Étude de faisabilité d'une identification d'émetteurs AIS en environnement contrôlé par analyse de signaux

Emma BOISRIVEAU Jean-Jacques SZKOLNIK Delphine DARÉ-EMZIVAT Steven COLLIN Tristan AVERTY
Institut de Recherche et d'Études Navales (IRENav), École Navale / Arts et Metiers ParisTech, 29240 Brest, France.

Résumé – Dans cet article, nous présentons une nouvelle approche de l'identification d'émetteurs AIS en s'appuyant sur les caractéristiques des signaux reçus en bande de base. En effet, afin de contrer les usurpations d'identité de ces émetteurs, il est impératif de les différencier de manière robuste. Dans ce travail, nous proposons d'appliquer une technique de classification en exploitant notamment des attributs extraits de la fréquence instantanée du signal reçu. Une campagne de mesures expérimentales incluant l'utilisation de radios logicielles a permis de bénéficier d'un ensemble complet de données pour mener à bien ce travail. Les premiers résultats sont prometteurs et ont confirmé la pertinence de cette approche. Une séparation efficace des différentes sources de signaux a été obtenue avec des valeurs de précision extrêmement satisfaisantes, prouvant la faisabilité d'une telle méthode. Ainsi, ces résultats, obtenus sur des signaux réels en environnement contrôlé, offrent une perspective intéressante pour l'amélioration de la sécurité maritime grâce à une identification plus fiable d'émetteurs AIS.

Abstract – In this article, we present a novel approach to the identification of AIS transmitters based on steady-state signal characterstics. Indeed, in order to avoid AIS spoofing by these transmitters, it is imperative to differentiate them in a robust way. In this work, we propose to apply a classification technique by exploiting attributes extracted from the instantaneous frequency of the received signal. A campaign of experimental measurements, including the use of software-defined radios, has provided us with a complete dataset to carry out this work. Initial results are promising and have confirmed the relevance of this strategy. Efficient separation of the different signal sources was achieved with extremely satisfactory accuracy values, proving the feasibility of such a method. These results, obtained on real signals in a controlled environment, offer an interesting prospect for improving maritime safety through more reliable identification of AIS transmitters.

1 Introduction

1.1 Contexte

Le Système d'Identification Automatique (SIA) (ou AIS pour *Automatic Identification System*) est un système d'échanges de messages automatisés par radio VHF en particulier entre navires/navires et navires/stations côtières [1]. Ce partage automatique d'information est essentiel à la sécurité et à la gestion maritime au regard de la densité du trafic actuel, en facilitant l'évitement des collisions et en améliorant la connaissance des zones de navigation intense. Au fil des ans, son champ d'application s'est étendu à la surveillance de zones maritimes spécifiques et au suivi de l'activité des navires. Ce système de nature collaborative repose entièrement sur la coopération de chacun et sur l'authenticité des informations communiquées. Des études récentes ont révélé que la falsification des messages AIS était possible d'où une réserve quant à la fiabilité de l'AIS. Des navires ont ainsi été déviés de leur trajectoire initiale à l'insu de l'équipage et des centres de surveillance. L'AIS est donc confronté à des défis importants en raison de l'émergence de ces pratiques malveillantes (usurpation d'identité, messagerie frauduleuse [2], etc.) conduisant à de nouveaux risques maritimes. Une approche possible pour reconnaître les émetteurs repose sur les techniques dites radiométriques qui exploitent les caractéristiques particulières des composants de l'émetteur, spécificités difficilement reproductibles donc difficilement falsifiables. En effet, lors de la fabrication des défauts peuvent apparaître au sein des composants d'un émetteur donné engendrant alors une particularité des signaux émis qui lui est propre bien que référencé au sein d'un ensemble de produits d'un même modèle. Deux catégories sont définies au sein de cette approche radiométrique selon la nature « transitoire » ou « bande de base » du signal reçu.

