rac.2023.112.1.org06
RACSG.2023;112(01):67-79
Recibido: 01/03/2022 | Aceptado: 12/05/2023

ORIGINAL

MATEMÁTICAS Y VEHÍCULOS AUTÓNOMOS

MATHEMATICS AND AUTOMATED DRIVING SYSTEMS

David Ríos Insua[1,2]; Roi Naveiro[3]
1. Académico de Número de la RAC.
2. Instituto de Ciencias Matemáticas, CSIC.
3. CUNEF Universidad.

RESUMEN
Los vehículos autónomos se están desarrollando rápidamente. Sin embargo, quedan numerosos problemas por resolver hasta garantizar la adopción masiva de esta tecnología. Muchos pueden asimilarse a problemas de decisión estadística. Aquí presentamos varios desafíos estadísticos que surgen al diseñar y operar vehículos autónomos. Para cada uno de estos problemas, se proporciona una solución inicial acompañada de una evaluación empírica de la misma.

Palabras clave: Vehículos autónomos; Análisis bayesiano; Toma de decisiones éticas; Tráfico heterogéneo; Aprendizaje automático adversario.

ABSTRACT
Automated driving systems are rapidly developing. However, their continued maturation is not inevitable. Numerous problems remain to be resolved to ensure this technology progresses. A large subset of these problems can be framed as statistical decision problems. Therefore, we present herein several important statistical challenges that emerge when designing and operating automated driving systems. For each of them, initial solution approaches are provided with accompanying empirical testing.

Keywords: Automated driving system; Bayesian analysis; Ethical decision making; Heterogeneus traffic; Adversarial machine learning.

Correspondencia
David Ríos Insua
Real Academia de Ciencias Exactas, Físicas y Naturales de España
Calle Valverde, 22 · 28004 · Madrid, España
E-mail: secretaria@rac.es

INTRODUCCIÓN

Las capacidades de los vehículos autónomos (VA) han crecido enormemente durante la última década. Los avances recientes en inteligencia artificial (IA), matemáticas y hardware permiten ya ejecutar algoritmos de control y percepción avanzados en tiempo real. Estos, combinados con la evolución sobre el concepto de propiedad del vehículo y la electrificación de los mismos, sugieren que se acerca un cambio de paradigma en el transporte caracterizado por menos accidentes, menos contaminación, menores tiempos de viaje y mayores oportunidades de movilidad (Burns & Shulgan 2019). Pero tal futuro está aún por forjar y para ello deben resolverse importantes desafíos matemáticos relacionados con la presencia de innumerables fuentes de incertidumbre en la operación y gestión de los VAs. Como ejemplo, la presencia de precipitaciones complica el funcionamiento de las cámaras y LIDARs que equipan al VA, produciendo errores en sus datos de entrada. Además, dado que los seres humanos cohabitan en el entorno de un VA, su presencia y su comportamiento también deben evaluarse, especialmente cuando se consideran las interacciones de un VA con otros conductores, peatones y vehículos, siendo el comportamiento humano una fuente de incertidumbre especialmente difícil de gestionar, debido a la ausencia de estacionariedad. Las incertidumbres asociadas con las operaciones de un VA sugieren importantes desafíos estadísticos que

deben resolverse para garantizar la adopción masiva de esta tecnología (Hawke et al. 2021). En este artículo, ahondaremos sobre los mismos centrándonos en problemas relacionados con la decisión de solicitud de intervención del conductor, el apoyo a la toma de decisiones éticas, las operaciones en tráfico heterogéneo y la robustez algorítmica.

UN POCO DE CONTEXTO

La investigación en VAs requiere un esfuerzo multidisciplinar. Desde una perspectiva tecnológica, los VAs se basan principalmente en herramientas y métodos de los campos de la estadística, las matemáticas, la robótica, la informática, y las ingenierías eléctrica y mecánica. Además, también son relevantes algunas disciplinas menos cuantitativas como la sociología o la psicología. Para una mejor comprensión de este dominio resulta conveniente introducir algunos antecedentes contextuales en relación con los VAs.

Estado actual de la tecnología de las VAs.

La incipiente tecnología de los VA está evolucionando gradualmente desde los vehículos guiados solo por personas (MV) hasta vehículos completamente autónomos, que se estima estarán plenamente disponibles en unos 20 años. Esta evolución probablemente seguirá la taxonomía de seis niveles de automatización establecidos en la Society of Automotive Engineers (2018). Tal taxonomía comienza en el nivel 0, que describe vehículos sin capacidades autónomas, y continúa por los niveles 1 al 4, con cada vez mayores capacidades autónomas, culminando en el nivel 5, con vehículos completamente autónomos. Antes del 2010, las carreteras mundiales estaban ocupadas exclusivamente por vehículos de nivel 0. Sin embargo, en la última década, se han comenzado a comercializar vehículos con niveles de automatización más altos. Por ejemplo, el ***asistente para mantenimiento de carril*** ya está presente en casi todos los automóviles producidos durante los últimos años (Consumer Reports 2019). En consecuencia, la población de VAs de niveles 1 y 2 aumenta anualmente. Volvo anunció en 2022 que lanzará un sistema de nivel 3. Igualmente, Mercedes-Benz se ha convertido en el primer fabricante mundial en obtener una aprobación regulatoria válida internacionalmente para producir vehículos de nivel 3. Otras empresas están probando ya vehículos de niveles 4 y 5 en entornos reales muy controlados. Como ilustraremos más adelante, los problemas a resolver serán diferentes en función del nivel de VA que consideremos.

Impacto de tecnologías VA.

El transporte afecta a casi todos los aspectos de nuestras vidas. Así, dado que la adopción de los VAs revolucionará el transporte, también deben esperarse efectos en cascada sobre muchos otros aspectos. Además, numerosos factores exógenos afectarán también a la disposición de la sociedad a adoptar esta tecnología. La Figura 1, adaptada de Caballe-

