Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1376

(01/2021)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Aplicaciones y servicios seguros (2) – Seguridad de los sistemas de transporte inteligentes (STI)

Mecanismo de detección de conductas indebidas relacionadas con la seguridad mediante macrodatos para vehículos conectados

Recomendación UIT T X.1376

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (STI)	**X.1370–X.1379**
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
SEGURIDAD DE 5G	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1376

Mecanismo de detección de conductas indebidas relacionadas con la seguridad mediante macrodatos para vehículos conectados

Resumen

En la Recomendación UIT-T X.1376 se describe un mecanismo de detección de conductas indebidas relacionadas con la seguridad para los vehículos conectados, destinado a ayudar a las partes interesadas a utilizar los datos de automoción para mejorar la seguridad de los vehículos.

A medida que aumenta la conectividad de los vehículos, el número de vulnerabilidades aumenta debido al desarrollo de una tecnología compleja. Estas vulnerabilidades traen consigo más amenazas para los vehículos conectados. El análisis de una gran cantidad de datos de automoción resulta de gran utilidad útil para evaluar la seguridad de los vehículos conectados.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1376	01-07-2021	17	11.1002/1000/14448

Palabras clave

Vehículos conectados, detección de conductas indebidas.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente o derecho de autor, que pueda ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT-T disponibles en el sitio web del UIT-T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1376

Mecanismo de detección de conductas indebidas relacionadas con la seguridad mediante macrodatos para vehículos conectados

1 Alcance

En la presente Recomendación se describe un mecanismo de detección de conductas indebidas relacionadas con la seguridad para los vehículos conectados. El mecanismo incluye los siguientes pasos:

a) Recopilación de datos. Especificación de los tipos de datos e información que pueden ser recopilados a partir de diferentes fuentes, incluyendo la industria automotriz y de infraestructuras, y los proveedores y fabricantes de equipos originales, para la detección de conductas indebidas. Los métodos y procedimientos de recopilación de datos quedan fuera del ámbito de esta Recomendación.

b) Detección. Análisis de los datos recopilados para detectar conductas indebidas.

La presente Recomendación se aplica a los vehículos conectados para que los diseñadores y proveedores de soluciones de seguridad detecten comportamientos indebidos. Los métodos de utilización de las notificaciones quedan fuera del alcance de esta Recomendación.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se alienta a los usuarios de esta Recomendación a que investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

Ninguno.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se define el término siguiente:

3.2.1 Conducta indebida: Proporcionar datos falsos o engañosos de manera que se obstaculice a otras personas a recibir una prestación de servicios o que se opere fuera del ámbito autorizado. Las conductas indebidas pueden deberse a componentes internos o externos del sistema del vehículo.

NOTA 1 – Basado en [b-ISO/TR 17427-4].

NOTA 2 – Las conductas indebidas incluyen comportamientos sospechosos como en tipos de mensajes o frecuencias equivocadas, inicios de sesión inválidos y accesos no autorizados, o mensajes firmados o encriptados incorrectos, ya sean intencionados o no.

4 Abreviaturas y acrónimos

Esta Recomendación utiliza las siguientes abreviaturas y acrónimos:

ADAS Sistema avanzado de asistencia al conductor (*Advanced Driver-Assistance Systems*)

ABS Sistema de frenado antideslizante (*Anti-skid Braking System*)

AEB Frenado de emergencia autónomo (*Autonomous Emergency Braking*)

API Interfaz de programación de aplicaciones (*Application programming interface*)

CAN Red de controlador de zona (*Controller Area Network*)

GNSS Sistema mundial de navegación por satélite (*Global navigation satellite system*)

ITS Sistemas de transporte inteligente (*Intelligent transport systems*)

IP Protocolo Internet (*Internet protocol*)

LiDAR Detección y localización por ondas luminosas (*Light Detection and Ranging*)

MCU Unidad de microcontrolador (*Microcontroller Unit*)

OEM Fabricante de equipo original (*Original Equipment Manufacturer*)

TCU Unidad de control electrónico (*Telematics Control Unit*)

URL Localizador uniforme de recursos (*Uniform resource locator*)

5 Convenios

Ninguno.

6 Modelo de mecanismo de detección de conductas indebidas

En la Figura 1 se presenta el modelo del mecanismo de detección de conductas indebidas para los vehículos conectados. El mecanismo consta de dos pasos, la recopilación y detección de datos, que se aplican mediante dos sistemas.

