alla manipolazione efficiente di espressioni matriciali.

*Codice Soluzione*

Si riporta in questa sezione il codice risolutivo del problema individuato.

Listing 2.1: Definizione delle variabili del problema

```
A = [1, 1; 0, 1]; %dynamic of the falling body
B = [1/2; 1]; %dynamic of the falling body
I = eye(2); %identity matrix
C = [1, 0]; %measurment process is given by acquiring directly
      the position
Q = [0, 0; 0, 0]; %no process noise
R = 1; %assumed covariance of measurment source
g = 1; %assumed gravitational acceleration
```

Listing 2.2: Inizializzazione del Filtro di Kalman

```
a_priori_pred_err_cov = R; % covariance of a priori state
      prediction initialized as the covariance of measurment
      source
init_vel = 0; %initial velocity
init_height = 100; %initial height of fall
state = [init_height; init_vel]; %initial state
a_priori_pred = state; %initial a priori state prediction is
      known and given by initial state
t = 1:10; %assuming to observe process each
      second for 10 seconds
m = [100,97.9,94.9,92.7,87.3,81.3,75.8,67.5,59.17,51.1]; %
      measurment vector
predicted_values_height = zeros(1,10); %array where store
      predictions of height
predicted_values_vel = zeros(1,10); %array where store
      predictions of speed
predicted_covariances = cell(1,10); %array where store
      post prediction error covariance
```

Listing 2.3: Algoritmo individuato dalle Equazioni di KF

```

for i=1:length(t)
    %---PREDICT---
    k = t(i); %actual k is the time t(i)
    a_priori_pred = A*a_priori_pred + B*(-g); %predict state
        using the only process input, which is always the
        gravitational acceleration g
    a_priori_pred_err_cov = A*a_priori_pred_err_cov*A' + Q;
        %compute a priori prediction error covariance
    %---PREDICT---

    %---UPDATE---
    update_with = m(i);
    kalman_gain = (a_priori_pred_err_cov * C') * inv(C*
        a_priori_pred_err_cov*C' + R); %compute kalman gain
        matrix
    post_prediction = a_priori_pred + kalman_gain * (
        update_with - C * a_priori_pred); %update
        prediction with actual measurment
    post_pred_err_cov = (I - kalman_gain * C) *
        a_priori_pred_err_cov; %compute post prediction
        error covariance
    predicted_values_height(i) = post_prediction(1); %
        store post_prediction height in array
    predicted_values_vel(i) = post_prediction(2); %
        store post_prediction speed in array
    predicted_covariances{i} = post_pred_err_cov; %
        store post_pred_err_cov in array
    %---UPDATE---
endfor

```

### Risultati

Nelle figure 12, 13 viene mostrato il grafico che compara i valori stimati di velocità e posizione con i veri valori delle medesime grandezze; infatti tali valori sono determinabili analiticamente come soluzioni esplicite della (3).

Tali grafici danno un'idea immediata della capacità che ha l'algoritmo di stimare la posizione e la velocità in maniera affidabile anche in presenza di un processo di misura affetto da rumore.

