Stratégie de détection des Falsifications de Position Contenues Dans les Messages AIS Par Application du Filtre IMM

Maelic Louart[+*], Jean-Jacques Szkolnik[*], Abdel Boudraa[*],
Frédéric Le Roy[+], Jean-Christophe Le Lann[+]

[*]IRENav, EA3634, BCRM Brest CC 600, Ecole Navale, 29240 Brest Cedex 9, France;
[+]Lab-STICC, UMR CNRS 6285, ENSTA Bretagne, 29806 Brest cedex 9, France

Introduction

Automatic Identification System (AIS) :

- L'AIS est un système de communication automatique d'information de navigation (position, identité, ...) entre bateaux pour renforcer la sécurité du trafic maritime. Son installation est obligatoire pour les navires de jauge brute supérieure à 300 effectuant des voyages internationaux.

Problématique :

- L'AIS n'est pas sûr, il peut être facilement piraté et transmettre de fausses positions pour masquer des activités illicites (piraterie, pêche illégale ...) ou justifier de fausses violations de territoires.

État de l'art :

- Méthode de collaboration entre plusieurs capteurs [1]. A partir de mesures provenant de différents capteurs la position du navire est estimée et comparée à celle transmise par l'AIS. Cependant cette méthode n'est pas précise, prend du temps et nécessite du matériel supplémentaire à l'AIS.
- Méthode suivant les trajectoires transmises par l'AIS pour détecter des sauts de position [2].

Proposition :

- Nous suivons la trajectoire en implémentant un filtre à modèles multiples interactifs (IMM) utilisant deux filtres de Kalman (KF).

Filtre de Kalman

Hypothèses :

- la vitesse du navire est supposée constante (**H1**);
- le bruit d'accélération (σ_w) est supposé constant sur chaque période d'échantillonnage et indépendant entre ces périodes (**H2**);
- les bruit de mesures (σ_v) et de modèle (σ_w) sont supposés blancs gaussiens et de moyenne nulle (**H3**).

Modèle d'évolution :

$$X_{n+1} = A_{n+1}X_n + \Gamma_{n+1}w_n \tag{1}$$

avec :

- $X_n = \begin{pmatrix} x_n \\ \dot{x}_n \end{pmatrix}$, $A_{n+1} = \begin{pmatrix} 1 & \Delta T_{n+1} \\ 0 & 1 \end{pmatrix}$, $\Gamma_{n+1} = \begin{pmatrix} \frac{\Delta T_{n+1}^2}{2} \\ \Delta T_{n+1} \end{pmatrix}$
- $n \in \mathbb{N}$ est l'indice de temps discret;
- X_n est le vecteur d'état contenant la position x_n (latitude/longitude) et la dérivée première de x_n par rapport au temps;
- A_{n+1} est la matrice de transition à l'instant $n+1$;
- Γ_{n+1} est la matrice de gain du bruit à l'instant $n+1$;
- $\Delta T_{n+1} = t(n+1) - t(n)$ est l'intervalle de temps séparant la réception de deux messages consécutifs et w_n est le bruit de modèle à l'instant n.

Modèle d'observation :

$$Y_n = CX_n + v_n \tag{2}$$

Bruits de mesure et de modèle :

- $\sigma_v = 5.3m$;
- $\sigma_w = 0.8 \times 0.5 \times \Delta a$ with $\Delta a = 1nd.s^{-1}$

Équations prises dans [3] :

Covariance du vecteur de bruit du modèle W_n:
$Q_n = COV(W_n) = \mathbb{E}[W_n W_n^T] = \begin{pmatrix} \frac{\Delta T_n^4}{4} & \frac{\Delta T_n^3}{2} \\ \frac{\Delta T_n^3}{2} & \Delta T_n^2 \end{pmatrix} \sigma_w^2$;

Covariance du vecteur de mesure Y_n:
$R_n = COV(Y_n) = COV(V_n) = \mathbb{E}[V_n V_n^T] = \sigma_v^2$

Équation de prédiction du vecteur d'état:
$\widehat{X}_{n|n-1} = A_n \widehat{X}_{n-1|n-1}$

Équation de la matrice de covariance de $\widehat{X}_{n|n-1}$:
$\widehat{P}_{n|n-1} = COV(\widehat{X}_{n|n-1}) = A_n \widehat{P}_{n-1|n-1} A_n^T + Q_n$

Équation du gain du filtre :
$K_n = \widehat{P}_{n|n-1} C^T [R_n + C\widehat{P}_{n|n-1}C^T]^{-1}$

Équation d'estimation du vecteur d'état:
$\widehat{X}_{n|n} = \widehat{X}_{n|n-1} + K_n \tilde{Y}_n$ avec : $\tilde{Y}_n = Y_n - C\widehat{X}_{n|n-1}$

