Auteur: Ir.drs J. van der Vlugt CISA CRISC. Jurgen is zelfstandig professional voor Information governance- en risk management advisering en audit. Jurgen is te bereiken via jvdvlugt@xs4all.nl.

AI, Max!

In deel 1 zagen we dat zelfrijdende auto's – zelfs in combinatie met menselijke back-up chauffeurs – nog (veel) te weinig zelf kunnen om veilig zelfstandig de weg op te mogen (1). Waarbij voor het gemak nog voorbij was gegaan aan de kwetsbaarheden die aan al die software kleven. Er schijnt in Gelderland een stuk weg te zijn waar al diverse T…'s (betreffende autofabrikant zal wel anoniem willen blijven) naast de weg in de sloot zijn beland. Een soort anti-lane departure correctie. Is dat nou een feature of een bug (2)?

Deel 3 van 3: Auto's, besturing en reflexen

Zo zullen er ongetwijfeld nog vele kleine 'dingetjes' net niet helemaal netjes zijn uitgewerkt. Het is evenmin zo dat iedereen doelgerichte proefritten gaat maken om nieuwe functionaliteiten te testen om zo een patch op het motormanagement door te (laten) voeren. Dat doen uw IT-beheerders voor nieuwe software-patches wel, waarom zouden de 'eindgebruikers' dat voor auto's niet hoeven doen? Aansprakelijkheid is een heikel ding, in de autowereld.
Andere kwetsbaarheden die nog ongenoemd waren, liggen op het vlak van beheer en beveiliging in engere zin (afscherming). Wie denkt dat het met het Identity- en Access Management (IAM) wel goed zit, heeft hopelijk een goede levensverzekering voor de nabestaanden. Zie bijvoorbeeld het prijswinnende Hacker gehackt van Joost Geerts in iB-Magazine 2020-5: een inbraak zit in een klein hoekje. En het gaat niet alleen om de spraakmakende inbraken waarbij een complete autobesturing wordt overgenomen (qua haalbaarheid al aangetoond) – wat in zulke gevallen bijna gelijk een class break is; alle auto's met dezelfde software kunnen door hetzelfde gaatje worden gehackt. Het gaat óók over de hele software-ontwikkelketen. Waar ransomware steeds vaker via supply chain attacks binnenkomt, zal dat voor autosoftware-kraken zeker ook een optie zijn en blijven.
Waar we in de informatiebeveiligingswereld onszelf bezighielden met statische servers (3) en de in de loop der tijd geëvolueerde software-ontwikkelmethodieken alsook informatiebeveiligingsformules (denk aan 'standaard' IAM, OTAP-straten, Change Management-procedures, et al.), zien we dus een forse toename in de reikwijdte van ons werk; waarvoor we nog bezig zijn de standaarden te ontwikkelen. Evolutie van de huidige standaarden kan al te weinig zijn om de exponentiële complexiteitsgroei van de problematiek aan te kunnen. En uiteraard is OT-security (4) voor velen een nog veel te onontgonnen terrein: voor vakgenoten én voor onze klanten; in het land der blinden lijkt eenoog al snel koning. Dus wie een halve-carrièreswitch overweegt: Kijk eens naar dat OT-security…!

Sturing door overheid

In deel 2 bleek ook dat 'centrale' aansturing of hulp niet gaat helpen of van de wal in de sloot qua privacy en eigen verantwoordelijkheid (5). Misschien kunnen we nog wel wat met dynamische wegmarkering – maar dat riekt natuurlijk direct weer naar 'sturing door een overheid' en de ervaring leert dat zulks niet vanzelf altijd maar goed gaat. Smart parkeerplaatsen, verkeerslichten: idem – stel je voor dat een fabrikant het voor elkaar krijgt om de eigen auto's bij de verkeerslichten voorrang te laten krijgen (6). Al hetgeen met centrale besturing samenhangt, komt al snel uit bij de Grote Drie van bezwaren tegen overheidsbemoeienis:

1. Ik wil niet dat de overheid weet waar ik ben;
2. Ik wil niet dat de overheid stuurt op basis van potentieel (sic) willekeurige discriminatie of wat dan ook tegen art.1 van de Grondwet;
3. Integriteit van data is niet in het belang voor diegene die de integriteit kan beheersen.