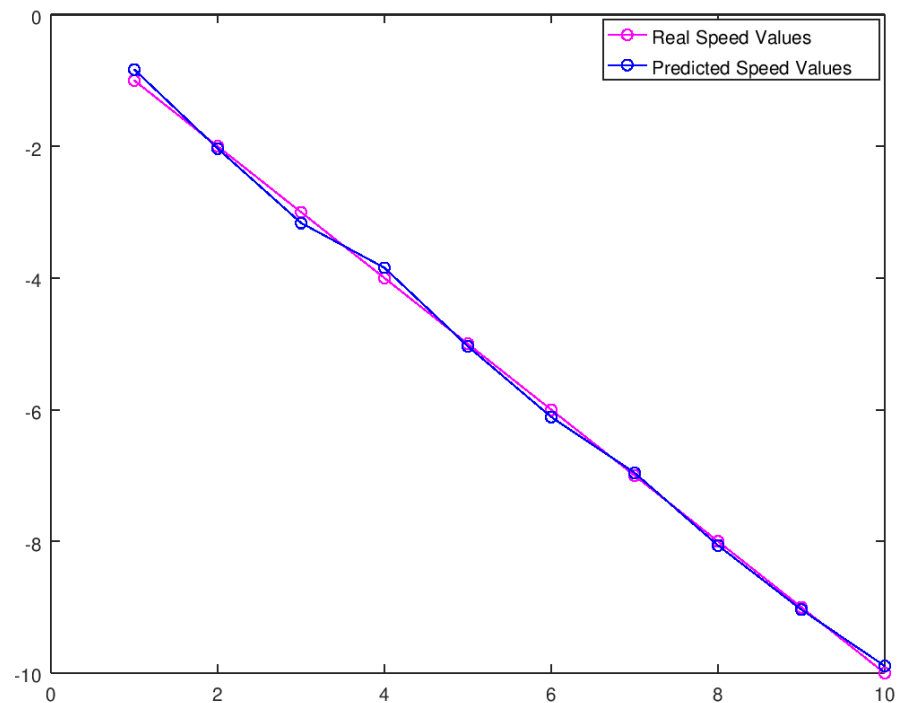


Figura 12: Stima della velocità del corpo in caduta

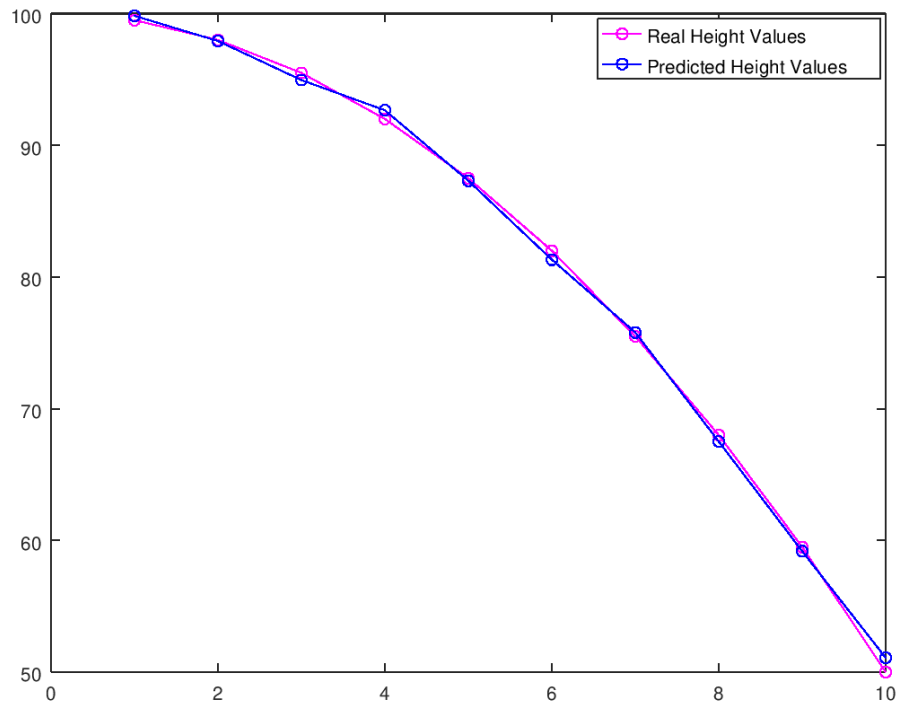


Figura 13: Stima della posizione del corpo in caduta

In tabella 3 viene riportata una sintesi dei dati prodotti dall'esecuzione dell'algoritmo.

Nelle tabelle 4 e 5 è mostrato un paragone fra l'errore a posteriori ( $x_k - \tilde{x}_k$ ) e l'errore della misura rispetto alla posizione reale.

Si noti che per ciascun istante  $t$ , l'errore a posteriori sul valore di posizione è minore, in valore assoluto, della distanza fra la misura osservata e la posizione reale del corpo.

Questo porta alla conclusione che l'utilizzo di KF ha permesso di ottenere misure sempre più affidabili rispetto a quelle ottenute dalla sorgente.

$t$ (s)	Misura (m)	Pos.(m)	Stima Pos. (m)	Vel. ( $\frac{m}{s}$ )	Stima Vel. ( $\frac{m}{s}$ )
1	100	99.5	99.833	-1	-0.83333
2	97.9	98	97.9167	-2	-2.0333
3	94.9	95.5	94.9545	-3	-3.1636
4	92.7	92	92.6611	-4	-3.8444
5	83.7	87.5	87.3074	-5	-5.037
6	81.3	82	81.3184	-6	-6.1105
7	75.8	75.5	75.7941	-7	-6.9588
8	67.5	68	67.5076	-8	-8.0606
9	59.17	59.5	59.174	-9	-9.0358
10	51.1	50	51.0892	-10	-9.8922

Tabella 3: Risultati generali dell'algoritmo

$t$ (s)	$\hat{x}_k$	$x_k$	$x_k - \hat{x}_k$
1	(99.833, -0.83333)	(99.5, -1)	(-0.333333, -0.166667)
2	(97.9167, -2.0333)	(98, -2)	(0.083333, 0.033333)
3	(94.9545, -3.1636)	(95.5, -3)	(0.545455, 0.163636)
4	(92.6611, -3.8444)	(92, -4)	(-0.661111, -0.155556)
5	(87.3074, -5.037)	(87.5, -5)	(0.192593, 0.037037)
6	(81.3184, -6.1105)	(82, -6)	(0.681579, 0.110526)
7	(75.7941, -6.9588)	(75.5, -7)	(-0.294118, -0.041176)
8	(67.5076, -8.0606)	(68, -8)	(0.492424, 0.060606)
9	(59.174, -9.0358)	(59.5, -9)	(0.326024, 0.035783)
10	(51.0892, -9.8922)	(50, -10)	(-1.089216, -0.107843)

Tabella 4: Errori a posteriori

<b>t (s)</b>	<b>Errore a posteriori (pos.) (m)</b>	<b><math>\Delta(\text{pos, misura})</math> (m)</b>
1	-0.333333	$(99.500 - 100) = -0.5$
2	0.083333	$(98 - 97.9) = 0.1$
3	0.545455	$(95.5 - 94.9) = 0.6$
4	-0.661111	$(92 - 92.7) = -0.7$
5	0.192593	$(87.5 - 87.3) = 0.2$
6	0.681579	$(82 - 81.3) = 0.7$
7	-0.294118	$(75.5 - 75.8) = -0.3$
8	0.492424	$(68 - 67.5) = 0.5$
9	0.326024	$(59.5 - 59.17) = 0.33$
10	-1.089216	$(50 - 51.1) = -1.1$

Tabella 5: Confronto tra errore a posteriori sulla posizione, e distanza fra valori reali di posizione e misure di posizione



---

## APPLICAZIONE DI SFA: LA TRAMVIA DI FIRENZE

---

In questo capitolo verrà analizzata una particolare applicazione di SFA al problema del posizionamento ferrotramviario.