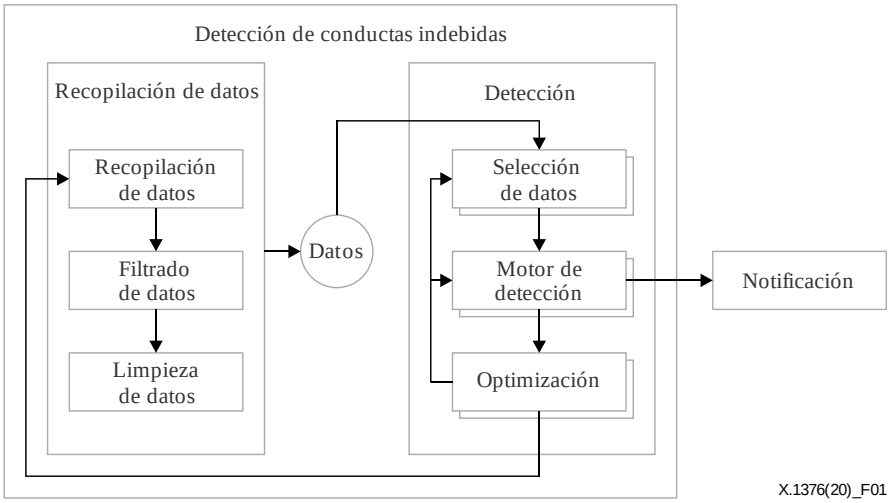


Figura 1 – Modelo de mecanismo de detección de conductas indebidas

Como los métodos y procedimientos de recopilación de datos quedan fuera del ámbito de aplicación de la presente Recomendación, el sistema de recopilación de datos (por ejemplo, el filtrado y la depuración de datos) de la Figura 1 es solo un ejemplo informativo de una aplicación práctica de la detección de conductas indebidas.

Los datos del sistema de recopilación se envían al sistema de detección, y la recopilación de datos se procesa según los tipos descritos en la sección 7.

El sistema de recopilación de datos incluye los siguientes módulos:

a) recopilación de datos: recopilación de datos para detección a partir de diferentes fuentes, por ejemplo, proveedores de servicios, sistemas corporales y sensores;

b) filtrado de datos: filtrado de datos recopilados en función de la clasificación de datos;

c) limpieza de datos: operaciones de deduplicación y reducción de ruido de los datos recopilados.

El sistema de detección incluye los siguientes módulos:

a) selección de datos: selección de conjuntos de datos basados en diferentes métodos de detección de conductas indebidas, y posterior envío al motor de detección;

b) motor de detección: detección de conductas indebidas basándose en métodos de detección, y envío posterior de los resultados de la decisión a los módulos de optimización y notificación, según proceda;

c) optimización: uso de resultados de la detección del motor de detección para mejora de la selección de datos, el motor de detección y la recopilación de datos.

La notificación es un módulo que envía los resultados del motor de detección a las partes interesadas. Queda fuera del alcance de la presente Recomendación.

7 Recopilación de datos

La recopilación de datos suele constar de recopilación de datos, limpieza de datos y filtrado de datos. Como los métodos y procedimientos de recopilación de datos quedan fuera del alcance de la presente Recomendación, solo se abordarán los tipos de datos utilizados en el procedimiento de detección. Todos los datos personales confidenciales deberían protegerse mediante tecnologías adecuadas, como la anonimización, la cual queda fuera del alcance de la presente Recomendación.

Sobre la base de los datos y la información recopilados a partir de diferentes fuentes, en la presente sección se especifican los tipos utilizados en el mecanismo de detección de conductas indebidas, a saber, datos de situación, datos de control y datos de inteligencia, como se muestra en el Cuadro 1.

Cuadro 1 – Tipos de datos

Tipo	Subtipo	Fuentes de datos	Ejemplos de datos
Datos de estado[a]	Datos de aplicación o servicio	Proveedor de contenido o proveedor de servicios	Datos de información y diversión
		Datos de servicio de mapas	Navegación, posicionamiento
		Datos de aplicaciones móviles	Datos relacionados con aplicaciones
	Estado del vehículo	Sistema de seguridad	Sistema de frenado antideslizante (ABS), airbag, frenado de emergencia autónomo (AEB), sistemas avanzados de asistencia al conductor (ADAS)
		Sistema corporal	Puerta, ventana, limpiaparabrisas
		Sistema de chasis	Par de torsión, curva

Cuadro 1 – Tipos de datos

Tipo	Subtipo	Fuentes de datos	Ejemplos de datos
		Sistema de energía	Velocidad, velocidad de rotación, válvula del acelerador, calado
	Sensores ambientales	Radar	Radar de ondas milimétricas
		Detección y localización por ondas luminosas (LiDAR)	Nube de puntos
		Sensores ultrasónicos	Distancia
		Cámara	Imagen envolvente
		Sensores de sistemas de transporte inteligente (ITS)	Señal de instalaciones en carretera
Datos de control[b]	Control local	Controlador en vehículo	Apertura de puerta, cierre de puerta
	Mando a distancia	Automatización, telemática	Diagnóstico remoto
Datos de inteligencia[c]	Datos de inteligencia interna	Investigación de seguridad, resultados de pruebas	Vulnerabilidades, errores, problemas internos de ciberseguridad
	Comunicación de datos de inteligencia al exterior	Cliente, proveedor, comunidad, conferencia o literatura, web	Dirección del Protocolo Internet (IP), valores generadores (hash), localizador uniforme de recursos (URL), nombre de dominio, vulnerabilidades y exposiciones comunes (CVE), etc.

