Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1376

(01/2021)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Applications et services sécurisés (2) – Sécurité des systèmes de transport intelligents

Mécanisme de détection des mauvais comportements liés à la sécurité des véhicules connectés utilisant les mégadonnées

Recommandation UIT-T X.1376

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	**X.1370–X.1389**
Sécurité de la technologie des registres distribués	X.1400–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DE LA 5G	X.1800–X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1376

Mécanisme de détection des mauvais comportements liés à la sécurité des véhicules connectés utilisant les mégadonnées

Résumé

La Recommandation UIT-T X.1376 décrit un mécanisme de détection des mauvais comportements liés à la sécurité des véhicules connectés, afin d'aider les parties prenantes à utiliser les données automobiles pour améliorer la sécurité des véhicules.

Plus la connectivité des véhicules augmente, plus les vulnérabilités sont nombreuses en raison du développement de technologies complexes. Ces vulnérabilités font peser davantage de menaces sur les véhicules connectés. L'analyse d'une grande quantité de données automobiles est très utile pour évaluer la sécurité des véhicules connectés.

Historique

Édition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1376	07-01-2021	17	11.1002/1000/14448

Mots clés

Véhicules connectés; détection des mauvais comportements.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1376

Mécanisme de détection des mauvais comportements liés à la sécurité des véhicules connectés utilisant les mégadonnées

1 Domaine d'application

La présente Recommandation décrit un mécanisme de détection des mauvais comportements liés à la sécurité des véhicules connectés. Ce mécanisme comprend les mesures suivantes:

a) Saisie de données. Spécification des types de données et d'informations qui peuvent être saisies à partir de différentes sources, notamment les fabricants et fournisseurs de l'automobile et des infrastructures ainsi que les fabricants et fournisseurs d'équipements d'origine (OEM), pour la détection des mauvais comportements. Les méthodes et procédures de saisie des données n'entrent pas dans le cadre de la présente Recommandation.

b) Détection. Analyse des données saisies pour détecter les mauvais comportements.

La présente Recommandation s'applique aux véhicules connectés et vise à aider les concepteurs et les fournisseurs de solutions de sécurité à détecter les mauvais comportements. Les méthodes d'utilisation des notifications n'entrent pas dans le cadre de la présente Recommandation.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

Aucune.

3 Définitions

3.1 Termes définis ailleurs

Aucun.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 mauvais comportement: le fait de fournir des données fausses ou trompeuses et d'agir de manière à gêner d'autres bénéficiaires de services ou à agir en dehors du domaine d'activité autorisé de ces derniers. Un mauvais comportement peut être dû à des composants internes ou externes du système du véhicule.

NOTE 1 – Fondé sur la publication [b-ISO/TR 17427-4].

NOTE 2 – On entend par mauvais comportement notamment des comportements suspects, délibérés ou non, tels que les types de messages ou les fréquences erronés, les connexions non valables et l'accès non autorisé, ou les messages signés ou chiffrés incorrects.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ABS système de freinage antipatinage (*Anti-skid Braking System*)

ADAS système évolué d'aide à la conduite (*Advanced Driver-Assistance System*)

AEB freinage d'urgence autonome (*Autonomous Emergency Braking*)

API interface de programmation d'applications (*Application Programming Interface*)

CAN gestionnaire de réseau de communication (*Controller Area Network*)

GNSS système mondial de navigation par satellite (*Global Navigation Satellite System*)

IP protocole Internet (*Internet Protocol*)

ITS système de transport intelligent (*Intelligent Transportation System*)

LiDAR détection et localisation par la lumière (*Light Detection and Ranging*)

MCU microcontrôleur (*Microcontroller Unit*)

OEM fabricant d'équipements d'origine (*Original Equipment Manufacturer*)

TCU unité de commande télématique (*Telematics Control Unit*)

URL localisateur uniforme de ressources (*Uniform Resource Locator*)

5 Conventions

Aucune.

6 Modèle de mécanisme de détection des mauvais comportements

On trouvera à la Figure 1 le modèle de mécanisme de détection des mauvais comportements pour les véhicules connectés. Ce mécanisme comporte deux étapes, à savoir la saisie de données et la détection, qui sont mises en œuvre par deux systèmes.