Nell'ambito di un progetto di ricerca finanziato dall'Unione Europea, si è voluto studiare l'usabilità di SFA come sistema di posizionamento ferrotramviario alternativo a quello descritto nel Capitolo 1, il quale fa un largo uso di apparati installati a terra, fatto che si vorrebbe minimizzare. La linea ferrotramviaria scelta come ambiente di prova è la linea T1 della Tramvia di Firenze, che collega la stazione di *Villa Costanza*, sita nel comune di Scandicci, all'ospedale di *Careggi*, sito quest'ultimo nel comune di Firenze. La linea è mostrata in figura 14.

L'idea di base è quella di utilizzare un *accelerometro* per misurare i

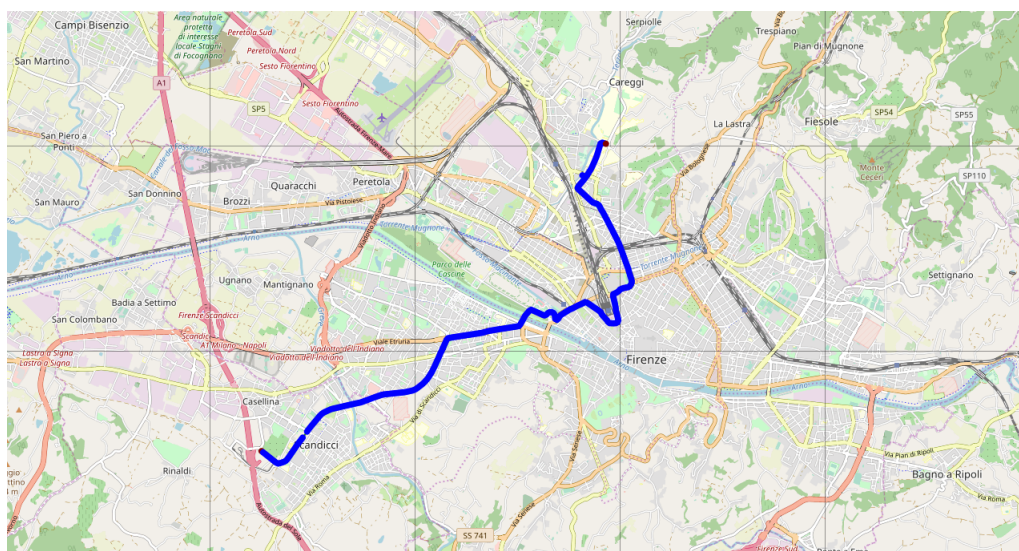


Figura 14: Tramvia di Firenze - Linea T1

valori di accelerazione a istanti di tempo sufficientemente ravvicinati e determinare, tramite essi, la posizione del treno lungo la traccia. Per

quanto esposto nel Capitolo 2, non è accettabile, in un contesto *safety-critical*, l'utilizzo esclusivo dell'accelerometro con doppia integrazione rispetto al tempo; in quanto il rumore nel processo di misura rende sempre meno affidabili le misurazioni con il passare del tempo.

### 3.1 ARCHITETTURA DI SISTEMA

Il sistema progettato ha lo scopo di eseguire SFA su una piattaforma hardware installata bordo treno, la quale riceve i dati *raw* dai sensori e li elabora al fine di stimare la progressiva chilometrica del treno in ciascun istante di tempo.

Tale posizione sarà inviata, attraverso un modem LTE:

- All'OBCU, per essere utilizzata attivamente all'interno del sistema di *interlocking*
- Ad un arbitrario host che esegue un software grafico di tracciamento del treno: il RailTrackTool (RTT)

È possibile descrivere l'architettura di sistema a due differenti livelli: architettura a livello *hardware* e architettura a livello *software*.

#### 3.1.1 Architettura Hardware

Sul treno è stata installata una scheda Nvidia TX-Jetson quale piattaforma di elaborazione dei dati. I sensori atti a campionare le misurazioni sono stati collegati alla scheda mediante appositi bus dati.

Il *sensor set* utilizzato in quest'applicazione è composto dai seguenti sensori:

- *Inertial Measurement Unit* (IMU):  
Sensore incaricato di misurare i vettori accelerazione ( $\mathbf{a}$ ) e velocità angolare ( $\mathbf{v}_{\text{ang}}$ ) attraverso l'uso combinato di un accelerometro e un giroscopio. Le misure di IMU sono prese rispetto alla Terra<sup>1</sup> e sono espresse in unità stabilite dallo standard internazionale (SI):

$$\mathbf{a} \left[ \frac{\text{m}}{\text{s}^2} \right] \quad \mathbf{v}_{\text{ang}} \left[ \frac{\text{rad}}{\text{s}} \right]$$

Si tratta del sensore principale su cui si basa l'esecuzione di SFA, ed è caratterizzato da un *drift*, il quale fa discostare il valore di acce-

<sup>1</sup> Approssimata come un *sistema inerziale*.

lerazione misurato da quello reale, in una quantità che è funzione del tempo.

- Odometro:

Per realizzare l'odometro è stato installato un rilevatore radar su una ruota del treno. Il radar misura il tempo impiegato dalla ruota a compiere un giro completo, e determina la velocità angolare della ruota  $\varphi'(t) = \frac{2\pi}{\text{tempo}} \left[ \frac{\text{rad}}{\text{s}} \right]$ .

