(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 089 665**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **18 72512**

(51) Int Cl[8] : ***G 06 N 5/04*** *(2019.01), G 07 C 5/08, G 06 F 11/30, 21/55, B 60 W 50/04*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 07.12.18.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 12.06.20 Bulletin 20/24.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *PSA Automobiles SA Société anonyme* — FR et *Institut Mines-Télécom Etablissement public* — FR.

(72) **Inventeur(s) :** Guilley Sylvain, Danger Jean Luc, Karray Khaled et EL AABID MOULAY ABDELAZIZ.

(73) **Titulaire(s) :** Institut Mines-Télécom Etablissement public, PSA Automobiles SA Société anonyme.

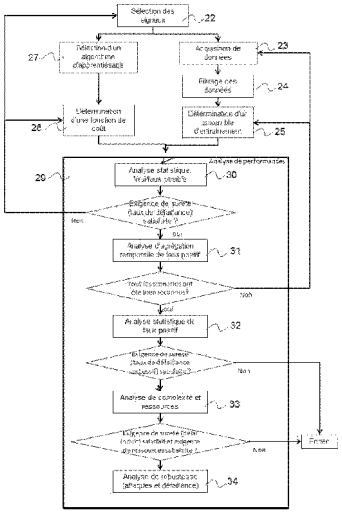
(74) **Mandataire(s) :** PSA AUTOMOBILES.

(54) Procédé et dispositif de paramétrage d'un module de supervision de données échangées sur un bus de données d'un véhicule soumis à des contraintes de sureté de fonctionnement.

(57) L'invention a pour objet un procédé de paramétrage d'un module de supervision d'un signal cible émis sur un bus de données d'un véhicule, ledit module de supervision comportant un modèle comportemental destiné à prédire des valeurs du signal cible, caractérisé en ce qu'il comporte des étapes de :

- sélection (22) de signaux à partir du signal cible,
- acquisition (23) de données correspondant aux signaux sélectionnés,
- mise en forme (24) des données acquises,
- détermination (25) d'un ensemble de données d'apprentissage à partir des données acquises,
- sélection (27) d'un algorithme d'apprentissage,
- détermination (28) d'une fonction de coût à minimiser par l'algorithme d'apprentissage,
- génération du modèle comportemental par apprentissage de l'algorithme sélectionné avec les données de l'ensemble d'apprentissage et la fonction coût déterminée,
- Evaluation (29) du module de supervision intégrant le modèle comportemental

Figure pour l'abrégé : figure 2



FR 3 089 665 - A1

Description

Titre de l'invention : Procédé et dispositif de paramétrage d'un module de supervision de données échangées sur un bus de données d'un véhicule soumis à des contraintes de sureté de fonctionnement

Domaine technique de l'invention

[0001] L'invention concerne les systèmes de supervision de données échangées sur un bus de données d'un véhicule et plus particulièrement le paramétrage de ces systèmes.

Etat de la technique

[0002] Deux exigences importantes des voitures d'aujourd'hui sont un haut niveau de sureté et de connectivité avec le monde extérieur. Cela implique l'utilisation de technologies avancées basées sur une infrastructure informatique composée de nombreux calculateurs électroniques, nommés ECU pour Electronic Control Units, embarqués à l'intérieur du véhicule. Ces calculateurs sont chargés de traiter les données collectées à l'aide de capteurs intégrés et de les transformer en commandes pour les actionneurs. A cet effet, les calculateurs communiquent entre eux via des bus de communication.

[0003] Ces bus sont utilisés pour échanger des messages périodiques et basés sur des événements qui permettent aux calculateurs de surveiller l'état du véhicule en supervisant les états des capteurs et des actionneurs. Un des bus de communication les plus utilisés dans le domaine automobile est le Controller Area Network (CAN).

[0004] Récemment, le protocole CAN est devenu le centre de multiples questions de cybersécurité. On connait par exemple des attaques dans lesquels l'attaquant se connecte physiquement au réseau CAN et rejoue ou injecte des messages sur le bus CAN. On connait aussi des attaques pour lesquelles l'accès physique au bus de communication n'est pas nécessaire. L'attaquant prend le contrôle à distance d'un calculateur légitime et l'utilise pour envoyer des messages non-légitimes.

[0005] Selon l'état de la technique, les méthodes de détection de ces attaques sont basées sur la détection d'anomalies d'intégrité de protocole comme les anomalies dans la périodicité des messages et la syntaxe du protocole. Ces méthodes permettent de détecter un attaquant qui a un accès physique au bus de communication embarqué mais ne détectent pas des attaques dans lesquelles un attaquant prend le contrôle d'un des calculateurs légitimes du véhicule (accès indirect et à distance au bus de communication embarqué du véhicule).

