# Proactive threat detection for connected cars using recursive Bayesian estimation

# Proactive Threat Detection for Connected Cars Using Recursive Bayesian Estimation

Haider al-Khateeb, Gregory Epiphaniou, *Member, IEEE*, Adam Reviczky,
Petros Karadimas, *Member, IEEE*, and Hadi Heidari, *Senior Member, IEEE*

***Abstract*— Upcoming disruptive technologies around autonomous driving of connected cars have not yet been matched with appropriate security by design principles and lack approaches to incorporate proactive preventative measures in the wake of increased cyber-threats against such systems. In this paper, we introduce proactive anomaly detection to a use-case of hijacked connected cars to improve cyber-resilience. Firstly, we manifest the opportunity of behavioural profiling for connected cars from recent literature covering related underpinning technologies. Then, we design and utilise a new dataset file for connected cars influenced by the Automatic Dependent Surveillance – Broadcast (ADS–B) surveillance technology used in the aerospace industry to facilitate data collection and sharing. Finally, we simulate the analysis of travel routes in real-time to predict anomalies using predictive modelling. Simulations show the applicability of a Bayesian estimation technique, namely Kalman Filter. With the analysis of future state predictions based on the previous behaviour, cyber-threats can be addressed with a vastly increased time-window for a reaction when encountering anomalies. We discuss that detecting real-time deviations for malicious intent with predictive profiling and behavioural algorithms can be superior in effectiveness than the retrospective comparison of known-good/known-bad behaviour. When quicker action can be taken while connected cars encounter cyber-attacks, more effective engagement or interception of command and control will be achieved.**

***Index Terms*—Connected Cars, Cyber Physical Systems, Cyber Threat, Proactive Detection, Bayesian Estimation, Kalman Filter.**

## I. Introduction

SEVERAL technological trends have converged to allow and advance new semi and indeed fully autonomous Cyber-Physical Systems (CPS) that are taking over and shape the traffic of the public space from automotive transportation through marine vessels, aerial vehicles of drones and aircraft systems. New Mobile Ad Hoc Networks (MANET) and Vehicular Ad Hoc Networks (VANET) are utilised to exchange traffic data and steer vehicles through new Intelligent Transportation Systems (ITS). The rationale for this paper was motivated by the challenge of increasing cyber-threats posed by and to CPS [1], more precisely, the gap of resilience in addressing the security design of such systems and the lack of real-time cyber-threat detection of malicious intruders. Advancements in modern machine learning and algorithms for profiling and behavioural analysis to aid decision making are already widely used, with the knowledge of Intrusion Detection and Prevention Systems (IDPS) and anomaly detection through Big Data Analytics at networks' perimeter, known-good behaviour can be deduced at large-scale movement flows of regulated traffic [2]. However, current implementations are narrow-focused on reactive signature-based models. Furthermore, malfunction of sensors and rogue behaviour [3] has not been managed by automated vehicles, which is essential for levels 4 and 5 of the driving automation classification scheme defined by the Society of Automotive Engineers (SAE). These levels expect no human intervention or driver's attention for safety, hence require automated fail-safe mechanisms. The different levels of automation from manually driven, semi-autonomous to fully autonomous connected vehicles are described and explained in the book: "Preparing a Nation for Autonomous Vehicles" [4]. For this case study, the baseline will be set on level 5, fully autonomous connected cars. However, weaknesses in semi-autonomous (autopilot) cars have been reported as well, it is projected that interconnecting these systems will lead to an even bigger attack surface.

The utilisation of the internet, a global system that has no central governance, to communicate elementary and aggregated sensory data often in real-time via ubiquitous devices [5] would introduce cyber-threats [6] [7] [8] to the architecture [9] of autonomous vehicles, like the particular instance of cyber-hijacking presented in our case study. Currently, the industry is moving ahead to produce self-driving cars, buses and trains, autonomous flying drones and various other transportation systems, whilst the aspect of built-in security is falling short. Moreover, the Internet of Things (IoT) creates a world where devices and systems can be taken over and cause significant disruptions in our day-to-day lives.

With over a billion cars owned in the world and being potentially replaced with new connected vehicles, this paper provides empirical results as a proof-of-concept on how resilience can be improved by means of performing behavioural analysis of such systems with the help of profiling by looking particularly at autonomous connected cars. Profiling will help to address the correlation of various systems, whereas through behavioural analysis it can be deducted whether an expected state of a sensor reading is within the margin of error. A proactive approach to detect and react to a specific use case

Manuscript received XXX; revised XXX; accepted XXX. Date of publication XXX; date of current version XXX
H. al-Khateeb and G. Epiphaniou are with the Wolverhampton Cyber Research Institute (WCRI), School of Mathematics and Computer Science, University of Wolverhampton, UK (email: H.Al-Khateeb@wlv.ac.uk; G.Epiphaniou@wlv.ac.uk)
A. Reviczky is with the Dept. of Engineering and Environment, University of Northumbria, London Campus, UK (e-mail: adam.reviczky@northumbria.ac.uk)
P. Karadimas and H. Heidari are with the School of Engineering, University of Glasgow, G12 8QQ, Glasgow, UK (e-mail: Petros.Karadimas@glasgow.ac.uk; Hadi.Heidari@glasgow.ac.uk)

of cyber-hijacking will be presented in order to demonstrate that effective proactive security can be built-in to create resilience towards cyber-attacks. In contrary to this approach, current implementations utilise supervised machine learning algorithms [10] but they are impractical for live analysis of vehicles' movements due to the training elements required to develop the inductive bias for the algorithm [11].

We claim that Recursive Bayesian estimation is superior to supervised machine learning for real-time predictive modelling of future states for comparable travel routes and actual motion patterns [12]. A behavioural profile helps to detect any deviation from the norm for a journey conducted by a Level 5 car using mathematical probability density functions, anomaly detection can then be reacted upon far quicker than before. This research is looking at the current related efforts of methods in profiling and behavioural analysis [13] and discusses their drawbacks or suitability for proactive threat detection. If significant improvements to reaction times is achieved, malicious intent can be thwarted to eliminate the intended harm. A proactive stance can be taken instead of the current re-active solutions to predict cyber security-threats as early as they happen in the kill chain.