Noto il raggio  $r$  [m] della ruota, è possibile determinare la velocità lineare alla circonferenza della ruota  $x'(t)$  attraverso la relazione cinematica  $x'(t) = r\varphi'(t) \left[ \frac{\text{m rad}}{\text{s}} \right] = r\varphi'(t) \left[ \frac{\text{m}}{\text{s}} \right]$ .

Approssimando il treno come un *corpo rigido*, questa sarà la velocità lineare con cui il treno si sta muovendo.

- Global Positioning System (GPS):

Sensore che riceve i dati di posizione attraverso il sistema satellitare GPS.

Le misure di GPS sono riportate in formato standard come tripla di coordinate (latitudine, longitudine, altitudine), rispettivamente espresse in gradi N-S, in gradi E-O e in metri.

In generale queste misure sono le meno affidabili in quanto la *varianza* della variabile aleatoria che modella tale sorgente è la più significativa.

Ad una data frequenza, i sensori inviano dati verso la scheda; quest'ultima, dopo aver eseguito un'iterazione di SFA, invia a OBCU (e/o a RTT) la stima della posizione del treno attraverso apposita modulazione di segnale elettromagnetico, in accordo con il protocollo LTE. Lo schema riportato in figura 15 mostra un diagramma dell'architettura hardware appena descritta.

### 3.1.2 Architettura Software

Sulla scheda è installato il sistema operativo Ubuntu 16.04 LTS, basato su kernel Linux.

Qualunque software menzionato in questa Tesi è stato sviluppato in linguaggio C++.

Un set di tre moduli software, denominati *interface-modules*, sono in esecuzione sulla scheda.

Sia  $MOD_i$  l' $i$ -esimo modulo software del set e  $SERIAL_i$  l' $i$ -esima

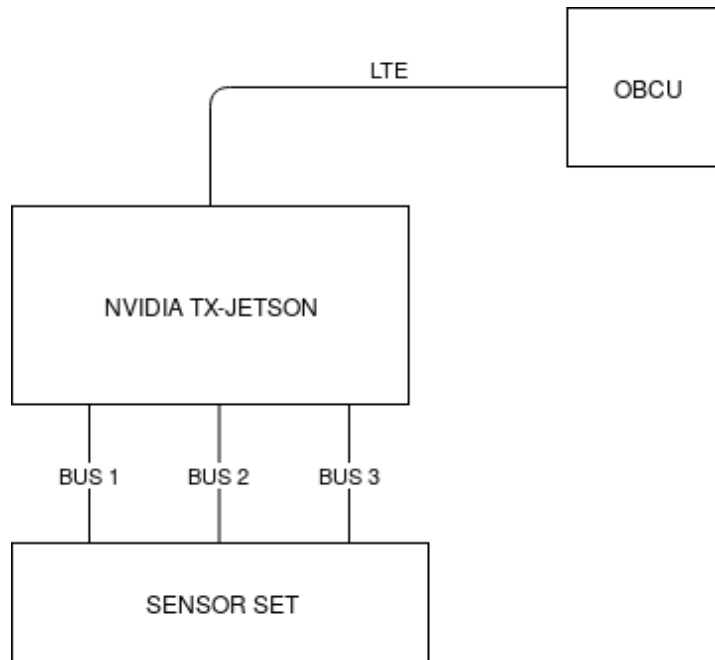


Figura 15: Architettura hardware bordo treno

interfaccia seriale della scheda, per  $i = 1, 2, 3$ .

Il funzionamento di interface-modules è il seguente:

- IMU invia la coppia (accelerazione, velocità angolare) a SERIAL\_1, MOD\_1 legge i valori da SERIAL\_1 e li invia a un secondo modulo software, denominato listener, attraverso l'interfaccia di rete loopback, in quanto listener esegue anch'esso sulla scheda;
- Odometro invia il valore di velocità lineare a SERIAL\_2, MOD\_2 legge i valori da SERIAL\_2 e li invia a listener;
- GPS invia i valori di (latitudine, longitudine, altitudine) a SERIAL\_3, MOD\_3 legge i valori da SERIAL\_3 e li invia a listener.

La comunicazione fra interface-modules e listener avviene attraverso un protocollo applicazione stabilito arbitrariamente, sia esso INPUT\_PROTOCOL, mentre a livello di trasporto si utilizza UDP.

I valori ricevuti da listener vengono salvati in apposite *strutture dati* rappresentanti misure della stessa sorgente:

- I vettori accelerazione e velocità angolare rilevati da IMU vengono convertiti nella struttura dati IMU\_POD;

- La velocità rilevata dal Radar/Odometro viene convertita nella struttura dati ODO\_POD;
- La posizione rilevata dal GPS viene infine convertita nella struttura dati GPS\_POD.

Il software che esegue effettivamente SFA è compilato come una libreria, *FusionLib*, utilizzata da *listener*. *FusionLib* dispone di interfacce software in entrata e in uscita, ossia *listener* è in grado di inviare le misurazioni a SFA, quali variabili di tipo IMU\_POD, ODO\_POD, GPS\_POD ed altresì di ricevere la stima della posizione del treno, essendo questo l'output dell'algoritmo, quale variabile di tipo SFA\_OUTPUT\_POD.

Ogniqualevolta *listener* riceva un'uscita da SFA, si fa carico della comunicazione tra scheda e OBCU/RTT. Questa comunicazione, fisicamente possibile attraverso l'utilizzo del modem LTE, avviene utilizzando un protocollo di rete arbitrario a livello applicazione, sia esso OUTPUT\_PROTOCOL, mentre al livello di trasporto la scelta è nuovamente ricaduta su UDP per ragioni di efficienza.

Uno schema dell'architettura software è quello mostrato in figura 16.

