Autonoma bilar, teknologi och säkerhet

Max Westerback 38886

Kandidatavhandling i Datavetenskap

Handledare: Annamari Soini

Åbo Akademi

2019

Innehållsförteckning

[1. Inledning 1](#_Toc4593840)

[2. Tekniska tillvägagångssätt 2](#_Toc4593841)

[2.1 Tesla 2](#_Toc4593842)

[2.1.1 Teslas säkerhetsaspekter 3](#_Toc4593843)

[2.2 Google Waymo 6](#_Toc4593844)

[2.3 Använding av neurala nätverk 8](#_Toc4593845)

[2.4 Waymo ChauffeurNet 11](#_Toc4593846)

[3. Säkerhetsaspekter 13](#_Toc4593847)

[3.1 Djup maskininlärning och felaktiga bilder 13](#_Toc4593848)

[3.2 Autonoma bilar, kommunikationstekniker och datasäkerhet 14](#_Toc4593849)

[4. Diskussion: 17](#_Toc4593850)

[Referenser 18](#_Toc4593851)

# Inledning

En autonom bil är en datorkontrollerad bil som kan köra sig själv utan mänsklig förare. I dagens läge är dessa bilar även kända som självkörande bilar, obemannade markfordon och robotbilar. De kan använda sig av GPS för att hjälpa med navigeringen och olika typer av sensorer, kameror, radar och artificiell intelligen (AI) för att undvika kollisioner. De har potentialen att rädda liv genom att drastiskt reducera fordonsrelaterade olyckor, minska trafikens överbelastning och energiförbrukning, öka produktiviteten och ge mobilitet till de som inte kan köra. Society of Automative Engineers (SAE) släppte 2014 ett klassificeringssystem baserat på sex olika nivåer av automation och det är idag den standard som används för att bedöma fordons nivå av automation. De sex nivåerna är:

1. Fordon utan automation
2. Fordon som hjälper med en funktion som styrning, acceleration eller inbromsning.
3. Fordon med delvis automation som hanterar åtminstone två olika funktioner.
4. Fordon med villkorlig automation där alla aspekter är automatiserade under vissa omständigheter men föraren måste vara beredd på att överta kontrollen.
5. Fordon med en hög nivå av automation som inte kräver en mänsklig förare förutom i situationer som dåliga vägar eller väldigt dåligt väder.
6. Fordon med full automation som hanterar körningen i alla olika situationer.

AI-tekniken är den centrala teknologin som avgör inom vilken nivå fordonet faller. Ju högre automation, desto smartare behöver fordonet bli. Bilens intelligens kan delas i fyra delar: avläsning, uppfattning, förutsägelse och planering. I delen för avläsning samlas data från bilens sensorer, uppfattningsskedet ansvarar för att använda denna information för att skapa en förståelse för miljön runt bilen. Utvecklare av mjukvaran hos autonoma bilar använder sig av befintliga scenarier och träningsdata för att förutsäga nya utfall och situationer, så som ett objekts nästa rörelse, och planering är den fas där bilen fattar beslut om sina handlingar. De tre sista stadierna utnyttjar maskininlärning och djup maskininlärning för att skapa olika nivåer av automatiserade bilar.

I den första delen av denna avhandling kommer jag diskutera Tesla och Waymo, främst skillnaden mellan deras val av hårdvara och deras tillvägagångssätt för att samla in data. Hur neurala nätverk används inom autonoma bilar diskuteras även. I andra och sista delen presenteras säkerhetsrisker inom djup maskininlärning och autonoma bilar, främst sådana som hör till datasäkerheten.

# Tekniska tillvägagångssätt

I denna del av avhandlingen presenterar jag två olika företags strategier för att uppnå en hög nivå av automation och säkerhet. Tesla och Waymo är de två ledande företagen inom autonoma bilar som även använder sig av olika sorters teknologier för att samla in data, mera specifikt olika sorters hårdvara. Neurala nätverk är en teknologi som används inom autonoma bilar för att skapa mjukvaran för bilarna. Jag presenterar vad neurala nätverk är och hur de kan användas inom utvecklingen av autonoma bilar.

## 2.1 Tesla

För att skapa fullt autonoma bilar behövs enorma mängder data från vilka bilarna kan lära sig att köra sig själva. Det finns två olika företag med ett stort försprång inom kampen att samla in den data som behövs. Ett av dem är Tesla. Deras nuvarande bilar som är kommersiellt tillgängliga estimeras ligga mellan nivå 2 och 3 för autonoma bilar. De säljer ”Enhanced Autopilot” (EA) som sitt nuvarande autonoma system som ligger mellan nivå 2 och 3 med framtida planer för ”Full-self-driving” (FSD) som ska uppfylla kraven för nivå 4. Enligt Teslas hemsida är deras EA kapabel av att styra, accelerera och bromsa inom vissa körfält [27].