To prove that this approach of behavioural analysis can be a baseline of cyber-defence of CPS [14], this paper will demonstrate the technique on a specific scenario of connected cars as an example, from which it can be deduced that the approach has potential and is fit for purpose in the general application of land-based or aerial transportation. Particular anomalies representing events and threats have been considered in our case study in the nature of cyber-risk and the threat landscape of the wider Internet of Things. An example of a main risk that could arise from the cyberspace is a remote hack into the CPS to change course of action for the travel in a way to either divert or create damage by driving the vehicle against traffic rules and laws that everyone abides. For semi-automated cars, this could also include a dangerous lane deviation due to the driver's unconsciousness. Obviously, there are many more threats such as those posed by state-sponsored attacks, mass-hijacking of vehicles and nonetheless system and pilot errors. We should acknowledge the challenge of unsafe or untrustworthy transportation systems because any component in the car (including sensors that are being relied upon) can malfunction and give false readings. Proper redundancy, as well as a fail-over mechanism, should be in place on both hardware and software levels to filter out false events.

The remaining of this paper covers related work in Section II and research method in Section III. Results are presented and discussed in Section IV and finally conclusions and future work are shared in Section V.

## II. Related Work

Work on Connected Cars is subclassified within the broader Cyber-Physical Systems (CPS) umbrella term. CPS is an emerging research area defined by inevitably widely accepted attributes based on which they are described as being autonomous, timeliness, distributed, fault-tolerant, scalable, reliable and secure. In [15], a prototype architecture has been presented to demonstrate these attributes and identify challenges. CPS provides the opportunity to businesses to adopt innovative practices, [16] conducted action research based on innovation theory to investigate connected cars as a case study. Their empirical results showed that Volvo cars were more successful to pursue digital innovation through a set of capabilities such as opening design spaces and embracing complementary products. However, the complexity of CPS which includes but not limited to the different modes of operation and physical components introduced new challeneges to conventional system modelling.

### A. Data Storage, Communication and Modelling

Without capturing and storing validated quality data through the various sensors of the connected car, the analysis would be meaningless. Therefore, it is utmost important to define what data needs to be captured, through what means (readings of sensor data) and how the quality of reading is ensured, coupled with minimal misreading and errors. Some of the inevitably present abnormal readings left in the dataset can be filtered out with mathematical models.

The aviation industry has the Automatic Dependent Surveillance - Broadcast (ADS-B) as a globally supported tracking system to define prerequisite data types. Data is periodically sent for tracking purposes to air traffic control ground stations and other aircrafts [17]. Among the defined fields in the ADS-B scheme are flight ID, geolocation, time, speed and various other sensor readings. Furthermore, the industry has car data-sharing systems in place such as the CarSharing Module (CSM) which has two integrated microcontrollars with the ability to support Android Apps to provide additional features including Human Computer Interaction (HCI). A demonstration of their application in a real-world scenario can be seen in [18] were CSM data were used to analyse the impact of a parking price policy. Examples of captured data include the identification (ID) of an individual renting a car, reading of a battery charge indicator, location and speed.

A prototype platform by [19] presented a back-end for applications to communicate with connected cars. The platform provided an abstract layer to facilitate communications, identity management, and provided access to data storage components. Such proposals enable sensors, robots, smart meters and other CPSs to establish communication sessions with no, or very little, human intervention. This Machine-to-Machine (M2M) paradigm is usually tested or simulated based on small-scale M2M models [20], with recent attempts addressing future needs by increasing scalability to trillions of connected devices [20]. If we consider a case study of connected cars, information such as speed can be exchanged to optimise traffic control at an intersection. Even with the assumption that partial data will be missing because not all cars are connected, [21] showed that traffic signals can still learn to adapt and accomodate road demands to build more efficient traffic systems. In their experiment, [21] simulated various demand ratios to investigate the impact of updating the minimum green-time value on the penetration rate of cars.

Software agents can be autonomous and implement intelligent decision-making which makes them suitable for mod-

elling CPS. [22] developed a multi-agent model for a water distribution network with semantic capabilities to analyse data about the physical operations to the cyberspace. The literature shows that deterministic models such as differential equations and synchronous digital logic should be combined for better realisation of CPS with evidence from projects such as Ptides (Programming temporally-integrated distributed embedded systems), which shows that deterministic models can achieve faithful realisation in some distributed scenarios [23].

### B. Threat Detection and Prediction

Anomaly detection plays a crucial part in the proactive approach to detect cyber-threats. An overview of various detection techniques presented in [24] shows deviations from the norm through mean functions hitting a threshold and hence indicating a suspicious activity. Additionally, pattern matching is a process were common structure is found to compare and group against. Sequential and qualitative analysis utilises ordering and performs analytical methods on the data, whereas sampling focuses on bounding the collection of data. These are some of the techniques implemented in Intrusion Detection and Prevention Systems (IDPS) to analyse network traffic [25]. An Intrusion Detection Systems (IDS) for connected cars could share the same general internal processes of an IDS as demonstrated in Figure 1. In contrast to conventional signature-based solutions, modern trends in anomaly detection are more adaptive to emerging theats associated with dynamic systems such as CPS. Unlike Bayes Filters which stores the previous state of a system to detects future behaviour [26], supervised machine learning algorithms should be trained with signatures of known attacks [27]. However, training time to establish a baseline is disadvantageous when a rapid incident response is required [13].

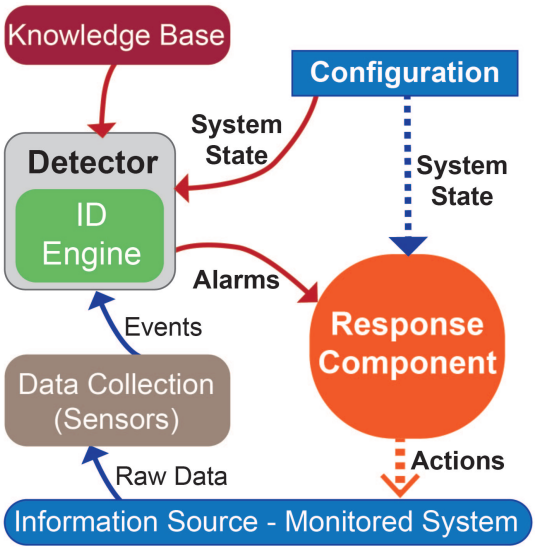


Fig. 1. Basic architecture of intrusion detection system (IDS).

Threat prediction techniques could utilise environmental factors such as vulnerabilities and existing attack graphs [28] or tackle the problem by means of quantifying the incorporated security principles such as privacy or anonymity [29]. Many predictive models are based on the Recursive Bayesian estimation, also known as Bayes Filters [28]. Other proposals utilise data-fusion frameworks, [30] demonstrate detection of asymmetric and adaptive threats with the help of intelligent agents where the prediction method is based on a decentralised Makov (stochastic) game model. Furthermore, insider threat prediction [31] is an interesting angle of how the behaviour of malicious intent tries to blend with legitimate actions (Figure 2). In conclusion, cyber-threat detection and prediction in connected cars should consider the applicability and suitability of the proposed approach. It is also useful to consider hybrid methods, [32] integrated different prediction methods into a framework for security to apply a proactive approach with the specific use case of remote cyber-hacking.

