Ethical and Moral aspects in UAV and artificial intelligence

Alfredo M. RONCHI
JRC S2D2 – Politecnico di Milano, Milano, Italy
Tel: +39 393 0629373, Email: alfredo.ronchi@polimi.it

Abstract: *Unmanned vehicles represent a successful sector of innovation, an incredible number of drones are actually flying over our heads and unmanned cars are tested along our roads. After few years the increasing diffusion of drones suggested to issue some regulations to frame the use of vehicles that may cause problems in different fields from accidents to privacy. The raising star of autonomous cars started with some safety features like automatic breaking, safety distance keeping, lane control, etc.. Soon radars, sensors, cameras and other devices become integral part of our car providing the opportunity to self-test the "intelligence" of our car. This trend aims to make our transportation means safer and more comfortable, they aim to reduce the stress due to rainy or foggy days or long queues on the motorways during rush hours. Few attentions are actually posed on ethical and moral issues deeply connected with autonomous vehicles. These aspects in addition to intelligent behaviours include, among the others, identification of responsibilities and risk of hacking.*

Keywords: *UAV, Drones, Ethics, Moral, Artificial Intelligence, Machine Learning, Narrow AI*

Introduction

Recently we started to have a better vision about the impact that the cyber era is already having and will have on our everyday life, the 1980s with the introduction of PCs provided a little impact on society, the true turning point was probably in the middle of the 1990s with the rapid spread of the Internet and web technologies together with the semantic shift from computers to household appliances. Since that time major transformations in everyday life and society appeared even if the path of cyber evolution wasn't clear yet. A number of technology-based solutions appeared; we cannot avoid considering networks of sensors, Internet of Things [1,2] and drones in this panorama of solutions. Networks of sensors including CCTV[1] and, even more, Internet of things provide an incredible support both in safety and security [3,4], monitoring or inhibiting hazardous behaviours, alerting people in case of impending danger, activating counter measures or mitigation processes. An incredible number of risky scenarios, including crimes, is mitigated or "solved" thanks to CCTVs [10,11]. We do not refer only to highway traffic control cameras and sensors or "snow" cameras on the mountains, very appreciated by skiers, to but even to forests' fire surveillance based on video

[1] Close circuit television, small intelligent video cameras, nowadays connected to the Internet; it is possible, if allowed, to directly connect to each single camera and watch the scene remotely. This is a typical service available on motorways in order to avoid traffic jams.

cameras mounted on power distribution pillars. In 2017 China was supervised by 180 million CCTV cameras, by 2020 Chinese on line cameras will be 450 million; they will control traffic and fine law's violations, identify bank account holders thanks to bio metric tools and enable ATM transactions or identify airplane passengers at airport gates. Internet of Things will contribute to making the environment "intelligent", enabling direct interaction between objects including smart phones and human wearables.

Autonomous Vehicles

Helicopters use to play a key role in rescue operations since their appearance; nowadays drones represent another true revolution in a large set of fields; usually we term "Drones" the UAVs - Unmanned Aerial Vehicles - but a similar approach applies even to terrestrial vehicles and boats or submarines. All these devices share the same attribute: there are no pilots on board. They may work autonomously or be controlled remotely. One of the first "drones" known by large audience was the military one, Lockheed D12, carried on top of the 1960s Lockheed SR71 codenamed Blackbird. It served as "additional" reconnaissance aircraft, a complete configuration SR71 plus D12 is nowadays on exhibit at the Museum of Flight in Seattle. The evolution of UAVs is not limited to the defence sector, in the nineties a kind of flying drone was developed by the University of Berkley to "scan" the 3D shape of a building.