Det som ger Tesla en fördel är att de redan är ute på marknaden. Med över 500 000 bilar runt omkring i världen kan de samla in stora mängder data som ger dem en inblick i hur människor och deras EA beter sig på vägen [2]. Enligt Tesla är deras bilar utrustade med 8 kameror, 12 ultraljudssensorer och en framåtriktad radar [28]. Med denna hårdvara kan de samla in data över bilarnas hastigheter, accelaration och inbromsning, säkerhet och även videoklipp från olyckor m.m [3]. Elon Musk, Teslas styrelseordförande och vd, sade i en blogg att de samlar in data från över 5 miljoner kilometer av körning per dag [4]. Denna data är dock inte bara från då EA är aktiverad eftersom det fortfarande bara är en semi-autonom funktion. Tesla säger att denna hårdvara är tillräcklig för att i framtiden nå nivå 4 [28], så de har valt att behandla autonoma bilar mera som ett mjukvaruproblem istället för ett hårdvaruproblem. Deras val av hårdvara gör bilarna billigare att producera men är även deras största nackdel; de använder sig inte av ”Light Detection and Ranging”(LIDAR). LIDARs använding inom autonoma bilar diskuteras närmare i kapitel 2.2. Tesla har valt att fokusera på kameror för att de ser LIDAR som en krycka som gör det lättare på kort sikt men som blir för dyr och skrymmande i längden [5]. Tesla har valt kameror och AI som deras lösning för att i framtiden nå fullt autonoma bilar. Att bearbeta den data de får från sin hårdvara visar sig vara svårt för Tesla. Fast de har stora mängder data så är deras dataset inte lika detaljerad som den skulle vara med hjälp av LIDAR, vilket gör det svårt för fordonet att lära sig från datan.

### Teslas säkerhetsaspekter

Enligt Tesla är deras bilar ett säkert och tryggt val ute i trafiken [7], dock så finns det säkerhetsrisker kopplade till mjukvaran. 2016 lyckades Keen Security Lab i Kina utnyttja flera säkerhetsproblem vilka gav dem möjligheten att kontrollera flera aspekter av bilen på distans utan att ha någon fysisk kontakt med själva fordonet [8]. Då webbläsaren användes och bilen var fysiskt nära och ansluten till en illvillig Wi-Fi-hotspot kunde de attackera bilens CAN-buss, en databuss som används i fordon för att flera noder eller styrenheter i fordonet kan sända meddelanden till varandra. Detta gav dem möjligheten att öppna soltaket, flytta bilsätet, aktivera svängsignalen, inaktivera kontrollskärmen och låsa upp dörrarna då bilen var parkerad. Då bilen var i rörelse kunde de fjärraktivera vindrutetorkarna, vika in bakspeglarna, öppna bagageutrymmet och aktivera bromsarna från 19 kilometers avstånd. Efter 10 dagar släppte Tesla en programuppdatering som adresserade säkerhetsproblemen [9].

Forskare vid Katholieke Universiteit Leuven (KU Leuven) i Belgien har utnyttjat en säkerhetsbrist med systemet ”Passive Keyless Entry and Start” (PKES) för att låsa upp en Tesla Model S på några sekunder[14]. PKES-systemet tillåter bilen att låsa upp och starta beroende på fysiska närheten av den parade fjärrnyckeln (eng. key fob), ingen användarinteraktion krävs. Teslas PKES-system använder sig av ett ”Challenge response protocol” , se figur 1.

A screenshot of a cell phone

Description automatically generated

Figur 1: PKES system. Hämtad från [14]

En av säkerhetsbristerna med systemet är att det saknas ömsesidig autentisering vilket leder till att om man vet bilens identifierare, som är offentlig, så kan man skicka och motta meddelanden från bilens fjärrnyckel. Största säkerhetsbristen är dock valet av kryptografins algoritmer för att beräkna det svarmeddelandet på 24 bitar. Teslas system använder sig av en utdaterad skyddad chiffer, vilket betyder att algoritmens källkod är dold, kallad DST40. DST40 (Digital signature transponder) är en kryptografiskt säker radiofrekvensidentifikations (RFID) enhet som förvandlar utmaningsmeddelandet på 40 bitar till svarsmeddelandet på 24 bitar. Denna omvandling är beroende på den hemliga kryptografiska nyckeln på 40 bitar i DST40 [33]. Eftersom svaret (24 bitar) är mindre än utmaningen(40 bitar) betyder det att det finns många olika kryptografiska nycklar som skulle producera samma svar för en utmaning. Tidigare forskare har lyckats demontera(eng. *reverse engineer*) en DST40s algoritmer vilket visade att de behöver två par av utmaning/svar-meddelanden för att bestämma en unik nyckel [34]. Angriparen testar varje nyckel på den första utmaningen, och när ett svar matchar verifierar angriparen ifall nyckeln också fungerar på det andra utmaning/svar-paret.

Eftersom bilens identifierare är offentlig kan man skicka utmaningar till dess fjärrstyrda nyckel och observera svaret. Eftersom DST40 har en så liten mängd möjliga nycklar, i detta fall , och ingen ömsesidig autentisering är det möjligt att utföra en ”Time-Memory Trade-Off”(TMTO) attack. TMTO står för en algoritm som förbättrar(förkortar) körtiden genom att använda mera utrymme(minne), eller som på ett motsvarande sätt som förbättrar minnesanvändningen på bekostnad av längre körtid[35]. Tanken är då att utföra förutberäkningar och lagra resultaten. Dessa resultat kommer att minska antalet beräkningar och därmed tiden som krävs för att utföra varje efterföljande nyckelåterställning (eng. *key recovery*). KU Leuvens forskare använde sig av en utmaning(0x636f736963) och beräknade svaret för varje nyckel. Därefter grupperades alla nycklar som producerat samma svar i en enda fil, se figur 2.

A close up of a sign

Description automatically generated

Figur 2: Visuell representation för datastrukturen. Hämtad från [14]

För att få nyckeln för en specifik fjärrnyckel skickar forskarna deras tidigare utmaning(0x636f736963). Genom att använda svaret kan de läsa den rätta filen från deras TMTO-datastruktur. Filen ger en lista på 2^16 nycklar. Nästa steg är att fråga efter ett nytt svar för en annan utmaning. Det är så de får deras andra utmaning/svar-par vilket gör att de kan söka filen för den rätta nyckeln. Sista steget tar i genomsnitt 2 sekunder att utföra i mjukvaran hos en Raspberry Pi 3 Model B+. Att söka igenom alla 2^40 nycklar skulle det ta dem 777 dagar.