Équation de la matrice de covariance de $\widehat{X}_{n|n}$:
$\widehat{P}_{n|n} = COV(\widehat{X}_{n|n}) = (I - K_n C)\widehat{P}_{n|n-1}$

Initialisation :

$$\widehat{X}_{1|1} = \begin{pmatrix} Y_1 \\ \frac{Y_1 - Y_0}{\Delta T(1)} \end{pmatrix} ; \widehat{P}_{1|1} = \begin{pmatrix} R & \frac{R}{\Delta T_1} \\ \frac{R}{\Delta T_1} & \frac{2R}{\Delta T_1^2} \end{pmatrix} \tag{3}$$

Dynamique des navires suivis

Modes principaux de la dynamique des navires :

- mode 1 : le navire se déplace à vitesse et route constants, $\sigma_w = 0.5 \times \Delta a \propto 0.02nd.s^{-1}$;
- mode 2 : le navire accélère, décélère et change de route, $\sigma_w = 0.5 \times \Delta a \propto 0.5nd.s^{-1}$;

Prise en considération de ce changement de mode :

- σ_w est fixé à 0.8 fois sa valeur maximale (mode 2);
- utilisation d'un filtre IMM.

Filtre à modèles multiples interactifs

Principe :

- deux filtres de Kalman sont exécutés en parallèle, chacun suivant un des deux modes;
- le mélange entre les variables d'état prédites et estimées des deux filtres se fait en utilisant une matrice de transition (Π).

$$\Pi = \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix} = \begin{pmatrix} 0.90 & 0.10 \\ 0.10 & 0.90 \end{pmatrix} \tag{4}$$

Le filtre IMM applique successivement les équations suivantes. Dans ces équations, $i, j \in \{1; 2\}$ et $r = 2$.

Intéraction/mélange
Probabilités que la cible soit dans le mode j après interaction :
$C_{j,n-1} = \sum_{i=1}^{r} \Pi_{ij} \mu_{i,n-1}$

Probabilités de mélange :
$\mu_{ij,n-1} = \Pi_{ij} \mu_{i,n-1} / C_{j,n-1}$

Mélange des vecteurs d'état estimés et de leur matrice de covariance :
$\widehat{X}^0_{j,n-1|n-1} = \sum_{i=1}^{r} \mu_{ij,n-1} \widehat{X}_{i,n-1|n-1}$
$\widehat{P}^0_{j,n-1|n-1} = \sum_{i=1}^{r} \mu_{ij,n-1} (\widehat{P}_{i,n-1|n-1} + D\widehat{P}_{ij,n-1})$
où $D\widehat{P}_{ij,n-1} = D\widehat{X}_{ij,n-1|n-1} D\widehat{X}^T_{ij,n-1|n-1}$
avec $D\widehat{X}_{ij,n-1|n-1} = (\widehat{X}_{i,n-1|n-1} - \widehat{X}^0_{j,n-1|n-1})$

Application des r filtres de Kalman
(les équations du filtre de Kalman sont appliquées à :
$\widehat{X}^0_{j,n-1|n-1}$ et $\widehat{P}^0_{j,n-1|n-1}$ pour obtenir $\widehat{X}_{j,n|n-1}, \widehat{P}_{j,n|n}, S_{j,n}, \tilde{Y}_{j,n}$, $\widehat{X}_{j,n|n}$ et $\widehat{P}_{j,n|n}$)

Vraisemblance de chaque mode :
$\Lambda_{j,n} = \frac{exp(-d^2_{j,n}/2)}{\sqrt{(2\pi)S_{j,n}}}$, avec $d^2_{j,n} = \tilde{Y}^T_{j,n} S^{-1}_{j,n} \tilde{Y}_{j,n}$

Mise à jour des probabilités de chaque mode
$\mu_{j,n} = \Lambda_{j,n} C_{j,n-1} / C_{n-1}$, avec $C_{n-1} = \sum_{i=1}^{r} \Lambda_{i,n} C_{i,n-1}$

Combinaison des vecteurs d'état et matrices prédits et estimés
Prédictions globales du vecteur d'état, de sa matrice de covariance et de la matrice de covariance de l'innovation :

$\widehat{X}_{n|n-1} = \sum_{i=1}^{r} C_i \widehat{X}_{i,n|n-1}$; $\widehat{P}_{n|n-1} = \sum_{i=1}^{r} C_i \widehat{P}_{i,n|n-1}$
$S_n = C\widehat{P}_{n|n-1}C^T + R$

Estimations globales du vecteur d'état et de sa matrice de covariance :
$\widehat{X}_{n|n} = \sum_{i=1}^{r} \mu_i \widehat{X}_{i,n|n}$; $\widehat{P}_{n|n} = \sum_{i=1}^{r} \mu_i \widehat{P}_{i,n|n}$

Comparaison des performances des deux filtres

Simulation de Monte-Carlo :

- 1000 excusions d'un même scénario qui dure 341s et contient 42 mesures de position;

