Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2019.DOI

Privacy Challenges with Protecting Live Vehicular Location Context

MATTHEW BRADBURY[1], PHILLIP TAYLOR[2], UGUR ILKER ATMACA[1], CARSTEN MAPLE[1], and NATHAN GRIFFITHS[2]

[1]WMG, University of Warwick, Coventry, United Kingdom, CV4 7AL
[2]Department of Computer Science, University of Warwick, Coventry, United Kingdom, CV4 7AL

Corresponding author: Matthew Bradbury (e-mail: M.Bradbury@warwick.ac.uk).

This work was supported by PETRAS: UK Research Hub for Cyber Security of the Internet of Things project [EPSRC Grant EP/N02334X/1] and by Jaguar Land Rover and the UK-EPSRC grants [EP/N01300X/1, EP/N012380/1] as part of the jointly funded Towards Autonomy: Smart and Connected Control (TASCC) Programme.

ABSTRACT Future Intelligent Transport Systems (ITS) will require that vehicles are equipped with Dedicated Short Range Communications (DSRC). With these new DSRC capabilities new privacy threats are emerging that can be taken advantage of by threat actors with little experience and cheap components. However, the origins of these privacy threats are not limited to the vehicle and its communications, and extend to non-vehicular devices carried by the driver and passengers. A shortcoming of existing work is that it tends to focus on a specific aspect of privacy leakage when attempting to protect location privacy. In doing so, interactions between privacy threats are not considered. In this work we investigate the privacy surface of a vehicle by considering the many different ways in which location privacy can be leaked. Following this, we identify techniques to protect privacy and that it is insufficient to provide location privacy against a single threat vector. Privacy preservation techniques need to consider the wider threat landscape and collaborate to ensure location privacy is protected where possible.

INDEX TERMS Location Privacy; Connected Vehicles; Privacy Surface; Technique Interaction

I. INTRODUCTION

CONNECTED and Autonomous Vehicles (CAVs) are expected to be widely deployed on road networks globally within the next decade. As part of this, transportation networks are expecting to deploy ITSs to manage these vehicles. An issue with these systems is that they raise privacy concerns due to the ease in which these systems allow a vehicle to be tracked. However, vehicle tracking has been of interest to threat actors trying to violate privacy for some time. In the recent past, violating location privacy has only been generally available to resource rich threat actors for mass surveillance, or knowledgeable threat actors that focus on individual vehicles. For example, Automatic Number Plate Recognition (ANPR) allows vehicles to be tracked en masse, but it requires a deployment of ANPR cameras over a large area that is both expensive and noticeable. Individual vehicles can be tracked by threat actors with limited resources using location recording devices, but physical access is required for installation and they may be noticed by the driver. New vehicular technologies provide new methods of vehicle tracking that are cheaper with fewer limitations, easier to deploy, and in some cases, harder to detect.

These new tracking techniques usually do not focus solely on the vehicle's location, but also consider its identity and the time at which it was detected. This can be because the threat actors are interested in who was where at specific times, or how the location of a vehicle changes over time. Location, time, and identity are types of context information. Protecting the privacy of the context in which a vehicle performs actions is often harder than protecting against content privacy leaks. While content privacy is protected using encryption, context privacy requires bespoke solutions for the context being protected and the different scenarios it is protected in.

There are two main issues with existing work on protecting vehicular location privacy. The first is that there is a lack of positioning of the context in which location privacy is being provided. This necessary to understand which threats an adversary will take advantage of and why. In response, we propose a privacy surface which identifies the threat actors, their motivations, and capabilities. This landscape consists of existing threats, techniques to counter them, and a classification of both threats and techniques. In this paper, we focus on live privacy threats and briefly cover historical. This is

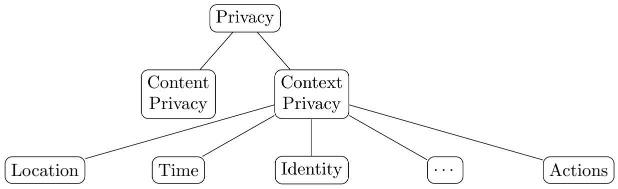


FIGURE 1: Privacy Hierarchy

because live privacy can be converted into historical privacy threats by threat actors logging data. Different types of live privacy threats can be protected by the same approaches when converted to historical privacy threats, whereas the live threats themselves need to be protected in different ways.

The second issue is that existing privacy preserving techniques tend to be developed in isolation and do not consider the impact the wider threat landscape has on the implementation. The majority of survey papers focus on specific areas (such as Location Based Services [1, 2, 3]) instead of considering a wider range of privacy threats. Some look at privacy in general [4] but do not present a wide range of privacy threats. To address this, the privacy landscape classes are used to predict ways in which privacy preserving techniques will need to be adjusted to consider different simultaneous privacy threats. We also identify a number of specific cases that warrant future investigation into how to protect location privacy when privacy threats interact.

The remainder of this paper is structured as follows. The survey of privacy threats to a vehicle will be presented in Section II. The threat actors will be identified in Section III before the survey of privacy preserving techniques is presented in Section IV. In Section V we will analyses the impact that privacy preserving techniques have on each other, before discussing our work in Section VI. In Section VII will present future work on this topic. Finally, this paper concludes in Section VIII.

II. LOCATION PRIVACY THREATS

Modern vehicles are identifiable by more than just their appearance and licence plate numbers. This is a result of their increased complexity and functionality, provided by new technologies that enable communication with road infrastructure and other vehicles, such as Dedicated Short-Range Communications (DSRC). These communication vectors provide possibilities for vehicle identification, and thus may compromise privacy. If a threat actor is able to obtain a detailed history of a vehicle's location it will be capable of creating analyses of this data which reveal information the owner of the vehicle wishes to keep private. One example analysis is a heatmap representing the frequency of locations where the vehicle has been. An example heatmap generated from data collected over a two week period from the same person is shown in Figure 2. In this map there are three points of interest, including their home, workplace, and a local bar, accompanied by the routes used between them. Linking even this small series of GPS trajectories to a map, it is possible to elicit the details of someone's pattern of life [5].

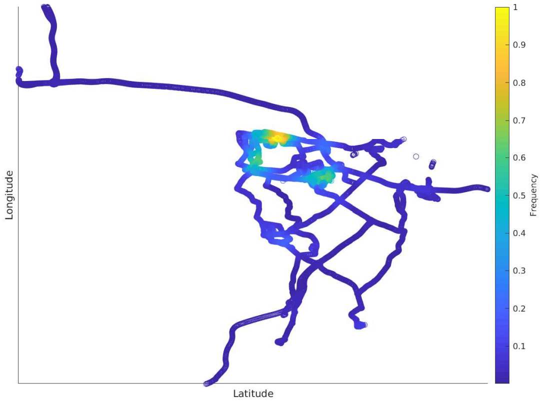


FIGURE 2: Heatmap of GPS trajectory collected over two weeks.

In this section we identify the various privacy threats through which the location privacy of a vehicle may be compromised. In Section IV the privacy preserving techniques that correspond to these threats will be presented. The privacy threats are classified into eight classes: (A) Direct Access to GNSS Data, (B) Visual Identification, (C) Services, (D) Internal Vehicle Communication, (E) External Vehicle Communication, (F) Non-vehicle Communication, (G) Behaviour, and (H) Historical Data. Each class has a number of different techniques that can be used to preserve privacy that will be discussed in Section IV. As threat identification is a continuous process, not all live privacy threats may be present in this categorisation.

A. DIRECT ACCESS TO GNSS DATA

One of the simplest ways in which a vehicle can be tracked is to attach a Global Navigation Satellite System (GNSS) sensor (such as GPS) to the outside of a vehicle, along with a battery and a cellular radio to report the location to the threat actor. Additional sensors, such as accelerometers can be included to improve accuracy. These devices are cheap and easy to obtain[1]. The downside is that a device needs to be attached to each vehicle that a threat actor wishes to track, which makes mass vehicle tracking infeasible.

These vehicle tracking devices may be intentionally installed by some authority. For example, a logistic firm may wish to track and manage their fleet of vehicles. Even if unintentional, it is possible that the data captured may be personal to the driver and privacy sensitive. Similarly, personal information is available by insurance companies who give preferential rates to those willing to install a black box in their vehicle [6].

[1] https://www.lifewire.com/best-car-gps-trackers-4158961

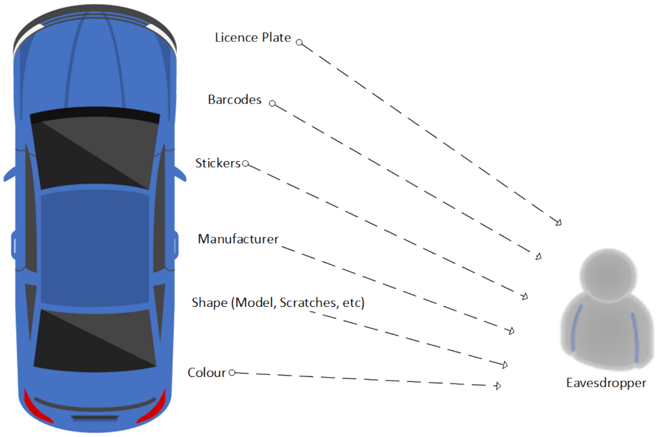


FIGURE 3: Some of the identifiable features of vehicle

B. VISUAL IDENTIFICATION

Vehicles have been partially identifiable since their inception by their colour, shape, manufacturer, and other aspects such as tyre tread. Since the beginning of the 20th century it has been mandatory to have an identifying number plate attached to the vehicle.The United Kingdom passed the Motor Car Act 1903 [7, §2(1–2)], making unique licence plates mandatory in 1904, around the same time some states in the USA also introduced them. Since then, it has been possible to identify a vehicle upon inspection of the series of letters and numbers attached to it. With the advent of Automatic Number Plate Recognition (ANPR) [8] this identification was automated, and widespread tracking of vehicles became possible.

ANPR operates by first finding number plates in an image and processing it to allow optical character recognition to identify the symbols attached to the vehicle. Due to inexpensive image recording equipment and the development of reliable image processing algorithms, ANPR is now used by law enforcement throughout the world. It is also used in many other scenarios, such as on toll roads and bridges, and car parks. London, for example, has several tracking systems for the Congestion Charge, the Low Emission Zone, the Dartford Crossing, as well as several other law enforcement systems for speeding and other offences [9]. In total, there are over 8500 cameras deployed in the UK which process over 25 million licence plates every day [10].

If a vehicle can be identified at several checkpoints across the road network, it is possible to build a picture of the vehicle's location over time. With more checkpoints in the road network, a more accurate tracking of the vehicle's route can be performed. When a vehicle is identified at one checkpoint, for example using ANPR, it is possible to re-identify the vehicle at a later checkpoint using only it's visual characteristics [11], such as its shape and colour [12], model [13], or a combination of several features [14, 15].

Another approach that does not rely on images of vehicles is to use the patterns provided by magnetic induction loops, which differ based on the shape of a vehicle and the metals from which it is made [16]. While these systems in general are less reliable than ANPR, due to the many similarities of different vehicles, they are more robust to occlusions of certain parts of the vehicle, such as the number plate.

C. SERVICES

Attaching an external GNSS sensor requires physical access to the vehicle, but modern vehicles often disclose their location directly to Location-Based Services (LBSs), in order to provide location context to their requests. For example, the current location can be used to improve the accuracy and speed of searches in a navigation system, or to provide information regarding local attractions. Depending on the requirements, the service might use a single location or trajectory of the owner [17], or the location and trajectories of multiple vehicles. Temporal and identity information are also aspects that will need to be protected [18, 19], however, context linking attacks might be conducted to obtain a consistent identity [19].