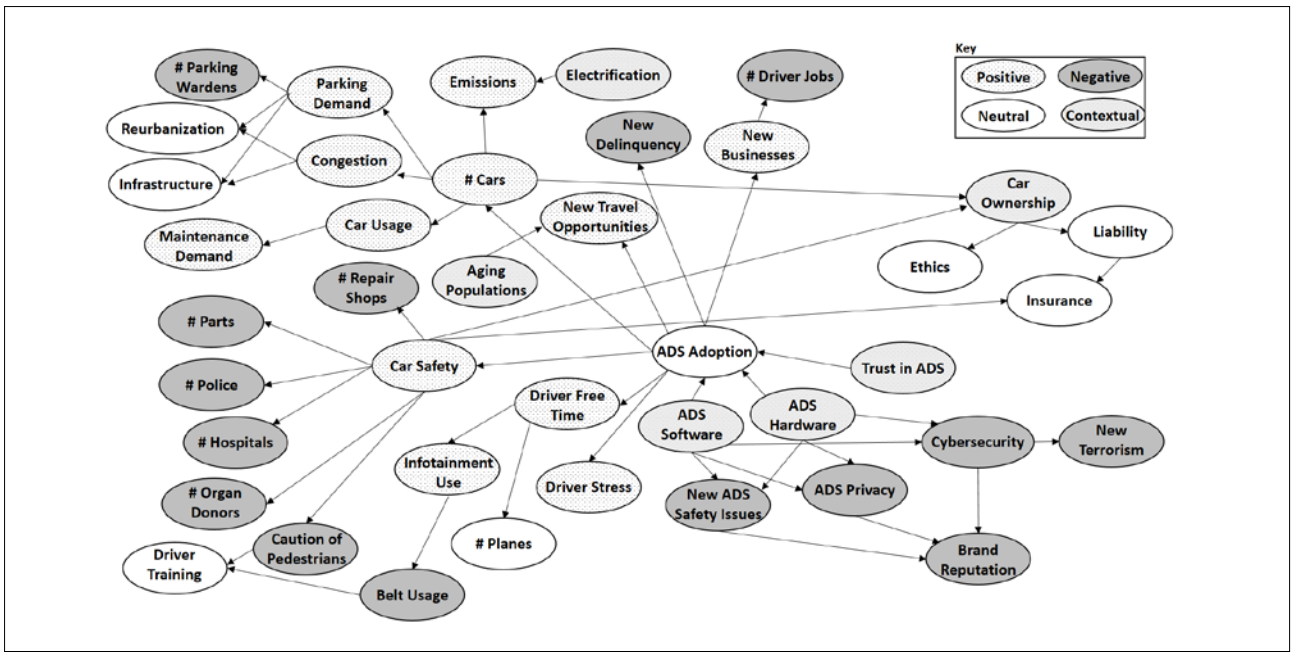


Figura 1. Red que refleja los impactos sociales de los VAs.

ro et al. (2021), presenta los impactos anticipados de los VAs en la sociedad junto a los factores que afectan a su adopción. Los nodos punteados se refieren a impactos positivos; los de color gris claro a impactos negativos y los blancos a impactos neutrales. Los nodos de color gris oscuro hacen referencia a factores contextuales (p. ej., la confianza en los VA) que pueden tener influencia en el despliegue masivo de esta tecnología. La figura pone de manifiesto el carácter multidisciplinar de la investigación en este campo como ya indicamos más arriba.

Arquitecturas para toma de decisiones en VAs.

Se dispone de varias arquitecturas de toma de decisiones en VAs (véase McAllister et al. 2017). Sin embargo, todas suelen presentar los siguientes elementos comunes: a) las entradas a los sensores del VA se procesan mediante componentes de detección de objetos para comprender la escena de conducción; b) tal entendimiento se incorpora a un componente de predicción de evolución de la escena; y, finalmente, c) un componente de toma de decisiones emplea las predicciones para adoptar los controles requeridos en la conducción.

Los componentes de detección de objetos son fundamentales en el esquema anterior. A menudo, se emplean grandes conjuntos de datos relativos a escenas de conducción para, con técnicas de aprendizaje profundo, detectar los objetos presentes. Sin embargo, incluso si una escena de conducción puede percibirse con precisión (p.ej., Bojarski et al. 2016), su utilidad viene limitada por la precisión de la componente predictiva. Las técnicas para percibir y predecir el entorno se toman a menudo prestadas de otros dominios de aplicación. Suelen emplear variantes de redes neuronales convolucionales (CNN) y modelos de espacio de estados (Grigorescu et al. 2020). Estas técnicas permiten determinar los controles de dirección y velocidad dadas las imágenes de entrada, vinculando las entradas de los sensores con los controles del vehículo, como sucede, por ejemplo en PilotNet (Bojarski et al. 2016). También se emplean métodos de aprendizaje por refuerzo profundo para agilizar la toma de decisiones en VAs como se describe, por ejemplo, en Grigorescu et al. (2020).

Prueba de tecnologías VA.

Puesto que los VAs han de interactuar con humanos existe riesgo de accidentes fatales, especialmente cuando se emplean nuevas arquitecturas. Así, la experimentación con VAs sigue un ciclo en el que el realismo del entorno se incrementa progresivamente. Se suele comenzar con un simulador numérico relativamente sencillo; si los resultados son satisfactorios, la funcionalidad del VA se prueba en un simulador más realista. Posteriormente, se emplea un entorno de pruebas tridimensional virtual, potencialmente aumentado con agentes humanos. Se continúa con un VA físico en un entorno cerrado. Finalmente, las pruebas culminan con experimentos en entornos variados del mundo real. Obviamente, cada una de estas etapas introduce sus propias complicaciones estadísticas.

LA DECISIÓN DE SOLICITUD DE INTERVENCIÓN

Los VAs de niveles 3 y 4 operan en un dominio operativo (DO) que introduce restricciones a su funcionamiento. Esto conlleva que estos vehículos deban en ocasiones transferir el control al conductor. Dadas sus posibles consecuencias fatales, la decisión de transferencia de control al conductor es muy importante y se inicia mediante un comando denominado solicitud de intervención (RtI, por sus siglas en inglés), que se ejecutaría cuando las condiciones operativas se acerquen a los límites del DO. Hasta que los vehículos completamente autónomos predominen en las carreteras, la gestión de RtI será una cuestión crucial para la que esbozaremos un modelo. Pueden verse más detalles en Ríos Insua et al. (2022).

Metodología.

Consideremos un VA (de nivel 3 ó 4) con tres modos de conducción (autónomo, manual y emergencia). Dadas las restricciones del DO, debemos gestionar los RtI de forma continua. La evolución temporal incierta del estado del sistema subyacente complica la gestión, pues tal incertidumbre debe incorporarse a la toma de decisiones. Aquí presentamos un marco para la gestión de RtI que agrega información histórica para la inferencia y la predicción, haciendo uso de un enfoque bayesiano que aprovecha de forma iterativa los datos isponibles. Este marco viene descrito en el proceso cualitativo de la Figura 2. D_t designa los datos recogidos hasta el instante t. Típicamente, las decisiones de los VAs se adoptan considerando un horizonte de tiempo variable (por ejemplo, $k = 10$ intervalos de tiempo de $0{,}5$ segundos), como hacemos aquí.

La solicitud de una RtI puede resumirse como sigue. Los sistemas de monitorización del entorno y del estado del conductor (DSM, por sus siglas en inglés) perciben el estado de los mismos en tiempo t y los predicen hasta el $t + k$; actualizan la trayectoria planificada y deciden si se debe ejecutar un RtI; en caso afirmativo, evalúan dicha ejecución por medio de una evaluación del desempeño de la intervención del conductor (DIPA, por sus siglas en inglés). Este proceso se repite iterativamente.