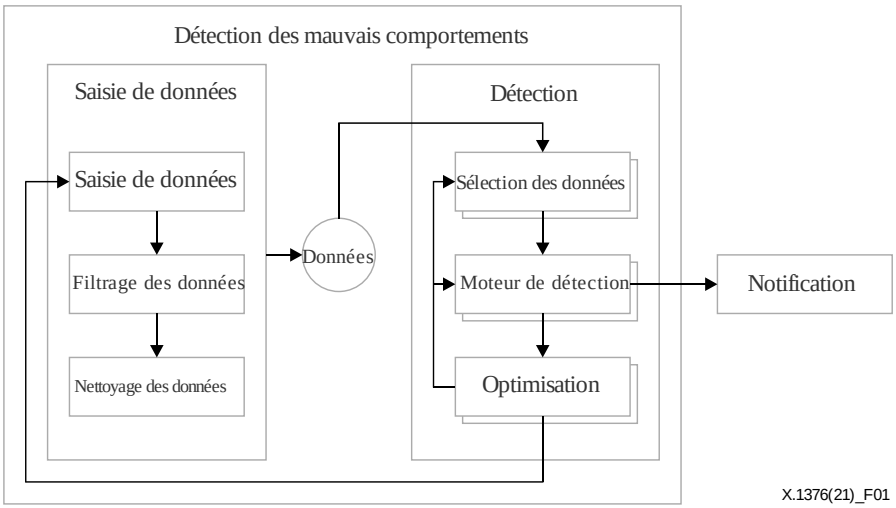


Figure 1 – Modèle de mécanisme de détection des mauvais comportements

Étant donné que les méthodes et procédures de saisie des données n'entrent pas dans le cadre de la présente Recommandation, le système de saisie de données (par exemple le filtrage et le nettoyage des données) présenté à la Figure 1 n'est qu'un exemple de mise en œuvre pratique de la détection des mauvais comportements fourni à titre d'information.

Les données provenant du système de saisie sont envoyées au système de détection, et la saisie des données est traitée selon les types décrits au § 7.

Le système de saisie des données comprend les modules suivants:

a) collecte de données: collecte de données pour la détection à partir de différentes sources, par exemple le fournisseur de services, le système corporel et les capteurs;

b) filtrage des données: filtrage des données saisies sur la base de la classification des données;

c) nettoyage des données: opérations de déduplication et de réduction du bruit pour les données saisies.

Le système de détection comprend les modules suivants:

a) sélection des données: les ensembles de données sont sélectionnés sur la base de différentes méthodes de détection des mauvais comportements, puis sont envoyés au moteur de détection;

b) moteur de détection: les mauvais comportements sont détectés sur la base des méthodes de détection, puis les résultats de la décision sont envoyés à l'optimisation et à la notification, selon le cas;

c) optimisation: les résultats de la détection provenant du moteur de détection sont utilisés pour améliorer la sélection des données, le moteur de détection et la saisie des données.

La notification est un module qui envoie les résultats provenant du moteur de détection aux parties prenantes. Elle n'entre pas dans le cadre de la présente Recommandation.

7 Saisie des données

La saisie des données comprend généralement la saisie des données, le nettoyage des données et le filtrage des données. Étant donné que les méthodes et les procédures de saisie des données n'entrent pas dans le cadre de la présente Recommandation, seuls les types de données utilisés dans la procédure de détection sont indiqués. Il convient de protéger les données personnelles sensibles à l'aide de technologies adaptées telles que l'anonymisation, qui n'entre pas dans le cadre de la présente Recommandation.

Sur la base des données et des informations saisies à partir de différentes sources, le présent paragraphe précise les types utilisés dans le mécanisme de détection des mauvais comportements, à savoir les données de statut, les données de contrôle et les données d'intelligence, comme indiqué dans le Tableau 1.

Tableau 1 – Types de données

Type	Sous-type	Sources de données	Exemples de données
Données de statut[a]	Données d'application ou de service	Fournisseur de contenu ou fournisseur de services	Données d'infoloisirs
		Données de service de carte	Navigation, positionnement
		Données d'applications mobiles	Données relatives aux applications
	Statut du véhicule	Système de sécurité	Système de freinage antipatinage (ABS), airbag, freinage d'urgence autonome (AEB), systèmes évolués d'aide à la conduite (ADASs)
		Système corporel	Porte, fenêtre, essuie-glace

Tableau 1 – Types de données

Type	Sous-type	Sources de données	Exemples de données
		Système de châssis	Couple de torsion, angle
		Système d'alimentation	Vitesse, vitesse de rotation, soupape d'étranglement, décrochage
	Capteurs environnementaux	Radar	Radar en ondes millimétriques
		Détection et localisation par la lumière (LiDAR)	Nuage de points
		Capteurs ultrason	Distance
		Caméra	Image environnante
		Capteurs de système de transport intelligent (ITS)	Signalisation des installations routières
Données de contrôle[b]	Contrôle local	Systèmes de contrôle embarqué	Ouverture de la porte, fermeture de la porte
	Contrôle à distance	Automatisation, télématique	Diagnostic à distance
Données d'intelligence[c]	Données d'intelligence internes	Recherche concernant la sécurité, résultats de tests	Vulnérabilités, bugs, incidents de cybersécurité internes
	Partage externe de données d'intelligence	Client, fournisseur, communauté, conférence ou publications, web	Adresse IP (protocole Internet), valeurs de hachage, localisateur uniforme de ressources (URL), nom de domaine, vulnérabilités et expositions courantes (CVE), etc.

[a] Données et informations relatives au statut des véhicules, des applications, des services, des capteurs et d'autres installations dans un système ITS.