Nowadays on the shelf drones cover the wide range of sizes and on-board equipment, many APP developers created applications to macro-program drones to operate following specific instructions. The mission could be to "scan" a specific portion of territory or depth of the sea. The field of civil applications is really vast: aerial photography and video, aerial crop surveys, real-time intervention in human/natural disasters, search and rescue, coordinating humanitarian aid, counting wildlife, detection of illegal hunting, monitoring bio-diversity, forest's fire detection and large-accident investigation/monitoring, delivering medical supplies, inspection of power lines and pipelines, crowd monitoring and direct intervention in difficult or dangerous situations. Last but not less diffused the use of drones to inspect trees in urban areas to detect dead branches before they will fall down or various inspections finalised to assist in building refurbishment or restauration. In recent past a research project studied and developed a small airship to 3D scan huge interiors of palaces getting close to vaults and ceilings. In recent times MIT has developed a drone named RFly[2]; such drones may find missing objects using battery-free RFIDs. They are a perfect solution in order to scan warehouses and identify parcels.

In the early stages of drone deployment, they were used even as advertisement tools to attract customers; some hotels used drones to serve breakfast or to deliver ice-cream on the beaches.

Of course, more relevant applications were tested such as first aid kit provision in Russia in the case of a street accident. Law enforcement agencies use drones to fight against crime in different situations; this activated some counter measures such as the anti-aircrafts artillery based on "fireworks" derived missiles. Some implementations of safety and security [6] services in smart cities are based on the use of drones that, activated by sensors and IoT, start flying over specific areas.

[2] https://www.media.mit.edu/projects/wireless-sensing-for-drones-agile-robots-robotics/overview/

Similar solutions have been implemented in facility surveillance; following a randomised program or activated by sensors or cameras, drones take off and reach the required location.
The use of drones is actually regulated by law in different countries, requiring a special "driving licence", and sometimes is restricted due to both safety and security problems.

Ethical and Moral aspects in UAV and artificial intelligence

The previous paragraph emphasized the wide and even increasing number of sectors taking advantages from the use of UAV, thanks to the undoubted added value they offer in a so wide range of sectors we will cohabit with even increasing number of them in the near future. A relevant and recently developed and tested family of Unmanned Vehicles is attracting the public opinion and more specifically drivers; they are autonomous cars, lorries and busses.

We already entered the era of Unmanned Vehicles, drones, boats and more recently cars are going to be "driven" by software, sensors, cameras, radars and more are the senses of our vehicles, the «brain» who drives the vehicle is artificial intelligence. If the risk that a flying or floating drone can be hacked is concerning us as well as the temporary lack of specific legislation, what about the concerns related to ethical and moral aspects, not neglecting the legal ones, concerning autonomous road vehicles such as cars, lorries and buses[3]?

Safety and security standards for such devices are not set actually, how will behave two cars, both from the same builder or not, in case of imminent collision? Of course, the cyber-driver is supposed to be perfect but the environment may introduce some bias, hence on the moral and ethical [12,13] side how will the cyber-driver take decisions?

Let's try to foresee a potential scenario, the Big "Driver" will improve "his/her" artificial intelligence thanks to deep learning and long-term knowledge acquired by big data analytics, s/he will know about causes and effects of thousands of accidents and more or less correct behaviour of each car model reacting in real time to any potential risk. S/he will know the identity of each passenger on board on each car in the surrounding area and in case of collision will probably consider how to minimize damages and if there is no other choice who is going to be sacrificed, the old man or the baby?

The Big Driver will be centralised like air-control or distributed? The same application same release driving each vehicle or different? As it uses to happen with software we will have releases and patches to fix bugs and errors major releases to solve general problems and customised patches to consider events and experiences or adapt to specific car models.

Accordingly with consolidated trends customised A.I. options will appear on the market, today we upload customised software to add horsepower or reshape the behaviour of cars, tomorrow we will look for A.I. options may be to infringe speed limits or be chosen as survival in case of serious accidents.