De overheid heeft geen belang bij de integriteit, die mij specifiek zou kunnen hinderen, u en ik wel. Voor toezichts- of controlemogelijkheden is het andersom, een typisch geval van verkeerd belegde incentives en afschuifbare externaliteiten.
Vooralsnog blijken ook degenen die middenin de ontwikkelingen rond zelfrijdendheid (7) bezig zijn, te beseffen dat de wereld iets ingewikkelder is dan gedacht. Het als grote jongen roepen van uitdagen¬de doelstellingen is altijd een risico en zeker als het om realiseringsdatums voor zelfrijdende auto's gaat. Ene Elon M. van garage T. moest al op zijn beloften terugkomen (8). Ook anderen zijn voorzichtiger geworden of zijn zelfs opgehouden met vooraan te willen lopen.

Complex

Als tussentijdse conclusie moet dan ook gelden dat de 'AI' van zelfrijdende auto's niet verder is dan bijvoorbeeld dat andere 'poster child' Watson in het medische domein; namelijk, echt nog niet beter dan mensen (9). Ook de winst van Watson (niet één maar 42 samenwerkende machine learning systemen!) bij Jeopardy was niet zo indrukwekkend als men wel denkt. De vragen waren in een nog steeds relatief gesloten, beperkt domein. Watson won maar net en had een aantal domme foute antwoorden en onbegrijpelijke missers. En het basis opzoek- en rekenwerk was niet zo 'intelligent' (10).
Het enige werkveld waar redelijk ongestoord voortgang wordt gemaakt, is er een waar we dat misschien niet echt zouden moeten willen: autonoom schietende killer bots. Nu nog heel experimenteel in het militaire domein, met de nodige blunders, ethische vragen (11) en praktische problemen. Zo meteen misschien al paramilitair of 'orde handhavend' bij onwelgezinde politieke demonstraties? Hoewel deze auteur nog wel nut ziet in na-montage van zoiets als accessoire (12).
De autowereld heeft natuurlijk bovendien ook wel bij uitstek te maken met complexiteit. Binnen de auto (het blijft een beperkte fysieke ruimte en het functioneren van de onderdelen

is gesneden koek), maar vooral ook in de omgeving. Zóveel actoren en passieve objecten vind je niet snel in andere domeinen waar het met AI ook al niet opschiet, dus voor auto's wordt het lastig. Waar vinden we zoveel actoren?

Tot nu toe bleek een fietser die achter een stilstaand voorwerp vandaan komt – waar die eerst achter uit beeld raakte – twee verschillende objecten met onbekende bewegingsrichting en -snelheid (13). Een bal die, om het nog erger te maken, onverwachts de weg op stuitert wordt nogal eens gevolgd door een klein kind; veel kwetsbaarder dan die bal op zich. Dat weet iedereen. Maar uw auto nog lang niet. Logisch (sic) maar niet handig.

Training

Waar is de niet-acterende, passieve omgeving zó complex en onregelmatig? De ene boom ziet er net wat anders uit dan de andere. En verkeersdrempeltjes zijn soms slechts chauffeur wakker schuddend, soms forse hobbels. Je ziet het niet altijd aankomen. En er verandert zo veel in de omgeving, zelfs wat stil lijkt te staan. Omleidingen, rijbaanverleggingen, etc. – ja, de wereld om ons heen verandert voortdurend (14). Waarnaast natuurlijk het rijgedrag van overige weggebruikers hoogst variabel is. De ene fietser reageert beslist anders dan de andere. Succes, zelfrijdende auto in Amsterdam…! Maar ook… de ene oude-Saab-rijder reageert nog slechter dan de andere (15).

Wat dus nodig zal zijn – en de eerste ontwikkelingen in labopstelling gaan die kant gelukkig ook op – is een exponentiële schaalvergroting in de complexiteit van algoritmiek en berekening. Niet alleen een enorme schaalvergroting en -verdieping van neurale netwerken kan ons redden. Hoeveel lagen méér we nodig hebben en hoeveel breder die moeten zijn (mét variaties in de triggerfuncties op de nodes, de backpropagation etc. etc.), met navenant méér trainingsdata; wie het weet mag het zeggen. "Heul veul," is wel het minste.

En dan houden we over de issues met:

De huidige 'AI'/ machine learning;

Van het alleen maar kunnen interpoleren met de zo snelle afname van relevantie bij extrapolatie;

Eerste en tweede ordefouten, die niet noodzakelijkerwijs kleiner worden, etc.