1.2 Travaux existants

Erwan Alincourt *et al.*, dans leurs travaux, proposent d'utiliser les caractéristiques des signaux transitoires du signal AIS pour distinguer les transpondeurs [3]. L'idée retenue consiste à considérer que les signaux transitoires émis par les transpondeurs AIS présentent des spécificités uniques comme les temps de montée en puissance, temps de descente en puissance, temps avant et après modulation en puissance. Ces singularités peuvent être utilisées pour identifier précisément chaque transpondeur. Cette méthode de la signature unique permet de différencier les transpondeurs entre eux, même s'ils émettent des messages AIS similaires (comme les positions des navires), en se basant uniquement sur la signature physique de leur émission radio. La reconnaissance des navires, dont les transpondeurs sont employés de manière inappropriée est facilitée. Toutefois, la notion de transitoire implique un intervalle de temps très court d'où la difficulté de calculer ces caractéristiques sur un tel laps de temps [4, 5]. Les travaux de Maélic Louart [6] introduisent une méthode dynamique pour la détection de l'usurpation d'identité (*AIS spoofing*). Cette approche consiste à s'intéresser au signal reçu en régime permanent et plus particulièrement à l'évolution temporelle du décalage présent sur la fréquence porteuse, dénommé CFO pour *Carrier Frequency Offset*. La transmission des signaux AIS est réalisée à partir d'une modulation GMSK (pour *Gaussian Minimum Shift Keying*) sur deux fréquences porteuses VHF (161,975 MHz et 162,025 MHz). Or, les imperfections des oscillateurs présents au sein même des émetteurs (et des récepteurs) se traduisent par des valeurs de fréquences porteuses légèrement différentes de celles attendues d'où l'apparition d'une fréquence parasite sur le signal en bande de base. Ce CFO est unique car les défauts matériels sont propres à chaque transpondeur. Ainsi un système AIS d'un bateau donné sera

identifiable à partir de la connaissance de son CFO. La mise en œuvre d'un filtrage de Kalman permet de suivre l'évolution de la variation du décalage de la fréquence de la porteuse dans le temps. Cette signature radiométrique des signaux reçus caractérise matériellement le transpondeur et rend possible leur identification indépendamment de l'identité que constitue le numéro MMSI (pour *Maritime Mobile Service Identity*) qu'ils transmettent dans leurs messages AIS. L'approche de Morge-Rollet [7] combine à la fois l'approche transitoire et régime permanent. Elle propose une taxonomie complète des méthodes qui assurent de la véracité des messages radio transmis en recourant à l'authentification par empreinte radio. Ce type de méthodes exploite soit les imperfections des composants de l'émetteur radio comme les distorsions de phase, les variations de fréquence et les non-linéarités causées par les imperfections du matériel, soit celles du canal de propagation utilisé. Une connaissance des imperfections spécifiques à l'appareil est également possible par le biais d'une modélisation spécifique des composants [7].

1.3 Positionnement de cet article

S'appuyant sur la taxonomie décrite par Morge-Rollet [7], notre étude se concentre exclusivement sur les signaux AIS en régime permanent avec l'hypothèse d'une stabilité des caractéristiques physiques dans le temps. Cette hypothèse permet d'extraire de multiples attributs calculés à partir de différentes représentations des signaux reçus. Ainsi, nous nous intéressons à la fréquence instantanée du signal dont des attributs statistiques et spectraux sont extraits et à la représentation $\mathbf{I}/\mathbf{Q}$ du signal dont une analyse en constellation est proposée. Les attributs extraits de ces différentes représentations sont alors mis en entrée d'un algorithme de classification permettant ainsi d'identifier les différents émetteurs. La méthode proposée fournit un nouveau cadre pour la détection des anomalies des émetteurs et l'amélioration des capacités opérationnelles en temps réel.

2 Méthodologie

2.1 Échange de messages AIS de type 1

Les messages véhiculés par l'AIS peuvent être regroupés en 27 types. Le message de type 1 est le plus fréquemment rencontré car il renseigne le numéro MMSI du bateau, sa position, son cap et sa vitesse qui sont les informations de base. Dans cette étude, nous nous intéressons donc essentiellement à ce type de message.