Ett koncepttest lät forskarna klona en fjärrnyckel på några sekunder med hjälp av en enhet som består av en Raspberry Pi 3 model B+, Proxmark3, Yard Stick One och ett USB-batteri. Raspberry Pin kopplas till en smarttelefons WiFi-hotspot så att den kan ladda ner filer från en 6-TB-hårddisk som innehåller forskarnas TMTO-tabeller. Se artikel [14] för koncepttest av attacken.

Tesla har bemött kritik mot deras EA-system. Namnet Autopilot lurar vissa förare att tro att deras bilar är mera kapabla än vad de verkligen är [13] [30]. Eftersom EA inte är helt automatiserad krävs det att man ska vara beredd att ta kontroll när som helst och EA meddelar med ett två minuters intervall att man ska ha händerna på ratten. Detta har lett till att förare försöker lura systemet genom att använda sig av en ”Autopilot Buddy” [10], en magnetisk rämsa som fäster sig på ratten, eller andra föremål som vattenflaskor och appelsiner[11]. Att utnyttja systemet leder till böter och det är förbjudet att sälja Autopilot buddy i USA [12].

Navigant Research, en konsultfirma för fordon, gjorde 2018 en undersökning på 20 olika företags autonoma bilar. Undersökningen baserades på 10 kriterier: företagets självkörande vision; marknadsstrategi; partners; produktionsstrategi; teknologi; försäljning, marknadsföring och distribution; produktens förmåga; produktkvalitet och tillförlitlighet; produktportfölj; och uthållighet. På basen av dessa kriterier landade Tesla andra från botten och på toppen har vi Googles Waymo. [32]

## 2.2 Google Waymo

Teslas största konkurrens inom datainsamling är Googles Waymo. Största skillnaden mellan företagen är deras val av tillvägagångssätt för att samla in data. Medan Tesla fokuserar på att använda sig av data från deras hundratusentals bilar ute på vägen använder sig Google av kraftfulla datorsimuleringar. Sent i 2018 meddelade Waymos vd att deras bilar har kört över 16 miljoner kilometer utan mänsklig förare och över 11 miljarder kilometer i simuleringar [6]. Medan Tesla använder sig av sensorer och kameror har Waymo valt LIDAR. LIDAR påminner mycket om en vanlig radar, men istället för att använda sig av radiovågor använder den sig av reflekterat ljus från en pulserande laser. Genom att mäta tiden det tar för en sensor att registrera ljusstrålens reflektion kan man beräkna avståndet till objektet. Med hjälp av LIDAR kan Waymo skapa tredimensionella kartor av bilens omgivning med en räckvidd upp till 50 meter. LIDARs bildkvalitet påverkas inte heller av mörker som är ett problem för kameror, radar och ultraljud. LIDAR är dock inte optimalt i dåligt väder eftersom snö och regn kan störa lasern vilket kan få bilen att se hinder som inte existerar. Medan valet av LIDAR är kostsamt leder det till ett mera detaljerat dataset vilket är viktigt för säkerheten och gör det lättare att bygga en realistisk simulering.

Waymo har skapat en virtuell verklighet kallad ”Carcraft” där de kör simuleringar där deras bilar kör i simulerade städer med bilister, cyklister och fotgängare dygnet runt. Simuleringarna gör det möjligt att testa alla sorters händelser som skulle vara för specifika eller farliga i verkliga världen.

A circuit board

Description automatically generated

*Figur 3: Karta av en simulerad värld. Hämtad från [16]*

En stor del av simuleringarna är baserade på situationer där deras bilar har upplevt problem ute på vägen, vilket gör det möjligt att snabbt testa och hitta lösningar för svåra situationer. Waymo använder sig av **sårbarhetstestning för att testa unika och oförutsägbara händelser. Sårbarhetstestning innebär att man kör igenom samma simulering samtidigt som man lägger till slumpmässiga variationer varje gång, för att se om dessa störningar kan orsaka olyckor eller att saker går sönder. Se figur 4 för exempel av sårbarhetstestning.**

A close up of a map

Description automatically generated

*Figur 4: Exempel av Waymos sårbarhetstestning. Hämtad från [16]*

**Waymo har förutom datorsimuleringarna också byggt en dedikerad testanläggning i Kalifornien där de kan bygga upp gator med specifika egenskaper eller skapa olika scenarier som verkar ge deras fordon mest problem. Dessa testningsmetoder har kommit till priset av stora investeringar, resurser, tid och ansträngning men eftersom Waymo är ett dotterbolag till Google har det inte äventyrat företagets framtid. Detta är en stor fördel Waymo har över Tesla.**

Eftersom Waymo samlar in stora mängder data från virtuella världar är det svårt att säga när deras bilar är ett säkert val ute på vägen. Oberoende av hur bra simulering kan skapas så är de ändå en förenklig av den verkliga världen. RAND Corporation, en tankesmedja, släppte 2016 en studie som fokuserade på hur många verkliga kilometer en autonom bil måste köra för att visa sig vara säker. Deras slutsats var att autonoma fordon skulle behöva köras hundratals miljoner kilometer och ibland hundratals miljarder kilometer för att visa sin tillförlitlighet när det gäller dödsfall och skador [17].

