CENTRE *for* DOCTORAL TRAINING *in*
CYBER SECURITY

CDT Technical Paper

06/15

Revisiting Linkability for Vehicular Communications: Continuous Linkability

Louise Axon

Revisiting Linkability for Vehicular Communications: Continuous Linkability

Louise Axon, University of Oxford
louise.axon@cs.ox.ac.uk

***Abstract*—Vehicular communications have important applications for improving the safety of our increasingly populated roads, however they have privacy implications: the broadcast of safety messages can create opportunities for tracking of vehicles and drivers. For several proposed safety applications, it is desirable that nearby vehicles communicate continuously with one another, with the ability to link the sender of any one message to their previous messages - *linkability*. We observe that in academic literature and in industry, this linkability provision in not optimal. In protocols designed to give time-based *linkability* for nearby drivers, and *unlinkability* to prevent tracking, the continuity of communications is disrupted by unlinkable transitions; however for certain safety applications a continuous communication without this disruption in linkability is more fitting. In this light, we review the security requirements for safety messaging in Intelligent Transportation Systems (ITS). We propose a new distance-based approach to providing continuous linkability, and outline solutions for its provision.**

I. Introduction

High-level problems

The large and increasing number of vehicles on the roads each year means road safety and efficiency is becoming increasingly difficult to manage. Vehicular communications have numerous proposed applications within Intelligent Transportation Systems (ITS) for improving the safety of driving on roads.

With numerous governmental and industrial plans in place for their development, vehicular communications technologies are very much expected to penetrate the automotive market in the near future. According to [1], providers in Germany and the US in 2014 had predicted 100% market penetration of vehicular communications within 14-15 years. The first implementations of ITS are already a reality. In Japan, a high proportion of vehicles are equipped with Electronic Toll Collection On-Board Units (OBUs) and further driver information and warning services have been integrated into OBUs through Smartway, operational since 2006 [2]. In Europe and North America, the penetration of vehicular communications systems into the vehicular market is a close reality, with numerous projects for ITS technologies being having been tested in Europe over the last few years, and the industrial Car-to-Car Communications Consortium (C2C CC) has developed plans to implement their first vehicular (V2X) communications in 2015.

Vehicular communications can offer either automatic vehicular behaviour, in line with autonomous vehicle development, or driver assistance. ITS has applications falling broadly into three categories: road safety, traffic management, infotainment. We consider safety messaging in particular. Vehicular safety messaging has the potential to increase the safety of driving through cooperative awareness, sharing of safety-related information, and sharing of intended movements to enable cooperation. In such a scheme, safety messaging beacons are broadcast periodically by vehicles. In this way, dangerous situations and collisions can be reduced, or their impact decreased. There are, however, privacy implications for vehicles of sending such messages: linking the identity of subsequently-broadcast beacons can enable eavesdroppers to track the whereabouts of vehicles. The driver's right to privacy is a right by law in many countries, and so any vehicular communications system designed must provide appropriate privacy. In particular, the prevention of tracking capabilities, or of driver identity recognition, through the reception of safety messages is important.

Specific problems

We focus on the provision of appropriate privacy and safety for ITS; in particular, we look to define appropriate linkability requirements. Proposed safety applications require linkability of safety messages for communicating parties, where linkability is the property that two different messages sent by the same sender can be recognised to have been sent by the same sender. Conversely, unlinkability is required for unauthorised parties: the property that, given two messages sent by the same sender, unauthorised parties cannot link them to the same sender.

Safety applications are proposed by the European Telecommunications Standards Institute (ETSI) [3]: several road safety applications which rely on "cooperative

awareness" and require vehicles to communicate continuously with one another information such as their position, speed and direction. Key applications for this context are overtaking vehicle warning; lane changing assistance; lane merging; collision avoidance.

Safety-critical ITS applications such as these are best-suited to *continuously*-linkable communications; however, to the best of our knowledge, the need for such continuity is not addressed by previously-proposed safety messaging protocols. We argue that current solutions, and even the security requirements they are designed to give, are not optimal; and argue the need for *continuous linkability*, where the provision of continuous linkability means that, on receiving different safety messages from the same vehicle, V_1, within a specified "close" distance, a nearby vehicle V_2 can recognise - "link" - that these safety messages have indeed been sent by V_1, and at no point, while the vehicle V_2 remains within the "close" distance of V_1 does it become unable to link the messages sent by V_1.

ETSI also defines privacy requirements for vehicular communications: ETSI is working on standardisation such that, when deployed, ITS is legally compliant in terms of privacy and data protection. In particular, ITS must comply with the Data Protection Act; Driver's Privacy Protection Act (US); Article 8 of the EU Convention for the Protection of Human Rights and Fundamental Freedoms. This means specifying levels of privacy against the authorities (it is foreseen that authorities' ability to disclose private data will be collaborative only); and against other third parties (foreseen that other third parties will not have tracking capabilities, by design).