The widespread usage of LBSs has allowed service providers to gather massive amounts of location information about where vehicles are and at what time. This information is often used to provide better services to the vehicles, such as real time traffic speeds in maps apps such as Google Maps or Waze. However, this information can be analysed to extrapolate travel patterns and traffic analysis [2] such as an individual's driving behaviour, hobbies, home and work locations, and other personal information. The service providers are trusted to not abuse this information and to protect it from other threat actors. Further threats against historical information will be discussed in Subsection II-H.

D. VEHICLE COMMUNICATION (INSIDE VEHICLE)

Vehicles are equipped with many sensors to report on various statuses, including the wheel speeds, steering angle, and suspension movements. The majority of sensors are hard-wired to an Electronic Control Unit (ECU), as this offers high reliability and fast communication. ECUs are connected via a Controller Area Network (CAN) bus (or equivalent), which can be accessed using a On Board Diagnostic (OBD) reader on the OBD port or using vulnerabilities that enable remote access [20]. Modern vehicles typically have a GNSS sensor connected to an ECU, meaning that location is usually available via the CAN. Installing an OBD reader requires internal access to the vehicle, and remote access is challenging and limited, meaning it would likely be easier for a threat actor to attach their own external sensor.

Due to lower costs and practical restrictions, some sensors transmit their readings wirelessly. For example the Tire Pressure Monitoring System (TPMS) consists of a sensor inside each tire that transmit pressure measurements wirelessly. Messages in the TPMS contain a unique identifier that cannot be changed, and are broadcasted unencrypted [21] to a range of around 40 metres. This unencrypted broadcast enables a nearby adversary to eavesdrop the messages and identify the vehicle. Further, as the identity cannot be altered

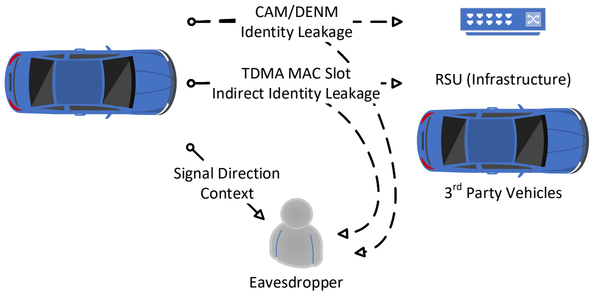


FIGURE 4: Vehicle Communication Threats

without changing the tires, certain protection schemes (such as pseudonyms [22]) are unsuitable to protect privacy.

Another wireless vehicular communication system that uses unique identifiers, and thus are a vector for location privacy leakage, is Remote Keyless Entry (RKE) [23]. When a button press is required, there is only a single sequence of short-range broadcasts when the key is used, which is likely to be insufficient to track the vehicle [24]. Passive RKE (PRKE) systems, which unlock the vehicle when the key is in proximity, rely on a periodically broadcasted beacon in either the key or the vehicle. While the low power of these broadcast make them difficult to intercept, this repeated communication containing the unique identifier increases the possibility of tracking and is a particular issue when the beacon is in the key, which travels with the driver even outside the vehicle.

E. VEHICLE COMMUNICATION (V2X)

While internal vehicle communications can reveal the location context of the vehicle, one of the most likely privacy threats are when the vehicle broadcasts its own location. The cooperative awareness message (CAM) is a European Telecommunication Standards Institute (ETSI) Intelligent Transportation System (ITS) standard that is periodically broadcasted by ITS Stations (including vehicles) [25]. CAMs are mainly used to facilitate vehicular awareness of vital traffic events by exchanging status information, where the content differs depending on the station type. For vehicles, the CAM contains the time, location, speed, heading, time, acceleration and other attributes. The information transmitted by CAMs are essential for many safety services in ITS network such as hazardous location warning, road condition warning, traffic condition awareness, and collision avoidance [26].

CAMs are sent with a digital signature that allows receivers to verify the authenticity of the message. They are not encrypted to minimise the processing time of the messages in safety critical scenarios, as the processing time is not allowed to exceed 50 milliseconds to maintain safety [27]. This combination leaks identity information (via the digital signature) and highly accurate information on where a vehicle is at a given point in time. By recording multiple CAMs a vehicle's route can be tracked. As CAMs are expected to be generated frequently (between 0.1 and 1 second [25]) this information has a very high time resolution.

In ITS networks, the applications can be classified into three groups such as traffic management, user-oriented services and safety services. Although ANPR systems are employed for traffic management, alternatives include barcodes, Radio Frequency Identification (RFID), Dedicated Short-Range Communications (DSRC), and Bluetooth. Barcode systems are rarely used to track moving vehicles, as they are affected negatively in adverse weather conditions and, as with ANPR, requires line of sight to the vehicle. Vehicles equipped with an RFID transponder can communicate receivers on the roadside, enabling vehicle tracking and automatic toll payments [28]. In Norway, autoPASS requires vehicles to have a DSRC transponder, which communicates with toll plazas even when the vehicle travelling up to 100 kph. The unique identifiers broadcasted from vehicles in the autoPASS system can be recorded by anyone with appropriate DSRC equipment.

Safety services have mandatory requirements of bounded transmission delay and low access delay to keep the highest level of safety while user-oriented services require broad bandwidth. The Medium Access Control (MAC) layer has an important role fulfilling these needs [29]. User-oriented services are the value-added services, which can provide road information, advertisements and entertainment during the travels. One example are Time-Division Multiple Access (TDMA) based MAC protocols, that divide time into slots and allocates the slots so no more than one ITS node has access to send messages in a specific slot. The advantage of this is that wireless collisions are avoided and the timeliness of protocols can be guaranteed. However, the slot in which a vehicle broadcasts acts as an identifier. This means that a unique TDMA MAC slot will allow a semi-local threat actor to track the trajectories of vehicles by listening to the wireless communication channel.

F. NON-VEHICLE COMMUNICATION

It is not just communication from the vehicle that can leak privacy, but also communication from additional devices and peripherals within the vehicle. For example, when a mobile phone is within range of a single cell tower, the telecommunication companies will be aware that the phone is within range of that single tower. Multiple towers can be used to accurately trace the location of a phone over time [30]. This information is often recorded and shared with authorities, including the police. This kind of tracking is applicable to vehicles because cellular devices are usually within the vehicle (such as mobile phone), but also because vehicles increasingly ship with cellular radios to support standards such as eSIM[2].

Many of the location privacy violations that will be presented require a unique identity to allow tracking a user over time. The first example of such an identity is the International Mobile Subscriber Identity (IMSI), which is unique across

[2] https://www.gsma.com/newsroom/press-release/automotive-industry-adopts-gsma-embedded-sim-specification

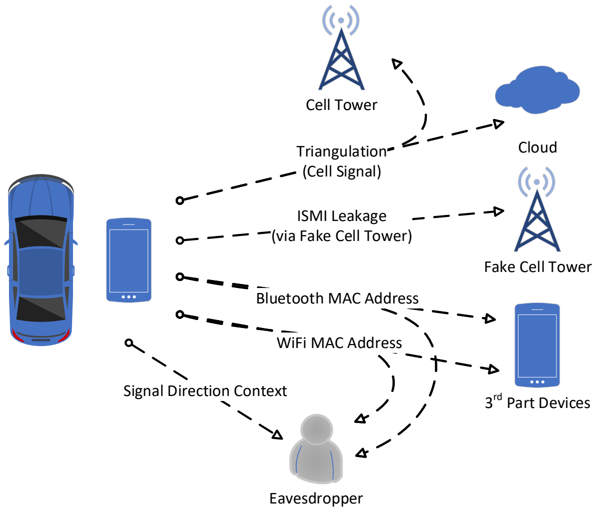


FIGURE 5: Non-vehicle Communication Threats

all mobile phone users worldwide. IMSI catchers are devices that can be used to obtain the IMSI of active users. The different cellular protocols require different approaches to obtain the IMSI number. Typically, a device is required to act as a fake base station that has mobile devices connect to it instead of the real base station, allowing a man-in-the-middle attack to be performed [31]. This is easy to perform in 2G/GSM as there is authentication in only one direction (the phone does not authenticate the cellular network). Man-in-the-middle attacks are possible on both 3G [32] and 4G/LTE [33]. Eavesdropping attacks against the 4G network can also allow an attacker to recover the IMSI number of targets [34]. Other techniques have also been investigated where IMSI numbers can be obtained over WiFI [35]. To avoid privacy issues with the ISMI number, Globally Unique Temporary Identifiers (GUTI) are allocated and used in most scenarios in an attempt to provide identity privacy. However, the GUTI values do not change frequently enough across a city area to obfuscate the user's identity. The work in [36, Table 1] concluded that the GUTI tended to remain the same over the 3 days a device was monitored in a city.

The problem with IMSI leakage for vehicles is that users will bring their mobile phones into vehicles, so leaking a uniquely identifying number for users will also leak a uniquely identifying number for the vehicle the user is in. The downside is that location context is only leaked via the proxy of signal strength. An adversary would need multiple IMSI catchers, or a mobile IMSI catcher in order to track a vehicle over a long distance.

An alternative to using ISMI numbers to track users is to instead take advantage of vulnerabilities in the 4G/LTE Radio Resource Control (RRC) protocol [36]. As the user equipment (UE) (i.e., a phone) does not verify (intentionally for one case, and unintentionally — a bug — for the other) that a request for information comes from a telecoms operator and because the request and response are unencrypted, a threat actor can trigger these messages to obtain a user's location. The responses can contain the radio tower the phone is connected or GPS coordinates if supported.

Bluetooth devices utilise a short range wireless link to communicate with each other. Examples of typical devices include MP3 players, wireless headphones, and mobile phones. An example of an application of mobile phones using Bluetooth is the rSAP (remote SIM access protocol), which allows a vehicle to access the SIM card of a phone to make calls. However, Bluetooth devices perform a periodic broadcast of an advertisement packet in order to inform nearby devices of their presence. Privacy is leaked by the inclusion of the device's MAC address in the advertisement packets [37]. By recording where and when Bluetooth MAC addresses have been detected, the route a device has taken can be calculated.

Cars are increasingly being equipped with IEEE 802.11 WiFi hotspots that devices within the vehicle can connect to. These hotspots are intended to offer internet connectivity via a cellular radio, or to allow devices to control certain aspects of the vehicle (such as the infotainment system). To enable connectivity WiFi hotspots broadcast beacon frames which contain the Service Set Identifier (SSID) among other information important for devices looking to connect to the hotspot. The SSID gives the network a name and this leads to identity leakage. Similar to Bluetooth, both the hotspot and 802.11 devices will broadcast their MAC addresses [38], the channel the hotspot communicates on is another dimension that can be used to identify a target in more detail, and there are a variety of additional pieces of information that can be used to fingerprint an IEEE 802.11 device [39].

In certain cases it is not necessary for the content of the message to be leaked for an adversary to be able to trace a target. For example, in the case of wireless sensor networks (WSNs) [40] just using the direction from which a message was received (a kind of context information) an attacker could trace back to a valuable asset. This direction context could be obtained using directional antennas, but it is more likely that multiple omni-directional antennas will be used instead. An attacker just receiving a CAM or DENM leaks the time and location of a vehicle. The velocity can be calculated by the difference in distance of subsequent messages, and those subsequent messages can be linked by checking that aspects of the calculated values are sensible. Examples of these checks include, position change and velocity change.