## 2.3 Använding av neurala nätverk

Enligt Waymo finns det fyra olika frågor en bil behöver kunna svara på för att uppnå målet med fullt autonoma bilar[18]:

1. Var är jag?
2. Vad finns runt mig?
3. Vad kommer hända härnäst?
4. Vad ska jag göra?

Ett vanligt sätt att svara på dessa frågor är att använda sig av djup maskininlärning(eng. *Deep learning*), mera specifikt djupa neurala nätverk. Maskininlärning fokuserar på utvecklingen av algoritmer som kan lära sig av och göra förutsägelser på data. Djup maskininlärning är en avancerad typ av maskininlärning där datorsystemet självt utvecklar program för att lära sig lösa problem. Ett vanligt syfte är att lära datorerna att känna igen olika objekt, så som bildklassificiering, och för detta krävs det stora mängder av data som systemet kan analysera och öva sig på. Algoritmerna inom djup maskininlärning efterliknar människans hjärna genom att använda artificiella neurala nätverk. [19]

Ett artificiellt neuralt nätverk(ANN) är ett datorsystem, inspirerat av biologiska nervsystemet, som lär sig lösa problem genom att man först tränar det. Nätverket har ingen förståelse av problemet som ska lösas men lär sig genom att träna med exempel där resultatet är känt. Neurala nätverk är själva ingen algoritm utan de är ramverk för många olika maskininlärningsalgoritmer som jobbar tillsammans för att hantera indata. Neurala nätverk består av tre typer av lager: indata, dolda och utdata, som var och en består av en eller flera noder. [20]

A picture containing text, map

Description automatically generated

Figur 6: Visualisering av ett artificiellt neuralt nätverk. Hämtad från [21].

Ett djupt neuralt nätverk(DNN) är ett ANN med många dolda lager mellan indata och utdata där flera matematiska funktioner är kombinerade i var och en av dem [22]. DNN kan användas på två olika sätt för att svara på frågorna presenterade tidigare i detta kapitel.

En vanlig lösning är att dela upp frågorna i olika komponenter och behandla dem i olika nätverk för att sedan kombinera resultaten från dessa och låta datorn göra ett beslut. Fördelar med detta tillvägagångssätt är: säkerheten kan beräknas och tränas tills en önskad noggrannhet uppnås; det är lättare att hitta och lösa problemen som uppstår, då lösningen är uppdelad i olika komponenter; och att komponenterna kan tränas för att hantera oförutsägbara och farliga situationer. Negativa aspekter är: det är flera komponenter som behöver programmeras samt tränas vilket är väldigt tidskrävande; det samlas även in onödiga data, eftersom allt som registeras inte är nödvändigt för att fatta ett beslut. [24]

Den andra lösningen till frågorna är att använda sig av ändpunkt till ändpunkt(eng. *end-to-end*) inlärning, vilket innebär att en enda DNN samlar bilens indata och beräknar ett beslut som utdata. Lösningens DNN lär sig köra automatiskt genom träning av data från riktig mänsklig körning, den lär sig alltså genom att imitera istället för att förlita sig på förekomsten av tidigare kända specifika egenskaper som kan detekteras. Fördelar med detta tillvägagångssätt är: nätverket behöver inte meddelas hur ett fordon eller körfält ser ut, istället klassificerar nätverket objekt som det upplever dem; ju mera tillgängligt data från olika situationer, desto snabbare och mera precist kan DNN tränas; och algoritmerna självoptimerar med målet att maximera systemprestandan istället för att optimera varje mänsklig komponent, sådana som att upptäcka körbanor, vilket leder till att systemet kräver ett mindre nätverk. Negativa aspekter är: det kan krävas andra algoritmer och mänsklig träning om det inte finns tillräcklig mycket data från mera specifika situationer;det är även väldigt tidskrävande att träna och finslipa olika beteenden och applikationer, vilket leder till att det ofta krävs modifieringar av olika nätverksarkitekturer. [ 24]

A picture containing green, road, grass, outdoor

Description automatically generated

Figur 7:NVIDIAs end-to-end lösning PilotNet. De lärde sig vad de skulle fokusera på genom observation utan att veta hur en väg ser ut eller vad en bil är. Hämtad från [25]

Det finns många fördelar och nackdelar med att använda djup maskininlärning för att skapa autonoma bilar. Positiva aspekter med att använda DNN är: maskiner blir bättre genom att lära sig, DNN lär sig mera än vad andra maskininlärningsalgoritmer gör med samma mängd data [29]; deras prestanda inom bildigenkänning är hög [30]; de är lätta att bygga med dagens öppenkällkodbibliotek(eng. *open source libraries*); och de lär sig snabbare tack vare dagens hårdvara, mera specifikt GPU. Negativa aspekter är: det är svårt att filtrera onödigt data samt kombinera data från olika sensorer som LIDAR och GPS; de tränas via ”supervised learning” , vilket betyder att de behöver stora mängder markerat data; de ses som en svart programlåda, vilket gör det svårt att veta hur nätverket dragit sin slutsats; säkerheten med manipulering av bilder, vilket diskuteras i kapitel 3.1; och det är svårt att beräkna deras säkerhet.