We consider that the protocol design should provide privacy in line with the corresponding privacy of the driver in the real world. In this light, we do not consider it necessary to provide unlinkability for drivers who are in close proximity to one another, and who could hence track one another's movements physically without using the safety messages. We develop linkability and unlinkability requirements stemming from this argument which, importantly, gives the opportunity for designing protocols that enable continuously linkable communications for drivers in close proximity.

State-of-the-art

The current state-of-the-art in vehicular safety messaging protocols does not provide an optimal balance between safety and privacy. In academia, there has been much work over the last decade on the design of security protocols to provide the security guarantees required for vehicular communications, with some focus on the linkability properties. To the best of our knowledge, previously-proposed solutions do not provide continuous linkability for nearby vehicles: protocols designed to provide the time-based short-term linkability and long-term unlinkability give a discontinuous short-term linkability, with unlinkable updates even for nearby vehicles.

In such protocols, keys are short-lived and updated at time intervals, so that the key used by an OBU before an update cannot be linked to its new key after an update. The aim of this is to preserve long-term unlinkability; however the unlinkable update causes disruption in the linkability of messages for nearby vehicles. Thus, despite remaining in close proximity and possibly line-of-sight, communicating vehicles experience a break in their ability to link a sender's messages; this is not ideal for safety applications requiring cooperation, and furthermore presents some conflict between the capability for physical recognition of nearby vehicles and the level of privacy given by the safety messages. We propose a *distance*-based approach to linkability, which enables better provision of continuity and is a closer fit to this physical situation. There has been some distance-based work on vehicle privacy - in particular location privacy, and secure location verification schemes. These distance concepts have not been applied to the provision of linkability.

Contribution

We review the current state-of-the-art in vehicular safety messaging protocols. We review the safety requirements for these protocols and argue that continuous linkability of safety messages for nearby vehicles - the property that nearby vehicles can continuously link, without breaks in linkability, safety messages sent by the same sender - is desirable for certain safety applications. Further, we argue that, rather than time-based (short-term) linkability, a more fitting property for this context is *distance*-based linkability, and propose solutions for its provision in protocol design.

With regard to the linkability properties, our argument can be summarised:

1) For safety applications, we require linkability for nearby vehicles
2) It is always possible for a party to link a vehicle that is close by, in line of sight, or through the detection of some unique signals that can be bound to the car
3) Whereever possible, unlinkability is required for privacy

Thus, we aim to achieve unlinkability (3), except in cases arising from (1) (because we explicitly design the

system for this) and (2) (because we fundamentally can't achieve it).

We proceed as follows. In Section II we give related academic and industrial work, and background on vehicular communications. In Section III we give our system model according to specifications in standards, and given assumptions. In Sections IV and V we give the security properties required for vehicular safety messaging, and the threat model. In Section VI we give our argument for continuous linkability in this context, and in Section VII we outline solutions for achieving continuous linkability.

II. Background and Related work

We begin by reviewing the development of protocols for safety messaging in vehicular communications. In 2007, [4], Raya et. al apply a traditional PKI infrastructure to Vehicular Ad-Hoc Networks (VANET). In the same year, in [5], a hybrid approach, the GSIS protocol, is proposed, in which different techniques are applied to the two separately-defined classes of problem: OBU-OBU communication, and RSU-OBU communication, according to their differing security requirements. A group signature technique, developed from that of Boneh et. al [6], [7] is applied to OBU-OBU communications; while the RSU-OBU communications, for which it is argued that privacy of RSUs is not required, use identity-based signature techniques.

The protocol proposed in [4] does not provide privacy or anonymity of the sender, and the adoption of a group signature -based approach, in which members sign anonymously on behalf of the group in which they are contained, is taken in subsequent protocols designs [5], [8], [9], [10]. Some of the group protocols are based on bilinear pairing operations to improve efficiency ([5], [8]), while in [10] the focus is on improving the efficiency of the certificate revocation checking process using a keyed Hash Message Authentication Code (HMAC).

In the 2008 paper [8], by the same research group as [5], an Efficient Conditional Privacy Preservation (ECPP) protocol is proposed, which is shown to be more efficient than the protocols proposed in [4] and [5], with reduced overheads for storage; complexity of message verification; and complexity of OBU tracking computations. The ECPP protocol uses short-time anonymous key certificates. An OBU requests an short-time anonymous key from an RSU when passing by the RSU, and updates it on reaching a new OBU. The motivation for this updating is not the provision of unlinkability, but the reduction of storage overhead for the revocation list. Furthermore, the group key signing is anonymous; public keys of each OBU are not broadcast, and there is therefore no provision of short-term linkability: two different messages sent by the same OBU cannot be linked to the same OBU by any other OBU.