[0006] Afin de détecter ces attaques, on connait des méthodes d'analyse du contenu de l'information utile des trames échangées sur le bus CAN. On connait par exemple, par le document US20180322711, un véhicule comprenant une pluralité de capteurs, un émetteur récepteur de communication sans fil et une unité de commande électronique

(ECU) qui peut être configurée pour commander le fonctionnement du véhicule et obtenir des informations à partir de la pluralité de capteurs. Le calculateur peut être configuré, par l'intermédiaire d'un apprentissage automatique, pour analyser les informations provenant de la pluralité de capteurs et pour émettre une alerte au véhicule en fonction de l'analyse. De telles méthodes ont pour inconvénients de nécessiter un paramétrage complexe pour lequel le document US20180322711 ne fournit aucun élément.

Exposé de l'invention

[0007] L'invention a pour objet de proposer un procédé et un dispositif de paramétrage (sous contraintes) d'un module de supervision de données échangées sur un bus de données d'un véhicule, configuré par l'intermédiaire d'un apprentissage automatique.

[0008] Elle propose plus précisément à cet effet un procédé de paramétrage d'un module de supervision d'un signal cible émis sur un bus de données d'un véhicule, ledit module de supervision comportant un modèle comportemental destiné à prédire des valeurs du signal cible, caractérisé en ce qu'il comporte des étapes de :

- sélection de signaux à partir du signal cible,
- acquisition de données correspondant aux signaux sélectionnés,
- mise en forme des données acquises,
- détermination d'un ensemble de données d'apprentissage à partir des données acquises,
- sélection d'au moins un algorithme d'apprentissage,
- détermination d'une fonction de coût à minimiser par l'algorithme d'apprentissage,
- génération du modèle comportemental par apprentissage de l'algorithme sélectionné avec les données de l'ensemble d'apprentissage et la fonction coût déterminée,
- Evaluation du module de supervision intégrant le modèle comportemental.

[0009] Le procédé selon l'invention permet de paramétrer automatiquement un module de supervision du véhicule. Le procédé permet de générer un modèle comportemental en sélection automatiquement des données et un algorithme d'apprentissage adapté.

[0010] Avantageusement, le procédé de paramétrage d'un module de supervision d'un signal selon l'invention comprend en outre une étape de téléchargement du module de supervision paramétré, intégrant le modèle comportemental, vers un calculateur du véhicule.

[0011] Avantageusement, le procédé de paramétrage d'un module de supervision d'un signal l'invention, comprend en outre une étape de supervision du signal cible par le module de supervision embarqué dans le calculateur du véhicule.

[0012] Avantageusement, l'étape d'évaluation comporte un test d'un taux de vrais positifs et

de faux positifs, de façon à vérifier si l'algorithme calibré répond à des exigences de sureté de fonctionnement.

[0013] Avantageusement, l'étape d'évaluation comporte en outre un test d'agrégation temporelle de faux positifs ou une analyse cumulative de faux positifs, de façon à détecter un éventuel scénario non reconnu par le module de supervision.

[0014] Avantageusement, l'étape d'évaluation comporte en outre un test statistique de faux positifs successifs, de façon à limiter un nombre d'échecs successifs du module de supervision paramétré.

[0015] Avantageusement, l'étape d'évaluation comporte en outre une analyse de complexité de façon à vérifier si l'algorithme calibré répond à des exigences de sureté de fonctionnement en terme de délais induit par le module de prédiction/supervision.

[0016] Avantageusement, l'étape d'évaluation comporte en outre un test de robustesse à des attaques et des défaillances.

[0017] L'invention concerne aussi un calculateur comportant au moins un processeur et une mémoire caractérisé en ce qu'il est configuré pour mettre en œuvre le procédé selon l'invention.

[0018] L'invention concerne aussi un véhicule caractérisé en ce qu'il comporte au moins un calculateur selon l'invention.

Brève description des figures

[0019] [fig.1]

représente un exemple d'une architecture d'un véhicule.

[0020] [fig.2]

montre un logigramme représentant le procédé selon l'invention.

Description détaillée de l'invention

[0021] L'architecture cyberphysique d'un véhicule est composée de plusieurs unités de contrôle électronique (ECU) contenant des capteurs et des actionneurs qui communiquent tous sur des bus de communication partagés. La figure 1 donne un exemple d'une telle architecture. Les calculateurs communiquent entre eux des blocs d'informations appelés signaux qui peuvent être des valeurs de capteurs, des états de capteurs, des commandes d'actionneurs, etc....