G. BEHAVIOURAL DATA

Different drivers behave differently and have different styles when interacting with the controls of the vehicle [41]. Some drivers may typically brake more sharply than others at traffic lights, for example, and some drivers may maintain a consistent speed whereas others may fluctuate regularly. These differences can be used to categorise their driving style [42, 43] and to assess skill of a driver [44], but the very personal behaviours behind a wheel can be used to identify the driver behind the wheel [41, 45], of if there is a change of driver [46]. Using twelve signals from the CAN, including steering wheel angle, velocity, pedal positions, and torque, Hallac et al. [47] were able to determine the driver from data collected around single corners.

It is possible to measure the driving behaviours visually and using RADAR, but velocity, road position, and accelerations can be observed only coarsely and intermittently. An alternative may be to use the accelerometers and other sensors in smartphones, which some apps may have permission to access. While GPS provides the location directly to apps, privacy conscious users may disable localisation while giving access to other sensors that are not obvious privacy issues. In [48], for example, the magnetometer is used to detect changes in the driving angle and then map those changes onto a potential route.

H. HISTORICAL DATA

Organisations may wish to legitimately collect location information about a user after being given affirmative consent to do so. This data could be used for a wide range of purposes. For example, Google gathers the live location of users to provide a number of features, such as live traffic densities and estimated journey times, how busy a venue is, and many others. The historical data used to provide these services will need to reside in a database. The information in this database could potentially be leaked to a threat actor who was not expected to be allowed to view the database[3]. This may be through vulnerabilities, such as SQL injections, insider attacks, or other attacks.

All the threats previously mentioned could potentially have data that leaks privacy stored in a database. This transforms the threat from gathering live information to gathering historical information. While this reduces the impact duration of the threat, it is possible to gain access to a database remotely, and the likelihood increases for threats with difficult and long setups. For example, whereas ANPR tracking requires a lengthy setup of cameras, networking, and software, accessing an ANPR database with locations can be remote and is more likely. In general, the number of vehicles impacted also increases, as a single database is likely to contain information about many vehicles.

Data summaries might be published with the intention to provide useful information but protect the privacy of specific individuals. However, it is important to ensure that privacy about a population or organisation is also not leaked. One example where this was not the case, is when the fitness tracking app Strava published heat maps of user activity. However, this data ended up revealing the physical layout of military bases around the world [49]. A privacy radius can be used, such that locations within a radius (typically centred on a user's home or workplace) are not disclosed. However, these are imperfect with overlapping privacy zones providing insight into their origins as well as the risk they may be part of a database leak.

Impact	Low	Medium	High
Vehicles Impacted	**Single**: A single vehicle is impacted	**Some**: A small number of vehicles are impacted	**Many**: A large number of vehicles are impacted
Threat Actor Presence	**Local**	**Semi-local**	**Remote**

TABLE 1: Ranking dimensions used to measure location privacy threats

Name	Class	# Vehicles Impacted	Presence Required
Physically Attached Sensor	T_A	Single	Local
Fleet Management and Black Boxes	T_A	Single	Remote
Smartphone Sensor Data (Permission — GNSS)	T_A	Single	Remote
ANPR Tracking	T_B	Many	Semi-Local
Tracking via Visual Features	T_B	Many	Semi-Local
Location Based Services	T_C	Some	Remote
CAN Bus Access	T_D	Single	(Varies)
Vehicular Sensor Network Identifier	T_D	Single	Semi-Local
PRKE	T_D	Single	Semi-Local
Signal Direction Context	T_D / T_E / T_F	Single	Semi-Local
TDMA MAC Slots	T_E	Single	Semi-Local
CAM/DENM Identifier	T_E	Single	Semi-Local
Triangulation (e.g., via Cell Tower)	T_F	Many	Semi-Local
ISMI Catchers	T_F	Many	Semi-Local
Bluetooth Identifier	T_F	Single	Semi-Local
WiFi Identifier	T_F	Single	Semi-Local
Driving Style	T_G	Single	Semi-Local
Smartphone Sensor Data (Permissionless — Magnetometer)	T_G	Single	Remote
Database Leak	T_H	Many	Remote

TABLE 2: Privacy Threat Summary

I. SUMMARY

In summary, there are many privacy threats against a vehicle, some of which actually come from the devices within the vehicle. Table 2 presents a summary of the identified threats and includes the presence the attacker requires to take advantage of that privacy threat. This summary includes the number of vehicles impacted by the privacy threat and the attacker's presence as defined in Table 1. The attacker's presence will be elaborated on in Section III. Note that a Database Leak is shown separately as any of the previous threats could be transformed into an attack on historical data by storing it in a database.

[3] https://turtler.io/news/top-11-worst-location-data-privacy-breaches

III. THREAT ACTORS

In order to properly understand how a privacy threat will be exploited, it is necessary to understand the threat actor performing the exploitation. There exist multiple actors who wish to violate the location privacy of a vehicle. These actors each have different capabilities, resources, and expertise, which changes the ways in which they are able to obtain location information about vehicles. These actors also have different intents, for some threat actor the usage of this data will have a malicious purpose, others will be interested in gathering data to provide services, whilst others will be looking to benefit all road users. This section will analyse the threat actors who may wish to violate location privacy and will consider the desire to protect against them.

To perform this analysis we identify four key attributes that indicate what actions threat actors can perpetrate: (i) capabilities, (ii) equipment, (iii) intent, and (iv) presence. Where capabilities indicates the knowledge, skills and experience the threat actor has, equipment specifies the resources available to the threat actor, intent is for what purpose the threat actor is violating location privacy, and presence indicates the location of the adversary.

A. THREAT ACTOR CAPABILITY

Layman → *Proficient* → *Expert* → *Multiple Experts*

- **Layman**: Basic knowledge and low technical proficiency. Uses existing tools to exploit vulnerabilities.
- **Proficient**: Able to develop new tools to exploit vulnerabilities based on having experiences in the past.
- **Expert**: Extensive knowledge in the system domain.
- **Multiple Experts**: Multiple individual with expert knowledge of the system. Will have insider knowledge that has not been made public.

The knowledge and skills that the threat actor has will specify the threats that the threat actor can take advantage of. Typically less capable threat actors will be able to perpetrate fewer privacy violations. However, more proficient threat actors may develop highly technical privacy attacks that with the intent of providing them to less capable threat actors to deploy. The capability level will also link with the setup time before privacy can be violated, with a higher capability leading to a lower setup time.

B. THREAT ACTOR RESOURCES

Off-the-shelf → *Standard* → *Specialised* → *Bespoke* → *Multiple Bespoke*

- **Off-the-shelf**: Access to reasonably priced off-the-shelf equipment. This equipment will be limited in its capabilities.
- **Standard**: Access to expensive widely available off-the-shelf equipment.
- **Specialised**: Access to expensive specialised equipment.
- **Bespoke**: Able to purchase or design custom equipment, but limited to small deployments.
- **Multiple Bespoke**: Able to purchase or design multiple piece of custom equipment and deploy in bulk.

The equipment that a threat actor has access to will determine which threats it is capable of taking advantage of. In some of the privacy threats discussed so far, such as tracking via Bluetooth and WiFi, simple and cheap off-the-shelf equipment will be sufficient. Other threats will require standard equipment such as cameras to perform ANPR tracking. Whereas, specialised equipment would be necessary to track CAM/DENM identifiers sent over 802.11p, and bespoke equipment needed to deploy ISMI Catchers. Alternatively, it may be possible to use standard equipment such as Software Defined Radios (SDRs) instead of the specialised or bespoke equipment. For example, a threat actor could implement an 802.11p radio using an SDR rather than purchasing 802.11p equipment. The downside to this is that the threat actor would require a greater technical knowledge and the setup time would be higher.

C. THREAT ACTOR INTENT

Benign → *Unintentional* → *Malicious*

- **Benign**: A threat actor that collects information that is kept secure and private. The information is used for good purposes, such as providing a service, or improving the transportation network.
- **Unintentional**: A threat actor that collects information and intends to keep it secure and private, but fails to do so. This may be due to poor security leading to data breaches, or released datasets not being properly anonymised.
- **Malicious**: A threat actor that intentionally obtains information that aims to use it for bad purposes. This may involve releasing or selling unanonymised data.

It is important to understand the intent of a threat actor. Different threat actors intend to collect data that violates the privacy of a vehicle for different reasons. The typical intent that is protected against is malicious, where the threat actor intends to violate privacy in order to cause harm to the vehicle or person privacy is violated against. However, in other cases the threat actor may not intend to violate privacy of users, but may unintentionally reveal it to many people. Command examples include government officials leaving unencrypted disks on public transport. It may also be the case that privacy violating information is collected to improve the lives of people the data is gathered about. Privacy preserving techniques will be different when considering different intends of the threat actor. Additional techniques will also be available to benign and unintentional threat actors to protect privacy.

D. THREAT ACTOR PRESENCE

Internal → *Local* → *Semi-Local* → *Remote*

- **Internal** presence is when the threat actor is able to access the inside of the vehicle. This includes physical access to components within the vehicle's body, but also if malware is deployed to internal components remotely.

Threat Actor	Motivations	Capability	Opportunity	Impact	Resources
Amateur (Cracker)	Curiosity, Self-actualisation, Passion	Layman	Open access knowledge (Low)	Unlinkable data, unidentified vehicle tracking	Low financial, Off-the-shelf equipment
Unorganised Crime (Hacktivist)	Financial gain, Vehicle theft, Passion	Proficient	Restricted knowledge (Medium)	Single identified vehicle tracking	Standard equipment
Organised Crime (Cyber Criminal)	Financial Gain, Ideology	Expert	Sensitive knowledge (Medium or High)	Single or multiple identified vehicle tracking	Specialised Equipment
Organised Corporation	Financial Gain, build services based off data, Ideology	Multiple Experts	Sensitive knowledge (High)	Multiple identified vehicles tracking	High financial, large bespoke deployments
Government	Improve infrastructure, track criminals, Political	Multiple Experts	Critical knowledge (Critical)	Single-multiple identified vehicles and traffic tracking	Nationwide bespoke deployments

TABLE 3: Example Threat Actors

- **Local** presence is when the threat actor is physically located outside of the vehicle (typically within several meters of the vehicle). This threat actor is able to attach devices to the outside of the vehicle.
- **Semi-Local** presence is when the threat actor is physically nearby the vehicle. They may be out of sight of the vehicle, but still in wireless range. This threat actor may be capable of eavesdropping or visually observing vehicles.
- **Remote** presence is when a threat actor only has access to vehicle information via the internet. This threat actor is incapable of observing the vehicle locally, but may gain control of devices within the vehicle in order to obtain **Internal** presence to observe events.

The presence of the threat actor is important in understanding the threats it can perpetrate. A local threat actor will be capable of perpetrating more privacy violations, but this comes at an increased difficulty and risk for the threat actor (such as capture by authorities). Whereas remotely violating privacy is limited in the privacy violations that can be performed, but comes with a lower risk to the threat actor. There is also an impact regrading the quantity of vehicles that a threat actor can violate privacy for, as semi-local and remote threat actors will likely be able to impact more vehicle's privacy.

E. EXAMPLE THREAT ACTORS

A table of example threat actors is shown in Table 3 which is created based on the works in [50, 51, 52]. These threat actors are specific examples of different combinations of intent, capabilities, and resources, but also includes details specifying the threat actor's: motivations (why does it want to violate location privacy), opportunity (how aware of situations in which privacy can be violated), and the impact it can have on location privacy. It is important to consider who is violating privacy, because there will be limitations to the privacy a technique can achieve based on the type of threat actor that is violating privacy.