D'un point de vue technique, ces messages sont constitués de 256 bits répartis à l'intérieur de blocs comme illustré par le Tableau 1. Nous pouvons ainsi citer le bloc « Séquence de conditionnement » qui correspond, quel que soit le transpondeur choisi, à une alternance de 0 et de 1 sur 24 bits et dure approximativement 2,5 ms. Le bloc « Fanion de début » est, quant à lui, toujours formé de la séquence 01111110. Le bloc « Données » est constitué de 168 bits et regroupe l'ensemble des données relatives au navire comme son identité MMSI, le type de navire, la destination, son statut (en route, au mouillage, en activité, etc.), la position, le cap et la vitesse pour un temps effectif de 17,5 ms. Les navires utilisant l'AIS sont authentifiés par leur identifiant MMSI qui constitue les premiers bits du bloc « Données ». Ainsi, même si un bateau falsifie son numéro MMSI, la signature radiométrique de son transpondeur correspondant aux 32 bits de sa séquence de conditionnement et son fanion de début restera inchangée et permettra de l'identifier et de détecter cette falsification.

Les navires se partagent les canaux en ayant recours à l'approche TDMA (*Time Division Multiple Access*). Avec un débit binaire de 9600 bits/s pour envoyer des messages de 256 bits, le temps est divisé en intervalles de temps de 26,7 ms. Le signal $s(t)$, ramené en bande de base, est représenté sous sa forme complexe par

$$s(t) = I(t) + \mathrm{j}Q(t) \tag{1}$$

Les deux voies $\mathbf{I} = I(t)$ et $\mathbf{Q} = Q(t)$ permettent de transmettre efficacement des informations en utilisant à la fois la phase et l'amplitude du signal tout en permettant une représentation dans un diagramme de constellation. De plus, comme le signal $s(t)$ est complexe, il est possible de définir sa fréquence instantanée $f_{\mathrm{inst}}(t)$ comme étant la dérivée de sa phase :

$$f_{\mathrm{inst}}(t) = \frac{1}{2\pi}\frac{\mathrm{d}}{\mathrm{d}t}\arg(s(t)). \tag{2}$$

Cette expression permet d'extraire les taux de changement « instantanés » de la phase du signal, ce qui fournit des informations essentielles sur les variations subtiles introduites par le matériel de l'émetteur. De telles variations en constituent alors des signatures uniques.

2.2 Dispositif expérimental

La campagne de mesures d'émissions/réceptions AIS a été menée en environnement contrôlé au sein de l'IRENav, signifiant que les émetteurs et les paramètres d'émissions sont connus. Pour cela, quatre radios logicielles National Instruments, configurées de manière identique et de sorte à émettre des messages AIS toutes les 100 ms pendant environ 120 secondes, ont été utilisées : trois USRP2930 (notés par la suite USRP2930_2, USRP2930_3 et USRP2930_4) et une USRPE310. Il est à noter que l'environnement dans lequel ont eu lieu les quatre campagnes de mesures est resté inchangé durant toute la durée de ces dernières. De plus, pour vérifier la conformité aux normes AIS des signaux générés et émis, un transpondeur Saab R5 AIS est ajouté. Le récepteur R&S®EM200 utilisé permet d'enregistrer, dans un format propriétaire traduit plus tard en fichier binaire, les signaux avec une fréquence d'échantillonage égale à 1.6 MHz. Les deux voies $\mathbf{I}$ et $\mathbf{Q}$ sont ensuite extraites de ces enregistrements. Étant donné que cette expérimentation a lieu en environnement clos, les problèmes de masquage des signaux ou d'apparition de trajets multiples dus aux objets et au personnel ajoutent de la complexité aux signaux reçus. Ce sont ces difficultés qui ont renforcé le besoin de méthodes d'identification robustes.

Temps de montée	Séquence de conditionnement	Fanion de début	Données	CRC	Fanion de fin	Tampon
8 bits	**24 bits**	**8 bits**	**168 bits**	**16 bits**	**8 bits**	**24 bits**

TABLEAU 1 : Structure d'une trame AIS constituée de 256 bits découpés en plusieurs blocs.

2.3 Détection des signaux et pré-traitements

Dans chaque enregistrement, les signaux utiles sont les trames AIS de 26,7 ms. Ces trames sont extraites automatiquement grâce à leurs durées et leurs amplitudes sur la voie **I** (utilisation d'un seuillage manuel de sorte à séparer les trames AIS du bruit de fond). Bien que les voies **I** et **Q** soient conservées pour une analyse en constellation, la majorité des traitements sera effectuée sur la fréquence instantanée (2) de ces trames. De plus, ce sont uniquement les bits générés avant le bloc « Données » qui sont à l'étude dans ce travail d'identification. Ainsi, une corrélation avec le motif de la Figure 1 est effectuée pour extraire le signal utile des trames AIS. Ce motif, constitué de 15 bits, est en réalité la fin de la séquence de conditionnement et le fanion de début. Un exemple de signal utile extrait d'un message AIS transmis par l'émetteur USRP2930_2 est donné en Figure 2a. Le Tableau 2 recense le nombre de messages extraits par émetteur.