[0022] On distingue principalement deux types de signaux : les signaux catégoriques et les signaux à valeur réelle. Un signal catégorique est une information qui prend un nombre limité et fini de valeurs (exemple : la commande d'allumage des feux de freins prend les valeurs 0 ou 1). Un signal à valeur réelle est une information qui prend un grand nombre de valeurs (généralement codées sur plus d'un octet) (exemple : la valeur de la vitesse du véhicule prend des valeurs entre [0 et 655,35] codé sur 2 octets d'information). Ces signaux sont sujets à des modifications intentionnelles (attaques)

ou non intentionnelles (erreur/défaillance). Afin de détecter et éventuellement d'atténuer ces attaques et ces défaillances, un module de supervision surveille au moins un signal sensible au moyen d'une prédiction basée sur des corrélations avec d'autres signaux. L'exemple de la Figure 1 montre cinq signaux qui sont communiqués sur le bus de communication partagé. On suppose que S1 est un signal sensible à surveiller. Le module de supervision exploite les autres signaux (S2, S3, S4 et S5) pour prédire la valeur la plus probable du signal S1 et ensuite comparer avec la valeur du signal reçu. Cette prédiction est basée sur un modèle comportemental.

[0023] Dans l'exemple, le signal S1 est un signal de vitesse. Le module de supervision fait des prédictions sur l'information de vitesse, basées sur d'autres signaux qui sont par exemple : le couple moteur (signal à valeur réelle), la vitesse de rotation du moteur (tr/min) (signal à valeur réelle), la position de la boîte de vitesses (signal catégorique), les signaux de commande des feux de freinage (signal catégorique) et le signal d'accélération du véhicule (signal à valeur réelle).

[0024] Le modèle comportemental nécessite un paramétrage préalable. Ce paramétrage est réalisé par l'intermédiaire d'un apprentissage automatique.

[0025] L'invention concerne un procédé de paramétrage d'un module de supervision d'un signal cible émis sur un bus de données d'un véhicule.

[0026] Le procédé comporte une étape de sélection 22 de signaux pouvant être utilisés pour le processus de prédiction pour prédire le signal cible. Ces signaux constituent l'entrée du module de prédiction. On comprend donc que cette sélection ne contient pas le signal cible, autrement dit le signal à prédire.

[0027] La sélection est réalisée à partir d'une description de l'architecture cyberphysique et de l'architecture du bus de communication embarqué du véhicule. En, effet, selon l'architecture, certains signaux peuvent être présents ou non et peuvent être accessibles ou non à partir de sous-réseaux.

[0028] De façon avantageuse, la sélection prend aussi en compte des métriques de sélection comme une analyse de corrélation de signal, une analyse d'information mutuelle, etc... sur le signal cible et les signaux d'entrée. Ces mesures permettent de sélectionner des signaux contenant suffisamment d'informations pour une prédiction précise. Ce qui permet en outre de limiter le nombre de signaux sélectionnés.

[0029] Cette étape peut être révisée en ajoutant ou en supprimant certains signaux au cas où les contraintes ne seraient pas respectées (Ces aspects sont détaillés plus loin dans la description dans la partie concernant l'étape d'analyse de la performance).

[0030] Dans l'exemple, si on considère l'information de vitesse comme signal cible, le procédé sélectionne par exemple cinq signaux d'entrée qui sont : le couple moteur, la vitesse de rotation du moteur (tr/min), la position de la boîte de vitesses, les signaux de commande des feux de freinage et le signal d'accélération du véhicule.

[0031] Le procédé comporte en outre une étape d'acquisition 23 de données. Au cours de cette étape 23, et après avoir défini le signal cible et les signaux d'entrée à l'étape précédente, l'objectif est de procéder à l'acquisition des données. Les données acquises peuvent être soit simulées (générées par des outils de simulation), soit générées à l'aide de bancs d'essai (comme les équipements Hardware in the loop...), soit issues directement d'un véhicule réel.

[0032] Au cours de cette étape, de multiples types de signaux hétérogènes sont collectés, c'est-à-dire de multiples signaux de types différents (catégoriques, à valeur réelle) et à diverses fréquences de mise à jour (dans l'exemple considéré, le coupe moteur est in signal dont la période de mise-à-jour est de 10 millisecondes, d'autres signaux peuvent avoir des périodes de mise-à-jour plus grande par exemple de 50 ms, 100 ms, 1s, ou bien moins grandes, 1ms) sont capturés pour être utilisés ultérieurement.

[0033] De façon avantageuse, les données acquises sont issues de plusieurs utilisateurs (conducteurs) dans plusieurs situations et conditions de conduite (comme le stationnement, la conduite sur autoroute, la conduite en ville, etc...). Ceci permet d'améliorer la polyvalence du modèle comportementale et donc sa capacité à s'adapter à différentes situations et cycles de vie des véhicules.

[0034] Le procédé comporte en outre une étape de mise en forme 24 des données acquises. L'étape comporte par exemple, des traitements pour lisser les données (filtrage) bruitées ou / et normaliser les données.

[0035] Le procédé comporte en outre une étape de détermination 25 d'un ensemble de données d'apprentissage. Cette étape comporte la détermination d'un ensemble d'apprentissage (utilisé pour entrainer les algorithmes d'apprentissage) et d'un ensemble de test (utilisé pour évaluer l'algorithme d'apprentissage, autrement dit le modèle comportemental une fois que celui a été entrainé).