## 2.4 Waymo ChauffeurNet

Medan en traditionell ändpunkt till ändpunkt lösning får rå indata från kameror, vilket ger kameror problem i obekanta situationer, har Waymos forskare presenterat en egen lösning på problemet kallad ”ChauffeurNet” [26]. Chauffeurnet använder sig av bilarnas LIDAR och kamerasystems utdata för att skapa en stack av perceptioner, som sedan matas in som indata i en modell tillsammans med förutsägelser om objekt och en förberäknad rutt. På grund av dessa tillvägagångssätt är ChauffeurNet inte jämförbart med de traditionella ändpunkt till ändpunkt lösningarna men det kan istället tänkas som en potentiell ersättare för traditionella rörelseplaneringsmodulerna. I en traditionell rörelsepaneringsmodul har man ett antal algoritmer som dikterar den exakta vägen för ett fordon längs en rutt, tillsammans med hastigheten och avståndet i förhållande till andra fordon. ChauffeurNet försöker uppnå detta genom att imitera mänskliga exempel. ChauffeurNet tränades med data från 60 dagar av mänsklig expertkörning men det visade sig inte vara tillräckligt för mera komplexa situationer som nätverket aldrig sett tidigare. Träningsdatan, som bestod av 30 miljoner exempel, innehöll inte ett tillräckligt brett spektrum av scenarier med tillräckligt hög frekvens för att lära ChauffeurNet hur man kör ordentligt. En bil som kördes enligt modellen skulle ofta fastna bakom andra bilar parkerade vid vägen eller krascha in i dem. Forskarna bestämde sig för att finjustera träningsdatan för att simulera det dåliga istället för att bara imitera det goda. Starten och slutet av en viss rutt, från den ursprungliga träningsdatan, är desamma men störningar(eng. *perturbations*) som kollisioner och plötsliga förändringar av bilens position på vägen läggs däremellan. Forskarna lär sedan ChauffeurNet att undvika sådana situationer genom att lägga till uttryckliga förluster som motverkar sådana kollisioner vilket de kallar miljöförluster (eng. *environment losses)*. Imitations förluster(eng. *imitation losses)* får modellen att imitera expertens demonstrationer. Forskarna valde sedan att ta bort slumpmässiga delmängder av träningsdatan för att öka effektiviteten av miljöförlusterna. Detta kallar de för imitationsavhopp (eng. *imiation dropout)*. Den ursprunliga träningsdatan ledde till att bilen krockade med en parkerad bil i 50% av försöken, efter att den nya träningsdatan introducerades sänktes detta till 10%, se figur 8.

A screenshot of a cell phone

Description automatically generated

Figur 8: Modell test på 3 olika situationer. Hämtad från [26]

ChauffeurNet är ett återkommane neuralt nätverk(eng. *recurrent neural network,* RNN). Medan data rör sig framåt i ett vanligt DNN kan data röra sig i vilket håll som helst i ett RNN. ChauffeurNet består av två delar: FeatureNet och AgentRNN. FeatureNet är ett faltnings neuralt nätverk (eng. *convolutional neural network)*, en klass av DNN som används specifikt inom analys av bilder, där det hanterar indatan och extraherar viktig information som bilkartan, trafikljusen, hastighetsbegränsningen, modellens rutt och nuvarande och tidigare positionen för andra bilar. Detta delas med AgentRNN som ger utdata som förutsäger de andra bilarnas framtida positioner så att ChauffeurNet kan reagera i enlighet med detta. Utdatan från ChauffeurNet ger rutten som modellen borde välja till en lågnivå kontroller. Kontrollern konverterar datan till instruktioner som säger vilket håll modellen ska styra mot, eller hur mycket den ska accelera eller bromsa. Kontrollern gör det möjligt att utföra funktionerna i simuleringar eller på riktiga vägar.

Waymos nuvarande AI-system använder DNN för perception med en kombination av maskininlärning och hårdkodade situationer för att kontinuerligt utvärdera ett stort antal möjligheter. Forskarnas slutsats var att ChauffeurNet inte ännu är fullständigt konkurrenskraftig jämfört med rörelseplaneringsmetoder men de anser att det är ett bra steg framåt för maskininlärda körmodeller. Se [26] för att läsa artikeln i sin helhet.

1. Säkerhetsaspekter

Autonoma bilar kommer med enorma möjligheter men även risker kopplade till DNN och datasäkerhet. Bilar kommer vid behov samla, skapa och byta ut en stor mängd personliga data. Alla tillverkare som är involverade i produktionen av autonoma bilar, från fordonstillverkare till företag som skapar sensorer eller anslutningslösningar, bör vara medvetna om riskerna för att säkerställa att deras data är korrekt samlade och skyddade.

I denna del av avhandlingen framhäver jag säkerhetsrisken kopplad till djup maskininlärning och igenkänning av bilder, samt attackpunkter inom autonoma bilars datainsamling och hårdvara.

## 3.1 Djup maskininlärning och felaktiga bilder

Perception är den viktigaste aspekten då det gäller autonoma bilars säkerhet. Att se olika objekt och sedan identifiera dem är en viktig del inom körning och sedan 2012 är DNN bättre än människor på att känna igen trafikskyltar [23]. Dock, som har diskuterats tidigare, är orsakerna till DNNs prestanda ännu inte helt uppenbara. De är också instabila med avseende på fientliga störningar som kan lura nätverket att felaktigt klassificera indata även om störningen är mindre eller omärklig för en människa, se figur 8. Det är inte bara slumpmässigt genererade störningar som orsakar dessa problem, det är även modifieringar av kamerabilder som att ändra storlek, beskärning eller förändring av ljusförhållanden. Med dessa störningar är det möjligt att sänka ett DNNs förmåga att identifiera ett objekt till 0 %. Testning har fokuserat på störningar som har introducerats artificiellt, men störningar som regn och snö kan leda till liknande resultat .[37]

A traffic light

Description automatically generated

Figur 8: Exempel på hur en störning kan påverka ett DNNs förmåga att identifiera objekt. Hämtad från [36]

Dessa problem är inte kopplade till enskilda DNN, ett exempel som felaktigt klassificeras av ett nätverk blir också felaktigt klassificerat av ett annat nätverk med en annan arkitektur, även om nätverkena har lärt sig av olika träningsdata [37].