[b] Données et informations utilisées pour contrôler les véhicules, les applications, les services, les capteurs et d'autres installations dans un système ITS.

[c] Données et informations relatives à la cybersécurité obtenues à partir de systèmes autres qu'un système ITS. On suppose que les sources des données présentent le niveau d'intégrité approprié.

8 Détection

Le module de détection comprend principalement la sélection des données, le moteur de détection et l'optimisation. Comme le montre la Figure 2, sur la base de données et d'informations provenant de différentes sources, le moteur de détection utilise l'analyse des mégadonnées pour identifier un mauvais comportement. L'optimisation utilise les mauvais comportements pour optimiser la sélection des données et le moteur de détection rend la détection des mauvais comportements plus précise et efficace.

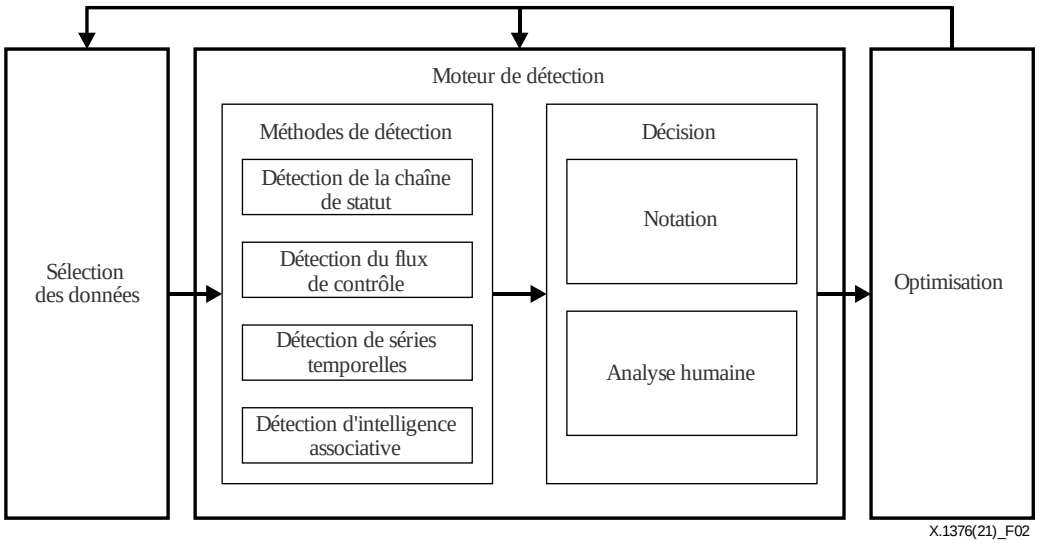


Figure 2 – Procédure de détection

8.1 Sélection des données

En fonction des différents besoins en matière de données des méthodes de détection, le module de sélection des données classe les données en différents ensembles de données, selon les exigences des moteurs de détection, comme indiqué à la Figure 3. Les données introduites dans le module de sélection des données proviennent du système de saisie.

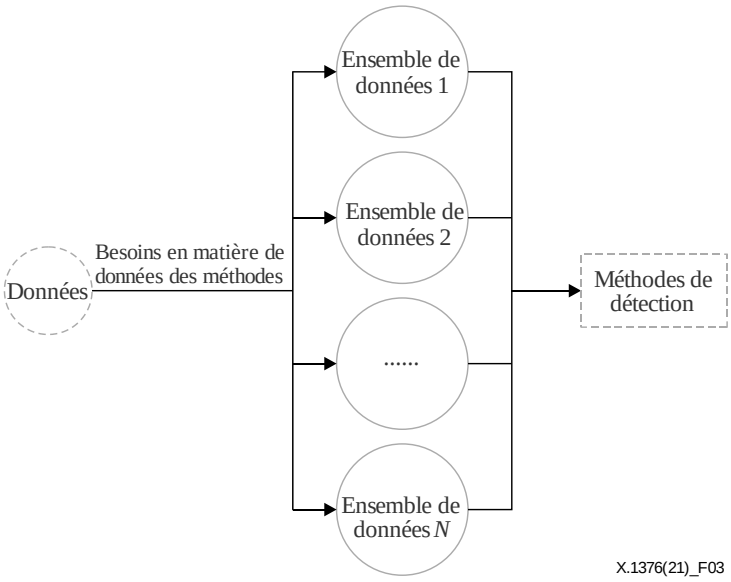


Figure 3 – Procédure de sélection des données

8.2 Moteur de détection

Le moteur de détection se compose de deux sous-modules, à savoir les méthodes de détection et la décision. Lorsque les ensembles de données entrent dans le sous-module des méthodes de détection, les méthodes les transforment en caractéristiques de comportement. Ensuite, le sous-module de décision prend une décision en fonction des caractéristiques de comportement. Il existe trois types différents de résultats des décisions: bloqués, suspects et autorisés. Un résultat bloqué signifie que celui-ci est anormal; un résultat suspect signifie qu'il est impossible de déterminer si les données sont refusées ou sécurisées; et un résultat autorisé signifie que les données sont sécurisées.