[0036] Selon un mode de réalisation de l'invention, cette étape comporte en outre la définition d'autres ensembles de données comme un ensemble de validation croisée qui peut être utilisé pour calibrer certains paramètres d'accord des algorithmes ou de la fonction cout.

[0037] Avantageusement, les données relatives aux différents cas d'utilisation sont équilibrées dans les ensembles de d'apprentissage et de test (et d'autres le cas échéant). Autrement dit, chaque ensemble comporte une part sensiblement équivalente de données correspondant aux différents conducteurs et/ou aux différentes conditions. Cette étape 25 comporte aussi une préparation des données pour le processus d'apprentissage automatique supervisé. Ceci inclut la configuration des caractéristiques d'entrée et des signaux cibles dans des vecteurs et des matrices prêtes à être traités par les algorithmes d'apprentissage.

[0038] Le procédé comporte en outre une étape de sélection 27 d'un algorithme

d'apprentissage. La sélection repose notamment sur le type de signal cible (catégorique, valeur réelle) pour choisir d'utiliser des algorithmes de classification ou des algorithmes de régression. La sélection tient aussi compte des contraintes de mémoire et de complexité lié au calculateur devant effectuer la supervision. La sélection est effectuée à partir d'un ensemble connu d'algorithme d'apprentissage supervisé. Exemple : Réseau de neurones, Arbre de décision, forêts d'arbres décisionnels (ou forêts aléatoires de l'anglais random forest classifier or regressor), méthode des k plus proches voisins (k nearest neighbors), etc…

[0039] Le procédé comporte en outre une étape de détermination 28 d'une fonction de coût ou fonction d'erreur à minimiser pendant le processus d'apprentissage.

[0040] Par exemple, lors de la construction d'un module de prédiction pour le signal de vitesse, et lors de l'utilisation d'algorithmes paramétriques d'apprentissage supervisé (comme la régression linéaire, le réseau de neurones de régression, ...) en faisant une hypothèse gaussienne sur l'erreur prédictive, et en utilisant un estimateur du maximum de vraisemblance pour estimer le signal cible, le procédé détermine que la fonction de coût à utiliser est la somme des erreurs au carré. Une autre fonction de coût (erreur) peut être la somme des erreurs au carré avec un terme de régularisation, etc...

[0041] Le procédé comporte aussi une étape génération du modèle comportemental par apprentissage de l'algorithme sélectionné avec les données de l'ensemble d'apprentissage et la fonction coût déterminée.

[0042] L'invention comporte aussi une étape d'évaluation du module de supervision et en particulier du modèle généré sous contraintes de sureté de fonctionnement et de ressources disponibles. L'étape d'évaluation comporte par exemple : un test 30 du taux de vrais positifs et de faux positifs, un test 31 d'agrégation temporelle de faux positifs ou une analyse cumulative de faux positifs, une analyse 32 statistique successive de faux positifs, une analyse 33 de complexité et d'adéquation des ressources allouées, et une analyse 34 de la résistance aux attaques et défaillances. Ces tests indiquent dans quelle mesure le ou les algorithmes d'apprentissage entrainés (calibrés) répondent aux exigences et contraintes imposées, et donnent une indication de qualité pour guider le choix du meilleur modèle comportemental à utiliser.

[0043] Le test 30 de taux de vrais positifs et de faux positifs permet d'évaluer, en l'absence d'attaques et défaillances, le modèle comportemental issu de l'algorithme d'apprentissage sélectionné, en utilisant des données collectées qui n'ont pas déjà été utilisées pour l'apprentissage (l'ensemble de test). Ce test vérifie si l'algorithme calibré répond à des exigences de sureté. Une première exigence de sureté concerne l'écart acceptable du signal. Par exemple, en considérant le signal vitesse comme signal cible, une exigence de sureté serait de considérer que toute prédiction de plus ou moins 5 km/h est acceptable, en dehors de cet intervalle la prédiction est considérée fausse. Et

donc l'exigence de sureté fixe un écart de vitesse acceptable de plus ou moins 5 km/h. Cet écart permet de définir quels sont les cas d'utilisation qui ont été correctement prédits et quels sont les cas d'utilisation qui n'ont pas été correctement prédits par l'algorithme de prédiction. La proportion de fausses prédictions définit le taux de faux positifs, qui est aussi le taux d'échec de l'algorithme d'apprentissage. Des exigences de sureté similaires peuvent également être définies pour les signaux catégoriques.

[0044] Une deuxième exigence de sureté consiste à vérifier que la proportion (ou probabilité) de fausses prédictions, également appelées faux positifs, satisfait au taux d'échec acceptable. Par exemple, on peut considérer une exigence qui fixe un taux d'échec acceptable de 1%, dans ce cas un algorithme ayant une proportion de fausses prédictions de plus de 1% (inversement, une précision inférieure à 99%) échoue le test.