Garanti på säkerhet och verifieringsmetoder för maskininlärning är dåligt undersökt. Den nuvarande internationella säkerhetsstandarden för fordon, ISO 26262 [38], har inte ett sätt att definiera säkerhet för självlärande algoritmer som djup maskininlärning, men autonoma bilar kommer adresseras i uppföljaren ISO 21448. Därför finns det fortfarande inget sätt att standardisera säkerhetsaspekter, dels på grund av den snabba utvecklingen inom teknologin.

Jag hänvisar till Marta Kwiatkowskas forskning för en djupare insikt över de metoder och verktyg som används inom verifieringen av autonoma bilars säkerhet. [37] [43] [44]

## 3.2 Autonoma bilar kommunikationstekniker och datasäkerhet

Autonoma bilar behandlar enorma mängder data som lagras och hämtas med hjälp av datormoln(eng. *cloud computing*). För att fordon ska kunna kommunicera med föraren, andra bilar och vägen, måste de utnyttja många olika kommunikationstekniker. Främst tre kommunikationsmekanismer används, fordon till fordon(eng. *vehicle-to-vehicle*, V2V), fordon till infrastruktur(eng. *vehicle-to-infrastructure*, V2I) och molnet, se figur 9.

A picture containing text, map

Description automatically generated

Figur 9: Illustration över autonoma bilars teknologi. Hämtad från [45]

Autonoma bilars teknologier, se figur 9, ger möjligheten att samla in och kommunicera med stora mängder data, men så mycket databehandling kan leda till sårbarheter. En hackare behöver bara infiltrera en inmatningspunkt, sådan som datormolnets databas eller bilens kommunikationsenhet, för att få tillgång till stora mängder data som sedan kan användas för att manipulera bilen. Angreppspunkterna ökar med behovet av ständig informationsöverföring, vilket betyder att datan inte får vara högt krypterade vilket skulle fördröja överföringen av data.

För att spara tid och pengar väljer företag att köpa komponenter från andra tillverkare. Varje tillverkare utnyttjar olika kodningssystem vilket betyder att dessa behöver anpassas för att göra informationsöverföringen kompatibel med andra komponenter. Detta leder till säkerhetsbrister eftersom det finns så många variabler som är inblandade i olika komponenter som interagerar med varandra, att identifieringen av svaga länkar kan vara utmanande. En lösning på problemet är att företag utnyttjar penetrationstestning. Penetrationstestning är testning av datorsystem där man letar efter sårbarheter som en angripare kan utnyttja.

Autonoma bilar utnyttjar V2V-kommunikation för att sända och hämta data i realtid från omgivande bilar för en smidig och säker körupplevelse. V2V är ett P2P-nätverk som använder 5.9 Ghz frekvensbandet, känt som IEEE 802.11. Principen är den att då två fordon är inom räckvidd för radiokommunikation, så kan de anslutas automatiskt och upprätta ett ad hoc-nätverk, ett nätverk för det särskilda ändamålet att övervaka utgående och inkommande trafik, där alla anslutna stationer kan dela information som position, hastighet, riktning, etc.

V2I-kommunikation ger möjligheten för fordon att ansluta till de elektroniska enheter som styr och övervakar den fysiska miljön inom vilken fordonet reser, t.ex. trafikljus. Infrastrukturen kan sedan använda denna information för att optimera trafikstyrningen för att maximera trafikens flöde, minimering av bränsleanvändning och förorening. V2I beskrivs som en centraliserad kontrollinfrastruktur, medan V2V är decentraliserad.

Att skapa autonoma bilar med en stor mängd av olika kommunikationsmekanismer kommer resultera i att de blir tillgängliga via en offentlig infrastruktur, som internet, eller att de sänder ut information till allmänheten. Det ökar potentialen för stora, automatiserade, och skadliga attacker. Några dylika attack är: totalsökning(eng. *brute-force attack)* , DoS/DDoS, nätverksprotokoll attacker(eng. *network protocol attacks)*, nätfiske(eng. *phishing)* och falska updatering(eng. *rogue update)*. [40]

Det är inte bara mjukvaran som leder till attackpunkter. Spoofing, vilseledande och blockering av GPS och LIDAR är möjligt utan större investering eller teknisk bakgrund. [40] Säkerheten av hårdvaran är värd att diskuteras, även utan en utomstående angripare. År 2014 visade en MIT Technology studie [41] att Google Waymos kameror är känsliga för plötsliga förändringar av belysning och samma år omkom en förare då dess Tesla fordon kolliderade med en vit långtradare eftersom dess kamera inte kunde skilja på den vita färgen och den starkt upplysta himmeln [42].

# Diskussion:

Syftet med avhandlingen var att undersöka de teknologier som används inom utvecklingen av autonoma bilar samt deras säkerhet. Litteraturen visar att autonoma bilar är på god väg och de gör varje år stora framsteg inom både hårdvaran och neurala nätverken. Det finns forskare och studier som visar hur säker en bil är eller hur effektiva nätverken är men något som saknas är studien på hur människor påverkas av autonoma bilar. Frågor som behandlar autonoma bilars inverkan på tillit, samhället och sociala och morala normer är värt att diskutera. Vilken nivå av säkerhet måste uppnås fören vi skickar våra barn med självkörande taxi till skolan, eller vem är ansvarig då en olycka inträffar. Vilka förändringar krävs av infrastrukturen och är vi redo att göra dem. Ska bilar utan automation beskattas mera än autonoma bilar eller rent av förbjudas för en ökad säkerhet. Hur och vem ska lösa ett moraliskt dilemma som spårvagnsproblemet, ska man rösta för deontologi eller utilitarism. En framtid med fullt autonoma bilar är ännu inte på horisonten men det är värt att studera den inverkan den framtiden skulle ha på vårat samhälle.