### 3.2 GESTIONE DELLA TRASMISSIONE DEI DATI

Nella precedente sezione sono stati brevemente introdotti i protocolli di comunicazione implementati per gestire la comunicazione UDP:

- In entrata, tra interface-modules e *listener* (INPUT\_PROTOCOL);
- In uscita, tra *listener* e OBCU/RTT (OUTPUT\_PROTOCOL).

#### 3.2.1 *Trasmissione in entrata*

Per trasmettere i dati da interface-modules a *listener*, e dunque dai sensori al modulo software che implementa SFA, è stato realizzato un protocollo di comunicazione denominato INPUT\_PROTOCOL.

Tale protocollo fa affidamento a livello trasporto su UDP per massimizzare la velocità di trasmissione senza dover necessariamente rinunciare all'integrità dei messaggi trasmessi, in quanto la comunicazione avviene tra processi in esecuzione sulla stessa macchina, e la probabilità che un messaggio venga perso o che questo venga ricevuto con errori, è assolutamente trascurabile.

Il protocollo definisce il formato del *payload* del pacchetto UDP che con-

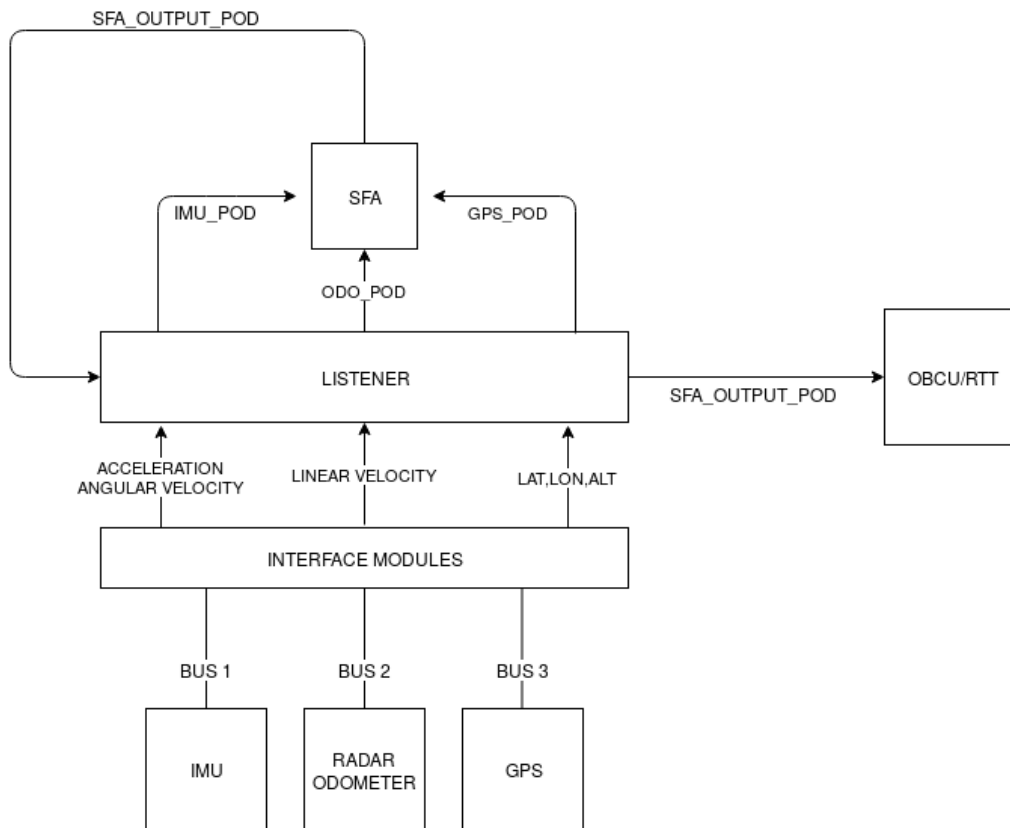


Figura 16: Architettura software bordo treno

tiene le informazioni di IMU, Radar/Odometro, o GPS, ed è descritto in tabella 6.

A discrezione del valore del campo `SENSOR_TYPE` si distingue il tipo di

Campo	Descrizione	Indici di bit	Tipo
<code>SENSOR_TYPE</code>	ID Sensore Sorgente	0-7	<code>uint8_t</code>
<code>Seq.NO</code>	Numero di sequenza	8-23	<code>uint16_t</code>
<code>N_INT</code>	Numero di interi trasmessi	24-31	<code>uint8_t</code>
<code>N_DOUBLE</code>	Numero di double trasmessi	31-38	<code>uint8_t</code>

Tabella 6: Protocollo di comunicazione in entrata

informazione trasportata dal pacchetto, come descritto in tabella 7.

I pacchetti `GROUND TRUTH` sono pacchetti di inizializzazione dell'algoritmo: alla ricezione del pacchetto `GROUND TRUTH` l'algoritmo si avvia leggendo i valori trasmessi in coda al pacchetto, in accordo al valore dei campi `N_INT` e `N_DOUBLE`. Tali valori forniscono informazioni come

Valore di SENSOR_TYPE	Sorgente del pacchetto
1	IMU
2	ODOMETRO
3	GPS
8	GROUND TRUTH
9	STROBE
10	STOP

Tabella 7: Significato del campo SENSOR\_TYPE

progressiva chilometrica e velocità iniziali del treno.

I pacchetti STROBE sono inviati ogni secondo e forniscono un solo valore double, ossia un timestamp che l'algoritmo utilizza per sincronizzarsi.