IV. PRIVACY PRESERVING TECHNIQUES

With an understanding of the threats to vehicular location privacy and the threat actors that perpetrate the threats, the techniques used to provide privacy can be examined. There has been much work performed in developing techniques to protect location privacy. This section will examine privacy protection techniques and classify them into five categories: (A) Signal Jamming, (B) Perturbing Identity, (C) Perturbing Data, (D) Changing Communication Patterns, and (E) Changing Behaviour. These categories are intentionally broad due to the wide range of privacy threats being considered. More specific categorisations have been considered in other work that focuses on specific location privacy threats (such as in [1]), but are not suitable for this broad range of threats.

A. JAM SIGNAL

To protect against certain types of threat a vehicle may seek to jam signals being broadcasted. For example, if a threat actor has attached a GNSS sensor to the vehicle, then jamming the GNSS signal would prevent location logging. The downsides are that (i) the vehicle would also not be aware of its location via GNSS, (ii) an additional signal is present that a threat actor could possibly track, and (iii) GNSS jamming is illegal in many parts of the world (e.g., Title 47 U.S.C §§ 301, 302(b) and 333 for the USA[4] and Section 68 of the Wireless Telegraphy Act 2006 for the UK[5]). For many threats, jamming signals would be unsuitable to provide location privacy because it denies availability.

[4] transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf

[5] legislation.gov.uk/ukpga/2006/36/pdfs/ukpga_20060036_en.pdf

B. PERTURBING IDENTITY

To protect the identity, one option is to encrypt the uniquely identifying number broadcasted in messages. For example, in a TPMS encrypting the per sensor identifier while leaving the rest of the message unencrypted protects the identity and facilitates issue diagnosis by humans due to the unencrypted contents [53]. Each time a message is broadcast a different encrypted value would be sent, essentially making it appear as if a random identifier was being used. This means that the message contents can still be used by existing tools, meaning both backwards compatibility and privacy are provided. To obtain a stronger encryption the authors of [53] propose the encrypted identifier be lengthened from 32 bit to 64 bit, but this would break backwards compatibility.

This technique works for TPMS because the sender and receiver are only a single communication hop away from each other, and hardware deployers can ensure the vehicle is aware of what TPMS identifiers to expect and how they will be encrypted. For other systems that do not have such a tight integration, this approach of encrypting the identifying information such that it is different with each broadcast may not be feasible.

To enable vehicle tracking, having a consistent identity that can be observed at different locations and times allows a threat actor to link individual observations into a more comprehensive dataset of the route taken. One of the key techniques to protect location privacy of vehicles is the use of temporary pseudonyms that change frequently. By changing pseudonyms the threat actor is less able to link between individual observations [54]. Such a technique is useful for a variety of communication protocols, such as V2X, WiFi, Bluetooth and others.

Pseudonyms can be used in different circumstances. For example, a benign threat actor may be gathering data (which they have been given permission to do so) and anonymising the data by generating pseudonyms for users themselves. Alternatively, the vehicles themselves may be periodically changing the pseudonyms they broadcast to other vehicles and road-side infrastructure to protect against data gathering by malicious threat actors.

One of the recent innovations currently being experimented with are digital number plates [55]. They use an e-ink display to show the vehicle's registration number and open the possibility to show alerts that change along with other messages. Because the number plate displayed is customisable, the registration number could be a pseudonym that is periodically changed. As this technique would then be similar to pseudonyms used in wireless broadcast techniques, unlinking strategies would be needed to ensure the old pseudonym could not be linked to the new pseudonym. An alternate approach could be to use adversarial machine learning. As the display on the number plate is customisable, it may be possible to display a pattern that prevents the optical character recognition component of ANPR from being able to discern the characters in the number plate [56].

Identity anonymity-based approaches are commonly used to protect the location privacy of LBS users. This is necessary because LBS providers are assumed to correctly process and respond to requests, but they might attempt to disclose identity of a user [57]. k-anonymity [58] is one of the most popular anonymity-based approaches, where it focuses on controlling the release of quasi-identifiers of users in a dataset, where quasi-identifiers are a combination of characteristics that enable linking to a user. The technique requires that the each quasi-identifier of an individual must be indistinguishable from $k-1$ other individuals, where $k > 1$.

In the context of protecting vehicular location privacy within LBS, the linking attack is successful if the user's location is revealed by the queries sent to a LBS. Anonymity can be achieved by cloaking a location area, such as by New Casper [59], Prive [60], and PrivacyGrid [61] which provide k-anonymity by cloaking an area that contains at least k users at the time of a query submission. Other approaches (such as [57]) introduced personalised minimum level of anonymity and used query submission delay to provide the minimum level of anonymity.

However, it can be difficult to achieve k-anonymity for LBS users in practice. The number of k vehicles might be very less in sparse traffic and keeping the boundaries of the cloaked location area is very large might cause a significant loss in the utility. Furthermore, a shortcoming of k-anonymity is that if an adversary has sufficient background information it may be capable of distinguishing an individual from the k others [62].

There are limitations to perturbing identity because certain aspects of the vehicle are immutable (or sufficiently difficult to change). For example, the colour and shape of a vehicle can contribute to uniquely identifying it and both would be difficult to change. Also as digital licence plates are in their infancy, nearly all vehicles will be fitted with standard number plates which require time and effort to change. The frequency that these kinds of identity can be changed is lower than other aspects of identity (such as wirelessly broadcast pseudonyms), which means they can be used to link higher rate identity change techniques.

There can also be limitation against specific privacy threats. For example, using temporary pseudonyms to prevent tracking of WiFi devices is insufficient as there are a number of implicit characteristics of using WiFi devices (network destinations, advertised SSIDs, IEEE 802.11 options, and sizes of broadcast packets) that allows a threat actor to be able to potentially identify a device [39]. This means that multiple privacy preserving techniques will need to be used for a subset of privacy threats.

C. PERTURBING DATA

Privacy of individuals can be also protected by perturbing records in a database. The existing data perturbation techniques include additive noise, aggregation, swapping records, or generating synthetic data based on statistics of the original data [63]. The data perturbation techniques recently got more attention in research as a consequence of being simple and cost-efficient compared to most of the other Privacy Preserving Data Mining (PPDM) techniques [64]. The data perturbation can be analysed in two categories as input perturbation and output perturbation. Input perturbation techniques, where the original data are randomised and the computation is done on the randomised data; and output perturbation, where the computation is done on the original data but the answers are published with noise [65]. Differential Privacy (DP) is an emerging privacy preserving technique which guarantees a strong privacy preserving. Centralised Differential Privacy (CDP) and Local Differential Privacy (LDP) are the main models used to achieve DP, however there are emerging studies on hybrid DP models [66]. CDP works based on output perturbation where the original data is aggregated in a trusted curator and the amount of perturbation is calibrated according to the query outputs. The main propose of CDP is, ensuring the query outputs are almost same with addition or removal of a single record in a database. Besides that, input perturbation techniques such as Randomised Response [67] can be used in LDP. In LDP, data owners locally perturb their data before transmitting them to the any other parties. The computations and analysis are run directly on the perturbed data. Thus the need of a trusted curator disappears for LDP and the data owners can have plausible deniability. LDP provides stronger privacy guarantee than CDP but concomitantly induces greater noise [68]. Alvim et al. [69] discussed the usage of some LDP techniques for metric space including location data. The challenge of LDP is that it can drop off the usability of data more than CDP depending upon the size of the data set. The extensive data sets with deployment of LDP provides better utility.

The application of DP for location data is an emerging research area. Most of the studies considered the CDP model. The notion of geo-indistinguishability [70] is proposed to preserve the exact locations of individuals in a radius r with the level of privacy preserving depending on r and a distance-based probabilistic noise is introduced to the location data. However, due to the distance based sensitivity measurement and sparsity of location dataset, it might be needed to add a large amount of noise to ensure DP. Cormode et al. [71] applied a hierarchical tree structure to decompose geometric areas into smaller areas. Herewith, they could reduce the amount of needed noise. Ou et al. [72] claimed the privacy model should not only LBS user‘s privacy but also location correlation among multi-user. They have proposed a model to quantify location correlation of two users by hidden Markov model and protect the multi-user location correlation. DP techniques promise a rigorous privacy preserving; there are limited applications that adopted DP in practise. In particular to the vehicular domain, the implementation of DP investigated for protection of floating car data [73].

D. CHANGING COMMUNICATION PATTERNS

As the MAC time slot assignment can be linked to the identity of a vehicle, if a vehicle changes its pseudonym then the MAC time slot remaining the same would allow a threat actor to link the old and new pseudonym. The work in [74] synchronises the change in MAC time slot and pseudonym to prevent the attacker from performing this linking.

To prevent a threat actor from gaining information, one option is for the vehicle and the devices to cease broadcasting for sufficient time to reduce the linkability of its location before it stopped broadcasting and the location after it starts broadcasting again. In most situations this is undesirable as it limits the availability of the services being provided, which could potentially lead to safety issues. It would also be unacceptable to users to cut off certain services whilst they are in use (e.g., during a call). However, there are some situations where staying silent does not lead to a significant safety decrease. For example, CAM pseudonym schemes rely on a silent period after changing pseudonyms in a large group to prevent linkability between the old and new pseudonyms [54]. Without the silent period a threat actor would be able to link the CAM pseudonyms.

The Received Signal Strength Indicator (RSSI) is a value that indicates how strong a wireless signal is while a message is being received. Base on this value the distance of the vehicle can be estimated [75]. By varying the DSRC transmit power the accuracy of the localisation of the vehicle can be reduced.

To resolve the issues with the way Bluetooth devices leak identity information that facilitate tracking, in the Bluetooth 4.2 standard a new feature called LE Privacy was introduced. The aim of this technology is to randomise the MAC address used to advertise the device [76, 77]. Once devices are paired they will both possess an Identity Resolution Key (IRK) which allows translation of the randomised MAC address into the real MAC address. This way devices can connect to each other and know if identity of the connected device, but observers see MAC addresses that appear to randomly change at a rate set by the manufacturers.

It is important that manufacturers provide a way to disable backwards compatibility with the old advertising technique, because if it and LE Privacy are both enabled then no privacy is provided. For example, in 2016 a report into fitness tracker privacy found that all devices except one of those investigated (Apple Watches) leaked persistent MAC addresses by not using BLE Privacy [78].

For WiFI additional perturbations need to be made as it can be insufficient to just change pseudonyms [39]. Additional aspects of using WiFi also need to be varied, including: network destinations, SSID probes, broadcast packet sizes and MAC protocol fields.

In order to track vehicles a correlation often needs to be made with the location at which the vehicle was detected and when that vehicle was detected. In order to prevent this correlation messages can be delayed and reordered [79]. However, this has limited uses in a vehicular context, as many message will be safety critical and therefore need to have minimal delay.

