Internet y nuevas tecnologías

Roberto Plá
Coronel de Aviación
http://robertopla.net/

INTELIGENCIA ARTIFICIAL
LO QUE HAY QUE TENER

La investigación en vehículos aéreos de combate tripulados por control remoto (UCAV) ha permitido avanzar de manera significativa en esta tecnología, que permite su funcionamiento con seguridad y eficacia controlado estas aeronaves desde increíblemente grandes distancias, aunque su uso se centra principalmente en escenarios de ataque de tierra.

Las limitaciones propias de las comunicaciones establecen plazos de milisegundos, suficientes para desaconsejar su uso cuando es necesario tomar decisiones críticas, como en el contexto de un combate aire-aire.

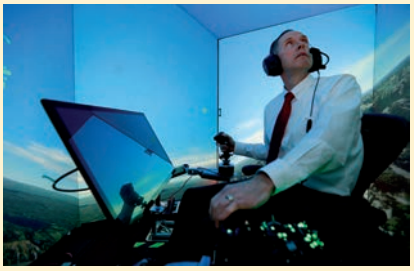
Muchos defensores de los vehículos remotamente tripulados destacan las ventajas que supone disponer de aeronaves que pueden realizar maniobras soportando fuerzas G extremadamente altas, a un precio más económico que el de aviones tripulados y sobre todo, con la inmensa ventaja de no exponer las vidas de nuestros pilotos, ni por supuesto su experiencia y formación.

Más allá de esto, el tiempo de reacción medio de la visión humana está entre 0,15 y 0,30 segundos y es necesario un tiempo aún más largo para pensar en planes óptimos y coordinarlos con las fuerzas amigas, lo que proporciona una enorme ventana de tiempo que la Inteligencia Artificial (IA) puede capitalizar para desarrollar sistemas que puedan tomar decisiones autónomas en tiempo real.

Hay una serie de obstáculos para que un sistema de IA sea eficaz dentro de este contexto. Las principales dificultades en el desarrollo de este tipo de aplicaciones son el gran número de entradas y salidas que deben ser considerados, así como la incertidumbre y la aleatoriedad implícitas en el problema.

La mayor parte de nuestras decisiones no se basan en datos exactos, sino en "impresiones": dejamos de comer cuando “creemos” haber comido suficiente, no cuando hemos ingerido una cantidad exacta de gramos de comida, calificamos a otra persona de “alta” o “baja”, sin referirnos, o incluso desconociendo su altura exacta, en función de criterios establecidos previamente como la cantidad de comida que es una ración “normal” la talla de una persona "baja" o de una "alta".

Para imitar las decisiones humanas y poderlas reproducir, los matemáticos han desarrollado herramientas que imitan ese proceso de razonamiento. Una



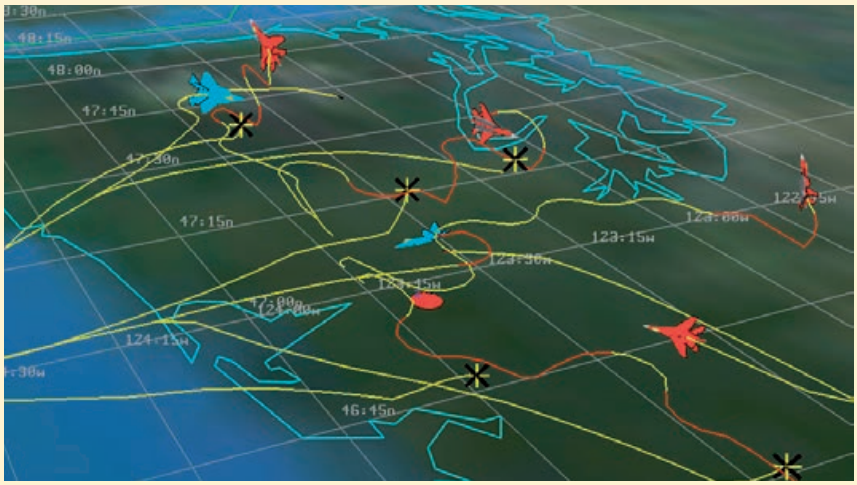
de ellas es la "lógica difusa". Este tipo de lógica toma dos valores aleatorios, pero contextualizados y referidos entre sí para obtener una solución o respuesta. Fue formulada en 1965 por el ingeniero y matemático azerbaiyano Lotfi A. Zadeh que desarrolló su trabajo en la universidad norteamericana de Berkeley.

En un trabajo sobre la aplicación de la lógica difusa a los sistemas de IA aplicados al combate aéreo un equipo norteamericano en el que han colaborado profesores de la Universidad de Cincinnati, ingenieros e investigadores del Laboratorio de Investigación de la Fuerza Aérea y pilotos de combate, ha demostrado que es posible desarrollar sistemas de inteligencia artificial que derroten en un “dog fight” a experimentados pilotos. Es importante destacar que se hizo usando nada más que la potencia de procesamiento disponible en una pequeña computadora Raspberry Pi, asequible y económica (menos de 30€ !), de la que hemos hablado aquí en otras ocasiones.