Referenser:

[1] ”*SAE International Releases Updated Visual Chart for its”Levels of Driving Automation*”,11.12. 2018 (Hämtad 05.03.2019)

<https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-driving-vehicles>

[2]Google doc med information samlad från olika källor(Hämtad 05.03.2019)

<https://docs.google.com/spreadsheets/d/1Vobg29R1t3FphlWjb8dwG4nkAWqyc_qMwkCjUT8SUno/pubhtml?gid=1805961368&single=true&chrome=false>

[3] Teslas privacy policy (Hämtad 06.03.2019)

<https://www.tesla.com/about/legal>

[4] Elon Musk, ”*Master plan, part deux*”, 20.07.2016(Hämtad 12.03.2019)

<https://www.tesla.com/blog/master-plan-part-deux/>

[5] Andrew J. Hawkins, ”*Elon Musk still doesn’t think LIDAR is necessary for fully driverless cars*”, 07.02.2018, ( Hämtad 14.03.2019)

https://www.theverge.com/2018/2/7/16988628/elon-musk-lidar-self-driving-car-tesla

[6]John Krafcik ,”*Where the next 10 million miles will take us*”, 10.10.2018,(Hämtad 14.03.2019)

<https://medium.com/waymo/where-the-next-10-million-miles-will-take-us-de51bebb67d3>

[7] The tesla team, ”*Tesla Q3 Vehicle safety report*”, 04.10.2018)( Hämtad 14.03.2019)

<https://www.tesla.com/blog/q3-2018-vehicle-safety-report>

[8] Keen Security Lab of Tencent, ”*Car hacking research: Remote attack Tesla motors*”,19.09.2016, (Hämtad 14.03.2019)

<https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/>

[9]Jordan Golson, ”*Car hackers demonstrate wireless attack on tesla models S*”, 19.09.2016, (Hämtad 12.03.2019)

<https://www.theverge.com/2016/9/19/12985120/tesla-model-s-hack-vulnerability-keen-labs>

[10] Autopilot buddy

<https://www.autopilotbuddy.com/>

[11]Walkinguy Network, ”*Hacking tesla autopilot | orange trick(delted video*)” , 20.01.2018(Hämtad 14.03.2019)

<https://www.youtube.com/watch?v=TYZrehVQouc>

[12] National Highway Traffic Safety Administration, ”*Consumer advisory: NHTSA deems ’Autopilot buddy’ product unsafe*”, 19.06.2018, (Hämtad 14.03.2019)

<https://www.nhtsa.gov/press-releases/consumer-advisory-nhtsa-deems-autopilot-buddy-product-unsafe>

[13] California Highway Patrol San, 19.01.2018, (Hämtad 14.03.2019)

<https://twitter.com/CHPSanFrancisco/status/954418933225762816?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E954418933225762816&ref_url=http%3A%2F%2Fwww.thedrive.com%2Fsheetmetal%2F18168%2Fpeople-keep-coming-up-with-ways-to-fool-teslas-autopilot>

[14] Eduard Marin, Lennert Wouters, Tomer Ashur, ”*Fast,furious and insecure: passive keyless entry and start in modern supercars*”, 10.09.2018,( Hämtad 14.03.2019)

<https://www.esat.kuleuven.be/cosic/fast-furious-and-insecure-passive-keyless-entry-and-start-in-modern-supercars/>

[15] The tesla team, ”*Sentry Mode: Guarding Your Tesla*”, 13.02.2019,( Hämtad 14.03.2019)

<https://www.tesla.com/blog/sentry-mode-guarding-your-Tesla>

[16] Matthew DeBord, ”*A waymo engineer told us why a virtual-world simulation is crucial tothe future of self-driving cars*”, 16.08.2018,( Hämtad 19.03.2019)

<https://nordic.businessinsider.com/waymo-engineer-explains-why-testing-self-driving-cars-virtually-is-critical-2018-8?r=US&IR=T>

[17] Nidhi Kalra, Susan M. Paddock, ”*How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability*? ”,2016,( Hämtad 19.03.2019)

<https://www.rand.org/pubs/research_reports/RR1478.html>

[18] Waymo tech(Hämtad 23.03.2019)

https://waymo.com/tech/

[19] djup maskininlärning definition från it-ord(Hämtad 22.03.2019)

<https://it-ord.idg.se/ord/djup-maskininlarning/>

[20] artificellt neuronnät definition fron it-ord(Hämtad 22.03.2019)

<https://it-ord.idg.se/ord/artificiellt-neuronnat/>

[21] Jayesh Bapu Ahire, ”*The artificial neural networks handbook: part 1*”,24.08.2018,( Hämtad 22.03.2019)

<https://medium.com/coinmonks/the-artificial-neural-networks-handbook-part-1-f9ceb0e376b4>

[22] Techopedia definition(Hämtad 22.03.2019)

<https://www.techopedia.com/definition/32902/deep-neural-network>

[23] Dan Cire ̧san, Ueli Meier, Jonathan Masci, J ̈urgen Schmidhuber, ”*Multi-Column Deep Neural Network for Traffic Sign Classification* ”, 23.01.2012,( Hämtad 22.03.2019)