### C. Behavioural Profiling

Profiling is the first stage of analysing and concatenating similar groups of behaviour together. Behaviour of like-minded people and drivers in similar roles can be argued to behave in almost identical patterns. Machine learning have been utilised to detect different types of online perpetrators based on their social interactions in the cyberspace [33]. Likewise, Bus drivers could have very similar reactions to speed, route and alertness. Different types of individuals but also systems behave differently, but deducing and predicting a collection of a group with similar correlation can lead to a conclusion on whether an expected behaviour is unusual. Creating profiles to detect patterns usually assigned to intruders breaking into the system [34] can help determine likelihoods of deviation and raise suspicion on anomalies. Looking specifically at these patterns for a system based profiling as compared to human behaviour profiling of Cyber-Physical Systems is adding value in combination with the estimation techniques discussed in the previous section. Network traffic behaviour has been researched and different profiling data groups have been established [35], which will be taken advantage of to create parallel profiling templates for connected cars. There has been done some research on human behaviour profiling, with different types of groups behaving in a similar pattern (commuting people, families and various other types like taxi drivers). In this paper the focus shifted towards whether a profile pattern can be established with autonomous systems in order to combine these groups with the machine learning estimation techniques. It has been shown that indeed it is even easier to group pre-defined system behaviour on predicted routes as compared to humans driving freely on the motorway. Through profiling it is now also possible to distinguish between autonomous and non-autonomous driven vehicles.

## III. Methodology

To address the research question which can be expressed as: How can cyber-resilience be improved proactively to predict cyber-threats in rea-time on connected cars in such a way as to counter cyber-attacks?, a quantitative data type research methodology approach was selected underpinned by

TABLE I
SAMPLE EXCERPT FROM THE PROPOSED DATASET FORMAT

| Connected Car (ID) | Date (UTC) | Time (UTC) | Position (latitude) | Position (longitude) | Position (elevation) | Orientation (degree) | Orientation (cardinal) | Ground Speed (m/s) | Reporting (system) |
|---|---|---|---|---|---|---|---|---|---|
| 2017:0db8:85a3 | 2017-03-11 | 06:50:27 | 47.82520828 | 12.54956887 | 456 | 190 | S | 9 | ADS-B |
| 2017:0db8:85a3 | 2017-03-11 | 06:50:29 | 48.24533500 | 12.53889999 | 455 | 191 | S | 11 | ADS-B |
| 2017:0db8:85a3 | 2017-03-11 | 15:30:40 | 48.24545299 | 12.53923599 | 449 | 12 | N | 7 | ADS-B |

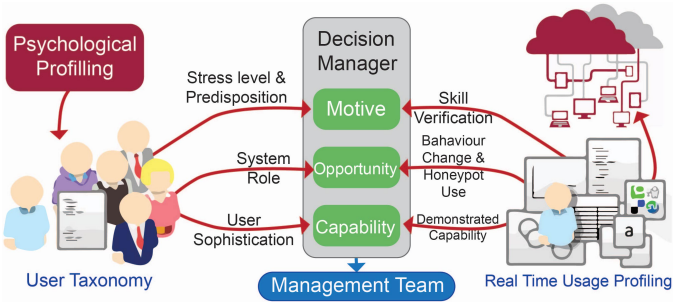


Fig. 2. Insider Threat Prediction Model.

empirical data (sample location data) to facilitate experiments on mathematical modelling (e.g. Bays filtering formulas) to correlate routes of connected cars.

The research is based on a sample set of routes data that has been created in order to show the behaviour of different possible vehicle movement. The data uses real Global Positioning System (GPS) coordinates but the routes should only resemble motion patterns and are not taken from real events (see: Table I). This set of data is then analysed for behavioural profiling as shown in Figure 4 and Figure 5.

### A. Case Study of Connected Cars

This paper is addressing the problem statement and proposed proactive threat detection approach by the means of a case study with autonomous connected cars. The scenario includes a route on the "Autobahn" in Germany. Sensors readings were oriented to the ones seen in the semi-autonomous vehicles found in the likes of Tesla Model X and BMW 13. Furthermore, the dataset for car movements on available routes could be utilised to analyse the behaviour of individual drivers or a pre-defined group of drivers (e.g. bus drivers required to comply with specific company regulation while driving) meanwhile this is not feasible with programmed system movement.

### B. Experiments

The proof of the research question is based on specific experiments of hijacked connected cars. In our work, we define 'Hijacking' as an attack from the cyberspace into the connected vehicle and changing the pre-defined route to a different destination, but could also be a more malicious intent of deliberate harm of driving into the wrong direction or off-street. Therefore, we assume that Eve can acquire knowledge about the parameters read and communicated between Alice (autopilot system) and Bob (command and control). Eve can also alter this communication. The model also assumes that Eve possesses the capacity to perform a Man-in-the-Middle (MITM) attack with unbounded access to the channel. On a holistic level a general experiment is proposed and formed as the following sequence of events:

- Defining a specific route between two cities (from A to B). This would be calculated and followed by a navigation system
- Sampling of profile characteristics along the route based on different behavioural factors
- Specification of the cyber-attack and route change being carried out (hijacking)
- Detection of the deviation from the norm route with Bayesian filtering (warning)

The following specific experiment has been conducted and presented in this paper: sample route is from Munich, Germany to Frankfurt, Germany on the motorways. The hijacking to deviate the car to Stuttgart will be programmed to the system. The deviation from a specific threshold value of comparable routes with Bayesian filtering will trigger a warning.

### C. Data Collection

Data collection consisted of two essential parts that need to be defined before forward processing is possible. Firstly, a collection of sensor readings that could create the schematics of the open data. In that regard the following readings have been defined:

- Speed metrics Mile/Hour (mi/h)
- Geolocation (longitude and latitude) via GPS positioning
- Elevation (altitude) via GPS positioning
- Orientation (cardinal direction) via gyroscopes
- UTC date-stamps via the Network Time Protocol (NTP)
- IPv6 addresses for unique identification of systems

The sample size is capped with an approximate target of 100 comparable routes of various vehicle movements. To illustrate the dataset, Table I shows an excerpt of the different types and fields of the data obtained. Each type of data is chosen in line with International System of Units (SI) measurements and universal or atomic definitions to abstract the proposed method in order to be applicable to a wide range of use-cases.

Secondly, once the data types have been defined, a new dataset template was created for this experiment as shown in Table III which has been based on the established format used for broadcasting aeroplanes in the aviation industry via ADB-S as shown in Table II.