[0045] De façon avantageuse, si certains modèles de prédiction ne réussissent pas ce test, le procédé comporte une itération de l'étape de détermination 28 de la fonction de coût (de à réviser certaines hypothèses faites à cette étape et/ou calibration de la fonction coût) ou une itération de l'étape de sélection 22 de signaux (de façon à supprimer certains signaux inclus à cette étape ou à ajouter d'autres signaux).

[0046] Le test 31 d'agrégation temporelle faux positif / analyse cumulative temporelle de faux positif permet d'évaluer, en l'absence d'attaques l'évolution dans le temps du nombre cumulé de faux positifs. Dans ce test, les données d'entrée sont envoyées aux algorithmes de prédiction dans l'ordre dans lequel elles sont apparues lors de l'acquisition des données. Ce test permet de détecter certains scénarios que l'algorithme de prédiction n'est pas bien entrainé à reconnaître (scénarios au cours desquels l'algorithme de prédiction fait plusieurs fausses prédictions successives). Si de tels scénarios ont été détectés et identifiés, le test est considéré comme échoué. Optionnellement on peut être amener à faire plus d'acquisitions (étape 23) ou a redéfinir l'ensemble d'entrainement (étape 25) pour inclure plus de vecteurs d'entrainements sur le(s) scenario(s) en question.

[0047] Le test 32 d'analyse statistique de faux positifs successifs permet de caractériser l'aspect statistique des faux positifs successifs (évalués dans le temps au test précédent). Cette analyse permet de comparer qualitativement différents algorithmes d'apprentissage et de choisir celui qui est le moins sujet aux échecs successifs (faux positifs). Une exigence de sureté définit par exemple un seuil de défaillances successives acceptables. Dans ce cas, un algorithme qui ne satisfait pas à cette exigence est considéré comme ayant échoué au test.

[0048] Le test 33 d'analyse de complexité et d'allocation des ressources permet d'étudier pratiquement la complexité du processus de prédiction pour chaque algorithme de prédiction et les ressources nécessaires à sa mise en œuvre. La vérification est effectuée de préférence sur la plateforme cible sur laquelle le processus de supervision

sera déployé. Une exigence de sureté concernant le retard maximum induit par l'algorithme de prédiction est avantageusement vérifiée à cette étape. Par exemple, l'exigence de sureté indique que le processus de supervision et donc de prédiction ne doit pas dépasser 2 millisecondes. Pour l'évaluation des ressources, il s'agit aussi de satisfaire une exigence qui indique les ressources qui peuvent être alloué et à ne pas dépasser. Par exemple, la mémoire utilisée par le processus de supervision ne doit pas dépasser un premier seuil X (exprimé en kbytes) de mémoire Ram et un deuxième seuil Y (exprimé en kbytes) de mémoire flash.

[0049] Le test 34 d'analyse de la robustesse face aux attaques et aux défaillances permet de tester la ou les fonctions de prédiction ayant réussi les tests précédents contre des situations réelles d'attaques et de défaillances afin d'étudier leur robustesse face à ces menaces et de caractériser leurs taux Vrai Négatif et Faux Négatif. Cette caractérisation permet de choisir l'algorithme de prédiction calibré le plus robuste à utiliser.

[0050] Le procédé de paramétrage comporte une étape de sélection d'un module de prédiction, sur la base des tests précédents.

[0051] Ensuite, le module de prédiction sélectionné est téléchargé dans le véhicule.

[0052] Le module de prédiction téléchargé dans le véhicule est utilisé pour supervisé le signal cible.

Revendications

[Revendication 1] Procédé de paramétrage d'un module de supervision d'un signal cible émis sur un bus de données d'un véhicule, ledit module de supervision comportant un modèle comportemental destiné à prédire des valeurs du signal cible, caractérisé en ce qu'il comporte des étapes de :
- sélection (22) de signaux à partir du signal cible,
- acquisition (23) de données correspondant aux signaux sélectionnés,
- mise en forme (24) des données acquises,
- détermination (25) d'un ensemble de données d'apprentissage à partir des données acquises,
- sélection (27) d'au moins un algorithme d'apprentissage,
- détermination (28) d'une fonction de coût à minimiser par l'algorithme d'apprentissage,
- génération du modèle comportemental par apprentissage de l'algorithme sélectionné avec les données de l'ensemble d'apprentissage et la fonction coût déterminée,
- Evaluation (29) du module de supervision intégrant le modèle comportemental.

[Revendication 2] Procédé de paramétrage d'un module de supervision d'un signal selon la revendication précédente, caractérisé en ce qu'il comprend en outre une étape de téléchargement du module de supervision paramétré, intégrant le modèle comportemental, vers un calculateur du véhicule.