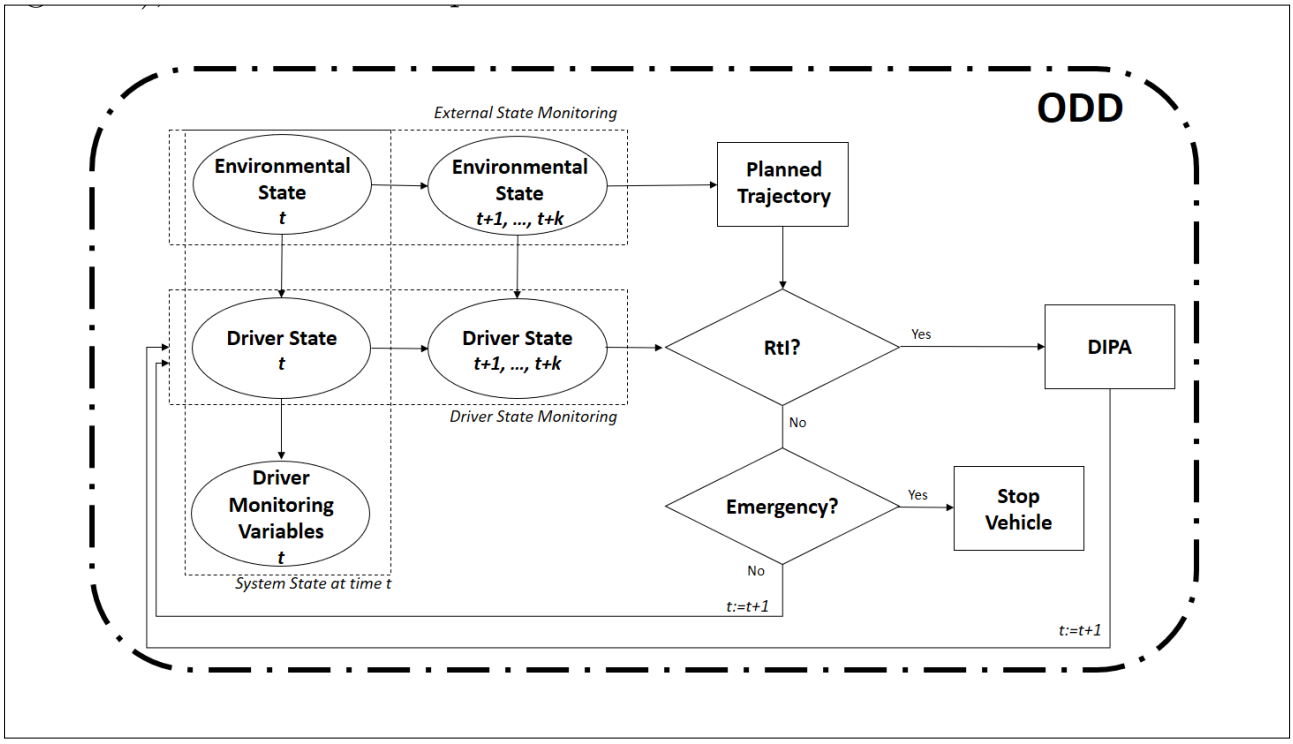


Figura 2. Marco para inferencia, predicción y soporte de decisiones de RtI

En más detalle, el VA debe operar según los límites de su DO, que define las condiciones bajo las que se puede emplear el modo autónomo. El DO se caracteriza típicamente a partir del estado de la calzada, el comportamiento del VA y el estado de sus subsistemas físicos; para ello, se emplean tres bloques de variables $\mathbf{g}_t^1$, $\mathbf{g}_t^2$, $\mathbf{g}_t^3$ evaluadas en el instante t (concatenadas en un vector $\mathbf{g}_t \in \mathbf{G}$, donde G representa el DO).

Usamos modelos probabilísticos para predecir la evaluación de tales variables, p.ej. modelos de espacio de estados (West & Harrison 2006), que facilitan la construcción recursiva de predicciones probabilísticas, k periodos a futuro. Basadas en ellos, el VA hace consultas sobre $\mathrm{p}\left(\mathbf{g}_{t+k} \notin \mathbf{G} | D_t\right)$. Cuando esta probabilidad es suficientemente grande, el VA debe emitir una alerta y abandonar el modo autónomo. Además, estos modelos probabilísticos también se pueden emplear para emitir avisos cuando se detectan cambios poco probables en las condiciones operativas.

El VA también debe monitorizar el entorno en el que opera. Supongamos η variables de entorno representadas mediante $\mathbf{Y}_t = \left(Y_t^1, Y_t^2, \ldots, Y_t^\eta\right)$, referidas e.g. al comportamiento de objetos o personas en la escena de conducción. Estas variables se monitorizan de manera similar a las variables del DO. Otro elemento clave se refiere al estado del conductor, ya que si este no está atento, un RtI puede tener un riesgo elevado de fallo: el VA debe predecir el grado de atención del conductor para determinar su disponibilidad para asumir el control del vehículo. Un sistema DSM incluye sensores que se emplean para inferir el estado del conductor (por ejemplo, su fatiga). Este se modeliza mediante una variable latente que se infiere empleando medidas relacionadas (por ejemplo, la postura del conductor), recopiladas por el VA en cada instante t. Se supone que las variables de monitorización del entorno afectan también al estado del conductor (por ejemplo, el conductor presta mayor atención durante una tormenta). De nuevo, empleamos un modelo de predicción probabilística que tiene en cuenta tales dependencias e informa las decisiones sobre el modo de conducción a adoptar y la emisión de advertencias.

Además, los VAs también están equipados con un sistemas de planificación de trayectorias que guían sus movimientos (p.ej. véase Claussmann et al. 2019), proporcionando en cada instante t un plan de trayectoria $\bar{Z}$ hasta el instante $t+k$ que intenta mantener el VA dentro de sus límites de DO. A su vez, esta trayectoria se utiliza como entrada para la gestión de RtIs. Para ello, se evalúa la utilidad esperada de los distintos modos de conducción en los siguientes k periodos, teniendo en cuenta las predicciones del estado del entorno, el del conductor, la trayectoria planificada y las variables de DO. La función de utilidad empleada evalúa la eficacia del modo de con-

ducción descrito más adelante. La utilidad predictiva esperada de los modos de conducción permite al VA elegir el modo más adecuado en el instante correspondiente.

Finalmente, en la gestión de RtI resulta útil comprender cuan capaz es un conductor al intervenir, lo que se realiza mediante una operación denominada DIPAs (del inglés driver intervention perfomance assessment) que registra como datos históricos las intervenciones del conductor, y compara los rendimientos reales e hipotéticos del mismo. Esta información se emplea para actualizar las creencias acerca del rendimiento del conductor para su uso en futuras decisiones RtI.

Una vez descritos los ingredientes fundamentales de nuestro marco de gestión de RtI, esbozamos cómo se pueden aprovechar conjuntamente para gestionar la transición entre los modos de conducción. Así, mientras opera en modo autónomo, el VA debe emitir periódicamente evaluaciones de riesgo predictivas sobre cumplimiento de su DO. Si $\mathrm{P}(\mathbf{g}_{t+k} \notin \mathbf{G} | D_t)$ es lo suficientemente grande, el vehículo alerta al conductor, y evalúa qué modo de conducción es preferible. Además, basados en los elementos discutidos, se puede emitir una RtI al conductor, en cuyo caso se debe realizar una DIPA. Si el rendimiento del conductor es adecuado este retiene el control hasta que desee volver al modo automático. De lo contrario, el VA puede decidir que el humano está incapacitado y activar el modo de emergencia, que debería detener el VA de forma segura. Después, el conductor puede seleccionar un modo de conducción al reanudar las operaciones. Este marco se resume cualitativamente en el Algoritmo 1. Las subrutinas detalladas de los procesos descritos se proporcionan en Ríos Insua et al. (2022).

Evaluación Empírica.

La experimentación inicial sobre este marco se realizó en un simulador numérico correspondiente a un entorno relativamente peligroso para garantizar que nuestro marco se estresa suficientemente. Los resultados detallados están en Ríos Insua et al. (2022). En general, la metodología RtI esbozada funciona adecuadamente. Destaquemos que durante la experimentación se manifestó un fenómeno que denominamos ***dilema fundamental*** de los VA de nivel 3 y 4. Cuando es probable que se excedan los límites del DO, es posible que el conductor no esté preparado para asumir el control del vehículo. El VA debe decidir si transfiere el control a un conductor distraído, o si lo retiene viéndose obligado a tomar decisiones de vida o muerte, lo que plantea problemas en el diseño del VA: si el control se transfiere al conductor distraído, éste se ve obligado a asumir la responsabilidad de su distracción; por el contrario, si el VA retiene el control, se puede obtener un mejor resultado, pero a expensas de la automatización de decisiones vitales. Tales cuestiones no tienen respuestas sencillas, pero ilustramos una resolución potencial basada en la maximización de la utilidad esperada.