Having established the data sources and the data types it should be noted that the local collection of cached data is important to run on-the-fly data analysis on the big data as well as for redundancy, error correction and not least forensics (for legal reasons). This could be achieved with data

TABLE II
AUTOMATIC DEPENDENT SURVEILLANCE: SAMPLE LOG

| Time | Position | Orientation | Groundspeed | Altitude | Reporting |
|---|---|---|---|---|---|
| Thu 01:18:41 | 34.87 27.54 | SE 138 | 520 | 37000 | ADB-B |
| Thu 01:19:11 | 34.81 27.59 | SE 138 | 520 | 37000 | ADB-B |
| Thu 01:19:41 | 34.76 27.65 | SE 138 | 520 | 37000 | ADB-B |
| Thu 01:20:11 | 34.70 27.71 | SE 138 | 519 | 37000 | ADB-B |
| Thu 01:20:41 | 34.65 27.77 | SE 138 | 521 | 37000 | ADB-B |
| Thu 01:21:50 | 34.52 27.90 | SE 139 | 521 | 37000 | ADB-B |
| Thu 01:22:49 | 34.47 27.96 | SE 139 | 528 | 37000 | ADB-B |
| Thu 01:28:10 | 33.82 28.63 | SE 139 | 527 | 37000 | ADB-B |
| Thu 01:28:46 | 33.77 28.68 | SE 139 | 529 | 37000 | ADB-B |
| Thu 01:29:21 | 33.69 28.77 | SE 136 | 533 | 37000 | ADB-B |
| Thu 01:32:01 | 33.39 29.00 | SE 147 | 0 | 37000 | ADB-B |
| Thu 01:33:01 | 33.27 29.09 | SE 147 | 0 | 37000 | ADB-B |

TABLE III
SAMPLE LOG FOR THE CAR'S MOVEMENT IN OUR EXPERIMENT

| ID | Time | Position | Elevation | Speed | Reporting |
|---|---|---|---|---|---|
| 2017:0db8:85a3:7334 | Sun 2017-03-11 | 47.82 12.54 | 456 | 9 | CSM |
| 2017:0db8:85a3:7334 | Sun 2017-03-11 | 48.24 12.53 | 455 | 11 | CSM |
| 2017:0db8:85a3:7334 | Sun 2017-03-11 | 48.23 12.52 | 435 | 10 | CSM |
| 2017:0db8:85a3:7334 | Sun 2017-03-11 | 48.13 12.58 | 509 | 9 | CSM |
| 2017:0db8:85a3:7334 | Sun 2017-03-11 | 48.24 12.53 | 449 | 7 | CSM |

recorders, also commonly known as black boxes for connected cars. Additionally, a central data collection service could be established to extend this proposal to support Intelligent Transportation Systems (ITS) and facilitate shared services for a better adaptive traffic control systems.

While more metrics could be captured and incorporated into the dataset, this minimalistic set of data was sufficient to profile and perform the behavioural analysis.

### D. Data Analysis and Modelling

Bayesian programming can be used to solve problems when important information is missing. It defines a method to compute a joint distribution over a set of relevant variables within experimental dataset $\delta$ with preliminary knowledge $\pi$ expressed as $P(X^1, X^2, ..., X^n|\delta\pi)$. This method could then be used to compute probability distribution $P(Searched|Known)$ to decide a value for variable $Searched$ which addresses the requirement of this study at a high-level. However, estimating the unknown density function of a dynamic system such as connected cars requires consideration to the time element while modelling stochastic states. Therefore, we utilise an extended method namely Recursive Bayesian estimation (a Bayes filter) [28], [36], [37] to model incoming measurements related to the car's movement (e.g. Latitude, elevation, cardinal direction etc) in real-time. Furthermore, we have applied specialisation of the Bayes filter with Kalman Filter due to its efficiency. It has a relatively low complexity, ability to provide the variance and wide applications in similar problems [26].

Nonetheless, a wide range of free and open-source tools and libraries are available to implement this statistical model of probability and density functions. For example, Stan (http://mc-stan.org/) can be used for statistical modelling, data analysis, and prediction in the social, biological, and physical sciences, engineering, and business. Full Bayesian statistical interfaces for R and Python. Other tools include PyMC for Bayesian statistical modelling and Probabilistic Machine Learning (version 2 and 3) and PyBayes which is a Python library for recursive Bayesian estimation (Bayesian filtering).

One of the good resources to get an overview of the tools and their utilisation for the experiments can be found in the Probabilistic Programming and Bayesian Methods for Hackers [38]. Further, by using the ShinyStan Software as a Service (SaaS) solution to plot the beta functions for density correlation it is possible to do a pairwise correlation.

Results of the statistical modelling could be interpreted with metrics of deviations of optimal routes defined with Bayesian filters calculated in percentage as key indicators. The balance of how much deviation to allow until it is flagged as anomaly is a considerable challenge.

## IV. RESULTS AND DISCUSSION

In relation to the data being used for analysis, an excerpt to demonstrate raw data collected from the sensors of a connected car for the particular routes in the experiment can be seen in Table III. It is important that security measures are planned to maintain the integrity of this data to prevent attacks including speed and location spoofing. Therefore, data collection should be automatic and depends solely on the car's navigation system (no external input). Moreover, in agreement with current initiatives to encrypt traffic of ADS-B systems [39], encrypting this information while stored or broadcast can be used to maintain privacy and protects against inappropriate or unauthorised use. Further to providing the required knowledge of the previous state of the system to the algorithm, we anticipate that Pay-As-You-Drive insurance schemes [40] will be one of many futuristic products to raise service provider's interest in this information. However, authorised access via Application Programming Interfaces (API) could be legitimately utilised to share situation awareness of the street and therefore achieve self-separation for the connected cars. Likewise, it could help governmental traffic control systems to detect congestions.

The main objective of this work was to research the applicability of predictive modelling in connected cars to estimate future states while travelling between two known locations to deduce anomaly behaviour. The literature review in Section II demonstrated a variety of mathematical models that could be applied including slower and/or costly by design classification machine learning models. The applicability of these is problematic because they could consume resources with extended complexity when implemented in live systems [11]. For instance, compiling large and effective Neural Networks require considerable processing power and other hardware computing resources [41]. They also require a pre-generated dataset of known-good/known-bad paths and car movements where 2/3 of the dataset will be used to train the algorithm with remaining 1/3 used for evaluation purposes; accuracy, recall, F1-measure, precision and False-Positive-Rate (FPP) are usually reported as a mean to measure the quality of the tested classifier. This is time consuming. In contrary, Kalman Filter accepts external uncertainty and can be satisfied with knowing the previous state of the system only without storing historic data or requiring training.