8.2.1 Méthodes de détection

Le sous-module "Méthodes de détection" est un ensemble de différentes méthodes de détection. Sur la base des types de données classés au § 7, quatre méthodes ont été conçues pour détecter les mauvais comportements à l'aide de ces données.

8.2.1.1 Détection de la chaîne de statut

La chaîne de statut contient une série de données de statut corrélées. Dans la chaîne de statut, la modification d'une donnée entraîne la modification simultanée d'autres données.

Voici quelques caractéristiques d'une chaîne de statut:

a) Nœud: service ou application dans un système ITS qui est utile pour une action.

b) Flux: direction et trajet des données modifiées résultant d'une action.

Les données de statut sont générées dans un système ITS et un contexte peut être créé avec ces données. La valeur des données suit également une certaine tendance et varie entre des limites convenues.

En substance, la chaîne de statut peut être subdivisée en deux modèles: la ligne et la branche. Ces deux modèles sont les suivants:

1) Ligne: chaque nœud n'a qu'un seul nœud qui reçoit son signal.

2) Branche: un nœud génère deux ou plusieurs données de statut en même temps, puis les envoie à différents nœuds.

Dans le modèle de ligne d'une chaîne de statut, les nœuds n'ont qu'une connexion unidirectionnelle. Voir la Figure 4.

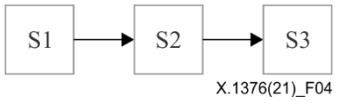


Figure 4 – Modèle de ligne d'une chaîne de statut
S: statut

Dans le modèle de branche d'une chaîne de statut, les nœuds peuvent être scindés en deux ou plusieurs modèles de ligne pertinents. Voir la Figure 5.

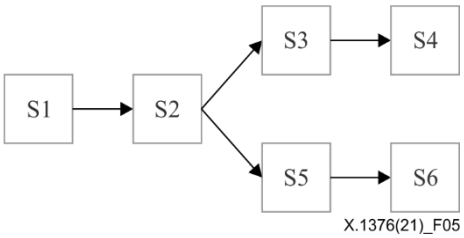


Figure 5 – Modèle de branche d'une chaîne de statut

Ainsi, les caractéristiques de chaque nœud comprennent:

i) le contexte dans la chaîne de statut;

ii) la valeur et la tendance de chaque nœud.

Les caractéristiques des nœuds de la chaîne de statut sont obtenues, puis sont envoyées à la fonction de notation.

8.2.1.2 Détection du flux de contrôle

Le flux de contrôle contient une série de données de contrôle corrélées. Dans le flux de contrôle, une commande de contrôle peut être composée de plusieurs sous-commandes de contrôle et affectera plusieurs systèmes.

Voici quelques caractéristiques du flux de contrôle pour décrire l'exécution des commandes de contrôle:

a) Nœud: service ou application dans un système ITS qui est utile pour une action.

b) Flux: direction et trajet des données modifiées résultant d'une action.

Lorsqu'une action de contrôle est en cours, les données liées au contrôle passent par des nœuds liés au contrôle et forment un flux de contrôle.

Chaque nœud de contrôle fonctionne de manière stable et régulière dans un système ITS. Lorsque de nombreux nœuds fonctionnent ensemble, le flux de contrôle a également un comportement stable, en raison de la période prescrite, des types déterminés et du nombre de messages.

En substance, le flux de contrôle peut être subdivisé en deux modèles: la ligne et la branche. Ces deux modèles sont les suivants:

1) Ligne: chaque nœud n'a qu'un seul nœud qui reçoit son signal.

2) Branche: un nœud génère deux ou plusieurs données de contrôle simultanément, puis les envoie à différents nœuds.

Dans le modèle de ligne d'un flux de contrôle, les nœuds n'ont qu'une connexion unidirectionnelle. Voir la Figure 6.

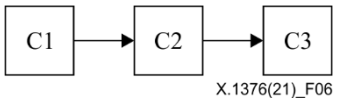


Figure 6 – Modèle de ligne d'un flux de contrôle
C: contrôle

Dans le modèle de branche d'un flux de contrôle, les nœuds peuvent être scindés en deux ou plusieurs modèles de ligne pertinents. Voir la Figure 7.

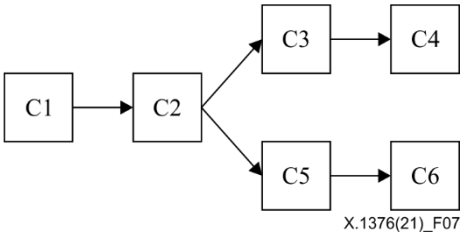


Figure 7 – Modèle de branche d'un flux de contrôle

8.2.1.3 Détection de séries temporelles

Une série temporelle est utilisée pour décrire les données qui changent selon le type. Tant que les données sont conformes aux types, la détection des séries temporelles peut être utilisée.