Il pacchetto STOP non contiene alcuna informazione utile: indica soltanto all'algoritmo di terminare l'esecuzione.

Alla ricezione di un pacchetto, listener legge il valore del campo SENSOR\_TYPE, e costruisce, in accordo alla relazione sorgente-struttura dati, la variabile da inviare a SFA.

Il corretto ordinamento dei pacchetti trasmessi a SFA è garantito attraverso l'esplicito utilizzo di un buffer, codificato all'interno di listener, in cui i pacchetti vengono temporaneamente salvati prima di essere inviati a SFA, ed eventualmente ordinati sulla base del valore del campo Seq.N0. Si osservi che se l'integrità non è minacciata dall'utilizzo di UDP quale protocollo di trasporto fra processi all'interno della stessa macchina fisica, altrettanto non si può dire dell'ordinamento dei messaggi. Questi potrebbero subire dei ritardi casuali in base allo stato del sistema operativo, in particolare lo *scheduling* dei processi può avere influenze determinanti sullo scorretto ordinamento dei messaggi trasmessi. Utilizzando TCP si ovvierebbe a questa problematica, ma l'overhead insito nel protocollo stesso causerebbe un notevole degrado delle performance di SFA.

### 3.2.2 Trasmissione in uscita

La trasmissione dei dati in uscita da SFA avviene, in accordo al protocollo OUTPUT\_PROTOCOL tra listener e OBCU, o comunque, tra listener e qualunque host arbitrario che intenda ricevere le informazioni in uscita, come ad esempio un PC sul quale viene eseguito RTT.

Come specificato, la comunicazione è posta in essere, a livello fisico, at-

traverso il protocollo LTE, ossia un un protocollo *wireless*; mentre a livello trasporto si è scelto di continuare a usare UDP in luogo di TCP, col fine di massimizzare le *performance* del sistema.

Il rischio di ricevere alcune informazioni in maniera errata, o non riceverle del tutto, è nettamente più elevato rispetto allo scenario precedente, nel caso in cui lo spazio fisico attraverso cui si propaga il segnale LTE è tale per cui quest'ultimo venga disturbato da sorgenti esterne.

Gli effetti deleteri di questa condizione sono particolarmente osservabili in alcuni tratti della linea feretrotramviaria, dove possono essere presenti numerose abitazioni e mezzi di trasporto in strada che si interpongono fisicamente tra la scheda NVidia TX-Jetson su cui esegue SFA e l'arbitrario host su cui viene eseguito RTT.

Occorre tuttavia osservare che il tracciamento del treno tramite RTT non è in alcun modo legato alla *safety* del sistema, in quanto le funzionalità *safety-critical* riguardano la comunicazione tra la scheda e OBCU, ossia tra la scheda e il sistema di *interlocking*.

Questa problematica è risolta attraverso l'esplicito utilizzo di un meccanismo di acknowledgment simile a quello utilizzato da TCP: ciascun pacchetto in uscita da SFA viene indicizzato con un *sequence number* e, in ricezione, viene inviato ogni secondo un *ack* replicante l'ultimo numero di sequenza correttamente ricevuto. Solo quando il mittente riceve l'*ack* i dal destinatario invierà il messaggio contenente l'uscita indicizzata con *sequence number*  $i + 1$ .

Anche in questo caso, il protocollo definisce il formato del *payload* del pacchetto UDP inviato da listener, ed è riportato in tabella 8.

In ricezione dovrà essere inviato il pacchetto *ack* al mittente, ed il suo

Campo	Descrizione	Indici di bit	Tipo
Seq.NO	Numero di sequenza	0-15	uint16_t
ECEF_X	Coordinata X del treno	16-79	double
ECEF_Y	Coordinata Y del treno	80-143	double
ECEF_Z	Coordinata Z del treno	144-207	double
FU_ARC_LEN	Progressiva chilometrica	208-271	double

Tabella 8: Protocollo di comunicazione in uscita

formato è descritto in tabella 9. Si osserva che SFA produce la stima della posizione del treno sia in termini di progressiva chilometrica che di coordinate ECEF.

ECEF è acronimo di *Earth Centered Earth Fixed* ed è uno standard che



Campo	Descrizione	Indici di bit	Tipo
ACK	Ultimo Seq.NO	0-15	uint16_t

Tabella 9: Formato del pacchetto di *ack*

misura le coordinate geografiche di un oggetto come la terna  $P = (x, y, z)$ . Ciascuna coordinata viene espressa considerando la *proiezione su piano* della Terra, e prendendo come origine O l'intersezione fra l'equatore e il meridiano di *Greenwich*.

Le coordinate ECEF misurano tre lunghezze, pertanto in accordo a SI, esse sono espresse in metri.

Nella prossima sezione, viene descritto uno scenario di esempio del comportamento del sistema a *runtime*.

### 3.3 SCENARIO DI ESEMPIO

Si suppongano le condizioni iniziali riportate in tabella 10.

Velocità	ECEF	Progressiva	IMU Sample Rate	ODO Sample Rate
$0\text{ms}^{-1}$	(0, 0, 0) m	0 km	100 Hz	20 Hz

Tabella 10: Condizioni iniziali

1.  $t = 0$ :

- interface-modules invia a listener il seguente pacchetto GROUND TRUTH:

SENSOR_TYPE	Seq. NO	N_INT	N_DOUBLE
0x08	0x00	0	5

E vi accoda i seguenti tre valori double: 0.0, 0.0, 0.0 ossia le coordinate ECEF iniziali, il seguente valore double: 0.0, ossia la velocità lineare iniziale, e infine il valore double: 0.0 che rappresenta la progressiva chilometrica iniziale.