The main idea of this work is based on the probabilistic Recursive Bayesian estimation. Estimating unknown future states (through incoming metrics) via recursive density functions allow the usage of three types of mathematical models:

- Filtering (estimate the current value)
- Smoothing (estimating past values)
- Prediction (estimating a probable future value)

These sequential Bayesian filtering methods, which are extensively used in robotics and other embedded control devices were found applicable on the data collected in our experiment to perform prediction analysis. Looking at probabilistic models using Bayesian methodology in programming for a unifying framework [42]. Several filtering and smoothing algorithms [43] can be incorporated and these could be tested in more comprehensive field studies to optimise performance.

The very next aspect on correlating events is how well the distribution of routes will create a profile based on the behavioural analysis performed by the detection method. This is shown in Figure 4. The plotting represents the behavioural pattern (profile) of the change in speed and geo-location. The line represents the RStan function calculating the baseline of the said profile to which we are comparing against and the deviation that will be measured against. The deviation is not based on a single point, so one sudden acceleration at a specific location will not necessarily give the alert, instead the comparing can be optimised based on multiple events along the route. Figure 5 provides a different representation for the baseline.

Nonetheless, we could present the possibility that motion behavioural profiles for connected cars are created for groups of drivers or common systems (think about Heavy Goods Vehicles (HGV) versus Taxis). Each of the correlation graphs building a picture of the profiles a driving group has in common. Although there is no need to actually pre-define these profiles, as grouping them will be sufficient for applying estimation techniques. Further research could be conducted on the results shown here for the specific group behaviours.

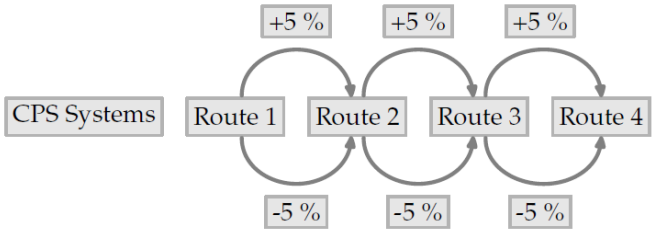


Fig. 3. Anomaly Threshold.

Collectively looking at the patterns these correlation graphs create, the deviation function becomes clearer. It has been shown through the analytical work that this deviation can be ring-fenced to a 5% margin with the estimation techniques using Bayes filters. This process has been illustrated in Figure 3.

These preliminary results from our experiment indicates that reducing the threshold of anomalies to a 5% margin for deviations from the baseline could be feasible. However, more field work will be required to conclude an ultimate value for our method. The comparisons in the plots, as shown in the examples of the Bayesian filters is as follows:

- Bayes filter plot with RStan: Figure 4 with a deviation prediction of 90% outside the 5% threshold
- Bayesian sampling with PyMC3: Figure 6 with a correlation of 87% inside the 5% threshold. This plot shows the distribution or plotting of two different profiles for the same route because the behaviour can differ in addition to how this has been factored while considering the whole route in terms of anomaly. Combining two profiles (or more) gives a more representative baseline for the route between A and B.
- Bayesian distribution and smoothing: Figure 5 is another demonstration of the mean function to compare against (baseline)
- Bayesian prediction with RStan: The chart in Figure 7 comparing three probabilistic functions to align the threshold. This is also a plot of speed and geo-location looking at a profile created between the two points of the route. This has 2 aspects to it, firstly, it uses Bayesian filtering algorithm with RStan which gives the baseline. Secondly, the effect of increasing and decreasing the tolerance has been demonstrated to count in the various routes that can be taken between cities A and B, which gives a minimum and maximum line of tolerance for the profile and the deviation (of 5%) to be measured against.

The baseline for comparison is primarily the average function of genuine routes marked as known-good and the correlation to this line with the added correction of errors. It has been shown, that the behavioural prediction creates a function that is better aligned to this baseline, as well as, that it reduces the error correction to a smaller deviation threshold. Further, the applications of the Bayes filter have also been compared with each other. Depending on the scenario, the sequential Bayesian filtering produced the best outcomes.

On the subject of false-positives, it has to be noted that the

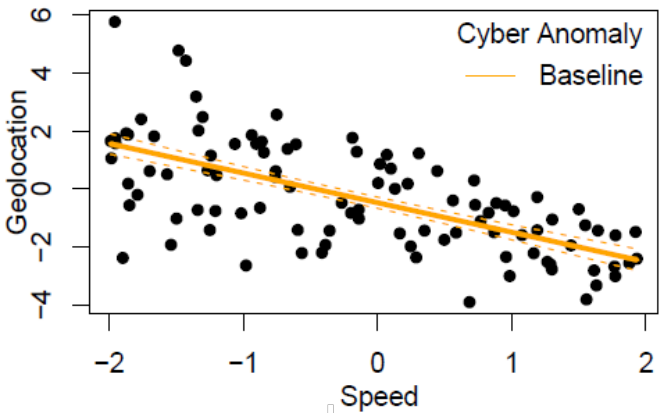


Fig. 4. RStan Bayesian Estimation: Distribution Graph.

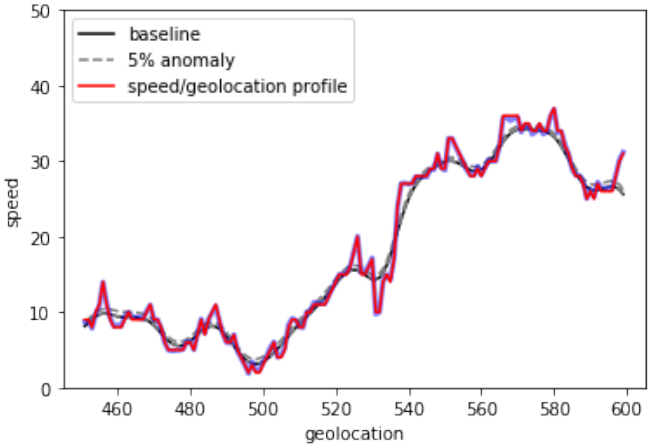


Fig. 5. Bayesian Estimation: Baseline versus the speed (mi/h) and geolocation profile.

development of reactive measurements and corrective actions need to incorporate and handle exceptions and incidents on legitimate routes in a way that the journey is not cut off suddenly, but coming to a safe halt.