La tendance changeante des données de séries temporelles a quatre types:

a) tendance: les données changent avec le temps ou en fonction de variables indépendantes, ce qui témoigne d'une tendance relativement lente et à long terme de même nature, c'est-à-dire une augmentation, une diminution ou un état inchangé continus, mais la fourchette de variation peut ne pas être égale;

b) périodicité: un facteur présente progressivement des caractéristiques répétées dans le temps, y compris des crêtes et des creux;

c) caractère aléatoire: les données changent de manière aléatoire, mais la situation globale est statistique;

d) superposition: le changement réel est une superposition ou une combinaison de plusieurs changements.

Voici quelques caractéristiques des comportements des séries temporelles:

1) Nœud: service ou application dans un système ITS qui est utile pour des séries de données temporelles.

2) Flux: indique le temps de façon chronologique.

De nombreuses données appartiennent à des séries de données temporelles, par exemple les messages du gestionnaire de réseau de communication (CAN). Le modèle de données peut être établi avec un ou plusieurs types de données pour trouver le mauvais comportement. Voir la Figure 8.

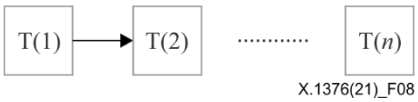


Figure 8 – Modèle de ligne de séries temporelles
T: temps

8.2.1.4 Détection d'intelligence associative

En ce qui concerne la méthode de détection d'intelligence associative, il est possible de détecter un mauvais comportement directement ou indirectement. Les données d'intelligence associative peuvent donc être subdivisées en deux catégories: directes et indirectes.

Intelligence associative directe: il est possible de détecter un mauvais comportement directement sur la base de cette intelligence, par exemple, un rapport sur les vulnérabilités externes, des recherches internes sur la cybersécurité et la divulgation des vulnérabilités courantes.

Intelligence associative indirecte: les mauvais comportements ne peuvent pas être détectés directement sur la base de cette intelligence, car celle-ci est utilisée pour décrire des événements normaux, par exemple la correction de bogues, la mise à disposition de nouvelles fonctionnalités, la mise à jour de logiciels et le remplacement de puces. En associant l'intelligence associative indirecte à d'autres données saisies, il est possible de détecter les mauvais comportements.

8.2.2 Décision

Le présent paragraphe traite de la procédure du sous-module de décision illustrée à la Figure 9.

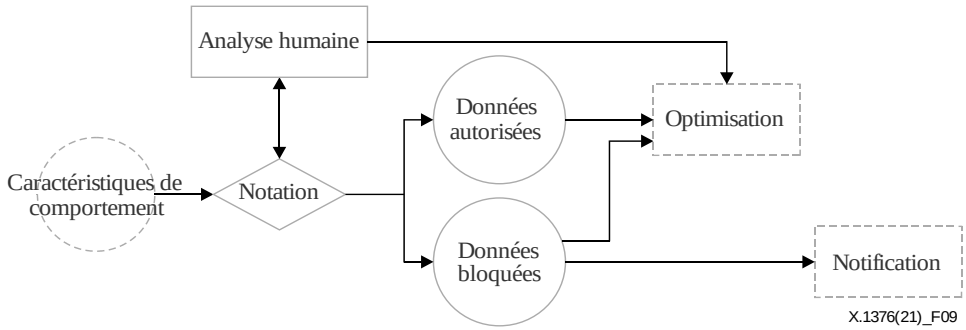


Figure 9 – Procédure du sous-module de décision

Le sous-module de décision est utilisé pour déterminer les résultats des méthodes de détection. Il comprend deux fonctions: la notation et l'analyse humaine. La fonction de notation détermine le type de données par caractéristiques de comportement, puis les note. En cas de mauvais comportement, par exemple un détournement ou une attaque par altération, cette fonction s'écarte du niveau de référence de la stabilité. Si la note ne correspond pas au seuil autorisé ou bloqué, elle sera considérée comme suspecte. Des analystes humains interviendront alors et aideront à prendre une décision jusqu'à ce que la note soit conforme au seuil autorisé ou bloqué.

8.3 Optimisation

L'optimisation est un module de retour d'information qui reçoit des données du moteur de détection et les utilise pour l'optimiser. Voir la Figure 10.