[a] Datos e información relacionados con el estado de los vehículos, aplicaciones, servicios, sensores y otras instalaciones en un ITS.

[b] Datos e información utilizados para controlar vehículos, aplicaciones, servicios, sensores y otras instalaciones en un ITS.

[c] Datos e información relacionados con la ciberseguridad obtenidos desde fuera de un ITS. Se supone que las fuentes de los datos tienen el nivel de integridad adecuado.

8 Detección

El módulo de detección consiste principalmente en la selección de datos, el motor de detección y la optimización. Como se muestra en la figura 2, a partir de datos e información de diferentes fuentes, el motor de detección analiza macrodatos para detectar conductas indebidas. En la optimización se utilizan las conductas indebidas para optimizar la selección de datos y el motor de detección hace que la detección de las conductas indebidas sea más precisa y eficiente.

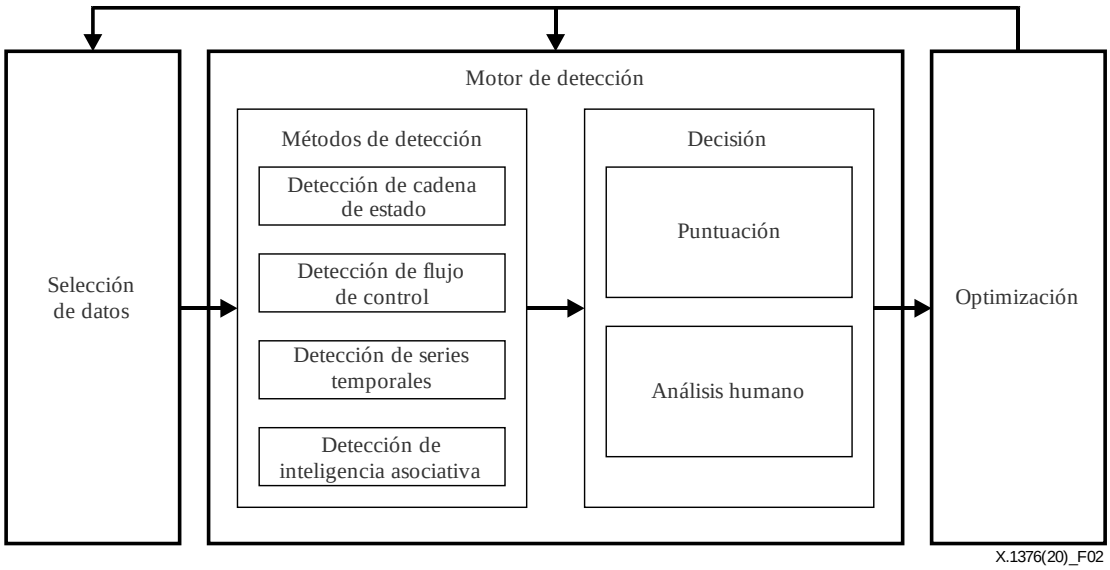


Figura 2 – Procedimiento de detección

8.1 Selección de datos

Sobre la base de los diferentes requisitos de datos de los métodos de detección, en el módulo de selección de datos se clasifican los datos en diferentes conjuntos según los requisitos de los motores de detección, como se muestra en la Figura 3. Los datos que entran en el módulo de selección de datos son los datos del sistema de recopilación.