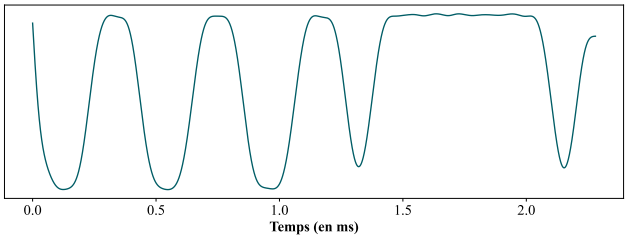


FIGURE 1 : Motif de corrélation servant à l'extraction des signaux utiles.

Émetteurs	Nombre de messages
USRP2930_2	1021
USRP2930_3	1028
USRP2930_4	1020
USRPE310	1015

TABLEAU 2 : Nombre de signaux utiles extraits des enregistrements bruts.

2.4 Extraction d'attributs

Pour caractériser les fréquences instantanées $(f_{\text{inst}}(n))_{1\leq n\leq N}$ des signaux utiles, les attributs suivants ont été calculés.

- Moyenne (μ) : Représente la fréquence instantanée moyenne sur toute la durée du signal, fournissant une estimation de la composante centrale de la fréquence.
- Écart-type (σ) : Mesure la dispersion de la fréquence instantanée autour de sa moyenne, indiquant la variabilité du signal.
- Puissance moyenne (P) : Mesure la puissance moyenne du signal utile et définie par

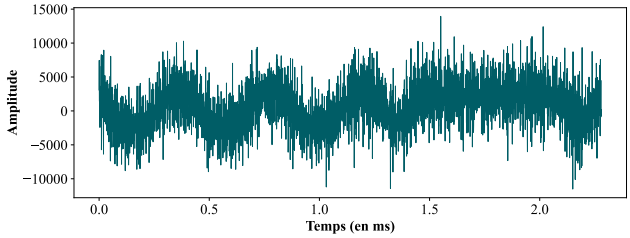
$$P = \frac{1}{N}\sum_{n=1}^{N} |f_{\text{inst}}(n)|^2 , \tag{3}$$

- Skewness (γ_1) : Décrit l'asymétrie de la distribution des fréquences instantanées autour de sa moyenne.
- Kurtosis (γ_2) : Fournit des informations sur la concentration de la distribution par rapport à une distribution gaussienne.
- 6 premiers pics spectraux classés selon leurs amplitudes associées : Permet d'identifier des caractéristiques supplémentaires liées au contenu harmonique des signaux.
- Centroïde spectral μ_F [8] : Pouvant être interprété comme une fréquence moyenne, il est défini par

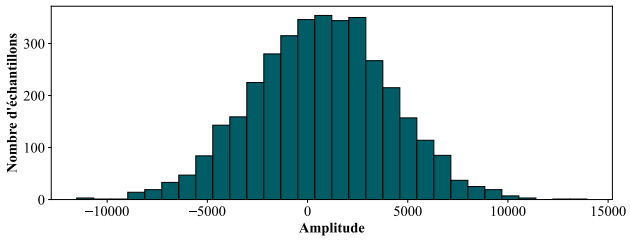
$$\mu_F = \frac{\sum_{n=0}^{N-1} f(n)S(n)}{\sum_{n=0}^{N-1} S(n)}, \tag{4}$$

où $S(n)$ représente l'amplitude de la fréquence $f(n)$ dans le spectre.

Les moments statistiques d'ordre supérieur, tels que le skewness et le kurtosis ont du sens dans ce travail puisque les fréquences instantanées des signaux analysés présentent bien des distributions unimodales comme en atteste la Figure 2b.



(a) Fréquence instantanée $f_{\text{inst}}(t)$.



(b) Distribution statistique de la fréquence instantanée $f_{\text{inst}}(t)$.

FIGURE 2 : Exemple d'un signal utile transmis par l'USRP2930_2.