[3] Suchi as the one recently activated in Paris

The traditional domain of Artificial Intelligence, generated along its path some specific domain of application making our software, home appliances, accessories and cars more “intelligent”. This evolution was accompanied by the usual philosophical debate on “Can machine think?”. The reference study in this sector is indubitably due to Alan Mathison Turing, mathematician, philosopher, cryptographer and more, and his article “Computing machinery and intelligence”[4] , the first paragraph entitled “The Imitation Game” starts with - “I propose to consider the question, "Can machines think?" This should begin with definitions of the meaning of the terms "machine" and "think." – and then explains his vision on “thinking machines” providing a more sophisticated definition and revolutionary insight on future technologies.

The evolution of Artificial Intelligence generated two main branches “strong AI” and “weak AI”. On one side we find a broad-spectrum artificial intelligence designed to face a wide range of problems, on the side of weak AI, also known as “narrow AI”, we find vertical solutions based on a well-defined domain of knowledge as it happens for instance for expert systems or car automatic driving systems. They are designed to deal with a specific domain of knowledge, characterised by well-defined rules and situations; they can be further trained and even implement machine learning; additional everyday examples are intelligent personal assistant, chatbots, SIRI, ALEXA, GOOGLE Assistant, Mercedes Benz and Volkswagen on board assistants.

Machine learning (ML) is an interesting subset of AI that is providing interesting solutions to complex problems, a typical field of application is the one non-approachable with algorithms and explicit programming. The basic principle is to analyse data and identify patterns that can suggest the way to extrapolate a significant result. The typical taxonomy of ML is at top level subdivided in supervised learning and unsupervised learning.
Supervised learning: a system “tutor” feeds the application with a set of inputs and expected outputs to train the system that has the identify a general rule that maps inputs and outputs; of course, this is a possible option when this “rule” is not clearly identifiable by the software programmer so a specific algorithm it is not doable.
Semi-supervised learning: the system receives only an incomplete training, there is not a complete set of outputs related to the list of inputs.
Reinforcement learning: the key feature of this approach consists in a dynamic environment that provides a score (positive or negative) rewarding the strategy to be followed to reach the requested output; thanks to this assessment cycle we can say that the system learns and provide better solutions as much as it runs[5].
Unsupervised learning: the learning algorithm is completely independent, it does not receive any information about the outputs or any score, it must identify by itself the structure of the input and discover potential hidden patters or identify a potential goal thanks to feature learning.

To better clarify the role of ML we can consider, among the others, two typical tasks it can perform:

[4] A. M. Turing (1950) Computing Machinery and Intelligence. Mind 49: 433-460., https://www.csee.umbc.edu/courses/471/papers/turing.pdf last access July 2018.

[5] Bishop, C. M. (2006), Pattern Recognition and Machine Learning, ISBN 0-387-31073-8, Springer

Classification: Inputs are divided into two or more classes; the system must produce a model that assigns additional random inputs to one or more of these classes[6]. As we will see in the following taxonomy this process is usually performed in a supervised manner, the classes are defined a priori. A typical example of classification tasks performed by ML is spam filtering; the two classes are, of course, "spam" and "not spam". The learning process will increasingly add filters to better perform the classification.
Clustering: The tasks is to divide a set of inputs into groups; it looks like the classification tasks but this time the groups are not known beforehand. This typically an unsupervised task.

Let's leave this side of the problem to face another relevant one, how to deal with responsibilities?
If we refer to air-control probably one of the closest sectors the choice is usually between technical problems and human factors. Many times, the final verdict is a mix of a number of causes that all together led to a disaster. Accordingly with the reports, 70% of aviation accidents can be attributed to human error. Why? Because humans are active players inside the systems, and they are the only components that during emergency situations have the capacity to adapt and adjust resources to try to cope with unexpected events. Off course these responsibilities are not only in charge to pilots, they are shared among: organisational failures, conditions of the operators (physical and mental state), physical and technological failures and finally human errors.