Los avances en la lógica difusa en sistemas genéticos, en especial la elaboración de la metodología denominada "árbol genético difuso" (Fuzzy Genetic Tree),han permitido desarrollar la inteligencia artificial basada en lógica difusa para su aplicación en problemas increíblemente complejos. Destaca su capacidad para obtener un rendimiento extremo y la gran eficiencia computacional, así como solidez en el tratamiento de aspectos como las incertidumbres y la aleatoriedad, que le permite adaptarse a escenarios cambiantes. Se aprecia asimismo la obtención de respuestas verificadas y validadas de forma que permiten seguir especificaciones de seguridad y doctrinas operativas a través de métodos formales. Por último, los desarrollos se han simplificado enormemente mediante herramientas que facilitan su diseño.

La cuestión de la verificabilidad y aplicación de métodos formales no es una cuestión baladí. En el combate aéreo, como en cualquier circunstancia en la que la mente humana se opone a una máquina, para vencer hay que explorar las grietas del sistema. Las opciones que no fueron programadas, o las situaciones en las que la IA no fue adiestrada. Es la forma de engañar y sorprender a la máquina. Por tanto la implementación de la capacidad de verificar y validar la IA es crucial, así como la capacidad de seguir no tanto unas respuestas prefijadas sino las indicaciones de una “doctrina” y la generación de una especie de “intuición artificial”.

Por supuesto, los sistemas de computación pueden tener accidentes y los



sensores pueden fallar, aunque esto es también cierto para los aviones tripulados y son cuestiones a las que se suele poner remedio mediante redundancias.

Tom Wolfe aludía en el titulo de su obra "The Right Stuff" (1979), traducido al español como "Lo que hay que tener" a esa característica especial que distingue a los Pilotos de Caza y a su evolución hacia las especies superiores de Pilotos de Pruebas y Astronautas. ¿La tecnología ha cambiado "lo que hay que tener" para obtener la superioridad aérea?.

http://delicious.com/rpla/raa845a

HACKING

EL ATAQUE A POLONIA

Hace un año, a principios de junio de 2015, unos hackers incluyeron en la página principal del ministerio lituano de defensa un documento con unos supuestos planes de Lituania para anexionarse Kaliningrado el enclave ruso situado entre Lituania y Polonia. Los hackers también declararon que el ejercicio Saber Strike era un simulacro militar preparatorio para tal anexión. En el ejercicio en cuestión participaban desde el primero de junio y en el marco de la OTAN , tanto Polonia como los países bálticos.

El día 22 del mismo mes se produjo el ataque hacker a los servicios de planamiento de vuelos de la linea aérea polaca LOT (RAA núm. 846), que impidió volar a 1.400 pasajeros en Polonia.

En la reunión realizada en Varsovia a primeros de julio de este año 2016, los líderes de la OTAN aprobaron la formación de cuatro batallones multinacionales en Polonia, Estonia, Letonia y Lituania, así como asumir el mando y control del sistema de defensa frente a misiles balísticos. El secretario general aliado, Jens Stoltenberg, declaró en rueda de prensa que esta acción era una acción defensiva que no amenazaba el sistema de disuasión balístico ruso, pero que reforzaba "el vínculo trasatlántico" y que “Un ataque a un aliado será considerado como un ataque a todos”.

Dias después se dió a conocer de forma anónima pero con gran parafernalia mediática, por un grupo de hackers que habían obtenido información y datos de los ordenadores del ministerio de defensa polaco.

El Ministerio de Defensa Nacional de Polonia, a través de su portavoz de prensa Bartolomiej Misiewic, restó importancia al allanamiento a la red informática del Ministerio de Defensa (lo cual certifica que realmente se produjo), asegurando que se trataba de "una manipulación cuyo objetivo era crear la sensación de un grave atentado cibernético" y que los datos provenían de la red abierta de Defensa, no contenían información confidencial, estaban desactualizados (1912) y se limitaban a una sola persona. Se aseguró que los sistemas seguían funcionando con normalidad y que se estaban realizando investigaciones para aclarar todas las circunstancias de este incidente.

El portavoz del ministerio de Defensa Nacional de Polonia, Bartolomiej Misiewic

Aunque parece que hay una relación evidente entre los movimientos de la OTAN y de Rusia en sus fronteras con Europa y los incidentes de hostigamiento informático. De estos, probablemente solo trascienden los que en realidad son operaciones de guerra de información y propaganda, más que auténtica ciberguerra. Si los hackers de uno u otro lado obtuvieran una vía para conseguir información operativa del adversario, obviamente no la desvelarían. De la misma forma que si descubrieran una vulnerabilidad similar en sus sistemas, la ocultarían o la aprovecharían para intentar suministrar información falsa a los intrusos. El engaño es una de las artes bélicas más antiguas y los ordenadores no han a cambiado sustancialmente su uso en los conflictos.

Por otra parte, la relación no implica la atribución. Los hackers no son ejércitos uniformados que se despliegan con sus banderas al frente. Un ataque de gran envergadura puede ser orquestado por una persona o un equipo pequeño, un gran número de activistas pueden movilizarse en función de un sentimiento patriótico o convicciones, sin necesidad de seguir directrices de una organización estatal, ni tienen necesidad de ejecutar sus acciones desde un territorio determinado.

En los ataques informáticos, tirar del hilo lleva muy pocas veces a la madeja. Las atribuciones se hacen en base a suposiciones o pistas sutiles y la pública acusación puede ser también una técnica de provocación o un tanteo para estudiar la respuesta, que por supuesto no espera otra cosa que los rotundos desmentidos oficiales que inexorablemente le siguen.

http://delicious.com/rpla/raa845b

Enlaces

Los enlaces relacionados con este artículo pueden encontrarse en las direcciones que figuran al final de cada texto