Par ailleurs, les voies **I** et **Q** permettent de construire le diagramme de constellation, représentation des échantillons dans le plan complexe. Les imperfections de l'émetteur, telles que l'instabilité de l'oscillateur local et les distorsions non linéaires, introduisent des décalages et des dispersions mesurables sur un tel diagramme. La Figure 3 montre le diagramme de constellation d'un signal utile par émetteur. Ainsi, l'émetteur USRPE310 présente un plus grand rayon de dispersion R que la série USRP2930. Cela suggère une plus grande variabilité du signal, ce qui se révèle être une caractéristique pertinente pour constituer un nouvel attribut. En revanche, cette caractéristique le sera moins si une distinction entre radios logicielles de même référence est recherchée.

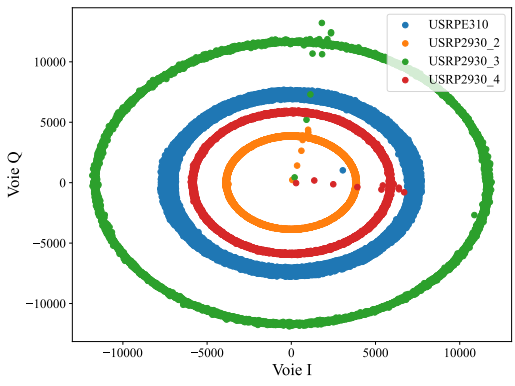


FIGURE 3 : Diagramme de constellation de 4 signaux utiles (un par émetteur).

3 Identification des émetteurs

Nous disposons d'une base de données de 13 attributs extraits des 4084 signaux utiles. Considérant le nombre réduit d'attributs ainsi que l'absence de corrélation entre ces derniers, l'application d'un algorithme de réduction de dimensions n'est pas pertinente. La base de données étant labellisée puisque les radios logicielles à l'origine des signaux utiles sont connues, nous utilisons une forêt aléatoire (*random forest*) comme algorithme d'apprentissage supervisé. Le principe de cet algorithme est l'entraînement aléatoire et indépendant d'une collection d'arbres dont les sorties sont agrégées afin d'obtenir une prédiction plus robuste et plus précise. De plus, comme les attributs sont considérés indépendamment les uns des autres lors de la phase d'entraînement, il n'est pas nécessaire de les normaliser. Par ailleurs, les forêts aléatoires se prêtent aussi bien pour une classification binaire ou multiclasses. Deux tâches sont considérées : la **tâche n° 1** a pour objectif de distinguer les deux types de radios logicielles (USRP2930 vs. USRPE310) et la **tâche n° 2** doit quant à elle distinguer les différentes références d'une même radio logicielle (USRP2930_2 vs. USRP2930_3 vs. USRP2930_4).

Pour ces deux tâches, nous séparons les bases de données respectives en deux sous-ensembles (80 % pour l'entraînement et 20 % pour le test) puis nous recherchons, par validation croisée à 10 couches, les hyperparamètres optimaux pour obtenir la meilleure forêt aléatoire possible. Pour la **tâche n° 1**, le meilleur modèle – entraîné avec les meilleurs hyperparamètres – fournit un taux de décisions correctes de 100 % sur la base de données de test, c'est-à-dire que tous les signaux utiles ont été assignés à la bonne radio logicielle source. La matrice de confusion obtenue par ce modèle est affichée en Figure 4. C'est un résultat très satisfaisant. Toutefois, il est clair que ce sont les résultats de la **tâche n° 2** qui sont les plus intéressants. Pour cette dernière, la matrice de confusion obtenue par le meilleur modèle sur le jeu de données de test fait l'objet de la Figure 5. Ce modèle obtient un taux de décisions correctes égal à 97.39 %, ce qui signifie que plus de neuf signaux utiles

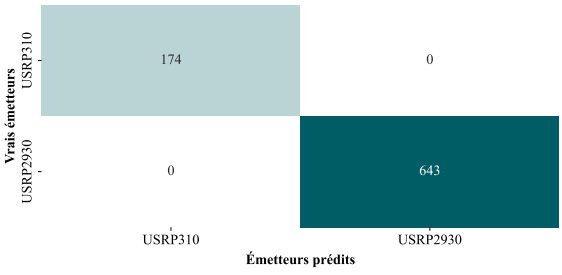


FIGURE 4 : Matrice de confusion du meilleur modèle de la **tâche 1**.