La Figura 3 tipifica cómo nuestro enfoque resuelve el dilema. Las carreteras del simulador se caracterizan por un pavimento resbaladizo; las probabilidades condicionadas se refieren a la presencia de un charco en la calzada, sin otros obstáculos. Las figuras 3a y 3b estiman la utilidad esperada y la proporción de RtIs abortadas en función de tal probabilidad. Al aumentar esta más allá de cierto límite, la utilidad esperada comienza a aumentar (Figura 3a): cuando se prevé que la carretera sea especialmente peligrosa, el VA detecta con mayor frecuencia el

Algorithm 1 Controlador del VA

Input: Función de utilidad; distribuciones a priori sobre las variables DO, ambientales y de estado del controlador.

Output: Trayectoria de ORIGEN a DESTINO (e implementación de comandos en modo AUTON o EMERG).

while DESTINO no alcanzado **do**

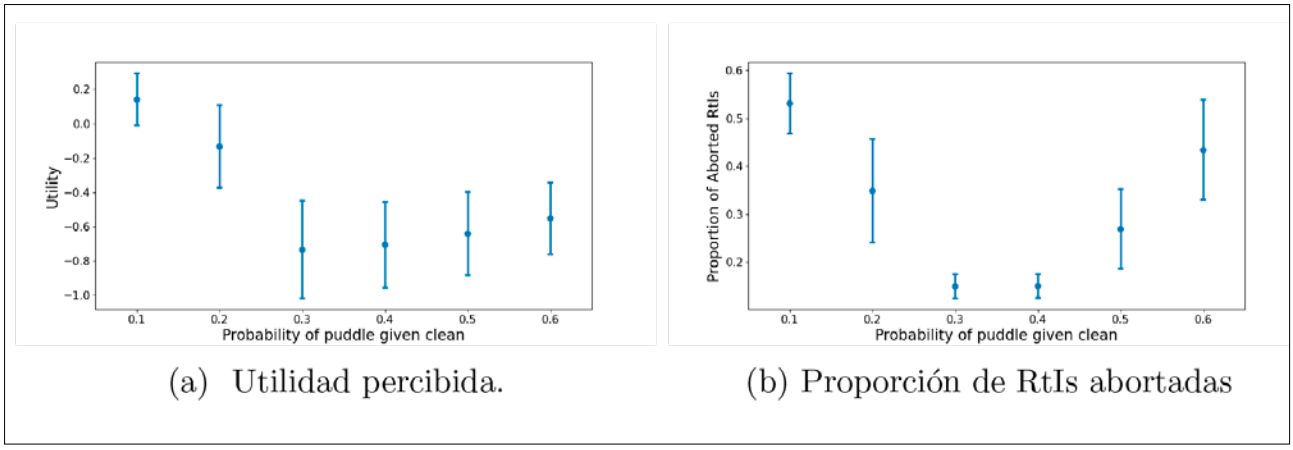
Leer sensores internos y externos.
Predecir variables ambientales k pasos en el futuro.
Predecir estado del conductor k pasos en el futuro.
Calcular trayectoria,
Evaluar y seleccionar MODO DE CONDUCCIÓN. Si necesario, AVISOS.
Gestionar desde MODO CONDUCCIÓN. Resolver cualquier DIPA pendiente.

end while

bajo rendimiento del conductor. Entonces, el VA decide no permitir que el conductor tome el control del vehículo con tanta frecuencia, como se observa en la Figura 3b: por encima de cierto valor de la probabilidad de charcos, las RtIs abortadas comienzan a aumentar y, por tanto, disminuye el riesgo de tener un conductor distraído, lo que, a su vez aumenta la utilidad esperada.

los mismos según sus prioridades y su perspectiva ética. Esto requiere, primeramente, identificar un conjunto amplio de objetivos junto con sus atributos.

El conjunto que empleamos se encuentra en el Cuadro 1. La primera columna representa los objetivos de nivel superior; la segunda, los de nivel inferior (Keeney et al. 1993) . Tales objetivos se identificaron



(a) Utilidad percibida. (b) Proporción de RtIs abortadas

Figura 3. Medidas de rendimiento para varios valores de p(yt+1 = puddle|yt = clean).

APOYO A LA TOMA DE DECISIONES ÉTICAS EN VAs

Como ocurre con las tecnologías revolucionarias, la adopción generalizada de los VA irá acompañada de numerosas incertidumbres morales. Los reguladores encargados de gestionar los VAs deberán enfrentarse a supuestos éticos complejos como el de la Sección 3. Aquí describimos un marco flexible que permite adoptar perspectivas éticas diversas en el control de VAs mediante la teoría de la decisión estadística. La estandarización de la toma de decisiones de VAs a través de un enfoque de maximización de la utilidad esperada hace este proceso transparente y reproducible. En esta sección, esbozamos este enfoque y su validación experimental.

Metodología.

Los objetivos que persigue un VA dependen de las partes interesadas involucradas: un propietario puede buscar minimizar el tiempo de viaje mientras que una aseguradora probablemente esté más preocupada por la seguridad de los vehículos. Para dar cabida a diversas perspectivas, desarrollamos un modelo de utilidad multi-atributo genérico para la gestión de la toma de decisiones de los VAs que permite a cualquier parte interesada adaptar el comportamiento de

mediante una revisión profunda de la literatura sobre transporte; se empleó después un mapa mental para agrupar los objetivos, que se segmentaron mediante un árbol con objetivos de nivel superior e inferior. Después fueron validados por un panel externo de expertos. Los atributos potenciales para cuantificar objetivos de nivel inferior se resumen en las últimas tres columnas del Cuadro 1. Caballero et al. (2022) proporciona una presentación detallada de cada atributo.

En la práctica, un conjunto de pares objetivo-atributo necesita un modelo de preferencia y un vector de pesos de los objetivos. Un enfoque de análisis de decisiones aprovecharía un procedimiento de asignación para determinar tales elementos. Observemos, sin embargo, que la selección del modelo de preferencias tiene consecuencias éticas. Por ejemplo, una función de utilidad multiplicativa corresponde, típicamente, a una perspectiva ética teleológica. Además, los pesos seleccionados aportan una capa adicional de matices éticos. Por ejemplo, si los pesos de los objetivos referidos a la seguridad de los pasajeros del VA y a la de los pasajeros de otros vehículos son iguales, se adopta una perspectiva ética igualitaria. Desde este punto de vista, las ventajas de nuestro modelo genérico de utilidad multiatributo son evidentes: se abordan simultáneamente preocupaciones operativas y éticas y también se puede utilizar con fines regulatorios y de control de los VAs. A su vez, el cumplimiento de dicha regulación podría informar procesos penales y de responsabilidad, entre otros.

Cuadro I: Resumen de objetivos y atributos				
Obj. Nivel Superior	Obj. Nivel Inferior	Atributo natural	Atributo construido*	Atributo proxy
Rendimiento	Min. consumo combustible Min. duración del viaje Min. incomodidad pasajero	Unidades monetarias Unidades monetarias/temporales	Sí	Movimiento del VA
Seguridad	Min. individuos heridos dentro (fuera) del VA	Número de heridos	Sí	Número de hospitalizados
	Min. víictimas dentro (fuera) del VA	Número de Víctimas / VSL	Sí	
	Max. respeto por la vida	Probabilidad de víctima/herido	Sí	
	Min. daño al VA	Unidades monetarias	Sí	
	Min. daño a infraestructuras	Unidades monetarias	Sí	
	Min. impacto medioambiental (global/local)	Unidades monetarias	Sí	
Reputación	Min. daño reputacional fabricante		Sí	Presencia mediática
	Min. daño percepciones sociales		Sí	Presencia mediática

Cuadro I

Evaluación empírica.