As cars get smarter with thousands if not millions of lines of programming codes, attack vectors and vulnerabilities will increase rapidly. It is therefore essential that all stakeholders from engineers to retailers and senior level management involved in the manufacturing supply chain will be working around standards and consistent guidelines such as those recently published in August 2017 by the Department for Transport, Centre for the Protection of National Infrastructure, and Centre for Connected and Autonomous Vehicles in the UK. The report titled "The key principles of vehicle cybersecurity for connected and automated vehicles", shares eight principles one of which is highly relevant. Principle 8 states that the system should be "designed to be resilient to attacks and respond appropriately when its defences or sensors fail". Therefore, the utilisation of proactive detection methods (e.g. our proposal) should be part of a defence-in-depth approach (Principle 5 of the guidelines) which requires consoludating the car with further Artificial Intelligence (AI) systems.

To discuss an example within our scope (detection), The OpenCV (Open Source Computer Vision Library) can be used for AI in terms of discovery, mapping and tracking as shown in Figure 8. In sharp contrast, with the shown technique of predicting future states in motion patterns through correlation of historical data on the routes, instant analysis is possible to determine steering instructions for the selected routes as demonstrated with the route profile built in our experiment. And the general idea for predictive modelling can be reused on a variety of datasets and shown with different types of transportation systems.

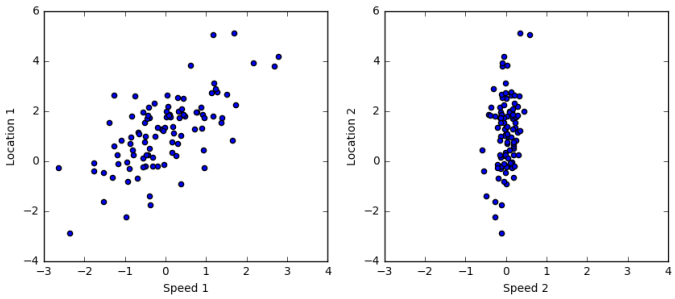


Fig. 6. PyMC3 Bayesian Distribution.

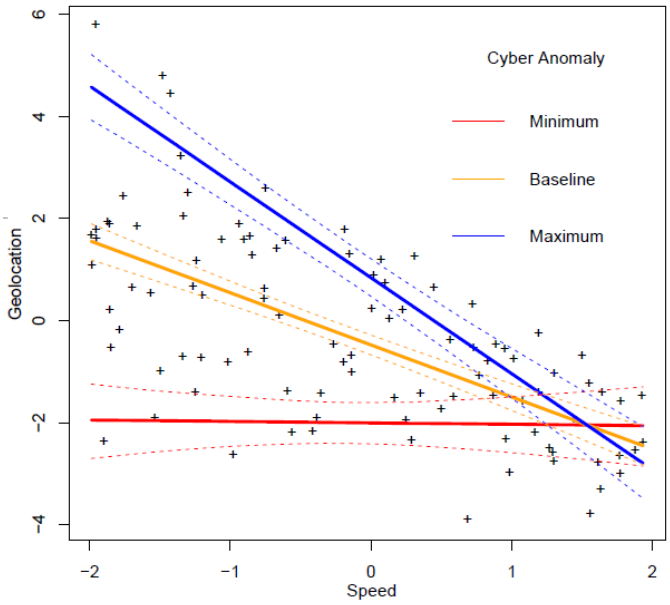


Fig. 7. RStan Bayesian Estimation: Filter.

Nonetheless, this emerging area of CPS resilience should also highlight a much needed discussion on the responsibility and accountability of fully autonomous systems and the implications their actions create raises questions such as:

- Will insurance cover the decisions taken by connected vehicles?
- Who will be defined as the owner of the vehicle in a society associated with a sharing economy?

The more pressing question is however how to program (instruct) the vehicle on reacting to events. What are the moral, ethical and philosophical duties [44] in case of unavoidable collisions? Do collision control algorithms need to weight on peoples life? Ultimately, observations on a change of

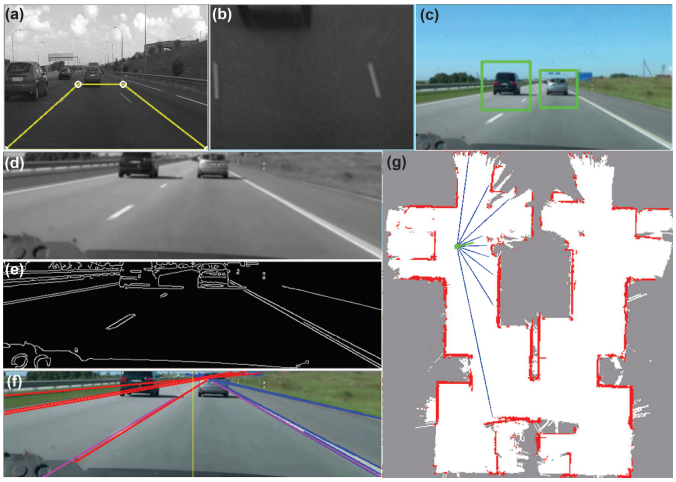


Fig. 8. Open Source Computer Vision Library: (a) distance and lane detection with radar and camera sensors, (b) perspective mapping and analysis, (c) vehicle detection with object discovery, (d) real-time lane and vehicle tracking, (e) edge and line detection for lane and vehicle mapping, (f) vehicle tracking with lane detection through the camera sensor, (g) OpenCV mapping through sensors (distance and obstacles).

behaviour will be inevitable with the increase of fully autonomous vehicles as they have a pre-defined way of driving. How will that affect the passenger who is not in charge of the control of the vehicle anymore? Moreover, there is a need for a method to determine the readiness of the society to start accepting "auto-pilot error" incidents. Lastly, with legislations in the likes of General Data Protection Regulation (GDPR), the aspect of data privacy and personal data (PII) has to be addressed. Incident reporting and protection of historical sensitive data will play a big part in dealing with data flows of future systems, not to mention the problems of identity and authentication of Cyber-Physical Systems.

## V. Conclusion and Future Work

Connected cars should be resilient -by design- to cyber-attacks. Appropriate responses when defences fail are triggered by detection methods. With the specific scenario of cyber-hijacking and change of routes, the threat modelling of remote hacking was highlighted as a potentially dangerous intrusion and it has been established that behaviour analysis and profiling can be the solution to this deficiency.