Wat erbij nodig zal zijn, is een koppeling met elementen uit de aloude Expert Systemen met hun relatief abstracte symboolmanipulatie op basis van declaratie van axioma's ('feiten') en productieregels. In combinatie met rechttoe-rechtaan gewone procedurele algoritmen (16) én anderzijds fuzzy logic. Of is dat laatste een, overgeslagen, extra stap bij machine learning? Gooi er dan nog een forse scheut seeding en tweetraps leren bij (inprogrammeren van heuristieken uit data

> Nee, voorlopig zullen we het moeten doen met, als het eventueel toch zou lukken, een Formule A(utomatically driven by software). De formule 1 e.v. waren toch altijd officieel bedoeld als testomgevingen voor het neusje van de zalm qua techniek. Nou, daar past het zelfrijdende, dat als neusje van de zalm qua autotechniek geldt (of ooit zal gelden), toch mooi bij? De belofte was 'juist het stukje Sturen te automatiseren' – dat was zowat als enige deelprobleem niet met techniek oplosbaar, maar nu wellicht wel. In plaats van wat waaghalzen-met-andermans-kapitaal kunnen we nu terug naar het testen van de beste nieuwe technieken! Maar dan is het geen showbizz meer maar (software-)vendors die tegen elkaar pitchen.
>
> Ga maar na: De situational awareness (andere Auto's, gele vlaggen wegens olielekken etc.), is voor alle teams gelijk te trekken met centraal verwerkte en doorgegeven beelden want het privacy-idee van artikel II is hier niet relevant. En wie wat extra's wil qua omgevingsawareness kan dat gemakkelijk toevoegen. Bandeslijtage, specifieke eigen technische parameters: laat maar zien dat die 'perfect' worden verwerkt. De verwerking van al die data kan in de auto óf gewoon in de pits zoals nu al wordt gedaan, toch?
>
> Het zal wat ver buiten ons beeld zijn – want saai (geen Max- maar Lewis-stijl) – en stil want we gaan er wel vanuit dat elektrisch de toekomst heeft. Dus is het voor publiek niet aantrekkelijk om te zien: live dan wel vanuit huis. Maar het kan bij uitstek een enigszins beperkt complexe 'omgeving' realiseren om het zelfrijdende van auto's steeds verder te ontwikkelen. Tot ze de weg op kunnen. Er is zelfs een minieme kans dat Tesla dan nog bestaat.

of menselijke ervaringen, semi-symbolisch, waarna verder kan worden getraind op data) met flexibele neurale-netwerkstructuren en wie weet krijgen we iets zinvols.

Ook pruning, het snoeiwerk in neurale netwerken, is vooralsnog te weinig van de grond gekomen. En als er na snoeien weinig connecties overblijven, misschien kunnen we dan terug redenerend wel tot kennelijke algoritmen komen, bij wijze van emergent properties in de data?! Pas dan hebben we inductieve wetenschap. Nou ja, inductieve berekeningen; naast de deductieve traditionele algoritmen.

Zo ver zijn we helaas nog lang niet. We zullen met 'AI' nog een derde keer (17) een 'AI-winter' ingaan. Hoewel vorige keren óók een klein aantal toepassingsgebieden best van de grond leken te komen, zal dit in het publieke discours beperkt zichtbaar blijven. Afgezien van die paar verschrik¬kelijk verkeerde toepassingen:

- Discriminerend, zodra (18) door de overheid ingezet;
- Privégegevens stelend, (19) als het door private partijen gebeurt en
- Ach, de paar puntoplossingen die 'AI' nu automatiseert in bedrijfsprocessen.

RPA is ten slotte ook maar het oude straight-through processing gekoppeld aan een net wat bredere variatiemogelijkheid in transacties dan het (sic) Six Sigma-denken (20). AI zijn er nog steeds een aantal betrokkenen die geloven dat het met rechttoe-rechtaan hard doorwerken zou moeten kunnen lukken, met automatisch rijdende auto's (21).

AI verder helpen

En laten we ondertussen in de gaten houden waar we met puntoplossingen puntproblemen kunnen aanpakken. Dus niet al te complex, want het lijkt wel alsof complexiteit van problematiek - inhoudelijk en qua context - de achilleshiel is van AI/machine learning. Misschien moeten we juist veel meer experimenteren met bijvoorbeeld RPA? AI is het een klein issue, met klein nut, we kunnen wel leren wat het kan en vooral wat het niet kan.

En we kunnen op zoek naar vergelijkbare 'probleemgebieden' om AI verder te helpen.

Zo ben ik vanuit een brede interesse in alles wat met wijn te maken heeft, heel blij met de ontwikkeling van geautomatiseerd wijngaardbeheer. Drones kunnen individuele stokken met spectraalanalyse controleren op het begin van ziektes en (rondrijdende) drones kunnen dan alleen de stokken die het nodig hebben, bespuiten met bestrijdingsmiddelen (22). Dat scheelt een hoop bestrijding! We zijn bijna zover: alleen de geautomatiseerde koppeling van lucht naar grond ontbreekt nog. Nu nog het snoeien en de pluk automatiseren. Moeilijk, want fysiek delicaat en zeer ervaring gebonden. En het proeven (23), dat mag u aan mij overlaten.