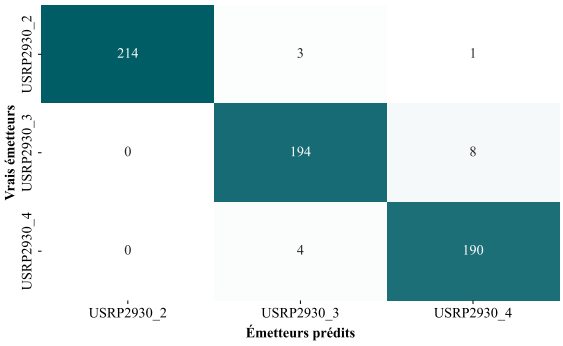


FIGURE 5 : Matrice de confusion du meilleur modèle de la **tâche 2**.

	Tâche n° 1	Tâche n° 2
Forêt aléatoire	100 %	97.39 %
SVM	100 %	92.18 %
Réseaux de neurones	100 %	95.44 %

TABLEAU 3 : Taux de décisions correctes de différents algorithmes.

sur 10 du jeu de données de test, *de facto* inconnus de l'algorithme de classification, sont attribués à la bonne référence d'une même radio logicielle. Ces résultats montrent que les attributs extraits sont extrêmement pertinents pour caractériser les radios logicielles émettrices.

Dans ce contexte d'apprentissage supervisé, un SVM ou un réseau de neurones peu profond (limité à 2 couches cachées) pourraient être mis à l'épreuve. Cependant, les résultats obtenus par ces derniers ne sont pas à la hauteur des performances d'une forêt aléatoire comme le montre le Tableau 3. En effet, sur le jeu de données de test, la forêt aléatoire détermine de manière exacte la radio-logicielle émettrice plus de 97 fois sur 100, soit 2 fois de plus qu'un réseau de neurones et 5 fois de plus qu'un SVM.

4 Conclusion

Dans cet article, nous présentons une étude de faisabilité concernant une nouvelle méthode d'identification des émetteurs AIS à partir de l'analyse de caractéristiques des signaux en régime permanent. Pour cela, une technique de classification exploitant notamment des attributs extraits de la fréquence instantanée du signal reçu a été proposée. Cette approche a été évaluée sur des signaux réels obtenus lors d'une campagne de mesures expérimentales incluant l'utilisation de radios logicielles. Les résultats expérimentaux sont prometteurs avec un taux de décisions correctes à plus de 97 % pour distinguer 3 émetteurs de même référence provenant du même fabricant. Il serait intéressant de mener des tests supplémentaires en considérant d'autres représentations et attributs des signaux.

Références

[1] « Recommendation ITU-R M. 1371-5 : Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band », 2014.

[2] C. IPHAR, A. NAPOLI, C. RAY, E. ALINCOURT et D. BROSSET, « Risk Analysis of falsified Automatic Identification System for the improvement of maritime traffic safety », *in ESREL*, p. 606–613, 2016.

[3] E. ALINCOURT, C. RAY, P.-M. RICORDEL, D. DARE-EMZIVAT et A. BOUDRAA, « Methodology for AIS signature identification through magnitude and temporal characterization », *in OCEANS-Shanghai*, p. 1–6, IEEE, 2016.

[4] V. BRIK, S. BANERJEE, M. GRUTESER et S. OH, « Wireless device identification with radiometric signatures », *in Proceedings of the 14th ACM international conference on Mobile computing and networking*, p. 116–127, 2008.

[5] N. XIE, Z. LI et H. TAN, « A survey of physical-layer authentication in wireless communications », *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, p. 282–310, 2020.

[6] M. LOUART, J.-J. SZKOLNIK, A.-O. BOUDRAA, J.-C. LE LANN et F. LE ROY, « An approach to detect identity spoofing in AIS messages », *Expert Systems with Applications*, vol. 252, p. 124257, 2024.

[7] L. MORGE-ROLLET, *Authentification par empreinte radio pour l'IoT*. Thèse doctorat, ENSTA Bretagne, 2023.

[8] G. PEETERS, « A large set of audio features for sound description (similarity and classification) in the CUIDADO project », *CUIDADO First Project Report*, vol. 54, p. 1–25, 2004.