[Revendication 3] Procédé de paramétrage d'un module de supervision d'un signal selon la revendication précédente, caractérisé en ce qu'il comprend en outre une étape de supervision du signal cible par le module de supervision embarqué dans le calculateur du véhicule.

[Revendication 4] Procédé de paramétrage d'un module de supervision d'un signal selon l'une des revendications précédentes, caractérisé en ce que l'étape d'évaluation (29) comporte un test (30) d'un taux de vrais positifs et de faux positifs, de façon à vérifier si l'algorithme calibré répond à des exigences de sureté de fonctionnement.

[Revendication 5] Procédé de paramétrage d'un module de supervision d'un signal selon l'une des revendications précédentes, caractérisé en ce que l'étape d'évaluation (29) comporte en outre un test (31) d'agrégation temporelle de faux positifs ou une analyse cumulative de faux positifs, de façon à détecter un éventuel scénario non reconnu par le module de supervision.

[Revendication 6] Procédé de paramétrage d'un module de supervision d'un signal selon

l'une des revendications précédentes, caractérisé en ce que l'étape d'évaluation (29) comporte en outre un test (32) statistique de faux positifs successifs, de façon à limiter un nombre d'échecs successifs du module de supervision paramétré.

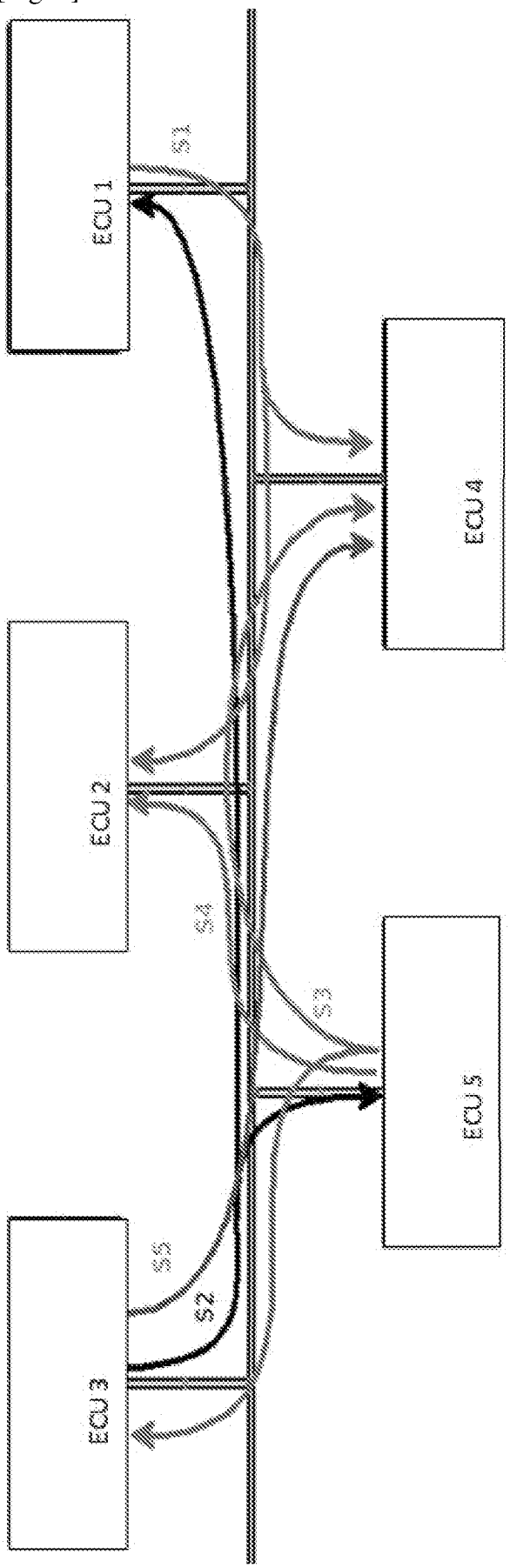
[Revendication 7] Procédé de paramétrage d'un module de supervision d'un signal selon l'une des revendications précédentes, caractérisé en ce que l'étape d'évaluation (29) comporte en outre une analyse (33) de complexité de façon à vérifier si l'algorithme calibré répond à des exigences de sureté de fonctionnement en terme de délais induit par le module de prédiction/supervision.

[Revendication 8] Procédé de paramétrage d'un module de supervision d'un signal selon l'une des revendications précédentes, caractérisé en ce que l'étape d'évaluation (29) comporte en outre un test (34) de robustesse à des attaques et des défaillances.