<http://people.idsia.ch/~juergen/nn2012traffic.pdf>

[24] KPMG, ”I *see. I think. I drive. (I learn*)”, 2016, (hämtad 22.03.2019)

<https://assets.kpmg/content/dam/kpmg/tr/pdf/2017/01/kpmg-isee-ithink-idrive-ilearn.pdf>

[25] Danny Shapiro, ”*Reading an AI car’s mind: How NVIDIA’s neural net makes decisions*” ,27,04,2017,( Hämtad 22.03.2019)

<https://blogs.nvidia.com/blog/2017/04/27/how-nvidias-neural-net-makes-decisions/>

[26]Mayank Bansal, Alex Krizhevsky, Abhijit Ogale, ”*ChauffeurNet: Learning to drive by imitating the best and synthesizing the worst*”, 07.12.2018,( Hämtad 22.03.2019)

<https://arxiv.org/pdf/1812.03079.pdf>

[27]The Tesla team, ”*Upgrading to Autopilot and Full self-driving capability*”, 01.03.2019,( Hämtad 23.03.2019)

<https://www.tesla.com/blog/upgrading-autopilot-and-full-self-driving-capability>

[28] hemsida för Tesla AutoPilot(Hämtad 23.03.2019)

<https://www.tesla.com/autopilot>

[29] Andrew Ng , ”*CS229-Deep learning*”, (Hämtad 23.03.2019)

<http://cs229.stanford.edu/materials/CS229-DeepLearning.pdf>

[30] ImageNet contest results (Hämtad 23.03.2019)

httpimage-net.org/challenges/LSVRC/

[31] American automobile association, ”*Advanced Driver Assistance Technology Names*”, 2019, ( Hämtad 23.03.2019)

<https://www.aaa.com/AAA/common/AAR/files/ADAS-Technology-Names-Research-Report.pdf>

[32] Navigant research, ”*Navigant research leaderboard: Automated driving vehicles*”, 2019, (Hämtad 23.03.2019)

<https://www.navigantresearch.com/reports/navigant-research-leaderboard-automated-driving-vehicles>

[33] Dennis Galvin, ”*RFID devices and cryptography: Analysis of the DST40*”,07.03.2006, (Hämtad 24.03.2019)

<https://courses.cs.washington.edu/courses/csep590/06wi/finalprojects/galvin.pdf>

[34] Stephen C. Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin, Michael Szydlo, ”*Security Analysis of a cryptographically-enabled RFID device*”,2005,( Hämtad 24.03.2019)

<https://www.usenix.org/legacy/event/sec05/tech/bono/bono.pdf>

[35] Martin E. Hellman, ”*A cryptanalytic Time-Memory Trade-Off*”,1980,( Hämtad 24.03.2019)

<http://www.cs.miami.edu/home/burt/learning/Csc609.122/doc/36.pdf>

[36] Marta Kwiatkowska, ”*Are we safe in self-driving cars*?”,2017,( Hämtad 24.03.2019)

<https://www.cs.ox.ac.uk/innovation/research-impact/case-marta-self-drive-car.html>

[37] Xiowei Huang, Marta Kwiatkowska, Sen Wang, Min Wu, ”*Safety verification of deep neural networks*”,05.05.2017,( Hämtad 24.03.2019)

<https://arxiv.org/pdf/1610.06940.pdf>

[38] National Instruments ”*What is the ISO 26262 Functional Safety Standard*?”,19.03.2019,( Hämtad 25.03.2019)

<http://www.ni.com/en-us/innovations/white-papers/11/what-is-the-iso-26262-functional-safety-standard-.html>

[39] Bill Howard, ”*V2V: What are vehicle-to-vehicle communcations and how do they work?”,*06.02.2014,( Hämtad 25.03.2019)

<https://www.extremetech.com/extreme/176093-v2v-what-are-vehicle-to-vehicle-communications-and-how-does-it-work>

[40] Simon Parkinson, Paul Ward, Kyle Wilson, Jonathan Miller, *”Cyber threats facing autonomous and connected vehicles: Future challenges”,*06.03.2017,( Hämtad 25.03.2019)

<http://eprints.hud.ac.uk/id/eprint/31446/8/__nas01_librhome_librsh3_Desktop_manuscript.pdf>

[41] L. Gomes, ”*Hidden obstacles for googles self-driving cars:Impressive progress hides major limitations of googles quest for automated driving*”,28.08.2014, (Hämtad 25.03.2019)

<https://www.technologyreview.com/s/530276/hidden-obstacles-for-googles-self-driving-cars/>

[42] Fred Lambert, *”Understanding the fatal Tesla accident on Autopilot and the NHTSA probe”*, 01.07.2016,( Hämtad 27.03.2019)

<https://electrek.co/2016/07/01/understanding-fatal-tesla-accident-autopilot-nhtsa-probe/>

[43] Marta Kwiatkowska, David Parker, *”PRISM-games: verification and strategy synthesis for stochastic multi-player games with multiple objectives”*, 29.11.2017, (Hämtad 27.03.2019)

<https://link.springer.com/article/10.1007/s10009-017-0476-z>

[44] Marta Kwiatkowska, Gethin Norman, David Parker, ”*PRISM 4.0: Verification of probabilistic real-time systems*”, 2011, (Hämtad 27.03.2019)

<http://www.prismmodelchecker.org/papers/cav11.pdf>

[45] James Kuhr, ”*Connected and autonomous Vehicles: The enabling technologies*”, 2017,(Hämtad 27.03.2019)

<https://www.slideshare.net/ctrutaustin/connected-and-autonomous-vehicles-the-enabling-technologies>