This paper has presented an approach to proactive anomaly detection for cyber-threat prevention by using concepts of behavioural analysis through Bayesian estimation techniques and a simulation has been carried out with the results as a proof-of-concept to argue that this can significantly improve resilience and reduce the time-cost required by supervised machine learning to predict new malicious intents. Connected cars have been chosen as a use case for the research to focus on a sub-set of Cyber-Physical Systems and conduct the behavioural analysis with a specific scenario of cyber-hijacking. A quantitative research design has been utilised by sampling a dataset of routes between two cities and the motion patterns including sensor data on which statistical methods and techniques are then applied. Through sampling, it can be shown that the deviations from normal routes can be recognised proactively which is an important improvement compared to traditional reactive solutions. Each profile is uniquely created for a specific car, although, some profiles can arguably be generalised for specific case studies such as the movement of buses following specific guidelines influenced by a company's policy. However, detection, in this case, could cover non-compliance with policies rather than hijacking.

Future work in this area includes the development of an integrated system with optimised methods based on a field study incorporating multiple cars and drivers. This will help to consolidate the system with corrective actions to identify exceptions related to external factors. Once identified, this external uncertainty can be used to enhance performance through better Bayesian prediction.

## References

[1] G. Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat*. Elsevier Science, 2015. [Online]. Available: https://www.elsevier.com/books/cyber-physical-attacks/loukas/978-0-12-801290-1

[2] A. Perallos, U. Hernandez-Jayo, I. Zuazola, E. Onieva, and I. Zuazola, *Intelligent Transport Systems: Technologies and Applications*. Wiley, 2015. [Online]. Available: http://eu.wiley.com/WileyCDA/WileyTitle/productCd-1118894782.html

[3] J. Graham, R. Olson, and R. Howard, *Cyber Security Essentials*. CRC Press, 2016. [Online]. Available: https://www.crcpress.com/Cyber-Security-Essentials/Graham-Olson-Howard/p/book/9781439851234

[4] D. J. Fagnant and K. Kockelman, "Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations," *Transportation Research Part A: Policy and Practice*, vol. 77, pp. 167 – 181, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0965856415000804

[5] M. Gerla, E. K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," pp. 241–246, March 2014.

[6] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, April 2015.

[7] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 10–21, Feb 2014.

[8] T. Ring, "Connected cars the next targe tfor hackers," *Network Security*, vol. 2015, no. 11, pp. 11 – 16, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1353485815301008

[9] L. Adouane, *Autonomous Vehicle Navigation: From Behavioral to Hybrid Multi-Controller Architectures*. CRC Press, 2016. [Online]. Available: https://www.crcpress.com/Autonomous-Vehicle-Navigation-From-Behavioral-to-Hybrid-Multi-Controller/Adouane/p/book/9781498715584

[10] J. Park, Z. Chen, L. Kiliaris, M. L. Kuang, M. A. Masrur, A. M. Phillips, and Y. L. Murphey, "Intelligent vehicle power control based on machine learning of optimal control parameters and prediction of road type and traffic congestion," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 9, pp. 4741–4756, Nov 2009.

[11] S. Suthaharan, "Big data classification: Problems and challenges in network intrusion prediction with machine learning," *SIGMETRICS Perform. Eval. Rev.*, vol. 41, no. 4, pp. 70–73, Apr. 2014. [Online]. Available: http://doi.acm.org/10.1145/2627534.2627557

[12] D. Fox, J. Hightower, L. Liao, D. Schulz, and G. Borriello, "Bayesian filtering for location estimation," *IEEE Pervasive Computing*, vol. 2, pp. 24–33, 2003.

[13] E. Alpaydin, *Introduction to Machine Learning*. MIT Press, 2014. [Online]. Available: https://mitpress.mit.edu/books/introduction-machine-learning

[14] NIST, "Framework for Cyber-Physical Systems," *Cyber Physical Systems Public Working Group*, Sep. 2016. [Online]. Available: https://pages.nist.gov/cpspwg/

[15] Y. Tan, S. Goddard, and L. C. Pérez, "A prototype architecture for cyber-physical systems," *SIGBED Rev.*, vol. 5, no. 1, pp. 26:1–26:2, Jan. 2008. [Online]. Available: http://doi.acm.org/10.1145/1366283.1366309

[16] F. Svahn, R. Lindgren, and L. Mathiassen, "Applying options thinking to shape generativity in digital innovation: An action research into connected cars," in *2015 48th Hawaii International Conference on System Sciences*, Jan 2015, pp. 4141–4150.

[17] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ads-b implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78 – 87, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548211000229

[18] M. Balac, F. Ciari, and K. W. Axhausen, "Modeling the impact of parking price policy on free-floating carsharing: Case study for zurich, switzerland," *Transportation Research Part C: Emerging Technologies*, vol. 77, no. Supplement C, pp. 207 – 225, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0968090X17300372

[19] T. Hberle, L. Charissis, C. Fehling, J. Nahm, and F. Leymann, "The connected car in the cloud: A platform for prototyping telematics services," *IEEE Software*, vol. 32, no. 6, pp. 11–17, Nov 2015.

[20] I. Stojmenovic, "Machine-to-machine communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 122–128, April 2014.

[21] S. I. Guler, M. Menendez, and L. Meier, "Using connected vehicle technology to improve the efficiency of intersections," *Transportation Research Part C: Emerging Technologies*, vol. 46, no. Supplement C, pp. 121 – 131, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0968090X14001211

[22] J. Lin, S. Sedigh, and A. Miller, "Modeling cyber-physical systems with semantic agents," in *2010 IEEE 34th Annual Computer Software and Applications Conference Workshops*, July 2010, pp. 13–18.

[23] E. A. Lee, "The past, present and future of cyber-physical systems: A focus on models," *Sensors*, vol. 15, no. 3, pp. 4837–4869, 2015. [Online]. Available: http://www.mdpi.com/1424-8220/15/3/4837

[24] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Computer Networks*, vol. 51, no. 12, pp. 3448 – 3470, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S138912860700062X

[25] C. Krügel, T. Toth, and E. Kirda, "Service specific anomaly detection for network intrusion detection," pp. 201–208, 2002. [Online]. Available: http://doi.acm.org/10.1145/508791.508835

[26] G. Ligorio and A. M. Sabatini, "A novel kalman filter for human motion tracking with an inertial-based dynamic inclinometer," *IEEE Transactions on Biomedical Engineering*, vol. 62, no. 8, pp. 2033–2043, Aug 2015.

[27] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vzquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & Security*, vol. 28, no. 12, pp. 18 – 28, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404808000692

[28] J. Wu, L. Yin, and Y. Guo, "Cyber attacks prediction model based on bayesian network," in *2012 IEEE 18th International Conference on Parallel and Distributed Systems*, Dec 2012, pp. 730–731.

[29] G. Epiphaniou, T. French, H. Al-Khateeb, A. Dehghantanha, e. H. Jahankhani, Hamid", A. Carlile, D. Emm, A. Hosseinian-Far, G. Brown, G. Sexton, and A. Jamal, *A Novel Anonymity Quantification and Preservation Model for UnderNet Relay Networks*. Cham: Springer International Publishing, 2016, pp. 371–384.