We zijn bijna zover: alleen de geautomatiseerde koppeling van lucht naar grond ontbreekt nog.

Referenties

(1) Goto HumanDriver Considered Dangerous, iB-Magazine 2021-3.
(2) Het is min of meer formeel gedocumenteerd, ergens, dus zouden sommigen het een feature noemen. Maar voor de gebruiker (de backup-chauffeur!) is dat niet leesbare commentaar dus een bug..?
(3) Ook de cloud is slechts 'andermans servers die fysiek ergens staan'.
(4) De Operational Technology in de auto, maar buiten scope van dit artikel ook in 'de' fabriek. De 'koppeling' van OT aan kantoorautomatisering staat qua integrale beveiliging ook nog in de kinderschoenen.
(5) Aangestuurd autorijden, iB-Magazine 2021-5
(6) Zo zou het een fabrikant ook niet kunnen schelen dat verkeerd gedrag van één Saab-rijder in software-updates zou worden verwerkt en alle Saab-rijders agressiever zou afstraffen. Zie ook (14)
(7) Men vreze, dat dit zojuist verzonnen woord niet in de nieuwste Van Dale is opgenomen.
(8) Eerst was het: www.inc.com/nick-hobson/elon-musk-says-hes-close-to-solving-one-of-hardest-technical-problems-thats-ever-existed-is-he-really.html maar ook toen was er al www.wsj.com/articles/self-driving-cars-could-be-decades-away-no-matter-what-elon-musk-said-11622865615, waarna Musk in www.theverge.com/2021/7/5/22563751/tesla-elon-musk-full-self-driving-admission-autopilot-crash moest terugkrabbelen.
(9) Met enige regelmaat komen er fraaie verhalen de wereld inzeilen, maar serieuze analyses gooien die verhalen telkens weer van tafel.
(10) Zie https://codeburst.io/ken-jennings-and-brad-rutter-were-tricked-by-watson-they-should-demand-a-rematch-6a5ba2661ab0
(11) Wie denkt dat zij/hij begrijpt hoe non-discriminatie- en ethische afwegingen in AI zouden moeten, kan https://pair-code.github.io/what-if-tool/ai-fairness.html bestuderen en oefenen. Eenduidige antwoorden zijn er niet.
(12) Zie ook (14).
(13) Gelukkig dat Heisenberg's Onzekerheidsprincipe op deze schaal niet van toepassing is. Voor de jeugdige lezers: dit betreft Heisenberg, de gigant in de theoretische fysica, niet die van de Netflix-serie.
(14) Hierin zit dus een hint: Vertrouw niet te veel op centraal verzamelde omgevingsdata! Maar ja, die zijn wel de basis voor routeberekeningen en het 'plaatsen' van gedetecteerde objecten. Of moet 'alle' omgevingsdetectie dan maar altijd opnieuw ter plekke worden gedaan door iedere zelfrijdende auto...?
(15) Ervaringsfeit van ondergetekende, geen Saab-fan.
(16) Tsja, ook gewoon programmeerwerk met Let, If-Then en Jump. Dat zijn de enige primitieven die nodig zijn...! Ook Call-Return, While, For-Next... u noemt ze maar, zijn herleidbaar tot die drie. Ook dit soort 'programma's' implementeren algoritmen! Dat de wereld zich de laatste vijf jaar zo druk maakt met het toezicht op 'algoritmes', is dus een halve eeuw te laat. Laten we hopen dat er in al die (overheids- en andere) systemen niet al te veel discriminatie is verwerkt.
(17) Na de jaren 50-70 en eind jaren '90.
(18) Noem eens een systeem waar de overheid niet in discrimineert.
(19) Social media krijgen betaald voor uw gegevens, dús zijn ze wat waard. Wat ziet u ervan terug? Verkokering (filter bubble)? Dat is inbreuk op privacy want de keuzevrijheid belemmerend.
(20) Dat eindelijk ontmaskerd is als nauwelijks verholen opvolger van Operations Research en daarvoor Scientific Management: Alles voor het terugdringen van afwijkingen, terwijl de klant juist meer flexibiliteit blijft vragen.
(21) Zie bijvoorbeeld boek: Autonomy The Quest to Build the Driverless Car and How It Will Reshape Our World van Lawrence Burns
(22) Wetende dat tot in de meest biodynamische methoden het platspuiten met kopersulfaat gewoon 'mag'. Dat is vreemd hè, want kopersulfaat is best agressief chemisch en vervuilt de bodem.
(23) Eenieder die weet wat proeven inhoudt, weet dat niet 'drinken' laat staan 'grote hoeveelheden drinken' bedoeld is!