Para explorar la eficacia de este marco, se realizaron pruebas en un entorno simulado que permitieron investigar el impacto de los parámetros del modelo propuesto sobre el comportamiento de un VA. De los objetivos en el Cuadro I, consideramos la duración del viaje y el daño a las personas dentro y fuera del VA. Los reguladores pueden aprovechar el marco propuesto para realizar simulaciones del comportamiento de VAs bajo diversas configuraciones hasta determinar cuáles son socialmente aceptables. Dichas configuraciones pueden volverse obligatorias por ley o recomendadas como estándares para la industria, expresadas, por ejemplo, como sigue: ***El número medio más dos desviaciones estándar de lesiones y muertes por cada X kilómetros no debe ser superior a 1,4 y 0,25, respectivamente***.

Como ejemplo, supongamos que el regulador desea determinar un estándar para la industria sobre los pesos de los objetivos de un VA. Al simular operaciones del vehículo, se pueden analizar diferentes configuraciones de pesos y, para cada una, el regu-

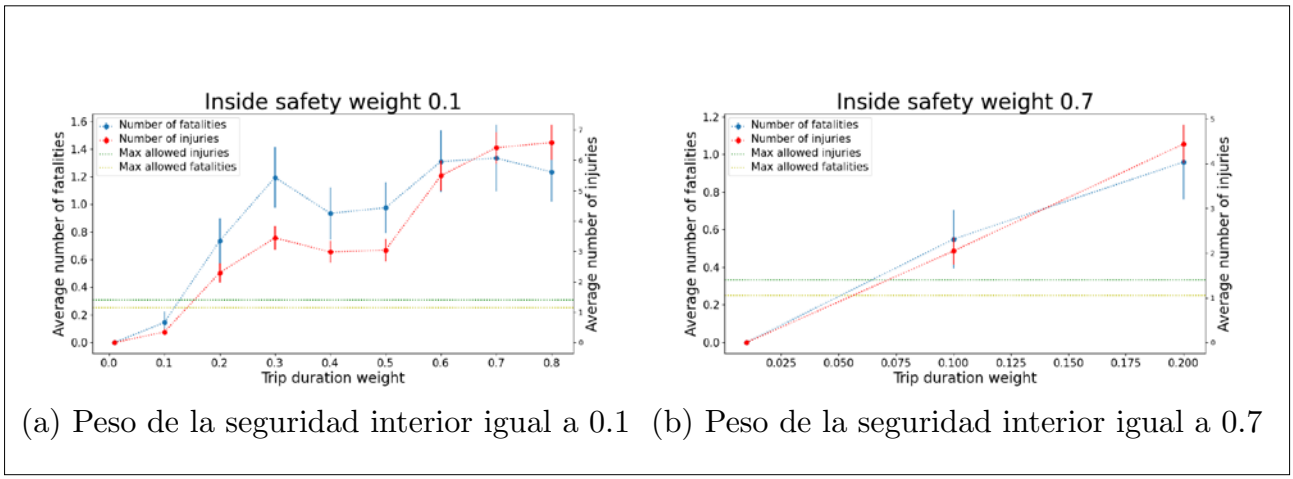
lador puede determinar si se cumplen los criterios de seguridad establecidos. La Figura 4a ilustra que si el peso para seguridad interior es 0,1, los pesos para duración del viaje mayores o iguales a 0,2 no cumplen con los criterios del regulador (líneas punteadas verdes y amarillas). Así, los pesos para duración del viaje por debajo de 0,2 podrían explorarse más a fondo para identificar el peso máximo que satisface las restricciones de seguridad. En nuestro caso, un peso 0,1 para duración de viaje es admisible según los criterios de seguridad.

Tras este análisis, el regulador identifica una combinación de pesos como estándar industrial, por ejemplo, proponiendo como pesos para seguridad interior, seguridad exterior y duración del viaje 0,1, 0,1 y 0,8, respectivamente. Supongamos que un fabricante considera que puede ganar cuota de mercado aumentando el peso de la seguridad interior hasta 0,7, a costa de disminuir el peso de la seguridad exterior. Si se produce un accidente, es natural preguntarnos si el fabricante es responsable debido a su desviación respeto del estándar. Para resolver esta cuestión, realizamos una simulación con su configuración de pesos, y comparamos los resultados con los criterios de seguridad prescritos. La Figura 4b muestra que, en nuestro ejemplo, los pesos seleccionados por el fabricante no cumplen con dichos criterios y sería razonable considerar al fabricante responsable.

muchos años. Los efectos asociados a esta convivencia son aún inciertos y llevan asociados una amplia gama de problemas matemáticos, especialmente en relación con el apoyo a la toma de decisiones de VAs e.g. en la decisión de cambio de carril, en la que aquí nos centramos, por ser la más compleja. Para modelizar esta decisión, se han aplicado principalmente razonamientos de teoría de juegos que, si bien resultan manejables, son sensibles a críticas referidas a las hipótesis de conocimiento común o racionalidad perfecta de los agentes involucrados. Esbozamos aquí un enfoque alternativo basado en el análisis de riesgos adversarios (ARA) (Banks et al. 2015).

Metodología.

Consideremos una carretera con dos carriles en la que un VA (A) es el vehículo objetivo que se enfrenta a una decisión de cambio de carril. Adoptamos una estructura de juego de Stackelberg de manera que nuestro VA es líder y el seguidor es un MV (M) que se encuentra en el carril adyacente. El VA toma una decisión que observa el MV. Éste elige su mejor respuesta en función de su observación. La interacción comienza cuando A recibe estímulos que desencadenan un cambio de carril y finaliza cuando ambos vehículos han ejecutado sus decisiones.



(a) Peso de la seguridad interior igual a 0.1 (b) Peso de la seguridad interior igual a 0.7

Figura 4. Número promedio de lesiones y muertes frente al peso dada la duración del viaje.

OPERACIONES DE VAs EN TRÁFICO HETEROGÉNEO

Debido a limitaciones tecnológicas y dilemas regulatorios (Lee & Hess 2020), se espera que los VAs se estabilicen en el nivel 3 en un futuro cercano, de forma que los MV operarán junto con los VA durante

La Figura 5 representa este problema mediante un diagrama de influencia bi-agente (Banks et al. 2015). El vehículo A toma la decisión a observada por M que, posteriormente, implementa su acción m. La decisión de cada vehículo se basa en su comprensión del estado del entorno, denotado por una variable latente θ, que resume las condiciones estructurales, físicas y de percepción. El VA infiere θ a través de

datos Y_A de sensores. Análogamente, el (conductor del) vehículo M emplea datos Y_M para construir sus creencias sobre θ. Estas entradas no son deterministas, modelizando así posibles errores de percepción. La interacción de las decisiones a y m, junto a θ, conducen a un resultado probabilístico S, con valor s. Los agentes A y M reciben sus respectivas utilidades u_A y u_M, dependientes de las correspondientes acciones y de s.