Back to road vehicles in case of law infringement or accident who is in charge as responsible, the passenger, the car builder, the software company, all of them? No one, the fate? We must consider that even the "road environment" is part of the system, horizontal and vertical signals, timely updates of maps and road works are integral part of the package. Some lane control systems are cheated by multiple lane lines due to old lines still visible. Some accidents involving cars and even humans already happened and the responsibilities are not yet undoubtedly assigned.

As an additional concern, today even cars may be subject to cyber-attacks [8,9] as it already happened to Jeep vehicles in the United States, if on one side the regular car service or re-call for update can be performed through the permanent car connection to the Internet, no more need to physically take the car back to the service (this might lead to unwanted outcomes), on the other side in case of cyber-attacks our car might behave in a unpredictable way.

The existence of knowledge "silos" unable to cooperate because of the different knowledge background and skills has been recently broken so in the last decades philosophers and humanists started to professionally deal with computer scientists and innovators. They use to consider mid and long-term impacts of technologies on society. Emerging technological trend in autonomous vehicles, robots, machine learning and artificial intelligence may pose significant questions to innovations.

[6] In case of more classes it is termed "multi-label classification".

Conclusions

On the occasion of the test phase of autonomous cars different accidents happened but a recent one posed concretely some of the question already expressed on the occasion of the ICCC 2017 conference held in New Delhi. The driver set the car on auto-pilot mode and drove along the street of the city causing an accident that killed a woman riding a bicycle. In that area the experimentation of automatic driving is allowed so the focus moves on possible bugs of the system or the usual combined action of minor problems causing altogether a disaster?

As a consequence, possibly before a mass diffusion of such vehicles, we must be aware about some aspects: the risk of cyber-attacks that may turn everyday commodities like cars into "weapons" and the "programmed" behaviour of cars in case of "risky" scenarios. Security standards [5] and harmonised "behaviours" together with an appropriate legal framework [7] will probably help.

Bibliography

[1.] SAS report on The Internet of Things - http://www.sas.com/it_it/offers/ebook/iot-visualise-the-impact/index.html
[2.] Babel Chris, Tackling Privacy Concerns Is Key to Expanding the Internet of Things, Wired Innovation Insights, Feb 2015
[3.] Ronchi Alfredo M., WSIS Forum 2015, High Policy Statements. https://www.itu.int/net4/wsis/forum/2015/Content/doc/outcomes/Policy_Statements_Booklet_WSIS2015.pdf
[4.] Ronchi Alfredo M., Duggal Pavan, et al., WSIS Forum 2016 Outcomes, https://www.itu.int/net4/wsis/forum/2016/Outcomes/
[5.] United Nations Manual on the prevention and control of computer-related crime, UN 2001
[6.] Whitman, M. & Mattord, H. (2005). Principles of information security. [University of Phoenix Custom Edition e-text]. Canada, Thomson Learning, Inc. Retrieved May 4, 2009, from University of Phoenix, rEsource, CMGT/432
[7.] Duggal Pavan (2018), Cyber Law 3.0, ISBN 978-81-3125-366-3, LexisNexis, Gurgaon, India
[8.] European Commission (2017), Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN (2017) 450 final
[9.] High Representative of the European Union for Foreign Affairs and Security Policy (2013), Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final
[10.] Burrus Daniel, Who Owns Your Data?, https://www.wired.com/insights/2014/02/owns-data/
[11.] BBC Ethics Guide, http://www.bbc.co.uk/ethics/introduction/intro_1.shtml
[12.] Information for All Programme (IFAP), Information Ethics, http://www.unesco.org/new/en/communication-and-information/intergovernmental-programmes/information-for-all-programme-ifap/priorities/information-ethics/
[13.] UNESCO and WSIS, Ethical dimensions of the Information Society (C10), http://www.unesco.org/new/en/communication-and-information/unesco-and-wsis/implementation-and-follow-up/unesco-and-wsis-action-lines/c10-ethical-dimension-of-the-information-society/