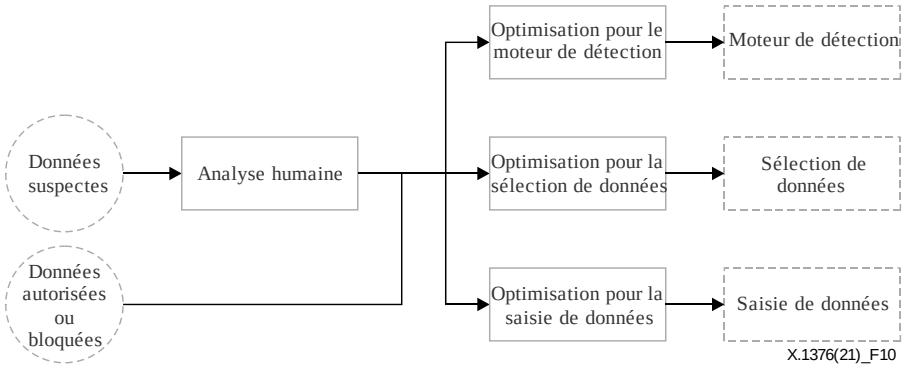


Figure 10 – Procédure liée à l'optimisation

8.3.1 Optimisation pour le moteur de détection

La caractéristique est la valeur clé de chaque donnée transmise dans le flux. Au début de la détection d'un mauvais comportement, les niveaux de référence de la stabilité sont générés par des caractéristiques normales provenant de l'environnement normal. La fonction de notation est initialisée.

Le moteur de détection est optimisé par ses données de sortie. Les méthodes de détection sont ajoutées, modifiées ou supprimées, afin d'améliorer l'efficacité de la détection; la fonction de notation est également optimisée moyennant l'adjonction de nouvelles connaissances issues de l'analyse humaine.

8.3.2 Optimisation pour la sélection de données

Les ensembles de données sont ajoutés, modifiés ou supprimés, afin d'améliorer la précision de la détection.

8.3.3 Optimisation pour la saisie de données

Les données saisies sont ajoutées, modifiées ou supprimées, afin d'améliorer la précision de la détection.

Appendice I

Cas d'utilisation de différentes méthodes de détection

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Le présent Appendice fournit des cas d'utilisation sur la manière de détecter les mauvais comportements en fonction des différentes méthodes de détection décrites au § 8.2.1.

I.1 Cas de la chaîne de statut

Il s'agit d'un cas de détection de la chaîne de statut correspondant au § 8.2.1.1.

Un véhicule possède un module de communication pour accéder à l'internet appelé unité de commande télématique (TCU). Étant donné qu'une unité TCU ne fonctionne pas en permanence, elle passe en mode basse consommation après l'arrêt du moteur du véhicule pour économiser de l'énergie. Avant le passage en mode basse consommation, elle envoie le statut du véhicule à la passerelle du véhicule (service d'arrière-plan), qui synchronise ce statut avec la mémoire cache de l'unité TCU. Le service de commande obtient alors ce statut à partir de la mémoire cache de l'unité TCU. Lorsqu'un utilisateur envoie une commande à son véhicule, le service de commande réagit en fonction du statut de l'unité TCU. Si l'unité TCU est en mode basse consommation, le service de commande envoie une demande au service de sortie du mode veille, qui sort alors l'unité TCU du mode veille. La Figure I.1 illustre un comportement normal. Le Tableau I.1 représente les données de statut concernées dans ce comportement normal.

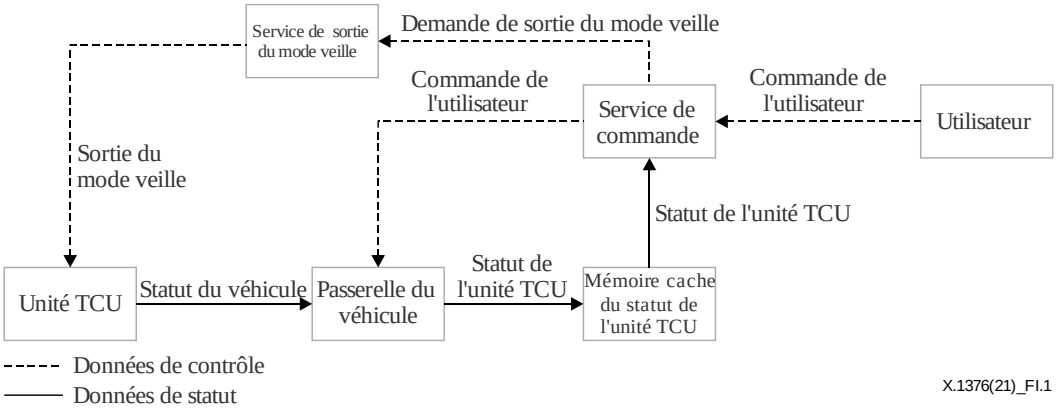


Figure I.1 – Comportement normal de la chaîne de statut

Lorsque les auteurs d'attaques voudront comprendre cette procédure, ils essaieront de modifier le statut de l'unité TCU pour voir les différents comportements que présente le service de commande. Il y aura alors une différence entre la mémoire cache du statut de l'unité TCU et la passerelle du véhicule.