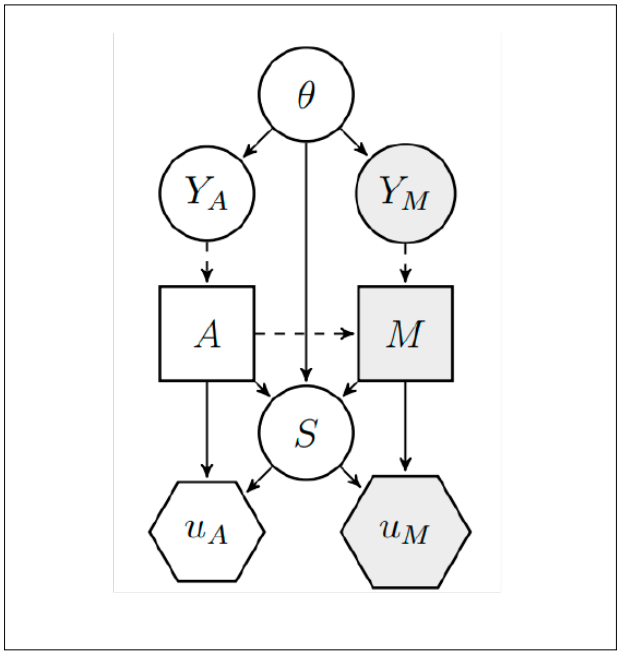


Figura 5. BAID del juego de dos carriles.

Para identificar la decisión óptima $a^*(y_A)$ del VA, debemos asignar su función de utilidad y sus creencias. La utilidad de tomar la decisión a e inducir el resultado s se denota $u_A(a,s)$. El término $p_A(\theta|y_A)$ representa su densidad de probabilidad sobre el estado del entorno dada la lectura del sensor $y_A \in \mathcal{Y}_A$. Su densidad de probabilidad sobre la acción m del MV condicionada a a e y_M se designa $p_A(m|a,y_M)$; las creencias sobre y_M dado θ se designan $p_A(y_M|\theta)$; finalmente, $p_A(s|m,a,\theta)$ representa la densidad del resultado s dadas las decisiones m y a, así como el estado del entorno. Las funciones de distribución asociadas con cada una de estas funciones de densidad se indican mediante $P_A(\cdot)$. Dadas estas entradas, el objetivo del VA es encontrar la acción a que maximice su utilidad esperada condicionada, lo que equivale a resolver:

Todos los ingredientes en (1) son estándar desde el punto de vista del análisis de decisiones, con la excepción de $P_A(m|a,y_M)$, que tiene un componente estratégico relacionado con cómo el MV resuelve su problema de decisión. Así, se requiere un análisis adicional para estimar esta cantidad. Para ello, el VA puede evaluar el problema de decisión del MV, similar a (1), pero basado en información conocida solo por el MV. Supongamos por un momento que el VA puede parametrizar la función de utilidad del MV y sus probabilidades son conocidas. Si M maximiza la utilidad esperada al observar a e y_M, se seleccionará la acción $m^*(a,y_M)$ que maximice su utilidad esperada. Sin embargo, el VA tendrá incertidumbre sobre las utilidades y probabilidades del MV; si modelizamos tal incertidumbre de manera bayesiana a través de utilidades y probabilidades aleatorias, esto inducirá incertidumbre sobre la acción óptima del MV, cuya distribución proporcionará el elemento requerido. Es sencillo obtener muestras de esta distribución simulando variables aleatorias de la función de utilidad y las distribuciones de probabilidad aleatorias y empleando después tales muestras para resolver el problema del MV.

Evaluación empírica.

Describimos brevemente la evaluación de esta propuesta, véase Naveiro et al. (2022) para detalles adicionales. En nuestro ejemplo consideramos $\mathcal{A} = \{a_1, a_2, a_3\}$ correspondientes a ***cambiar de carril***, ***permanecer en el carril*** y ***realizar una maniobra de emergencia***, respectivamente. De manera similar, el espacio de acciones del MV es $\mathcal{M} = \{m_1, m_2, m_3\}$ correspondiente a ***acelerar***, ***decelerar*** y ***cambiar de carril***. Con respecto a los resultados, establecemos $\mathcal{S} = \{s_1, s_2, s_3, s_4\}$ respectivamente asociados a ***accidente mayor*** (MV y VA resultan destruidos con muertes en ambos vehículos); ***accidente menor*** (daño físico menor a vehículos y pasajeros); ***interacción segura*** (sin daños físicos ni lesiones) y ***víctimas de peatones*** (si se requiere desvío de emergencia los peatones en riesgo fallecen). Finalmente, se consideran cuatro variables de entorno $\theta = (\theta_1, \theta_2, \theta_3, \theta_4)$, donde θ_1 indica si el pavimento está mojado o seco, mientras que θ_2, θ_3 y θ_4 representan, respectivamente, el número de personas en el VA, en el MV y los peatones en riesgo si se realiza una maniobra de emergencia.

Como se discutió en la sección anterior, se pueden considerar múltiples objetivos que rijan las operaciones del VA.

$$a^*(y_A) = \arg\max_{a\in\mathcal{A}} \int_{\Theta} \int_{\mathcal{Y}_M} \int_{\mathcal{M}} \int_{\mathcal{S}} u_A(a,s)\mathrm{d}P_A(s|m,a,\theta)\mathrm{d}P_A(m|a,y_M)\mathrm{d}P_A(y_M|\theta)\mathrm{d}P_A(\theta|y_A).$$

Consideramos seguridad interna, seguridad externa y duración del viaje, descritos mediante un vector $c_A(s,a) = \left(c_{A,1}(s,a), \ldots, c_{A,8}(s,a)\right)$ cuyos elementos se refieren respectivamente a número de heridos internos, fallecidos internos, proporción de daños del VA, heridos externos, fallecidos externos, proporción de daños del MV, peatones fallecidos y velocidad del VA. El modelo de preferencia es de una función de utilidad con aversión al riesgo absoluta constante (CARA) que agrega las consecuencias de forma aditiva, es decir; $u_A(s,a) = 1 - \exp\left(\rho_A \sum_{i=1}^{8} w_{A,i}\, c_{A,i}(s,a)\right)$, donde ρ_A es el coeficiente de aversión al riesgo del VA, y los pesos $w_{A,i}$ homogeneizan los criterios. Además, el VA debe formalizar las creencias sobre θ dado ; aquéllas sobre s dadas m, a y θ; y aquellas sobre y_M dado θ. Las selecciones específicas pueden verse en Naveiro et al. (2022).

El ARA requiere que los VAs formalicen sus creencias sobre el problema de decisión del MV para estimar $p_A(m|a, y_M)$. Suponemos que el MV basa su decisión en los objetivos de seguridad interna y duración del viaje (el MV actúa de manera menos altruista que un VA). Además, se asume un modelo de preferencia CARA, con $u_M(s,m) = 1 - \exp\left(\rho_M \sum_{i=1}^{4} w_{M,i}\, c_{M,i}(s,m)\right)$ donde ρ_M y $w_{M,i}$ representan respectivamente el coeficiente de aversión al riesgo y las ponderaciones del MV. El VA modeliza sus creencias sobre $(w_{M,1}, w_{M,2}, w_{M,3}, w_{M,4})$ mediante una distribución de Dirichlet, mientras que ρ_M se modeliza mediante una distribución uniforme. Además, para estimar la utilidad esperada del MV, el VA debe formalizar sus creencias sobre los modelos de probabilidad del mismo. Una aproximación útil basa estos modelos en los juicios del VA, con incertidumbre adicional para reflejar la falta de conocimiento. En conjunto, estas creencias describen un modelo sobre la utilidad esperada del MV cuyo máximo sobre m se emplea para estimar $\hat{p}_A(m|a, y_M)$.

Se utiliza simulación para estimar las probabilidades de las diferentes reacciones del MV dada la decisión del VA. A partir de estas probabilidades, una rutina maximiza la utilidad esperada del VA, con configuraciones específicas en Naveiro et al. (2022). Describimos los resultados de un experimento cuando (1) un solo peatón está presente, y (2) tanto el VA como el MV tienen un solo ocupante. El Cuadro 2(a) muestra la estimación $\hat{p}_A(m|a)$.