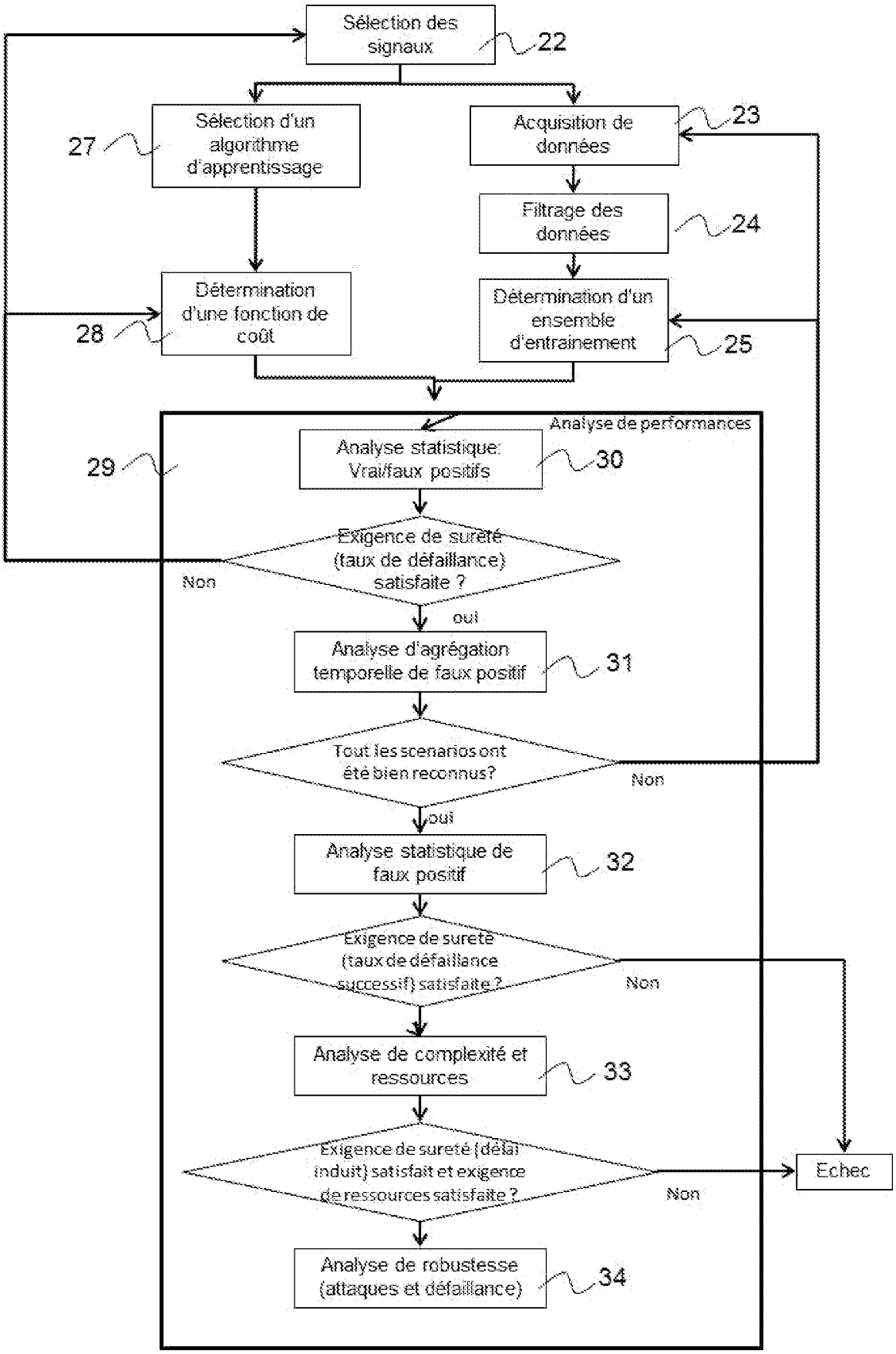
[Revendication 9] Calculateur comportant au moins un processeur et une mémoire caractérisé en ce qu'il est configuré pour mettre en œuvre le procédé selon l'une de revendications précédentes.

[Revendication 10] Véhicule caractérisé en ce qu'il comporte au moins un calculateur selon la revendication précédente.

[Fig. 1]



[Fig. 2]


Sélection des signaux
22
Sélection d'un algorithme d'apprentissage
27
Acquisition de données
23
Filtrage des données
24
Détermination d'une fonction de coût
28
Détermination d'un ensemble d'entrainement
25
Analyse de performances
29
Analyse statistique: Vrai/faux positifs
30
Exigence de sureté (taux de défaillance) satisfaite ?
Non
oui
Analyse d'agrégation temporelle de faux positif
31
Tout les scenarios ont été bien reconnus?
Non
oui
Analyse statistique de faux positif
32
Exigence de sureté (taux de défaillance successif) satisfaite ?
Non
Analyse de complexité et ressources
33
Exigence de sureté (délai induit) satisfait et exigence de ressources satisfaite ?
Non
Echec
Analyse de robustesse (attaques et défaillance)
34