En pareil cas, la détection de la chaîne de statut peut détecter un mauvais comportement en comparant le statut du véhicule dans la passerelle du véhicule et le statut de l'unité TCU dans la mémoire cache du statut de l'unité TCU. Si leurs statuts sont différents, il s'agit d'un mauvais comportement. L'unité TCU ne peut pas être en mode basse consommation lorsque le véhicule est en marche.

Tableau I.1 – Données sur le statut de conduite des véhicules

Noeud	Données
Passerelle du véhicule	Statut du véhicule
Mémoire cache du statut de l'unité TCU	Statut de l'unité TCU
Service de commande	Statut de l'unité TCU

I.2 Cas de flux de contrôle

Il s'agit d'un cas de détection de flux de contrôle correspondant au § 8.2.1.2.

Lorsqu'un utilisateur souhaite contrôler le véhicule à distance, il doit utiliser l'application installée sur son smartphone pour déclencher la fonction. L'application générera un journal des opérations. Ensuite, l'application enverra une demande au service d'interface de programmation d'applications (API) d'arrière-plan, qui enregistrera cette demande dans le journal d'accès. Le service API prétraitera ensuite la demande et la transmettra au point d'extrémité du véhicule, par exemple à l'unité TCU. L'unité TCU demandera un microcontrôleur (MCU) avec l'émetteur-récepteur et enverra une commande à l'exécuteur concerné. Enfin, le déclencheur exécutera la commande de contrôle du côté de l'utilisateur. Voir la Figure I.3. Le Tableau I.2 représente les données de contrôle concernées dans ce comportement normal.

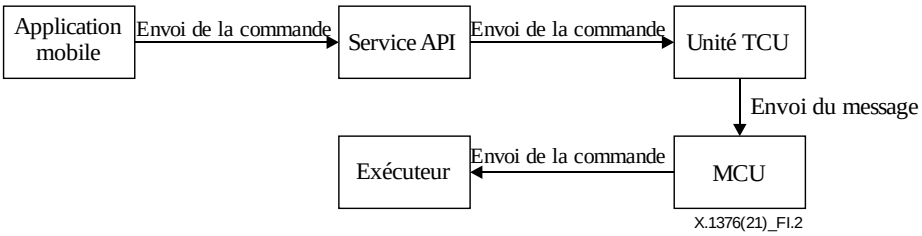


Figure I.2 – Comportement normal du flux de contrôle

En pareil cas, l'unité TCU envoie des messages au MCU uniquement lorsque le service API le demande. Si le MCU est demandé à partir d'un trajet anormal, il n'y aura pas de journal des opérations dans l'application mobile et le service API. Un mauvais comportement est alors détecté.

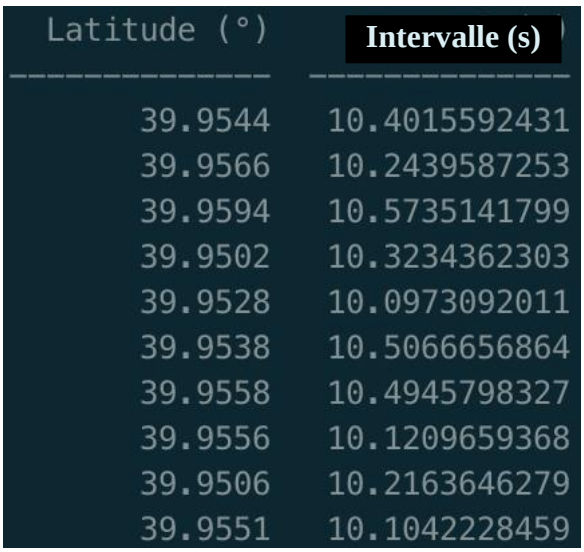
Tableau I.2 – Données de contrôle télématique

Noeud	Données
Application mobile	Journal des opérations
Service API	Journal d'accès
Unité TCU	Données reçues
MCU	Journal de demande
Exécuteur	Journal de l'exécuteur

I.3 Cas de détection de séries temporelles

Il s'agit d'un cas de détection de séries temporelles correspondant au § 8.2.1.3.

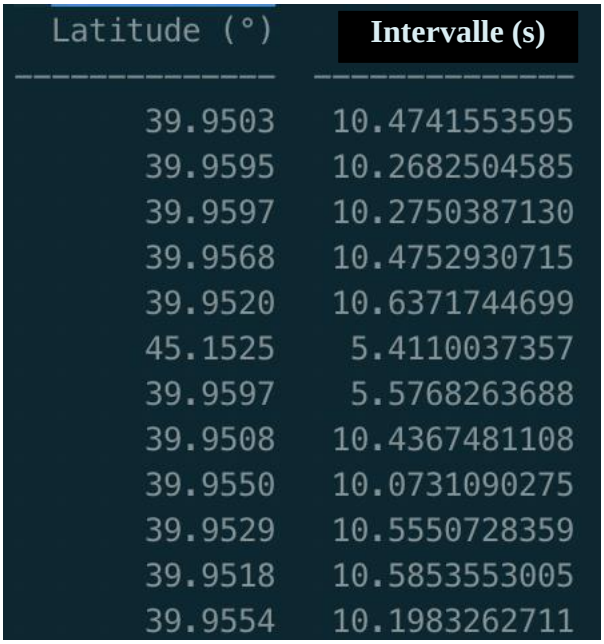
En pareil cas, l'unité TCU envoie périodiquement la position du véhicule au service d'arrière-plan. Voir la Figure I.3.