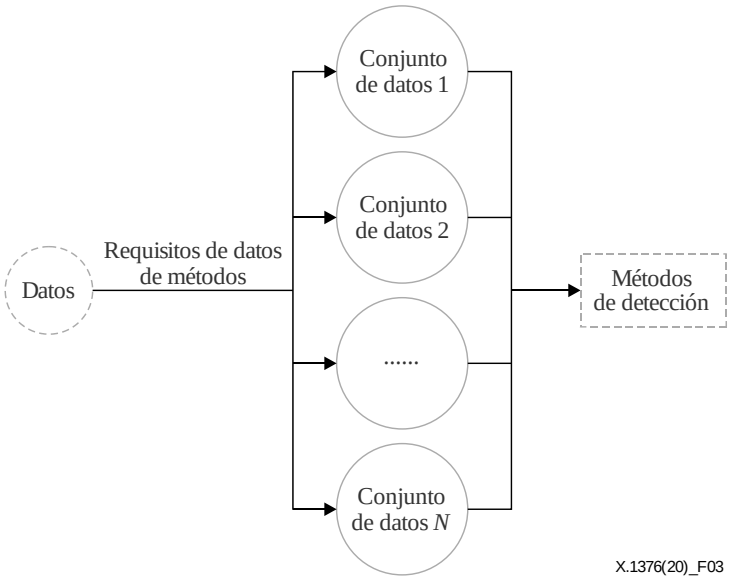


Figura 3 – Procedimiento de selección de datos

8.2 Motor de detección

El motor de detección consta de dos submódulos: métodos de detección y decisión. Cuando los conjuntos de datos llegan al submódulo de métodos de detección, los métodos los transforman en rasgos de comportamiento. Será entonces cuando el submódulo de decisión tomará una decisión basada en los rasgos de comportamiento. Hay tres tipos diferente de resultados de decisión: bloqueado; sospechoso; y permitido. Un resultado bloqueado significa que es anómalo; un resultado sospechoso significa que no puede determinarse si se niegan los datos o estos son seguros; y un resultado permitido significa que los datos son seguros.

8.2.1 Métodos de detección

El submódulo de métodos de detección es un conjunto de diferentes métodos de detección. Sobre la base de los tipos de datos clasificados en la sección 7, se han diseñado cuatro métodos para detectar conductas indebidas utilizando esos datos.

8.2.1.1 Detección de la cadena de estado

La cadena de estado contiene una serie de datos de estado correlacionados. En la cadena de estado, el cambio de un dato supone el cambio simultáneo de otros datos.

A continuación se presentan algunas características de la cadena de estado:

a) nodo: un servicio o una aplicación en un ITS que es relevante para una acción;

b) flujo: la dirección y el trayecto de los datos cambiantes como consecuencia de una acción.

Los datos de estado se generan en un ITS y puede crearse un contexto con esos datos. El valor de los datos también sigue una cierta tendencia y fluctúa dentro de un cierto rango.

En esencia, la cadena de estado puede dividirse en dos modelos: línea y rama. Los dos modelos son los siguientes:

1) línea: cada nodo tiene solo un nodo que recibe su señal;

2) rama: un nodo genera dos o más datos de estado al mismo tiempo y luego los envía a diferentes nodos.

En el modelo de línea de una cadena de estado, los nodos solo tienen una conexión unidireccional. Véase la Figura 4.

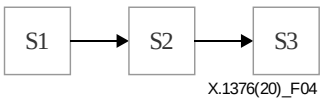


Figura 4 – Modelo de línea de la cadena de estado
S: estado

En el modelo de rama de una cadena de estado, los nodos pueden bifurcarse en dos o más modelos de línea relevantes. Véase la Figura 5.

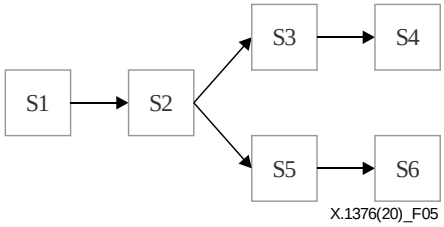


Figura 5 – Modelo de rama de cadena de estado

De este modo, los rasgos de cada nodo incluyen:

i) el contexto en la cadena de estado;

ii) el valor y la tendencia de cada nodo.

Se obtienen los rasgos de los nodos de la cadena de estado y se envían a la función de puntuación.

8.2.1.2 Detección del flujo de control

El flujo de control contiene una serie de datos de control correlacionados. En el flujo de control, un comando de control puede estar compuesto por múltiples comandos de subcontrol y afectará a múltiples sistemas.

A continuación se describen algunas características del flujo de control para describir la ejecución del comando de control:

a) nodo: un servicio o una aplicación en el ITS que sea relevante para una acción;

b) flujo: la dirección y el trayecto de los datos cambiantes como consecuencia de una acción.

Cuando se lleva a cabo una acción de control, los datos relacionados con el control pasarán a través de los nodos relacionados con el control y formarán un flujo de control.

Cada nodo de control funciona de forma estable y regular en un ITS. Cuando muchos nodos trabajan juntos, el flujo de control también es estable en su comportamiento debido al período prescrito, los tipos determinados y el número de mensajes.

En esencia, el flujo de control puede dividirse en dos modelos: línea y rama. Los dos modelos son los siguientes:

1) línea: cada nodo tiene solo un nodo que recibe su señal;

2) rama: un nodo genera dos o más datos de control al mismo tiempo, y luego los envía a diferentes nodos.

En el modelo de línea de flujo de control, los nodos solo tienen una conexión unidireccional. Véase la Figura 6.