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 861950
FR 1872512

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X,D	US 2018/322711 A1 (WEIMERSKIRCH ANDRE [US]) 8 novembre 2018 (2018-11-08) * abrégé; figures 1-3 * * alinéa [0001] - alinéa [0009] * * alinéa [0014] - alinéa [0046] * -----	1-10	G06N5/04 G07C5/08 G06F11/30 G06F21/55 B60W50/04
A	Daksh Kumar Vasistha: "DETECTING ANOMALIES IN CONTROLLER AREA NETWORK FOR AUTOMOBILES", , 1 août 2017 (2017-08-01), XP055622390, Extrait de l'Internet: URL:https://oaktrust.library.tamu.edu/bitstream/handle/1969.1/165769/VASISTHA-THESIS-2017.pdf?sequence=1&isAllowed=y [extrait le 2019-09-16] * abrégé * * chapitres 1, 2, 5-7 * -----	1-10	
A	NARAYANAN SANDEEP NAIR ET AL: "OBD_SecureAlert: An Anomaly Detection System for Vehicles", 2016 IEEE INTERNATIONAL CONFERENCE ON SMART COMPUTING (SMARTCOMP), IEEE, 18 mai 2016 (2016-05-18), pages 1-6, XP032917406, DOI: 10.1109/SMARTCOMP.2016.7501710 [extrait le 2016-06-28] * abrégé * * chapitres I,III,V,VI,VII * ----- -/--	1-10	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06N

1

Date d'achèvement de la recherche	Examinateur
17 septembre 2019	Totir, Felix

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 861950
FR 1872512

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	JICHICI CAMIL ET AL: "Examining the Use of Neural Networks for Intrusion Detection in Controller Area Networks", 9 novembre 2018 (2018-11-09), SERIOUS GAMES; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 109 - 125, SecITC 2018 (Conference), XP047501905, ISSN: 0302-9743 ISBN: 978-3-642-34128-1 [extrait le 2019-02-06] * abrégé; figure 1 * * chapitres 1-3 * -----	1-10	
A	BERGER IVO ET AL: "Comparative Study of Machine Learning Methods for In-Vehicle Intrusion Detection", 7 septembre 2018 (2018-09-07), SERIOUS GAMES; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 85 - 101, CyberICPS 2018/SECPRE 2018 (Conference), XP047502233, ISSN: 0302-9743 ISBN: 978-3-642-34128-1 [extrait le 2019-01-31] * abrégé * * chapitres 1-5 * ----- -/--	1-10	DOMAINES TECHNIQUES RECHERCHÉS (IPC)

1

Date d'achèvement de la recherche	Examinateur
17 septembre 2019	Totir, Felix

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 861950
FR 1872512

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	THEISSLER ANDREAS ED - YAO YIYU ET AL: "Detecting known and unknown faults in automotive systems using ensemble-based anomaly detection", KNOWLEDGE-BASED SYSTEMS, ELSEVIER, AMSTERDAM, NL, vol. 123, 20 février 2017 (2017-02-20), pages 163-173, XP029956130, ISSN: 0950-7051, DOI: 10.1016/J.KNOSYS.2017.02.023 * abrégé; figures 2-6 * * chapitres 1-5 * -----	1-10	
T	KARRAY KHALED ET AL: "Prediction-Based Intrusion Detection System for In-Vehicle Networks Using Supervised Learning and Outlier-Detection", 11 décembre 2018 (2018-12-11), SERIOUS GAMES; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 109 - 128, WISTP 2018 (Conference), XP047507652, ISSN: 0302-9743 ISBN: 978-3-642-34128-1 [extrait le 2019-05-12] * abrégé; figures 1-6 * * page 109, ligne 1 - page 126, dernière ligne * ----- -/--	1-10	DOMAINES TECHNIQUES RECHERCHÉS (IPC)

1

Date d'achèvement de la recherche	Examinateur
17 septembre 2019	Totir, Felix

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 861950
FR 1872512

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	KHALED KARRAY ET AL: "Attack tree construction and its application to the connected vehicle", CYBER-PHYSICAL SYSTEMS SECURITY, SPRINGER, CHAM, CHAM, PAGE(S) 175 - 190 , 6 décembre 2018 (2018-12-06), XP009516090, ISBN: 978-3-319-98934-1 Extrait de l'Internet: URL:http://link.springer.com/10.1007/978-3-319-98935-8_9 [extrait le 2018-09-16] * page 175, ligne 1 * * page 175, ligne 1 - page 188, dernière ligne * -----	1-10	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

Date d'achèvement de la recherche	Examinateur
17 septembre 2019	Totir, Felix

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

1

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1872512 FA 861950

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 17-09-2019
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2018322711 A1	08-11-2018	CN 108881364 A	23-11-2018
		DE 102018202822 A1	08-11-2018
		US 2018322711 A1	08-11-2018

EPO FORM P0465