Latitude (°)	Intervalle (s)
39.9544	10.4015592431
39.9566	10.2439587253
39.9594	10.5735141799
39.9502	10.3234362303
39.9528	10.0973092011
39.9538	10.5066656864
39.9558	10.4945798327
39.9556	10.1209659368
39.9506	10.2163646279
39.9551	10.1042228459

Figure I.3 – Séries temporelles normales de position

Si un capteur du système mondial de navigation par satellite (GNSS) se trouve dans une situation d'usurpation d'identité, les informations relatives à la position et l'intervalle seront manifestement différentes des données précédentes. Voir la Figure I.4.



Latitude (°)	Intervalle (s)
39.9503	10.4741553595
39.9595	10.2682504585
39.9597	10.2750387130
39.9568	10.4752930715
39.9520	10.6371744699
45.1525	5.4110037357
39.9597	5.5768263688
39.9508	10.4367481108
39.9550	10.0731090275
39.9529	10.5550728359
39.9518	10.5853553005
39.9554	10.1983262711

Figure I.4 – Séries temporelles normales de position en cas de mauvais comportement

Le Tableau I.3 présente les données des séries temporelles courantes dans le véhicule.

Tableau I.3 – Données des séries temporelles des capteurs automatiques

Noeud	Données
Service d'arrière-plan	Latitude, Intervalle

I.4 Cas de détection d'intelligence associative

Il existe deux cas de détection d'intelligence associative pour le § 8.2.1.4, de sorte que deux cas d'utilisation sont prévus, un pour chaque cas.

I.4.1 Cas de détection d'intelligence associative directe

Pour détecter un mauvais comportement, le moyen le plus simple, dans un véhicule connecté, est de recourir à l'intelligence associative directe. Toutes les formes d'intelligence associative directe permettent de détecter directement un mauvais comportement, par exemple l'adresse IP, le nom de domaine, l'adresse URL, les recherches internes sur la cybersécurité et le rapport sur les vulnérabilités externes. Toutes ces données comportent une caractéristique absolue permettant de détecter un mauvais comportement.

Le Tableau I.4 présente les formes courantes d'intelligence associative directe dans un système ITS.

Tableau I.4 – Données de détection d'intelligence associative directe

Noeud	Données
Système d'infoloisirs embarqué	Adresse IP URL Nom de domaine
Base de données d'intelligence	Rapport sur les vulnérabilités externes Recherches internes sur la cybersécurité

I.4.2 Cas de détection d'intelligence associative indirecte

L'intelligence associative indirecte ne peut pas être utilisée pour détecter un mauvais comportement de manière indépendante, mais peut être associée à d'autres sources d'intelligence. Dans certains cas, une seule vulnérabilité ne peut pas être exploitée, mais l'auteur d'une attaque peut utiliser plusieurs vulnérabilités pour construire une chaîne d'exploitation afin de parvenir à l'exploitation. Par exemple, tous les fournisseurs ne corrigent pas les vulnérabilités de façon qu'elles ne puissent pas être exploitées. Lorsque le moteur de détection reçoit un nouveau rapport technique sur le chaînage, il est possible d'obtenir une exécution de code arbitraire sur la base des publications [b-CVE-2017-11906] et [b-CVE-2017-11907]; la version du navigateur dans le système d'infoloisirs embarqué est saisie en vue d'être utilisée conjointement avec des données intelligentes pour détecter un mauvais comportement.

Le Tableau I.5 présente les formes courantes d'intelligence associative indirecte dans un système ITS.

Tableau I.5 – Données de détection d'intelligence associative indirecte

Noeud	Données
Base de données d'intelligence	Système d'infoloisirs embarqué Rapport technique externe

Bibliographie

[b-ISO/TR 17427-4] ISO/TR 17427-4:2015, *Systèmes intelligents de transport – Systèmes intelligents de transport coopératifs – Partie 4: Exigences minimales du système et comportement des systèmes principaux.*

[b-CVE-2017-11906] Vulnérabilités et expositions courantes, CVE-2017-11906 (2017). *Internet Explorer information disclosure vulnerability*. Bedford, MA: Mitre Corporation. Disponible [consulté le 21/02/2021] à l'adresse: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11906.

[b-CVE-2017-11907] Vulnérabilités et expositions courantes, CVE-2017-11907 (2017). *Scripting engine memory corruption vulnerability*. Bedford, MA: Mitre Corporation. Disponible [consulté le 21/02/2021] à l'adresse: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11907.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2021