- listener riceve il pacchetto e inizializza SFA con:
  - ECEF iniziali: (0, 0, 0)

- Velocità lineare iniziale: 0.0
- Progressiva chilometrica iniziale: 0.0

2.  $t = t_0$ :

- IMU campiona il seguente vettore accelerazione:

$$\mathbf{a} = (0.0001, -0.0001, -9.8100)$$

Assieme al seguente vettore velocità angolare:

$$\mathbf{v}_{\text{ang}} = (0.0003, -0.0001, 0.0002)$$

E lo invia, tramite SERIAL\_1, a MOD\_1 di interface-modules.

- MOD\_1 invia a listener il seguente pacchetto IMU:

SENSOR_TYPE	Seq. NO	N_INT	N_DOUBLE
0x01	0x01	0	6

Accodandovi nell'ordine il vettore accelerazione, e il vettore velocità angolare.

- listener riceve il pacchetto, crea e invia a SFA la seguente variabile IMU\_POD:
  - Seq.NO = 1
  - Epoch =  $t_0$
  - ACC\_X = 0.0001
  - ACC\_Y = -0.0001
  - ACC\_Z = -9.8100
  - GYRO\_X = 0.0003
  - GYRO\_Y = -0.0001
  - GYRO\_Z = 0.0002
- SFA elabora il pacchetto e inizia una computazione parallela per fornire a listener una variabile SFA\_OUTPUT\_POD della forma:
  - Seq.NO = 0
  - ECEF\_X =  $\bar{E}_X$
  - ECEF\_Y =  $\bar{E}_Y$

- ECEF\_Z =  $E_Z$
- FU\_ARC\_LEN =  $P_{KM}$

3.  $t_0 < t < t_0 + \frac{1}{\text{ODO\_SAMPLE\_RATE}} = t_0 + \frac{1}{20}$   
 Fintantoché l'odometro non campiona il suo primo valore di velocità, si ripetono le operazioni viste al passo precedente per ogni campionamento di IMU.

4.  $t = t_0 + \frac{1}{20}$

- Odometro campiona il seguente valore di velocità:

$$\mathbf{a} = (1.0010)$$

E lo invia, tramite SERIAL\_2, a MOD\_2 di interface-modules.

- MOD\_2 invia a listener il seguente pacchetto ODOMETRO:

SENSOR_TYPE	Seq. NO	N_INT	N_DOUBLE
0x02	Seq_NO	0	2

Accodandovi nell'ordine il valore di velocità rilevato, e il valore dello scarto quadratico medio della sorgente, noto a priori, in quanto caratteristica tecnica intrinseca dello strumento di misura, il radar; sia esso SIGMA\_RADAR.

- listener riceve il pacchetto, crea e invia a SFA la seguente variabile ODO\_POD:
  - Seq.NO = Seq\_NO
  - Epoch =  $t_0 + \frac{1}{20}$
  - vel = 1.0010
  - sigma = SIGMA\_RADAR
- SFA elabora il pacchetto e utilizza la rilevazione di velocità in maniera utile a correggere il *drift* di IMU, al fine di produrre una stima della posizione più accurata.

5.  $t = n t_0 \quad n \in \mathbb{N}^+$

Ogni secondo, il modulo STROBE di interface-modules, invia a

listener un pacchetto della forma:

SENSOR_TYPE	Seq. NO	N_INT	N_DOUBLE
0x09	Seq_NO	0	1

Accondandovi un *timestamp* che listener inoltra a SFA per scopi di sincronizzazione.

Quanto elencato viene ripetuto per ciascun campionamento successivo di IMU e odometro.

Non appena un' uscita di SFA si rende disponibile a listener questo si comporta come segue:

- listener riceve la variabile SFA\_OUTPUT\_POD, da SFA;
- listener costruisce il seguente pacchetto da inviare a OBCU, o a RTT:
  - Seq.NO = 0x00
  - ECEF\_X = SFA\_OUTPUT\_POD.E<sub>X</sub>
  - ECEF\_Y = SFA\_OUTPUT\_POD.E<sub>Y</sub>
  - ECEF\_Z = SFA\_OUTPUT\_POD.E<sub>Z</sub>
  - FU\_ARC\_LEN = SFA\_OUTPUT\_POD.P<sub>KM</sub>
- OBCU, o RTT, riceve il pacchetto e invia a listener l'*ack* 0x00.

### 3.4 POSSIBILI SVILUPPI

Il sistema, così come è stato descritto, rappresenta essenzialmente un *core* minimale di un sistema di posizionamento basato su SFA, limitato rispetto alle potenzialità dell'algoritmo e comunque non esente da vulnerabilità legate alla *security*. In questa sezione verranno discusse le principali problematiche della soluzione descritta, in che modo queste possono essere risolte, e quali tecniche possono essere usate per migliorare l'usabilità del sistema.

#### 3.4.1 Problematiche legate alla security

Per *security* si intende un insieme di tecniche che hanno come scopo la protezione dei dati, siano essi stoccati in un sistema informatico, oppure

transitanti attraverso un sistema di telecomunicazione.

Tale protezione viene assicurata contro specifiche *minacce*, le quali sfruttano opportune *vulnerabilità*.