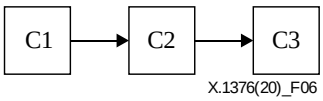


Figura 6 – Modelo de línea de flujo de control
C: control

En el modelo de rama de flujo de control, los nodos pueden bifurcarse en dos o más modelos de línea relevantes. Véase la Figura 7.

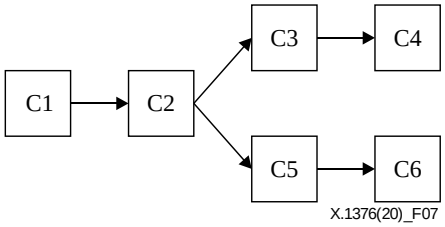


Figura 7 – Modelo de rama de flujo de control

8.2.1.3 Detección de series temporales

Se utiliza una serie temporal para describir los datos que cambian según el tipo. Siempre que los datos estén de acuerdo con los tipos, podrá utilizarse la detección de series temporales.

La tendencia cambiante de los datos de las series temporales tiene cuatro tipos:

a) tendencia: los datos cambian con el tiempo o con variables independientes, mostrando una tendencia relativamente lenta y a largo plazo de la misma naturaleza de continuo aumento, disminución o permanencia, pero el rango de cambio puede no ser igual;

b) periodicidad: un factor muestra gradualmente características repetidas a lo largo del tiempo, incluyendo picos y bajos;

c) aleatoriedad: los datos cambian aleatoriamente, pero la situación general es estática;

d) superposición: el cambio real es una superposición o combinación de varios cambios.

A continuación se presentan algunas características de los comportamientos de series temporales:

1) nodo: un servicio o una aplicación en el ITS que sea relevante para los datos de series temporales;

2) flujo: indica el tiempo cronológico.

Muchos datos pertenecen a series temporales, por ejemplo, los mensajes de la red de controlador de zona. El modelo de datos puede establecerse con uno o más tipos de datos para encontrar las conductas indebidas. Véase la Figura 8.

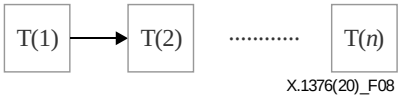


Figura 8 – Modelo lineal de series temporales
T: tiempo

8.2.1.4 Detección de inteligencia asociativa

En el caso del método de detección de inteligencia asociativa, las conductas indebidas pueden detectarse directa o indirectamente. Por consiguiente, los datos de inteligencia asociativa pueden dividirse en dos categorías: directos e indirectos.

Inteligencia asociativa directa: las conductas indebidas pueden detectarse directamente sobre la base de esta información, por ejemplo el informe sobre vulnerabilidades externas, la investigación interna sobre ciberseguridad y la divulgación de vulnerabilidades comunes.

Inteligencia asociativa indirecta: las conductas indebidas no pueden detectarse directamente sobre la base de esta inteligencia, ya que esta se utiliza para describir eventos normales, por ejemplo la corrección de errores, el lanzamiento de nuevas características, la actualización de software y la sustitución de chips. Combinando la inteligencia asociativa indirecta con otros datos recopilados, pueden detectarse conductas indebidas.

8.2.2 Decisión

En la siguiente Figura 9 se describen los principales submódulos de decisión.

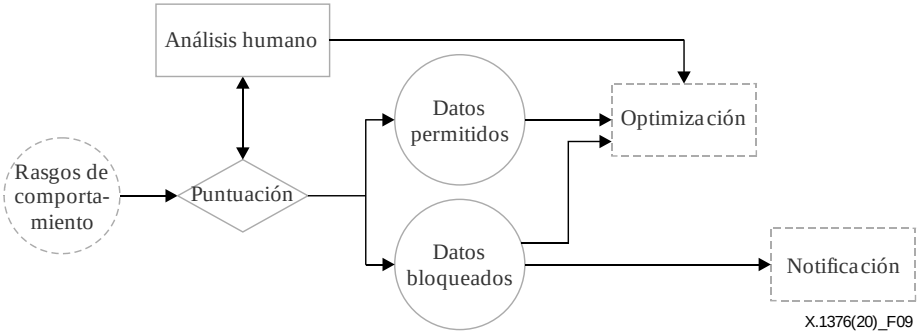


Figura 9 – Procedimiento en el submódulo de decisión

El submódulo de decisión se utiliza para determinar los resultados de los métodos de detección. Incluye dos funciones: puntuación y análisis humano. Con la función de puntuación se determina el tipo de datos por los rasgos de comportamiento, y luego se puntúan. Si se producen conductas indebidas, como un pirateo o un ataque de manipulación, se desvía de la línea de base de estabilidad. Si la puntuación no puede alcanzar el umbral permitido o bloqueado, será clasificada como sospechosa. Los analistas humanos actuarán entonces y ayudarán a tomar una decisión hasta que la puntuación alcance el umbral permitido o bloqueado.