Rather than delaying and reordering messages, if possible the messages could cease broadcasting. This technique would

Class	Name	Privacy Protection	Feasibility	Cost
P_A	Jam Signal	Denies access to GNSS sensor, or a communication link.	Low feasibility. Jamming is illegal in many places. Users will still want services.	Denies availability to services that are jammed.
P_B	Encrypt Unique Identifier	Prevent identity leakage.	Useful in specific circumstances, but infeasible in general.	Computational and communication overhead.
	Temporary Pseudonyms	Decorrelates identity of vehicle at specific time and location	High. Useful to many different privacy threats.	Computation and communication in obtaining pseudonyms and handling identity change. Safety costs in some applications (due to required silent period).
	k-anonymity	Group k data of individuals into a range to make each individual indistinguishable from $k-1$ others.	High. Can be used to group LBS users	Challenges when data has high-dimensionality, plus vulnerabilities to composition and background knowledge attacks.
P_C	Differential Privacy	Ensures the outcome of any analysis is not significantly affected by the removal or addition of a single record by perturbing data in a controlled manner.	Useful for providing strong privacy guarantee but the real-life applications are still under the research.	Introduces a trade off between privacy and efficacy (e.g. Privacy and Safety, Privacy and Efficiency).
	Generative Adversarial Networks	Generates new datasets with similar patterns based on large anonymised datasets.	High in general. Computationally expensive and still relies on a large quantity of real-world data.	Generated data is not real-world data and may not share all its detail and properties, meaning applications or models using it may be less successful. Privacy is not guaranteed and synthetic data may disclose information about participants in the training set.
P_D	Vary Transmit Time	Decorrelate the time at which a message was sent.	High in general. Low for applications where low latency is important.	Increase in delivery latency.
	Vary Transmit Power	Decorrelate the location and direction from which a message is sent.	High.	Decreased range in which other vehicles can receive messages.
	Cease Broadcasting	By not broadcasting a signal is not available for a threat actor to track.	Low in general, as this denies availability to the services provided. In specific use cases this may applicable.	Denies service availability.
P_E	Change route taken	Instantaneous position leaked, obfuscation over long-term history.	Limited by opportunities to drive in different ways (e.g., by road network layout and network degree).	Increased cost to driver (fuel, mental effort - thinking of new routes).

TABLE 4: Privacy Provision Techniques Summary

only be feasible to be used to protect certain types of privacy threats. For example, in PRKE systems, the key does not need to inform the car to unlock the doors when the driver is still in the car or while the car is moving. The key could detect these and similar scenarios and cease broadcasting the beacon to save power [80] and also to provide privacy.

E. BEHAVIOUR CHANGE

A vehicle can be tracked more easily if it takes the same route each day, compared to when its route varies. In particular, it is possible to use the same static sensors and cameras to track the vehicle when the same route is taken. One way to increase privacy, therefore, is to vary the route taken by a vehicle each day. Ideally, this would mean changing the end destination and the roads taken to get there. However, commuters typically travel to a single destination, meaning the vehicle is only able to vary the route taken. In this way, the vehicle is seen by different trackers and some uncertainty is introduced to its whereabouts and/or destination. However, with networked or centralised identification and tracking over a sufficiently large area, altering routes taken each day will likely be ineffective in providing privacy.

F. OPTIONS AVAILABLE TO A BENIGN THREAT ACTOR

To a threat actor that has gathered location information data for a non-malicious purpose there are additional techniques to protect privacy that those organisations can take. It may be important for them to provide this protection as there may be financial (e.g., fines) or reputation repercussions that the organisation wishes to avoid.

One of the simplest techniques to protect privacy is to delete the gathered information. For example, Transport for London is only allowed to keep ANPR tracking data for 28 days and the London Police are allowed to keep it for 2 years [9]. By deleting the data it will not be a resource that another threat actor could attempt to obtain.

An alternate to differential privacy may be to use Generative Adversarial Networks (GANs) [81]. GANs can be trained on the anonymised location traces stored in a database, and then be used to generate a new dataset with similar patterns to the datasets it was trained on. This could potentially allow a dataset to be released to the public (or sold to another entity) whilst protecting the privacy of the users whose location data was used to generate the new dataset. This technique would only be applicable to benign threat actors.

G. SUMMARY

There are many options to protect location privacy threats which are summarised in Table 4. However, to protect location privacy a trade-off often needs to be made. For example, when changing pseudonyms used in Cooperative Awareness Messages a silent period is needed to decorrelate the previous identity of a vehicle from the subsequent identity. This silent period means that some safety is traded-off for the proper functioning of the privacy preserving technique. It is important to understand what users are giving up in order for privacy to be provided. In some cases the cost may be too high compared to the privacy gained.

V. ANALYSIS

A. IMPACT OF TECHNIQUE INTERACTION

The techniques presented here mostly focus on individual problems, with the exception being MAC slots and pseudonyms in [74]. This means that the interaction of solutions is not considered by existing techniques. This is a problem for certain solutions, for example, when a vehicle changes the pseudonym it uses in the CAMs it broadcasts, unless all the other techniques that also use pseudonym change simultaneously no privacy will be provided. This is because an adversary will be capable of linking the old CAM identity to the new CAM identity via the other sources of identity within the vehicle. An example of this is shown in Figure 6 with a time period in the centre where an attacker can link pseudonyms. This is problematic for vehicles because there are many devices present in the vehicle that it may not have authority over to manage which pseudonyms are used to certain points, or how other privacy preservation techniques work.

To understand how threats and techniques relate Figure 7 shows a mapping between the class of threats and class of solutions that can be used to provide location privacy for that threat. This mapping has been created by first classifying privacy threats in Section II, classifying privacy techniques in Section IV, and then observing the class of techniques that can be used to protect against threats in a specific class.

Using this mapping between threats an techniques, a matrix of privacy threat interactions is presented in Figure 8 which is generated from Algorithm 1. It shows how the privacy preserving technique for the threat on the left may need to be changed when the privacy threat on the top is being considered. For some threats multiple aspects of the privacy techniques need to be considered (two triangles of different colours), but for others the entry is empty because the solution interaction either does not interact or there are no overlapping ways to protect privacy, and therefore changes do not need to be made to the privacy preserving technique. This interaction matrix is intended to be updated as new techniques are developed, or new privacy threats identified. The source code used to generate this diagram can be found at[6].

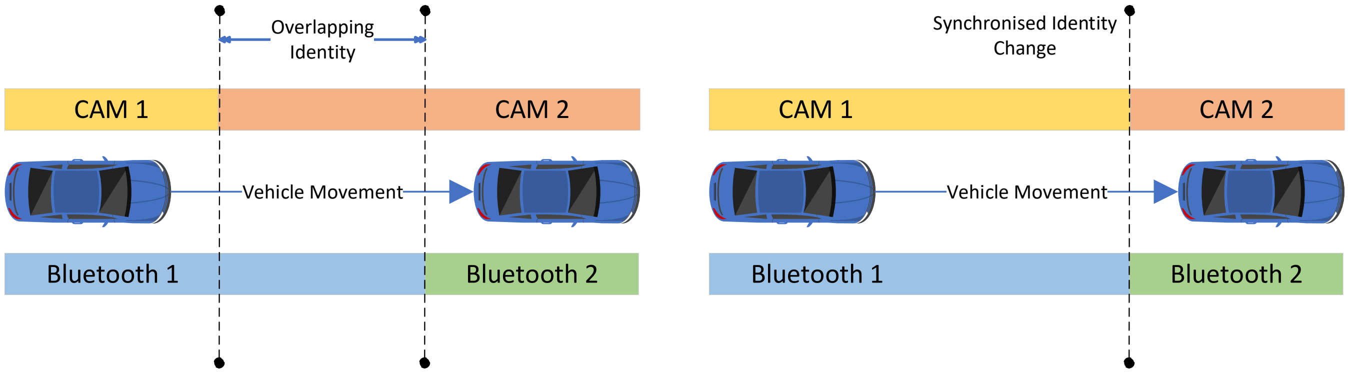
Algorithm 1 Technique Interaction Consideration

```
▷ What changes in the provision of privacy against $\text{threat}_1$ might need to be made when also protecting against $\text{threat}_2$?
function COMBINE($\text{threat}_1$, $\text{threat}_2$)
    ▷ Get the set of techniques used to protect against these two specific threats
    $\text{technique}_1 \leftarrow \text{TECHNIQUE}(\text{threat}_1)$
    $\text{technique}_2 \leftarrow \text{TECHNIQUE}(\text{threat}_2)$
    if $\text{threat}_1 = \text{threat}_2$ then
        return $\text{technique}_1$
    ▷ Which techniques are used by both threats?
    $\text{comb} \leftarrow \text{technique}_1 \cup \text{technique}_2$
    ▷ The threat class the specific threats are in
    $\text{threatclass}_1 \leftarrow \text{THREATCLASS}(\text{threat}_1)$
    $\text{threatclass}_2 \leftarrow \text{THREATCLASS}(\text{threat}_2)$
    ▷ The techniques used to protect a threat class
    $\text{threattech}_1 \leftarrow \text{THREATTECHNIQUES}(\text{threatclass}_1)$
    $\text{threattech}_2 \leftarrow \text{THREATTECHNIQUES}(\text{threatclass}_2)$
    ▷ Which techniques are used by $\text{threattech}_2$?
    $\text{comb} \leftarrow \text{comb} \cup \text{threattech}_2$
    ▷ Only consider techniques possible to protect against $\text{threat}_1$
    $\text{comb} \leftarrow \text{comb} \cap \text{threattech}_1$
    return comb
```

A consideration highlighted by Figure 8 is that privacy preserving techniques that previously only used one kind of protection may need to use new kinds of techniques when considering new threat combinations. For example, when broadcasting over WiFi, Bluetooth or DSRC 802.11p the device's identity needs to periodically be changed. But when considering threat actors who are analysing the directional context of signals, the transmit power or transmit time needs to also be varied to protect location privacy.

Similar considerations are need when privacy preserving techniques of different kinds of threats interact. For example in LBSs when moving from one area to another the vehicle's LBS queries will be mixed with a different set of vehicles, because of this the vehicle should change its identity (which should lead to other devices in the vehicle changing their identities) to prevent linking between the two different areas.

[6] https://github.com/MBradbury/vehicle-privacy-analysis



(a) Overlapping Identity Change

(b) Synchronised Identity Change

FIGURE 6: Identity Change Interactions

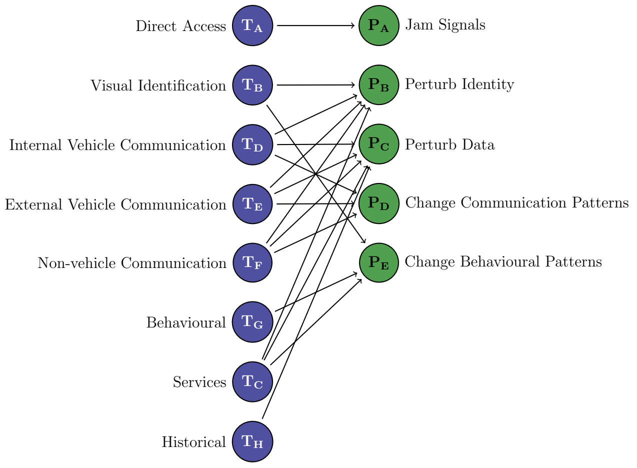


FIGURE 7: Mapping of Location Privacy Threat Classes to Privacy Preserving Technique Classes

Alternatively as indicated by Figure 8 the contents of V2X messages may need to change to protect privacy. However, due to the functional constraints on the accuracy of these messages (to ensure safety), protecting privacy in this manner may be infeasible.

B. THREATS CLASSIFICATION

What data does the threat actor obtain and how does it reveal the location of the vehicle?

- **Direct**: The data specifies the location of vehicle
- **Indirect**: The data needs to be analysed to obtain the location of the vehicle.

Direct access to the location means that a threat actor can see where the vehicle is at over time, without any further processing. For example, GPS coordinates from a GNSS sensor provides the location over time with high fidelity, and can be immediately viewed on a map. Indirect access requires some processing in order to extract or interpolate detailed trajectories. ANPR systems are able to view a vehicle driving through a road network, but the data is sparse and must be interpolated estimate where the vehicle is over time.