La *security* viene garantita attraverso l'uso di appropriate *tecniche preventive*, oppure *contromisure* applicabili in caso di violazioni alle principali *misure della security*:

- Integrità
- Confidenzialità
- Autenticazione

In un sistema *safety-critical* come quello descritto, una violazione di *security* potrebbe portare a una violazione di *safety*, pertanto è fondamentale ridurre al minimo le vulnerabilità del sistema. Nella fattispecie descritta in questa Tesi, tuttavia, la confidenzialità non è una misura fondamentale, mentre lo sono l'integrità e l'autenticazione.

#### *Minacce all'integrità*

È stato già discusso che l'utilizzo del protocollo UDP a livello di trasporto, non garantisce affatto che i messaggi ricevuti da OBCU siano corretti e ordinati.

Per ovviare al problema dell'ordinamento è stato implementato il già descritto meccanismo di acknowledgment, tuttavia esso fa l'implicita assunzione che se si è in grado di leggere correttamente il numero di sequenza del pacchetto ricevuto, questo non sia stato alterato.

Si consideri il seguente scenario:

- listener invia a OBCU il seguente pacchetto:
  - Seq.NO = 0x17
  - ECEF\_X = SFA\_OUTPUT\_POD.E<sub>X</sub>
  - ECEF\_Y = SFA\_OUTPUT\_POD.E<sub>Y</sub>
  - ECEF\_Z = SFA\_OUTPUT\_POD.E<sub>Z</sub>
  - FU\_ARC\_LEN = SFA\_OUTPUT\_POD.P<sub>KM</sub>
- OBCU riceve il seguente pacchetto:
  - Seq.NO = 0x25
  - ECEF\_X = SFA\_OUTPUT\_POD.E<sub>X</sub>

- $E_{CEF\_Y} = SFA\_OUTPUT\_POD.E_Y$
- $E_{CEF\_Z} = SFA\_OUTPUT\_POD.E_Z$
- $FU\_ARC\_LEN = SFA\_OUTPUT\_POD.P_{KM}$

Per come è stato descritto il protocollo, OBCU accetta passivamente che il numero di sequenza ricevuto sia 0x25, anche se prima di questo era stato letto il valore 0x16, ed invierà a listener l'*ack* 0x25.

In questo caso, OBCU dovrebbe essere progettato in maniera tale da controllare sempre di ricevere un numero di sequenza pari all'ultimo ricevuto +1. Dal momento che, viste le caratteristiche intrinseche del protocollo, è impossibile che listener abbia inviato il pacchetto con numero di sequenza 0x25 se l'ultimo *ack* ricevuto non era 0x24, è probabile che, attraversando il canale, il pacchetto abbia subito alterazioni casuali in tutti i suoi bit, e quindi anche l'informazione di posizione potrebbe essere alterata.

Per ovviare definitivamente alla problematica dell'integrità, è opportuno integrare nel protocollo l'uso di una *funzione hash*. Il protocollo verrebbe modificato come segue:

- listener prepara il pacchetto contenente le informazioni di SFA\_OUTPUT\_POD;
- listener calcola  $H(SFA\_OUTPUT\_POD) = y$ ;
- listener invia la coppia  $(SFA\_OUTPUT\_POD, y)$

In ricezione, OBCU ricalcola  $H(SFA\_OUTPUT\_POD) = y'$ , e accetta il messaggio solo se  $y' = y$ . Infatti, grazie alla proprietà delle funzioni *hash*, una minima variazione del messaggio  $m$  causa una grande variazione del *digest*  $H(m)$ , quindi è altamente improbabile che un'alterazione casuale dei bit trasmessi, sia essa  $(SFA\_OUTPUT\_POD\_WRONG, Y\_WRONG)$ , mantenga la proprietà  $H(SFA\_OUTPUT\_POD\_WRONG) = Y\_WRONG$ .

#### *Minacce all'autenticazione*

Si consideri il caso in cui un malintenzionato sia in grado di inviare messaggi a OBCU e abbia interesse nel non segnalare al sistema di *interlocking* l'avvicinamento del treno alla JA.

L'attaccante si comporta come segue:

- Intercetta il messaggio  $(SFA\_OUTPUT\_POD, H(SFA\_OUTPUT\_POD))$

- Modifica la posizione del treno ponendola lontano da una JA, forgiando un nuovo messaggio, sia esso SFA\_OUTPUT\_POD\_DANGEROUS
- Calcola  $H(\text{SFA\_OUTPUT\_POD\_DANGEROUS}) = Y\_DANGEROUS$
- Invia a OBCU la coppia (SFA\_OUTPUT\_POD\_DANGEROUS, Y\_DANGEROUS)

Per ovviare a questa problematica si potrebbero usare le seguenti tecniche:

1. Cifratura del *digest* della funzione *hash* con una chiave simmetrica condivisa tra listener e OBCU;
2. Cifratura del *digest* della funzione *hash* con la chiave privata di listener (Firma Digitale DSA);
3. Uso di una funzione *hash* che prende in ingresso sia il messaggio che una chiave simmetrica condivisa tra listener e OBCU (HMAC);
4. Accodare un segreto condiviso tra listener e OBCU al messaggio prima di calcolarne il *digest*.

In ciascuno di questi scenari, fatta assunzione di proprietà di *strong collision resistance* della funzione *hash* utilizzata, si garantisce che il messaggio può essere stato inviato solo da listener, in quanto un attaccante non avrebbe modo di modificare il messaggio e calcolare un *digest* valido. La soluzione meno dispendiosa in termini di complessità computazionale e più adatta a un simile scenario è la soluzione 4, in quanto non è necessario garantire anche la *non-ripudiabilità* ma solo l'autenticazione e l'integrità.

#### 3.4.2 Miglioramenti al servizio fornito