8.3 Optimización

La optimización es un módulo de retroalimentación que recibe datos del motor de detección y los utiliza para optimizarlo. Véase la figura 10.

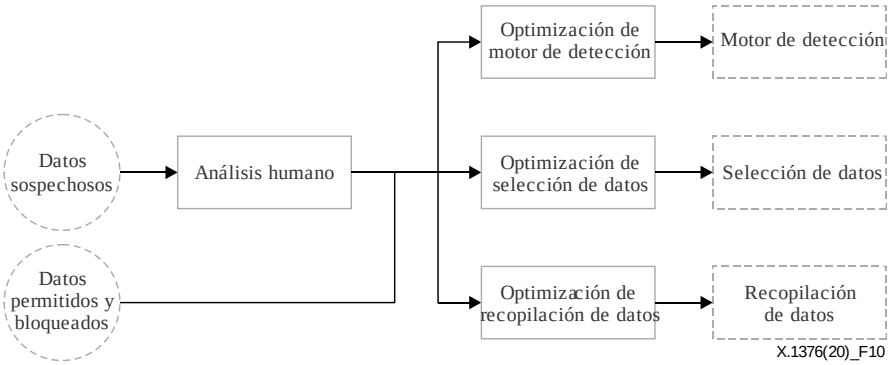


Figura 10 – Procedimiento en optimización

8.3.1 Optimización del motor de detección

El rasgo es el valor clave en cada dato transmitido en el flujo. Al principio de la detección de conductas indebidas, las líneas de base de estabilidad se generan por rasgos normales del entorno normal. La función de puntuación se inicializa.

El motor de detección se optimiza por sus productos. Los métodos de detección se añaden, modifican o eliminan para mejorar la eficiencia de la detección; la función de puntuación también se optimiza mediante la adición de nuevos conocimientos derivados del análisis humano.

8.3.2 Optimización de la selección de datos

Los conjuntos de datos se añaden, modifican o eliminan para mejorar la precisión de la detección.

8.3.3 Optimización de la recopilación de datos

Los datos recopilados se añaden, modifican o eliminan para mejorar la precisión de la detección.

Apéndice I

Casos de uso de métodos de detección diferentes

(Este Apéndice no forma parte integrante de la presente Recomendación.)

En el presente apéndice se muestran casos de uso de cómo detectar conductas indebidas, de conformidad con los diferentes métodos de detección de la sección 8.2.1.

I.1 Caso de la cadena de estado

Este es un caso de detección de la cadena de estado de la sección 8.2.1.1.

Un vehículo tiene un módulo de comunicación para acceder a Internet llamado unidad de control telemático (TCU). La TCU no funciona todo el tiempo, por lo que cambia al modo de baja potencia cuando el motor del vehículo se detiene para ahorrar energía. Antes del modo de bajo consumo, envía el estado del vehículo a la pasarela de vehículo (servicio auxiliar), la cual sincroniza ese estado con la caché de estado de la TCU. El servicio de comando obtiene este estado de la caché de estado de la TCU. Cuando un usuario envía un comando a su vehículo, el servicio de comando reacciona según el estado de la TCU. Si la TCU está en modo de baja potencia, el servicio de comando envía una solicitud al servicio de despertador, que despierta entonces a la TCU. En la Figura I.1 se muestra el comportamiento normal. En el Cuadro I.1 se muestran los datos de estado que intervienen en ese comportamiento normal.

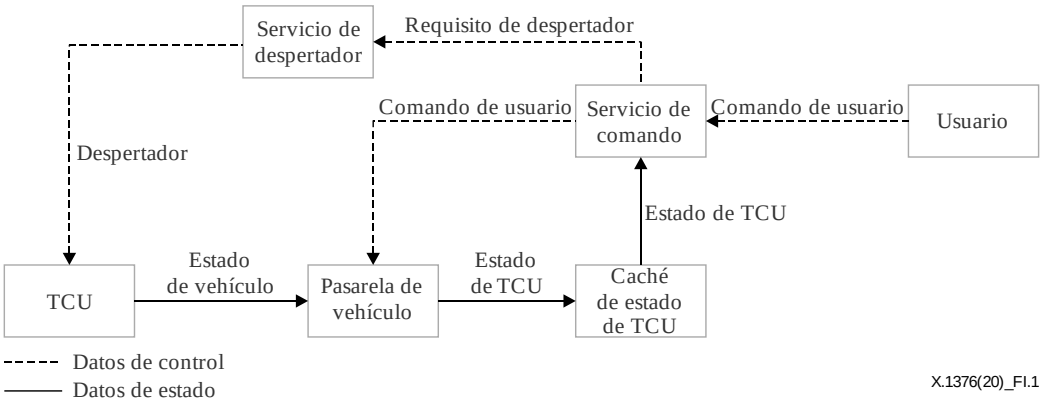


Figura I.1 – Comportamiento normal de la cadena de estado

Cuando los atacantes quieran conocer este procedimiento, intentarán modificar el estado de la TCU para ver los diferentes comportamientos que exhibe el servicio de comando. Entonces habrá una diferencia entre el caché del estado de la TCU y la pasarela de vehículos.