Los resultados confirman la intuición. En particular, si el VA cambia de carril (a_1), cree que lo más probable es que el MV decelere o, con menor probabilidad, cambie de carril. A su vez, cuando el VA decide permanecer en su carril (a_2), seguro que el MV acelerará. Finalmente, si el VA hace una parada de emergencia (a_3), el VA considera muy probable que el MV cambie de carril. Utilizando este modelo, el VA puede explorar cómo el comportamiento del MV afecta su decisión óptima. Finalmente, se realizó una serie de simulaciones de la interacción bajo distintos valores de θ_1 (no observado por los conductores). El Cuadro 2(b) presenta la proporción de simulaciones en las que cada acción del VA maximizó la utilidad esperada y la proporción de los diferentes resultados, cuando el VA selecciona la acción óptima: cuando el pavimento está seco, el VA generalmente prefiere cambiar de carril; cuando está mojado, tiende a actuar de forma más conservadora. Además, la proporción de resultados sugiere que la mayoría de las veces la interacción es segura.

PROTECCIÓN DE VAs FRENTE A ATAQUES ADVERSARIOS

Como se discutió en las secciones anteriores, las entradas de los sensores son determinantes en las operaciones de un VA. Los algoritmos de predicción se emplean para la estimación del estado del entorno que, posteriormente, se utiliza como entrada a los modelos de toma de decisiones. Es pues fundamental que estos componentes sean confiables, especialmen-

Cuadro II: (a) Estimación de $\hat{p}_A(m|a)$ (b). Probabilidades condicionadas de la acción preferida del VA y los resultados basados en el estado latente verdadero.

	m_1	m_2	m_3
a_1	0.000	0.860	0.140
a_2	1.000	0.000	0.000
a_3	0.024	0.027	0.949

(a)

	Acciones del VA			Resultados de la interacción			
θ_1	a_1	a_2	a_3	s_1	s_2	s_3	s_4
0	0.95	0.05	0	0.158	0.158	0.683	0.0
1	0.05	0.95	0	0.017	0.017	0.967	0.0

(b)

Cuadro II

te a la luz de las amenazas sobre los algoritmos de aprendizaje automático (ML, por sus siglas en inglés), como son los ejemplos adversarios: instancias de datos diseñadas estratégicamente para confundir a los algoritmos. Tales amenazas tienen una relevancia especial en los VAs, pues varios autores han demostrado cómo pueden diseñarse ataques para confundir los sistemas de percepción, siendo los efectos de los mismos muy perjudiciales para el rendimiento de un VA.

Así, para mejorar la seguridad de un VA, se requiere investigación fundamental en aprendizaje automático adversario (AML). Las investigaciones iniciales en este campo son prometedoras, pero el paradigma predominante para abordar la confrontación entre adversarios y sistemas basados en aprendizaje ha sido la teoría de juegos, que se basa en hipótesis de conocimiento común de dudosa validez en aplicaciones de seguridad (Hargreaves-Heap & Varoufakis 2004). Para aumentar el realismo de estos modelos, esbozamos un enfoque bayesiano a este problema.

Metodología.

Dado que un fabricante de VA controla su diseño, es previsible que los datos de entrenamiento empleados para desarrollar un algoritmo de ML en un VA sean confiables. No obstante, los datos operativos podrán estar sujetos a amenazas.

El paradigma de aprendizaje adversario bayesiano (BAL, por sus siglas en inglés) establecido en Ye & Zhu (2018) proporciona un marco para abordar situaciones en las que los datos de entrenamiento y de operaciones proceden de distribuciones diferentes. Suponiendo que haya datos de entrenamiento limpios disponibles, esta metodología produce datos amenazados artificialmente que intentan imitar cómo un atacante perturbaría los datos de entrada del VA. Esto permite que el sistema de percepción del vehículo se entrene en un entorno operativo realista. Suponiendo que este mapeo de datos limpios a contaminados incorpora la verdadera dinámica de la contaminación, el algoritmo de ML resultante será más robusto que uno entrenado con datos limpios. Así, BAL, en lugar de calcular una distribución a posteriori sobre los parámetros del modelo de ML utilizado como se haría en el ML estándar, estima una ***distribución a posteriori adversaria robusta***. Aunque el marco BAL está bien definido, el modelo de atacante se especifica de forma genérica, por lo que puede construirse un continuo de modelos variando diversos parámetros. Ríos Insua et al. (2020) explora más a fondo la flexibilidad del marco BAL aprovechando el ARA para desarrollar la distribución a posteriori robusta.

Evaluación empírica.

Para ilustrar la eficacia del ARA en BAL, esbozamos su aplicación al conjunto de datos MNIST, ampliamente utilizado en visión computacional. El algoritmo de ML tiene como objetivo identificar correctamente dígitos escritos a mano, mientras que un atacante perturba los datos para confundirlo. Un análogo en el dominio de los VA se correspondería con manipular una señal de ***stop*** para que el vehículo la confunda con un ***ceda el paso***. Supongamos que el atacante perturba las imágenes utilizando dos de los ataques más populares en AML: el método rápido del signo del gradiente (FGSM) (Goodfellow et al. 2015) y el del descenso de gradiente proyectado (PGD) (Madry et al. 2018). La Figura 6 muestra la eficacia de los ejemplos adversarios: mientras que tanto la imagen original como la perturbada representan el mismo dígito, utilizando una red convolucional (CNN), la primera se clasifica correctamente como un 2, pero la segunda se identifica incorrectamente como un 7.

(a) Imagen original (b) Imagen perturbada

Figura 6: Ejemplo de efecto de los ataques FGSM en los datos MNIST

Figura 6. Ejemplo de efecto de los ataques FGSM en los datos MNIST.

Utilizamos tres métodos para robustecer una CNN frente a estos ataques: entrenamiento adversario (AT), emparejamiento logit adversario (ALP, Kannan et al. 2018), ARA y los comparamos con un algoritmo no robustecido (NONE). La Figura 7 muestra las ***curvas de evaluación de seguridad*** para cada defensa, que representan la precisión del modelo robustecido frente a diferentes intensidades de ataque. La figura revela patrones de comportamiento notables. A baja intensidad de ataque, las cuatro defensas funcionan de manera similar. A medida que aumenta la intensidad del ataque, el rendimiento del clasificador estándar se deteriora rápidamente. Los tres enfoques robustos mitigan esta degradación, pero en distinto grado. El enfoque ARA es más robusto que las defensas AT y ALP ante intensidades más altas para ambos ataques.