Scénario :

- $t = 0$, position initiale : $P_0 = (32.55051, -97.2597)$, vitesse initiale : $v_0 = 2nd$.
- $t \in [0, 200]$, trajectoire rectiligne uniforme à vitesse quasi-constante (bruit d'accélération : $\sigma =\propto 0.02nd.s^{-1}$)), $\Delta T_n = 10s \pm 20\%$;
- $t \in [200, 220]$, $\Delta a = 1nd.s^{-1}$, $\Delta T_n = 10s \pm 20\%$;
- $t \in [220, 340]$ trajectoire rectiligne uniforme à vitesse quasi-constante (bruit d'accélération : $\sigma =\propto 0.02nd.s^{-1}$)), $\Delta T_n = 6s \pm 20\%$;

Résultats :

	RMSE $(X_{r,n} - X_{n\|n})$(m)				$\mu\left(5\sqrt{S_n}\right)$ (m)			
	sans man.		acc.		sans man.		acc.	
	K.	IMM	K.	IMM	K.	IMM	K.	IMM
Lat.	4.8	4.1	6.4	6.2	80	60	82	75
Lon.	4.7	4.1	6.3	6.3	95	72	97	85

	$\mu\left(\sqrt{\widehat{P}(1,1)_{n\|n}}\right)$ (m)				$\mu\left(\sqrt{\widehat{P}(2,2)_{n\|n}}\right)$ (m.s^{-1})			
	sans man.		acc.		sans man.		acc.	
	K.	IMM	K.	IMM	K.	IMM	K.	IMM
Lat. (m)	4.9	4.4	5.1	5.1	1.2	0.78	1.3	1.3
Lon. (m)	4.9	4.5	5.1	4.9	1.2	0.79	1.3	1.2

Table 1: Comparaison de la précision d'estimation des filtres de Kalman (K.) et IMM.

- le filtre IMM s'adapte mieux que le filtre de Kalman aux changement de dynamique du navire. Lorsque le bateau ne manoeuvre pas, le RMSE, le seuil et l'écart-type de l'erreur d'estimation du vecteur d'état sont inférieurs;
- les estimations du filtre IMM sont plus précises qu'en [2] pour un coût de calcul moindre.

Expérimentation sur des données réelles :

- **Données enregistrées** : 2103 messages provenant de 18 navires;
- **Scénario de falsification :** Ajout de 500m, pendant 10 minutes à la latitude.

Résultats :

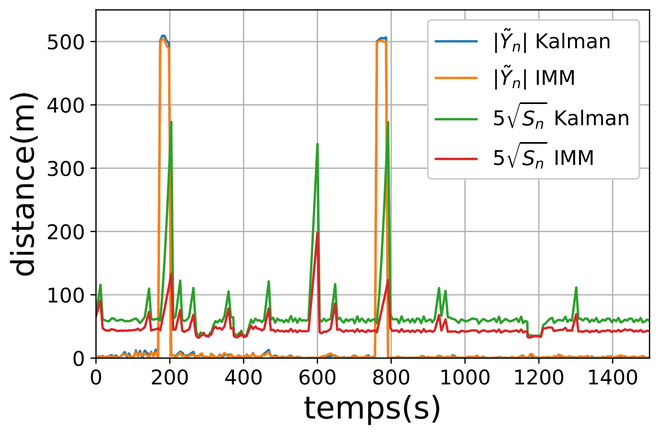

Figure 1: Evolution au cours du temps de l'innovation et du seuil sur la latitude pour le filtre IMM et le filtre de Kalman.

- Détection de la falsification de position de 500m;
- Aucune autre falsification de position n'a été détectée sur les autrse messages enregistrés;
- Le filtre IMM est plus sensible aux falsifications que le filtre de Kalman.

Conclusion

Nous avons développé une stratégie de détection des falsifications des positions transmises par les messages AIS. Cette stratégie applique un filtre de type IMM qui suit chaque trajectoire des bateaux. Les résultats obtenus sur des données simulées et réelles montrent de bonnes performances, meilleures que celle d'un filtre de Kalman : les trajectoires sont suivies précisément et la sensibilité à la détection des falsifications de position est largement satisfaisante.

References

[1] Martin Strohmeier, Matt Smith, Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. Crowdsourcing security for wireless air traffic communications. In *2017 9th International Conference on Cyber Conflict (CyCon)*, pages 1–18. IEEE, 2017.

[2] Gregor Siegert, Paweł Banyś, Cristina Sáez Martínez, and Frank Heymann. Ekf based trajectory tracking and integrity monitoring of ais data. In *2016 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, pages 887–897. IEEE, 2016.

[3] Yaakov Bar-Shalom, X Rong Li, and Thiagalingam Kirubarajan. *Estimation with applications to tracking and navigation: theory algorithms and software*. John Wiley & Sons, 2004.