En ese caso, la detección de la cadena de estado puede detectar conductas indebidas comparando el estado del vehículo en la pasarela de vehículos con el estado de la TCU en la caché de estado de la TCU. Si sus estados son diferentes, se tratará de conductas indebidas. La TCU no puede estar en modo de baja potencia cuando el vehículo esté en marcha.

Cuadro I.1 – Datos de estado de conducción de vehículo

Nodo	Datos
Pasarela de vehículo	Estado del vehículo
Caché de estado de la TCU	Estado de la TCU
Servicio de comando	Estado de la TCU

I.2 Caso de flujo de control

Se trata de un caso de detección de flujo de control de la sección 8.2.1.2.

Cuando un usuario quiere controlar el vehículo a distancia, tendrá que utilizar la aplicación instalada en su teléfono inteligente para activar la función. La aplicación generará un registro de operaciones. A continuación, la aplicación enviará una solicitud al servicio de la interfaz de programación de aplicaciones (API) auxiliar, que registrará esa solicitud en el registro de acceso. El servicio API tratará por anticipado entonces la solicitud y la remitirá al punto final del vehículo, por ejemplo, la TCU. La TCU invocará una unidad de microcontrolador (MCU) con el transceptor y enviará una orden al ejecutor correspondiente. Por último, el accionador ejecutará el comando de control desde el lado del usuario. Véase la Figura I.2. El Cuadro I.2 muestra los datos de control que intervienen en ese comportamiento normal.

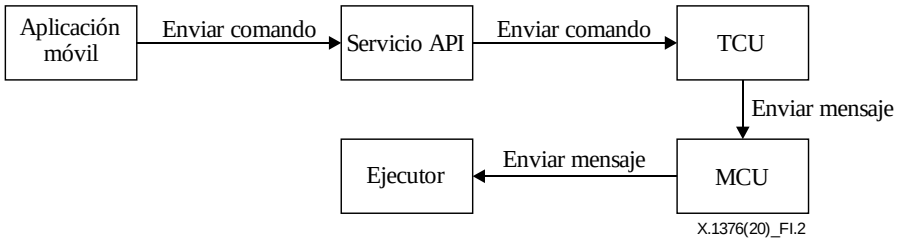


Figura I.2 – Comportamiento normal del flujo de control

En este caso, la TCU envía mensajes a la MCU solo cuando el servicio API así lo solicita. Si se invoca a la MCU desde un trayecto anormal, no habrá registro de operaciones en la aplicación móvil ni en el servicio API. Será entonces cuando se detecte una conducta indebida.

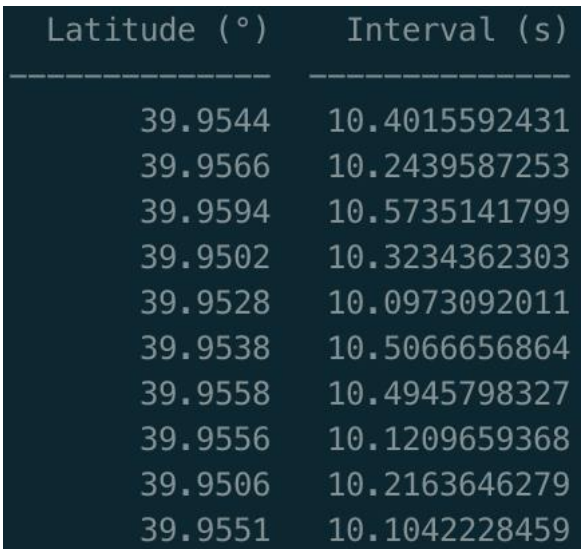
Cuadro I.2 – Datos de control telemático

Nodo	Datos
Aplicación móvil	Registro de operaciones
Servicios API	Registro de acceso
TCU	Datos recibidos
MCU	Registro de invocación
Accionador	Registro de accionador

I.3 Caso de serie temporal

Este es un caso de detección de series temporales de la sección 8.2.1.3.