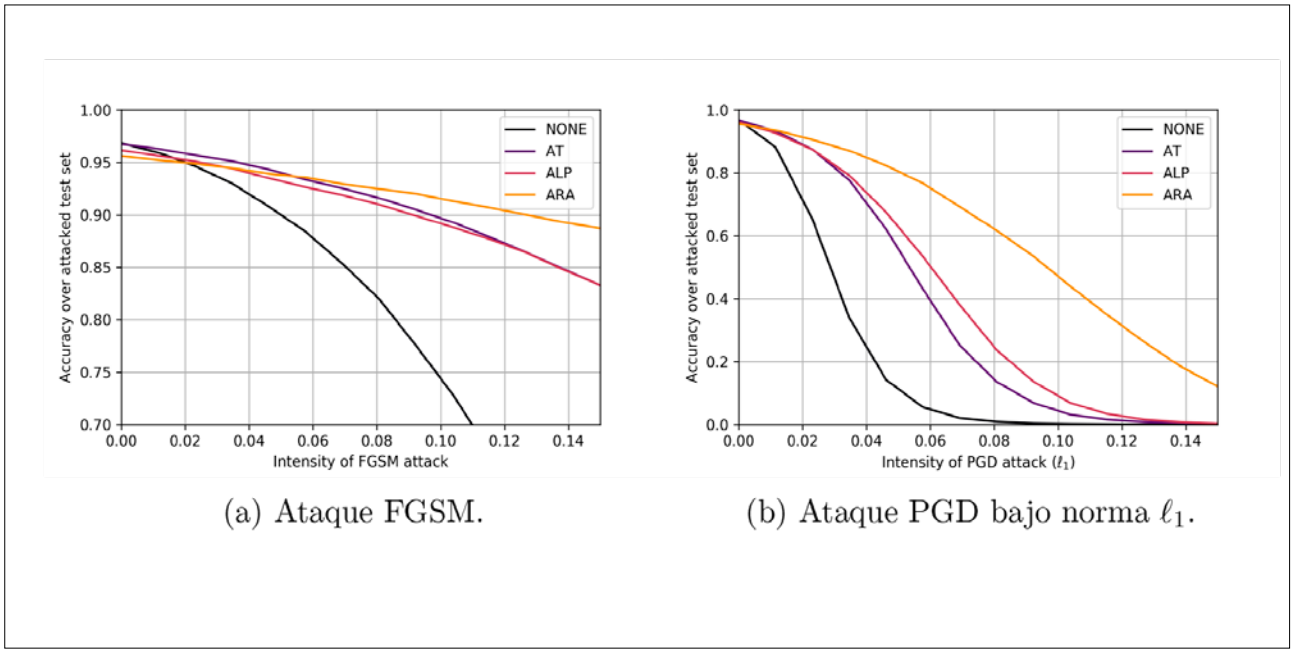


Figura 7. Precisión del clasificador bajo tres mecanismos de defensa y dos ataques.

CONCLUSIÓN

La tecnología de los VA avanza rápidamente, pero se estancará si los numerosos problemas tecnológicos, normativos y éticos pendientes no se resuelven. Aquí hemos descrito un subconjunto de tales problemas de carácter matemático-estadístico, así como algunas soluciones iniciales de los mismos. No obstante, hay muchos otros. Por ejemplo, hemos indicado cómo la tecnología de los VA depende fuertemente del aprendizaje profundo. Si bien los enfoques de aprendizaje profundo tradicionales han permitido un auge en el desarrollo de VAs, el aprendizaje profundo bayesiano traería beneficios importantes a este dominio (McAllister et al. 2017), debido a su capacidad para cuantificar adecuadamente la incertidumbre. Sin embargo, la mayoría de los algoritmos de entrenamiento de aprendizaje profundo se basan en máxima verosimilitud pues aún no se han identificado métodos bayesianos eficientes en redes profundas.

AGRADECIMIENTOS

Se agradece el apoyo de la Cátedra AXA-ICMAT, de los proyecto de la UE Horizonte 2020 815003 Trustonomy y AMALFI de la Fundación BBVA, del Ministerio de Ciencia e Investigación de España PID2021-124662OB-I00, de AFOSR FA-9550-21- 1-0239, y de EOARD FA8655-21-1-7042.

CONFLICTO DE INTERESES

Los autores/as de este artículo declaran no tener ningún tipo de conflicto de intereses respecto a lo expuesto en el presente trabajo.

REFERENCIAS BIBLIOGRÁFICAS

1. Banks, D., Rios, J., & Ríos Insua, D. (2015). Adversarial Risk Analysis. Francis Taylor.

2. Bojarski, M., Choromanska, A., Choromanski, K., Firner, B., Jackel, L., Muller, U., &

3. Zieba, K. (2016). Visualbackprop: visualizing cnns for autonomous driving. arXiv preprint arXiv:1611.05418, 2.

4. Burns, L. & Shulgan, C. (2019). Autonomy: The Quest to Build the Driverless Car—And How It Will Reshape Our World. ECCO.

5. Caballero, W. N., Naveiro, R., & Ríos Insua, D. (2022). Modeling ethical and operational preferences in automated driving systems. Decision Analysis, 19(1):21–43.

6. Caballero, W. N., Ríos Insua, D., & Banks, D. (2021). Decision support issues in automated driving systems. International Transactions in Operational Research.

7. Claussmann, L., Revilloud, M., Gruyer, D., & Glaser, S. (2019). A review of motion planning for highway autonomous driving. IEEE Transactions on Intelligent Transportation Systems, pages 1–23.

8. Consumer Reports (2019). Guide to lane departure warning & lane keeping assist. https://www.consumerreports.org/car-safety/lane-departure-warning-lane-keeping-assist-guide/.

9. Czarnecki, K. (2018). Operational design domain for automated driving systems taxonomy of basic terms. Tech Report, U. Waterloo.

10. Goodfellow, I., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. In International Conference on Learning Representations. Available at https://arxiv.org/abs/1412.6572.

11. Grigorescu, S., Trasnea, B., Cocias, T., & Macesanu, G. (2020). A survey of deep learning techniques for autonomous driving. Journal of Field Robotics, 37(3):362–386.

12. Hargreaves-Heap, S. & Varoufakis, Y. (2004). Game Theory: A Critical Introduction. New York, NY: Routledge.

13. Hawke, Jeffrey amd E, H., Vijay, B., & Kendall, A. (2021). Reimagining an autonomousvehicle. arxiv, 2018.05805.

14. Kannan, H., Kurakin, A., & Goodfellow, I. (2018). Adversarial logit pairing. arXiv preprint arXiv:1803.06373.

15. Keeney, R. L., Raiffa, H., & Meyer, R. F. (1993). Decisions with multiple objectives: preferences and value trade-offs. Cambridge university press.

16. Lee, D. & Hess, D. J. (2020). Regulations for on-road testing of connected and automated vehicles: Assessing the potential for global safety harmonization. Transportation Research Part A: Policy and Practice, 136:85–98.

17. Madry, A., Makelov, A., Schmidt, L., Tsipras, D., & Vladu, A. (2018). Towards deep learning models resistant to adversarial attacks. In International Conference on Learning Representations.

18. McAllister, R., Gal, Y., Kendall, A., van der Wilk, M., Shah, A., Cipolla, R., & Weller, A. (2017). Concrete problems for autonomous vehicle safety: advantages of bayesian deep learning. In Proc. 26th IJCAI.

19. Naveiro, R., Caballero, W., & Insua, D. R. (2022). An adversarial risk analysis for heterogeneous traffic management. Available at SSRN 4365987.

20. Ríos Insua, D., Caballero, W. N., & Naveiro, R. (2022). Managing driving modes in automated driving systems. Transportation Science.

21. Ríos Insua, D., Naveiro, R., & Gallego, V. (2020). Perspectives on adversarial classification. Mathematics, 8(11):1957.

22. Society of Automotive Engineers (2018). Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. Technical report, SAE.

23. Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2014). Intriguing properties of neural networks. In International Conference on Learning Representations.

24. West, M. & Harrison, J. (2006). Bayesian forecasting and Dynamic Models. Springer.

25. Ye, N. & Zhu, Z. (2018). Bayesian adversarial learning. In Proc. 32nd Int. Conf. Neur. Inf. Proc. Sys., pages 6892–6901. Red Hook, NY: Curran Associates Inc.

Si desea citar nuestro artículo:

Ríos Insua D, Naveiro R. Matemáticas y vehículos autónomos. RACSG.2023;112(01): 67-79. rac.2023.112.1.org06