When is the data from?

- **Current**: The threat actor has access to the live stream of data
- **Historical**: The threat actor has access to old data

In Figure 9 the difficulty of different classes of threat actors violating different classes of privacy threats is shown. Note that violating real-time privacy is typically harder than violating historical location privacy [19]. A real-time violation requires an attacker to either set up their own network of sensors, or gain access to an existing system. In either case, they must have the capabilities to process the data in real-time, and they may be thrown off a breached system at any time. A historical violation requires only access to a database, or database leak. This allows the attacker to proceed in their own time, and reduces the computational requirements.

The impact of violating different classes of privacy can be different based on the historical data present. A real-time attack which allows the vehicle's current location to be revealed, but depending on the age and time period of the historical data significant information may also be inferred. For example, if a historical violation grants access to old and out of date information, it may be less relevant to the vehicle and its user. However, historical data of a recent time period, or over a long duration can have a greater impact as it can be used to infer additional information about the vehicle's user. For example, by pattern of life analysis an adversary could predict where the vehicle will be in the future. This means both historical and real-time privacy leaks can be high impact threats.

VI. DISCUSSION

This paper has examined many privacy threats, threat actors interested in violating privacy, and privacy preserving techniques. However, there are many additional considerations when considering vehicular location privacy, especially as there are instances where tracking of vehicles is necessary, and other cases where violating privacy leads to a greater utility than protecting privacy. This section will discuss some of these additional issues around vehicular location privacy.

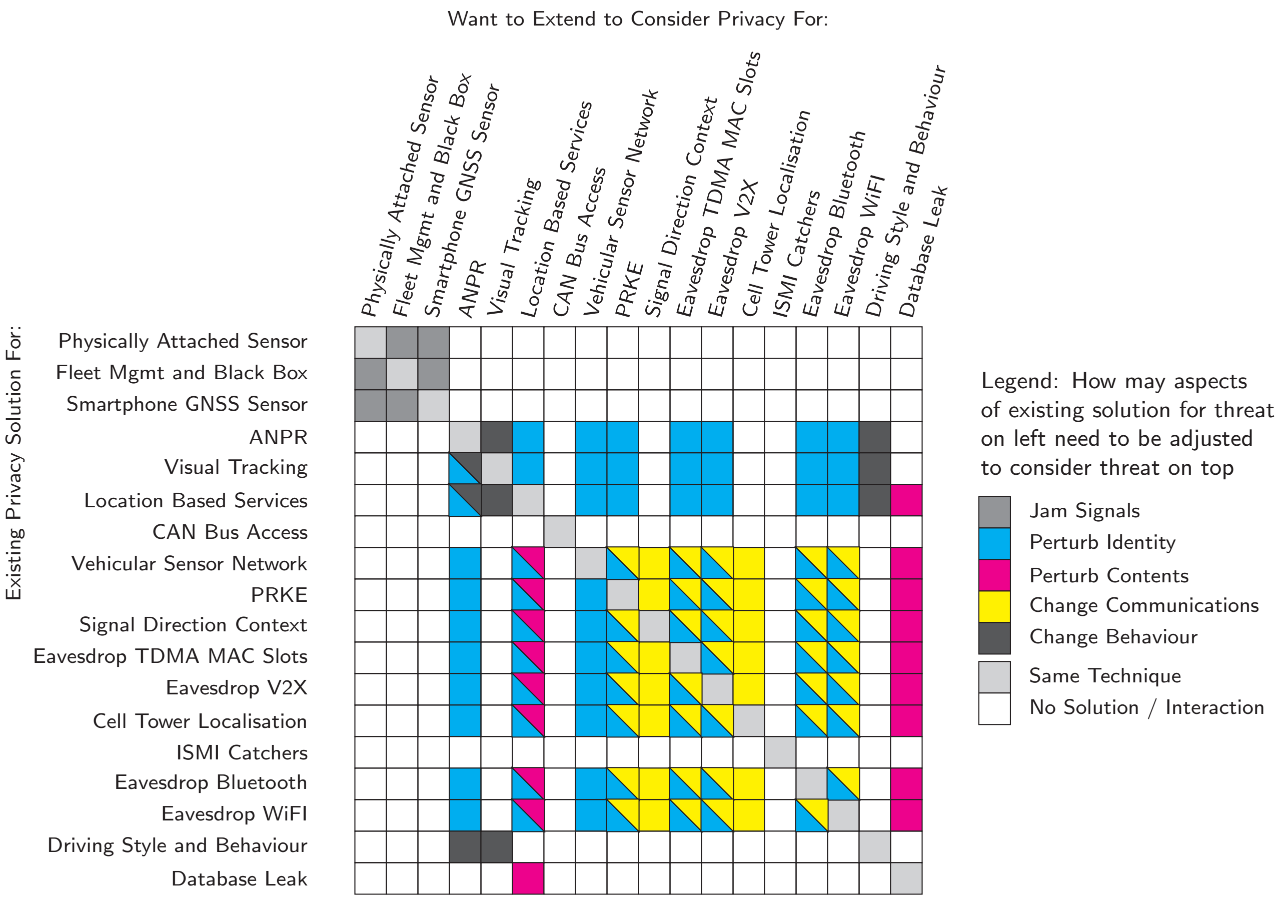


FIGURE 8: Threat Interaction Matrix

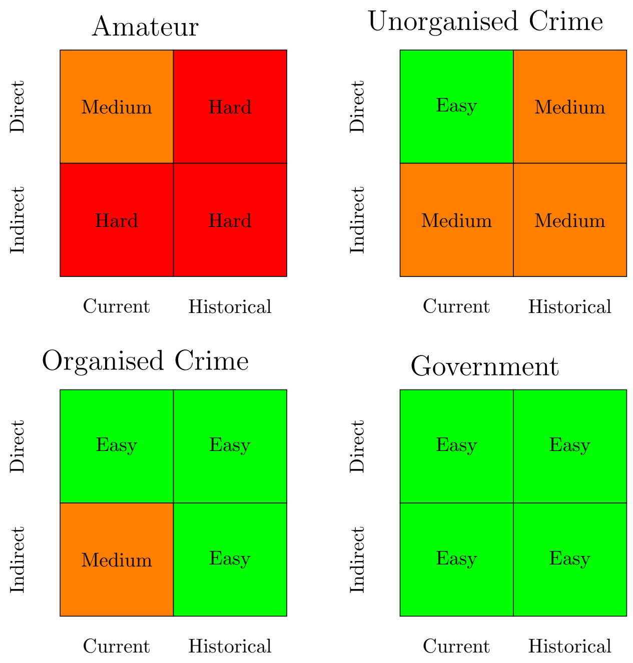
A. WHO SHOULD WE EXPECT TO BE ABLE TO TRACK VEHICLES?

This work has focused on the protection of vehicular location privacy, but there are many examples where users gain utility from revealing their location. Users will want to provide locations to LBS in order to get recommendations that are targeted to their journey. Autonomous vehicles will want to inform nearby vehicles of their location, velocity, identity and the time at which this data was recorded to ensure that other vehicles collaborate to ensure that no safety properties are violated. Toll Roads and Car Parks will track vehicles to ensure the owners are correctly billed for using those services. It is also the case that Governments will want to understand the behaviour of their citizens to better design services in a cost effective manner based on where demand is. The police force of a country will need to be able to track vehicles to ensure that criminals can be captured. For example, the EU Cross-Border Enforcement Directive [82] aims to track users who commit traffic offences in an EU member state different to the one the vehicle is registered in. Part of this directive involved sharing databases on drivers, which may contain sensitive location information.

These are just a subset of examples where vehicle tracking is required. There are many use cases where a user desires location information to be shared, where there is a contractual requirement to share location information, and where there is a legal requirement to share location information. It is important to consider these cases and their interactions with location privacy threats and techniques, as they add additional considerations when location privacy needs to be provided. However, they potentially allow privacy provision to be ignored and the cost of providing privacy protection to be avoided under certain use cases.

B. ACCEPTABLE PRIVACY VIOLATIONS

In certain cases the desire to remain private may be exceeded by the utility gained by a user revealing their location. One example of this is the eCall system, where upon a serious collision authorities will be automatically notified. The data sent to them may include “the triggering mode (automatic or manual), the vehicle identification number, vehicle type and propulsion, timestamp, vehicle direction, current and previous positions, and number of passengers” [83]. The key aspect of eCall is that it does not broadcast continuously, but



Amateur

	Current	Historical
Direct	Medium	Hard
Indirect	Hard	Hard

Unorganised Crime

	Current	Historical
Direct	Easy	Medium
Indirect	Medium	Medium

Organised Crime

	Current	Historical
Direct	Easy	Easy
Indirect	Medium	Easy

Government

	Current	Historical
Direct	Easy	Easy
Indirect	Easy	Easy

FIGURE 9: Difficulty Table

only in case of an emergency. This means that no privacy is leaked during the normal use of the vehicle. However, in rare circumstances where lives are at risk the vehicle will intentionally leak privacy with the intent to speed up life saving responses. It is likely most users would be willing to give up privacy to obtain a higher chance of survival.

C. LIMITATIONS

Many social media sites and messaging apps allow a user to provide their location to the LBS which is then shared with other users of the service. In some cases the user will share with a select few people, but in other cases the user may not have set up their privacy settings and will broadcast their location publicly on the internet. In this scenario, the user has wilfully chosen to opt-out of location privacy and therefore it is unnecessary to attempt to consider the privacy protection interactions from other privacy threats.

For some scenarios it may be desirable to provide short-term linkability, but long-term unlinkability. This means that in one event each vehicle should be aware of who is present, but in subsequent events it should not be possible to link vehicles between participating in these events. This long-term unlinkability will only be protected again certain threat agents, such as other vehicles on the road or malicious eavesdroppers. There may be the need to unpack the long-term unlinkability of a vehicle by a trusted authority. For example, in the case of a car crash the investigators and insurance companies may need to violate privacy in order to determine the events that occurred. Such a scheme could be provided by group signatures in [84]. An issue with this approach is that the trusted authority who issues the group signing keys and maintains a database of how to reveal the identities becomes a new privacy threat.

D. EFFECT OF AUTONOMY

As autonomous vehicles are going to become increasingly common on roads, they will lead to new privacy threats, but will also reduce the risk of existing privacy threats. For example, currently it is possible to use vehicle sensors data to identify different driving styles and drivers from their driving signatures [85, 86]. Once a driver's identity is disclosed, it allows linking other trajectories to that driver. However, the driving signatures will become less useful with autonomous vehicles because a human driver will not be in control of the vehicle (when it is fully autonomous). Any analysis of the driving behaviour will leak information about the systems controlling the vehicle, but the driving behaviour is unlikely to leak privacy of the passengers. To resolve other issues the movement of vehicles may be adjusted to arrive at a hub at the same time in order to synchronise the time at which pseudonyms are changed. Autonomy also facilitates cooperative driving of multiple vehicles. Within this context, the autonomy might remove some of the identifying behavioural information leaked while driving and enhance the location privacy [87].