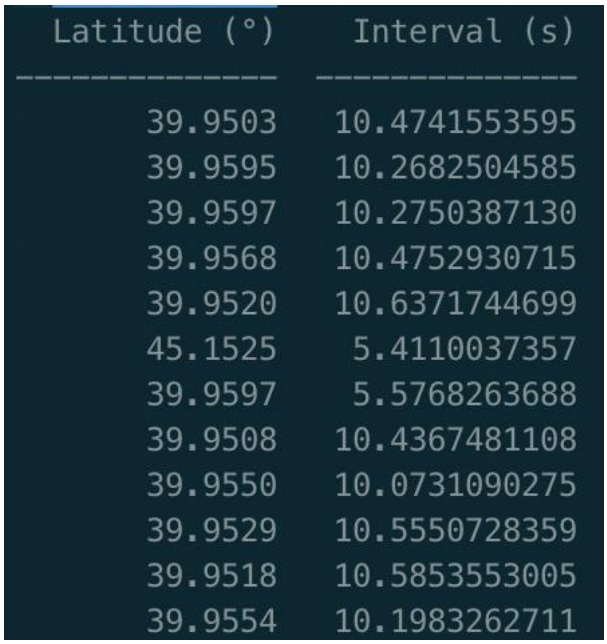
En este caso, la TCU envía la posición del vehículo al servicio auxiliar de forma periódica. Véase la Figura I.3.



Latitude (°)	Interval (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

Figura I.3 – Serie temporal normal de posición

Si un sensor del sistema mundial de navegación por satélite (GNSS) se encuentra en una situación de falsificación, la información de posición y el intervalo tendrán una diferencia obvia con los datos anteriores. Véase la Figura I.4.



Latitude (°)	Interval (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

Figura I.4 – Serie temporal de conductas indebidas de posición

El Cuadro I.3 muestra los datos comunes de series temporales en el vehículo.

Cuadro I.3 – Datos de series temporales de sensor automatizado

Nodo	Datos
Servicio auxiliar	Latitud, Intervalo

I.4 Caso de detección de inteligencia asociativa

Hay dos casos de detección de inteligencia asociativa para la sección 8.2.1.4, por lo que se proporcionan dos casos de uso, uno para cada una.

I.4.1 Caso de detección de inteligencia asociativa directa

Detectar conductas indebidas a partir de la inteligencia asociativa directa es más fácil en un vehículo conectado. Todas las formas de inteligencia asociativa directa apuntan directamente a conductas indebidas, por ejemplo dirección IP, nombre de dominio, URL, investigación interna sobre ciberseguridad e informe sobre vulnerabilidades externas. Cualquiera de esos datos incluye un rasgo absoluto para detectar conductas indebidas.

El Cuadro I.4 muestra inteligencias asociativas directas comunes en el ITS.

Cuadro I.4 – Datos de detección de inteligencia asociativa directa

Nodo	Datos
Sistema de información y diversión en vehículo	Dirección IP URL Nombre de dominio
Base de datos de inteligencia	Informe sobre vulnerabilidades externas Investigación interna de ciberseguridad

I.4.2 Caso de detección de inteligencia asociativa indirecta

La inteligencia asociativa indirecta no puede utilizarse para detectar conductas indebidas de forma independiente, pero puede combinarse con otras fuentes de inteligencia. En algunas circunstancias, aunque un atacante no pueda aprovecharse de una sola vulnerabilidad podrá utilizar varias vulnerabilidades para construir una cadena de explotación eficaz. Por ejemplo, no todos los proveedores arreglan las vulnerabilidades para que no puedan ser explotadas. Cuando el motor de detección recibe un nuevo informe técnico sobre el encadenamiento, [b-CVE-2017-11906] y [b-CVE-2017-11907] pueden llegar a la ejecución de códigos arbitraria; la versión del navegador en el sistema de información y diversión en el vehículo se recopila para ser utilizada junto con los datos inteligentes para detectar conductas indebidas.

El Cuadro I.5 muestra las inteligencias asociativas indirectas comunes en el ITS.

Cuadro I.5 – Datos de detección de inteligencia asociativa indirecta

Nodo	Datos
Base de datos de inteligencia	Sistema de información y diversión en vehículo Informe técnico externo

Bibliografía

[b-ISO/TR 17427-4] ISO/TR 17427-4:2015, *Intelligent transport systems – Cooperative ITS – Part 4: Minimum system requirements and behaviour for core systems*.

[b-CVE-2017-11906] Vulnerabilidades y riesgos corrientes (*CVE*) -*2017-11906* (2017). *Internet Explorer information disclosure vulnerability*. Bedford, MA: Mitre Corporation. Disponible [consultado el 21-02-2021] en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11906.

[b-CVE-2017-11907] Vulnerabilidades y riesgos corrientes (*CVE*) -*2017-11907* (2017). *Scripting engine memory corruption vulnerability*. Bedford, MA: Mitre Corporation. Disponible [consultado el 21-02-2021] en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11907.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2021