[30] G. Chen, D. Shen, C. Kwan, J. B. Cruz, and M. Kruger, "Game theoretic approach to threat prediction and situation awareness," pp. 1–8, July 2006.

[31] M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, and D. Gritzalis, "An insider threat prediction model," in *International Conference on Trust, Privacy and Security in Digital Business*. Springer, 2010, pp. 26–37.

[32] S.-H. Chien and C.-S. Ho, "A novel threat prediction framework for network security," *Advances in Information Technology and Industry Applications*, pp. 1–9, 2012.

[33] I. Frommholz, H. M. al Khateeb, M. Potthast, Z. Ghasem, M. Shukla, and E. Short, "On textual analysis and machine learning for cyberstalking detection," *Datenbank-Spektrum*, vol. 16, no. 2, pp. 127–135, Jul 2016. [Online]. Available: https://doi.org/10.1007/s13222-016-0221-x

[34] T. Lunt, "Detecting intruders in computer systems," vol. 61, 1993. [Online]. Available: http://www.csl.sri.com/papers/canada93/

[35] K. Xu, Z. L. Zhang, and S. Bhattacharyya, "Internet traffic behavior profiling for network security monitoring," *IEEE/ACM Transactions on Networking*, vol. 16, no. 6, pp. 1241–1252, Dec 2008.

[36] N. Bergman, "Recursive bayesian estimation: Navigation and tracking applications," 1999. [Online]. Available: http://www.student.nada.kth.se/kurser/kth/2D5342/

[37] A. Haug, *Bayesian Estimation and Tracking: A Practical Guide*. Wiley, 2012. [Online]. Available: http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470621702.html

[38] C. Davidson-Pilon, *Bayesian Methods for Hackers: Probabilistic Programming and Bayesian Inference*, 1st ed. Addison-Wesley Professional, 2015.

[39] C. Finke, J. Butts, and R. Mills, "Ads-b encryption: confidentiality in the friendly skies," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*. ACM, 2013, p. 9.

[40] C. Troncoso, G. Danezis, E. Kosta, J. Balasch, and B. Preneel, "Pripayd: Privacy-friendly pay-as-you-drive insurance," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 5, pp. 742–755, Sept 2011.

[41] H. Alemdar, V. Leroy, A. Prost-Boucle, and F. Ptrot, "Ternary neural networks for resource-efficient ai applications," in *2017 International Joint Conference on Neural Networks (IJCNN)*, May 2017, pp. 2547–2554.

[42] J. Diard, P. Bessiere, and E. Mazer, "A survey of probabilistic models using the bayesian programming methodology as a unifying framework," p. x, 2003. [Online]. Available: https://hal.archives-ouvertes.fr/hal-00019254

[43] S. Srkk, *Bayesian Filtering and Smoothing*. New York, NY, USA: Cambridge University Press, 2013.

[44] M. J. Sandel, "Justice: What's the right thing to do," *BUL Rev.*, vol. 91, p. 1303, 2011.

**Dr Haider M al-Khateeb** specialises in Cybersecurity, Digital Forensics and Incident Response (DFIR). He holds a first-class BSc (Hons) in Computer Science and PhD in Cybersecurity. Haider has published numerous professional and peer-reviewed articles on topics including authentication methods, IoT forensics, cyberstalking, anonymity and steganography. He was as a lecturer at the University of Bedfordshire, and currently a senior lecturer in Cybersecurity at the School of Mathematics and Computer Science, University of Wolverhamptonin. Haider conducts research within the Wolverhampton Cyber Research Institute (WCRI). He is also a consultant, trainer and a Fellow of the Higher Education Academy (FHEA), UK.

**Dr Gregory Epiphaniou** has been a leading trainer and developer for bespoke Cyber Security programmes with a dedicated, strong team of experts and trainers in several technical domains in both offensive and defensive security. He has also contributed to a numerous public events and seminars around cyber security, course development and effective training both private and government bodies. He was holding a position as a senior lecturer in Cybersecurity at the University of Bedfordshire and since Jan. 2018 is an associate Professor in Cybersecurity and Commercial Director of the Wolverhampton Cyber Research Institute (WCRI). He also holds several industry certifications around Information Security, and currently acts as a subject matter expert in the Chartered Institute for Securities and Investments.

**Adam Reviczky** has studied computer science in Budapest, Vienna and London. He has an MSc in Cyber Security from the University of Northumbria. Adam is a director of information security in the London office at Carlson Wagonlit Travel. His professional track record in the financial services industry includes roles as a security specialist within the CISO function of Deutsche Bank focusing on application security and being a cyber security IT risk manager aligned to the operational risk management at UBS. Growing up in Munich. Since 2011 he is a member of the GNOME foundation and regularly presents at the GUADEC conference.

**Dr Petros Karadimas** was born in Tripolis, Greece. He completed his Diploma (MEng) and PhD degrees in the Department of Electrical and Computer Engineering, University of Patras, Greece, in 2002 and 2008, respectively. In December 2009, he was appointed as a Research Fellow in the Centre for Wireless Network Design (CWIND) at the Department of Computer Science and Technology of University of Bedfordshire in UK. He was appointed as a Lecturer in Electronic Engineering in the same Department in October 2011, where he was promoted to Senior Lecturer in August 2015. In August 2016, he moved to the University of Glasgow, UK, as a Lecturer affiliated with the Glasgow College UESTC educational programs. His research interests are in the fields of Wireless Channel Characterization, Multi-Antenna Systems Performance, Wireless Security over the Physical Layer and Wireless Transceivers Performance. His research has been funded by major UK's funding organizations and councils, including EPSRC and CDE/DSTL

**Dr Hadi Heidari** is a Lecturer in the School of Engineering at the University of Glasgow. He received his PhD in Microelectronics from the University of Pavia (Italy) in 2015. He spent Postdoctoral at the University of Glasgow, before he joined the Glasgow College UESTC at the University of Glasgow in 2016. Dr Heidari is member of IEEE Sensors Council Administrative Committee, IEEE Sensors Council Young Professional Programme Chair and Senior Member of IEEE. He served on the organising committee of several conferences including General Chair of UK-China Emerging Technologies (UCET) 2017 Workshop, social media chair of the IEEE SENSORS 2016 and 2017 conferences, track chair at NGCAS 2017 conference, local organising committee of the IEEE PRIME 2015 conference, and organiser of a special sessions on the IEEE ISCAS 2016 and 2017 conferences. Very recently he started researching on Wireless Security over Physical Layer and Wireless Transceivers Performance."