E. LOCATION SHARING IN A MILITARY SCENARIO

Sharing location information within a collaborative work might be necessary in many cases. In an operation with multiple parties, each party might need to conduct computation based on the others location information; however, none of them might be willing to disclose their privacy. One of the most appropriate example for this case is the military operations consisted of allies who have mutual benefits of cooperation but cannot fully trust each other. To be more precise, in the case the multiple allies are proceeding to the same target, they would like to know about each others location to prevent friendly fire. The other scenario might be, the country A decided to bomb a target x location. However, A does not want to damage its relationship with its allies who might have some area of interests around x such as secret military bases or agencies. None of the countries would like to disclose their private areas to each other. While A would not like to disclose the exact location of x, similarly the allies would not like to disclose their private areas [88]. The similar scenario is valid for the proceeding military vehicle units of allies in an operation. While they might need the location of other units to ensure coordination among them, none of the allies would like to disclose their privacy. The question here is, how to do computation based on the data from multiple owners without disclosing the privacy. An external trusted third-party aggregator can solve this problem. However, the solution without using trusted aggregator has been assigned to the secure multi-party computation in the literature [89].

VII. FUTURE WORK

A. LOCATION PRIVACY AGAINST MULTIPLE SIMULTANEOUS THREATS

This work has argued that it is insufficient to consider protecting location privacy threats against vehicle in isolation. It is necessary to consider the wider privacy threat landscape, because the way privacy preserving techniques interact can lead to no privacy actually being provided. So when designing privacy preserving techniques, multiple threats need to be simultaneously considered.

As privacy provision must consider other privacy threats concurrently, another issue is how to coordinate the privacy provision between multiple devices. This could involve a central authority (such as the vehicle) being in control of how privacy techniques synchronise. Alternatively a consensus based protocol could be developed where multiple devices agree to synchronise privacy provision at specific times. A third alternative might be a reactive protocol where devices respond to changes in privacy techniques. Such techniques needs to be carefully designed to ensure a threat actor cannot alter how privacy is provided.

This means it will not longer be sufficient to look at privacy in a single domain, but necessary to provide cross-domain privacy. Here multiple sources of privacy leakages from different domains will need to collaborate to protect privacy. This may be difficult as technologies can evolve in unexpected ways (such as vehicles hosting WiFi access points). This collaboration will also need to occur in a way that does not leak privacy.

B. IMPACT ANALYSIS OF PRIVACY THREATS

When considering a privacy threat it is important to clearly understand which threat actor is being protected against. This includes understanding their motivations, resources and capabilities. For each threat actor a risk assessment can then be performed to analyse the likelihood and impact of a threat actor violating privacy. The risk analysis can then be used to (i) identify changes that need to be made to the system to preserve privacy, (ii) identify which changes needs to be focused on with a higher priority, and (iii) which privacy leakages to specific threat actors are acceptable (and do not necessarily need a privacy preserving technique implemented — e.g., eCall). When changes to the system are made the risk analysis can be re-performed to ensure that the likelihood of privacy loss and its impact have decreased. However, privacy provision is difficult to identify, as the interactions between privacy techniques can lead to unexpected privacy loss. The possibility for privacy preserving techniques failing to protect privacy needs to be addressed in the risk assessment.

VIII. CONCLUSION

There exists many ways in which a vehicle can be tracked, and much work has been done on individually addressing some issues. However, an issue is that the existing work focuses on their specific problem and does not consider attempting to protect context information leakages from other sources. The conclusion from this work is that it is important to not consider vehicular location privacy in isolation as location privacy schemes can be circumvented by simply using an alternate tracking method. The existing work mostly does not consider the impact of their privacy schemes on other privacy techniques. For example, [74] is the only example known to the authors where two sources of privacy leakage are addressed simultaneously. One of the key points of the work, was the need to synchronise pseudonym and MAC slot changes. Such synchronisation will be needed across the privacy preserving techniques that use pseudonyms to prevent vehicle tracking.

REFERENCES

[1] B. Liu, W. Zhou, T. Zhu, L. Gao, and Y. Xiang, "Location privacy and its applications: A systematic study," IEEE Access, vol. 6, pp. 17 606–17 624, 2018.

[2] P. Asuquo, H. Cruickshank, J. Morley, C. P. A. Ogah, A. Lei, W. Hathal, S. Bao, and Z. Sun, "Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges and countermeasures," IEEE Internet of Things Journal, pp. 1–1, 2018.

[3] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," Personal and Ubiquitous Computing, vol. 18, no. 1, pp. 163–175, Jan 2014.

[4] H. Talat, T. Nomani, M. Mohsin, and S. Sattar, "A survey on location privacy techniques deployed in vehicular networks," in 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Jan 2019, pp. 604–613.

[5] A. Thomason, N. Griffiths, and V. Sanchez, "Identifying locations from geospatial trajectories," Journal of Computer and System Sciences, vol. 82, no. 4, pp. 566–581, 2016.

[6] A. Shargall, "How does Black Box Insurance work?" May 2018, Accessed: 2018-11-16. [Online]. Available: https://www.moneysupermarket.com/car-insurance/how-does-black-box-insurance-work/

[7] A. H. Northcliffe, Motors and Motor-Driving, 4th ed. Longmans, Green, and Co., London, 1906, ch. The Motor Car Act 1903, pp. 449–454.

[8] S. Du, M. Ibrahim, M. Shehata, and W. Badawy, "Automatic license plate recognition (alpr): A state-of-the-art review," IEEE Transactions on Circuits and Systems for Video Technology, vol. 23, no. 2, pp. 311–325, Feb 2013.

[9] N. Winterbourne, "Met Intelligence ANPR Bureau Privacy Impact Accessment," Met Intelligence ANPR Bureau, Tech. Rep., 2014. [Online]. Available: https://www.london.gov.uk/sites/default/files/gla_migrate_files_destination/Appendix%20B%20-%20Metropolitian%20Police%20-%20ANPR%20Privacy%20Impact%20Assessment.pdf

[10] National Police Cheif's Council (NPCC), "Automatic number plate recognition: Use of anpr by police

forces and other law enforcement agencie," Online, Accessed 2018-08-31. [Online]. Available: http://www.npcc.police.uk/FreedomofInformation/ANPR.aspx

[11] X. Liu, W. Liu, H. Ma, and H. Fu, "Large-scale vehicle re-identification in urban surveillance videos," in 2016 IEEE International Conference on Multimedia and Expo (ICME), July 2016, pp. 1–6.

[12] D. Zapletal and A. Herout, "Vehicle re-identification for automatic video traffic surveillance," in The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, June 2016.

[13] K. Zhou, K. M. Varadarajan, M. Vincze, and F. Liu, "Hybridization of appearance and symmetry for vehicle-logo localization," in 2012 15th International IEEE Conference on Intelligent Transportation Systems, Sept 2012, pp. 1396–1401.

[14] Y. Tang, C. Zhang, R. Gu, P. Li, and B. Yang, "Vehicle detection and recognition for intelligent traffic surveillance system," Multimedia Tools and Applications, vol. 76, no. 4, pp. 5817–5832, Feb 2017.

[15] X. Liu, W. Liu, T. Mei, and H. Ma, "A deep learning-based approach to progressive vehicle re-identification for urban surveillance," in Computer Vision – ECCV 2016, B. Leibe, J. Matas, N. Sebe, and M. Welling, Eds. Cham: Springer International Publishing, 2016, pp. 869–884.

[16] S. Y. Cheung, S. Coleri, B. Dundar, S. Ganesh, C.-W. Tan, and P. Varaiya, "Traffic measurement and vehicle classification with single magnetic sensor," Transportation Research Record, vol. 1917, no. 1, pp. 173–181, 2005.

[17] L. Stenneth and P. Yu, "Mobile systems privacy: "mobipriv" a robust system for snapshot or continuous querying location based mobile systems," Transactions on Data Privacy, vol. 5, no. 1, pp. 333–376, 4 2012.

[18] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," Personal and Ubiquitous Computing, vol. 18, no. 1, pp. 163–175, Jan 2014.

[19] B. Liu, W. Zhou, T. Zhu, L. Gao, and Y. Xiang, "Location privacy and its applications: A systematic study," IEEE Access, vol. 6, pp. 17 606–17 624, 2018.

[20] S. Nie, L. Liu, and Y. Du, "Free-fall: Hacking tesla from wireless to CAN bus," in Black Hat, 2017. [Online]. Available: https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf

[21] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in Proceedings Of The 19th Usenix Conference On Security, ser. USENIX Security'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 21–21.

[22] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," IEEE Transactions on Vehicular Technology, vol. 61, no. 1, pp. 86–96, Jan 2012.

[23] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock it and still lose it —on the (in)security of automotive remote keyless entry systems," in 25th USENIX Security Symposium (USENIX Security 16). Austin, TX: USENIX Association, 2016. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia

[24] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in Network And Distributed Systems Security (NDSS) Symposium, 2011.

[25] "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service ," European Telecommunications Standards Institute, Cedex, FRANCE, Standard, Sep. 2014.

[26] "Intelligent Transport Systems (ITS); Vehicular Communications; C2C-CC Demonstrator 2008; Use Cases and Technical Specifications," European Telecommunications Standards Institute, Cedex, FRANCE, Standard, Jul. 2010.

[27] "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," European Telecommunications Standards Institute, Cedex, FRANCE, Standard, Mar. 2011.

[28] 4icom and Steer Davies Gleave, "State of the art of electronic road tolling," Tech. Rep. MOVE/D3/2014-259, Oct. 2015. [Online]. Available: https://ec.europa.eu/transport/sites/transport/files/modes/road/road_charging/doc/study-electronic-road-tolling.pdf

[29] M. Hadded, P. Muhlethaler, A. Laouiti, R. Zagrouba, and L. A. Saidane, "TDMA-based MAC Protocols for Vehicular Ad Hoc Networks: A Survey, Qualitative Analysis and Open Research Issues," Communications Surveys and Tutorials, IEEE Communications Society, 2015.

[30] K. Perera, T. Bhattacharya, L. Kulik, and J. Bailey, "Trajectory inference for mobile devices using connected cell towers," in Proceedings of the 23rd SIGSPATIAL International Conference on Advances in Geographic Information Systems, ser. SIGSPATIAL '15. New York, NY, USA: ACM, 2015, pp. 23:1–23:10.

[31] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "Imsi-catch me if you can: Imsi-catcher-catchers," in Proceedings Of The 30th Annual Computer Security Applications Conference, ser. ACSAC '14. New York, NY, USA: ACM, 2014, pp. 246–255.

[32] U. Meyer and S. Wetzel, "A man-in-the-middle attack on umts," in Proceedings Of The 3rd Acm Workshop On Wireless Security, ser. WiSe '04. New York, NY,

USA: ACM, 2004, pp. 90–97.

[33] S. F. Mjølsnes and R. F. Olimid, "Easy 4g/lte imsi catchers for non-programmers," in Computer Network Security, J. Rak, J. Bay, I. Kotenko, L. Popyack, V. Skormin, and K. Szczypiorski, Eds. Cham: Springer International Publishing, 2017, pp. 235–246.

[34] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy attacks to the 4g and 5g cellular paging protocols using side channel information," in Network And Distributed Systems Security (NDSS) Symposium, 2019.

[35] P. O'Hanlon, R. Borgaonkar, and L. Hirschi, "Mobile subscriber WiFi privacy," in 2017 IEEE Security And Privacy Workshops (spw), May 2017, pp. 169–178.

[36] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," in 23rd Annual Network And Distributed System Security Symposium (ndss 2016), 2016.

[37] H. Kikuchi and T. Yokomizo, "Location privacy vulnerable from bluetooth devices," in 2013 16th International Conference On Network-based Information Systems, Sep. 2013, pp. 534–538.

[38] M. Cunche, "I know your mac address: Targeted tracking of individual using wi-fi," Journal of Computer Virology and Hacking Techniques, vol. 10, no. 4, pp. 219–227, Nov. 2014.

[39] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, "802.11 user fingerprinting," in Proceedings Of The 13th Annual Acm International Conference On Mobile Computing And Networking, ser. MobiCom '07. New York, NY, USA: ACM, 2007, pp. 99–110.

[40] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), Jun. 2005, pp. 599–608.

[41] C. Miyajima, Y. Nishiwaki, K. Ozawa, T. Wakita, K. Itou, K. Takeda, and F. Itakura, "Driver modeling based on driving behavior and its evaluation in driver identification," Proceedings of the IEEE, vol. 95, no. 2, pp. 427–437, Feb 2007.

[42] C. M. Martinez, M. Heucke, F. Wang, B. Gao, and D. Cao, "Driving style recognition for intelligent vehicle control and advanced driver assistance: A survey," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 3, pp. 666–676, March 2018.

[43] C. Zhang, M. Patel, S. Buthpitiya, K. Lyons, B. Harrison, and G. D. Abowd, "Driver classification based on driving behaviors," in Proceedings of the 21st International Conference on Intelligent User Interfaces, ser. IUI'16. New York, NY, USA: ACM, 2016, pp. 80–84.

[44] N. P. Chandrasiri, K. Nawa, and A. Ishii, "Driving skill classification in curve driving scenes using machine learning," Journal of Modern Transportation, vol. 24, no. 3, pp. 196–206, Sep 2016.

[45] M. Enev, A. Takakuwa, K. Koscher, and T. Kohno, "Automobile driver fingerprinting," Proceedings on Privacy Enhancing Technologies, vol. 2016, no. 1, pp. 34–50, 2016.

[46] F. Martinelli, F. Mercaldo, A. Orlando, V. Nardone, A. Santone, and A. K. Sangaiah, "Human behavior characterization for driving style recognition in vehicle system," Computers & Electrical Engineering, 2018.

[47] D. Hallac, A. Sharang, R. Stahlmann, A. Lamprecht, M. Huber, M. Roehder, R. Sosič, and J. Leskovec, "Driver identification using automobile sensor data from a single turn," in 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Nov 2016, pp. 953–958.

[48] Z. Li, Q. Pei, I. Markwood, Y. Liu, M. Pan, and H. Li, "Location privacy violation via gps-agnostic smart phone car tracking," IEEE Transactions on Vehicular Technology, vol. 67, no. 6, pp. 5042–5053, Jun. 2018.

[49] BBC, "Fitness app strava lights up staff at military bases," Online, Accessed 2018-09-05. [Online]. Available: https://www.bbc.co.uk/news/technology-42853072

[50] J.-P. Monteuuis, A. Boudguiga, J. Zhang, H. Labiod, A. Servel, and P. Urien, "Sara: Security automotive risk analysis method," in Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, ser. CPSS '18. New York, NY, USA: ACM, 2018, pp. 3–14.

[51] D. Dominic, S. Chhawri, R. M. Eustice, D. Ma, and A. Weimerskirch, "Risk assessment for cooperative automated driving," in Proceedings of the 2Nd ACM Workshop on Cyber-Physical Systems Security and Privacy, ser. CPS-SPC '16. New York, NY, USA: ACM, 2016, pp. 47–58.

[52] S. Vidalis and A. Jones, "Analyzing threat agents and their attributes." in ECIW, 2005, pp. 369–380.

[53] D. K. Kilcoyne, S. Bendelac, J. M. Ernst, and A. J. Michaels, "Tire pressure monitoring system encryption to improve vehicular security," in Milcom 2016 - 2016 Ieee Military Communications Conference, Nov. 2016, pp. 1219–1224.

[54] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: A Practical pseudonym changing scheme for location privacy in VANETs," in 2009 IEEE Vehicular Networking Conference (VNC), Oct 2009, pp. 1–8.

[55] Reviver Auto, "Sacramento Becomes First City to Deploy Digital License Plates," Jun. 2018, Accessed: 2018-10-03. [Online]. Available: https://www.reviverauto.com/sacramento-becomes-first-city-deploy-digital-license-plates

[56] C. Song and V. Shmatikov, "Fooling OCR systems with adversarial text images," CoRR, vol. abs/1802.05385, 2018. [Online]. Available: http://arxiv.org/abs/1802.05385

[57] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," IEEE Transactions on Mobile Computing, vol. 7, no. 1, pp. 1–18, Jan 2008.

[58] P. Samarati and L. Sweeney, "Generalizing data to provide anonymity when disclosing information (abstract)," in Proceedings of the Seventeenth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, ser. PODS '98. New York, NY, USA: ACM, 1998, pp. 188–.

[59] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," in Proceedings of the 32Nd International Conference on Very Large Data Bases, ser. VLDB '06. VLDB Endowment, 2006, pp. 763–774.

[60] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Prive: anonymous location-based queries in distributed mobile systems," in Proceedings of the 16th international conference on World Wide Web. ACM, 2007, pp. 371–380.

[61] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with privacygrid," in Proceedings of the 17th international conference on World Wide Web. ACM, 2008, pp. 237–246.

[62] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, "L-diversity: privacy beyond k-anonymity," in 22nd International Conference on Data Engineering (ICDE'06), April 2006, pp. 24–24.

[63] B. C. Fung, K. Wang, A. W.-C. Fu, and P. S. Yu, Introduction to Privacy-Preserving Data Publishing: Concepts and Techniques, 1st ed. Chapman & Hall/CRC, 2010.

[64] Y. A. A. S. Aldeen, M. Salleh, and M. A. Razzaque, "A comprehensive review on privacy preserving data mining," SpringerPlus, vol. 4, no. 1, p. 694, Nov 2015. [Online]. Available: https://doi.org/10.1186/s40064-015-1481-x

[65] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in Theory of Cryptography, S. Halevi and T. Rabin, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 265–284.

[66] B. Avent, A. Korolova, D. Zeber, T. Hovden, and B. Livshits, "BLENDER: Enabling local search with a hybrid differential privacy model," in 26th USENIX Security Symposium (USENIX Security 17). Vancouver, BC: USENIX Association, 2017, pp. 747–764. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/avent

[67] S. L. Warner, "Randomized response: A survey technique for eliminating evasive answer bias," Journal of the American Statistical Association, vol. 60, no. 309, pp. 63–69, 1965, pMID: 12261830.

[68] G. Cormode, S. Jha, T. Kulkarni, N. Li, D. Srivastava, and T. Wang, "Privacy at scale: Local differential privacy in practice," in Proceedings of the 2018 International Conference on Management of Data, ser. SIGMOD '18. New York, NY, USA: ACM, 2018, pp. 1655–1658.

[69] M. Alvim, K. Chatzikokolakis, C. Palamidessi, and A. Pazii, "Invited paper: Local differential privacy on metric spaces: Optimizing the trade-off with utility," in 2018 IEEE 31st Computer Security Foundations Symposium (CSF), July 2018, pp. 262–267.

[70] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in Proceedings of the 2013 ACM SIGSAC Conference on Computer &#38; Communications Security, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 901–914.

[71] G. Cormode, C. Procopiuc, D. Srivastava, E. Shen, and T. Yu, "Differentially private spatial decompositions," in Proceedings of the 2012 IEEE 28th International Conference on Data Engineering, ser. ICDE '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 20–31.

[72] L. Ou, Z. Qin, Y. Liu, H. Yin, Y. Hu, and H. Chen, "Multi-user location correlation protection with differential privacy," in 2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS), Dec 2016, pp. 422–429.

[73] F. Kargl, A. Friedman, and R. Boreli, "Differential privacy in intelligent transportation systems," in Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, ser. WiSec '13. New York, NY, USA: ACM, 2013, pp. 107–112.

[74] Z. Liu, Z. Liu, L. Zhang, and X. Lin, "Marp: A distributed mac layer attack resistant pseudonym scheme for vanet," IEEE Transactions on Dependable and Secure Computing, pp. 1–1, 2018.

[75] R. S. Yokoyama, B. Y. L. Kimura, L. A. Villas, and E. D. S. Moreira, "Measuring distances with rssi from vehicular short-range communications," in 2015 Ieee International Conference On Computer And Information Technology; Ubiquitous Computing And Communications; Dependable, Autonomic And Secure Computing; Pervasive Intelligence And Computing, Oct. 2015, pp. 100–107.

[76] M. Woolley, "Bluetooth technology protecting your privacy," Apr. 2015, accessed: 2018-07-02. [Online]. Available: http://blog.bluetooth.com/bluetooth-technology-protecting-your-privacy

[77] S. Raza, P. Misra, Z. He, and T. Voigt, "Bluetooth smart: An enabling technology for the internet of things," in 2015 Ieee 11th International Conference On Wireless And Mobile Computing, Networking And Communications (wimob), Oct. 2015, pp. 155–162.

[78] A. Hilts, C. Parsons, and J. Knockel, "Every step you fake: A comparative analysis of fitness tracker privacy and security," Open Effect Report, Tech. Rep., 2016, accessed: 2018-08-10. [Online]. Available: https:

//openeffect.ca/reports/Every_Step_You_Fake.pdf

[79] P. Kamat, W. Xu, W. Trappe, and Y. Zhang, "Temporal privacy in wireless sensor networks: Theory and practice," ACM Trans. Sen. Netw., vol. 5, no. 4, pp. 28:1–28:24, Nov. 2009.

[80] J. D. King, "Passive remote keyless entry system," May 2001, US Patent 6,236,333. [Online]. Available: https://patents.google.com/patent/US6236333B1/en

[81] A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, and A. A. Bharath, "Generative adversarial networks: An overview," IEEE Signal Processing Magazine, vol. 35, no. 1, pp. 53–65, Jan 2018.

[82] Council of European Union, "Directive (EU) 2015/413 of the European Parliament and of the Council of 11 March 2015 facilitating cross-border exchange of information on road-safety-related traffic offences," Mar. 2015, Accessed: 2018-11-16. [Online]. Available: https://publications.europa.eu/en/publication-detail/-/publication/a6da0bdb-c94d-11e4-bbe1-01aa75ed71a1/language-en

[83] European Commission, "eCall — Do you have any concerns for your privacy? You shouldn't…," Jun. 2014, accessed: 2018-08-10. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/ecall-%E2%80%93-do-you-have-any-concerns-your-privacy-you-shouldnt

[84] J. Liu, L. Chen, M. Dianati, C. Maple, and Y. Yan, "Efficient anonymous signatures with event linkability for V2X communications," 2019, In Submission.

[85] B. Wang, S. Panigrahi, M. Narsude, and A. Mohanty, "Driver identification using vehicle telematics data," in WCX^{TM} 17: SAE World Congress Experience. SAE International, mar 2017. [Online]. Available: https://doi.org/10.4271/2017-01-1372

[86] V. Vaitkus, P. Lengvenis, and G. Zylius, "Driving style classification using long-term accelerometer information," in 2014 19th International Conference on Methods and Models in Automation and Robotics (MMAR), Sept 2014, pp. 641–644.

[87] J. M. Carter, "Connected cars: Privacy, security issues related to connected, automated vehicles," Jun 2017, accessed: 2018-08-25. [Online]. Available: https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected

[88] W. Du and M. J. Atallah, "Secure multi-party computation problems and their applications: A review and open problems," in Proceedings of the 2001 Workshop on New Security Paradigms, ser. NSPW '01. New York, NY, USA: ACM, 2001, pp. 13–22.

[89] O. Goldreich, "Secure multi-party computation," Manuscript. Preliminary version, vol. 78, 1998, Accessed: 2019-07-29. [Online]. Available: www.wisdom.weizmann.ac.il/~oded/pp.html