Perrig et. al in [9], similarly to [8], use a *temporary* key technique (TACKs - temporary anonymous certified keys). The basis for this is that regional authorities provide short-term certificates to authenticate short-term public keys to vehicles that are in the region they cover. In this work, the authors claim to give a protocol that provides short-term linkability, and long-term unlinkability. However, the long-term unlinkability is based on the assumption that multiple vehicles will enter any particular region simultaneously, and the issuing of their TACKs will thus be simultaneous and, because of this, anonymous. This assumption may not always hold true, and in particular renders the long-term unlinkability false for applications of the protocol in areas more sparsely-populated by vehicles, in which it is more likely that a vehicle may enter a region individually, rather than simultaneously with others. Furthermore, the scheme is vulnerable to Sybil attacks, in which one OBU may impersonate multiple OBUs, and requires a large amount of computational power at the RSUs, which may be unrealistic.

In general, protocols given by prior work address a set of security properties, and the solutions broadly provided address the provision of these properties as follows. In order to provide authentication and integrity of safety messages, messages contain a signature that verifies that their received content is that which was initially sent. Furthermore, the signature must be verifiable, such that the receiver can verify the authenticity of the sender. The provision of conditional anonymity is generally treated using pseudo-identities, initialised within groups, such that the real ID of the vehicle owner cannot be known from the safety messages. Certificate revocation mechanisms - often certificate revocation lists (CRLs) - are employed in prior work for limiting the impact of misbehaving users on a network by revoking their certificates, preventing their future participation in the network.

It is required that there be some tracing mechanism by which authorities may trace the actions of a user for the purposes of revocation in case of misbehaviour, or for liability-related issues. Cryptographic mechanisms are included in prior work by which authorities may trace network actors if required, and nonrepudiation is required for this action.Furthermore, it is desirable that tracing and nonrepudiation be collaborative; this is the case in both TACK [9] and GSIS [5], and again this is achieved through cryptographic mechanisms in the pro-

tocol, designed such that one party, a Tracing Manager, may retrieve an identity only if he has the collaboration of another authority - generally the RSU involved in the communication. This distributed responsibility means that there is no single point of failure: in both protocols, even if the secret tracing pair of the TM is compromised, the identity of the sender OBU of a message cannot be obtained without collaboration with the RSU overseeing the OBU at the time of sending. Of course, if an attacker were to compromise both the secret tracing pair of the TM, and the RSU concerned, then tracing of the OBU would be possible and any privacy guarantees would trivially be broken in this case.

It is in [9], that the provision of short-term linkability and long-distance unlinkability for VANET safety messaging is considered in the most depth. In the solution provided, TACK, the short-lived public/private key pairs at each OBU are updated at regular intervals, and the current public key broadcast by each OBU, so that for the time period in which the short-lived key pair remains the same, different messages sent by the same OBU using this key pair can be linked to the OBU, but messages sent by an OBU following a short-lived key pair update cannot be linked with those sent prior to the update. This creates discontinuity of the short-term linkability provision, and a solution for providing continuous linkability in the TACK framework is given in Section VII.

Location privacy schemes have been proposed, which focus specifically on preventing the tracking of vehicles through their pseudonyms. [11] gives an overview of work in this area. The basis of most work in this area is the changing of pseudonyms to prevent the linking of messages from the same pseudonym: providing vehicles with a set of pseudo-identities which changes periodically according to a pseudo-identity changing strategy. There is also work on preventing the linking of pseudo-identity changes: in particular, mix-zones [12] and random silent periods [13]. These methods of preventing linking are based on the creation of confusing and therefore obfuscating situations, and do not prevent linking selectively with regard to other parties. Continuity of linkability is not achieved by these schemes.

There has been much work on secure location verification schemes for vehicular communications applications. These have largely been aimed at providing secure location verification for routing protocols in vehicular communications networks, and at securing passive keyless entry (PKES) systems for vehicles against relay attacks using distance bounding between the vehicle and its key. In [14], the authors propose a localisation scheme for vehicles based on “beacon messages broadcast periodically by pairs of RSUs deployed on either side of the road”. Secure location verification for vehicles is highlighted as a key security issue for smart vehicles in [15], and tamper-proof GPS systems and verifiable multilateration (using distance bounding and multilateration) are given as solutions. The German Network on Wheels (NoW) project [16] concluded from attack surface examination for vehicular communications in 2010 that position forging attacks represented a key vulnerability in the system. Clearly, for privacy considerations in this context in particular, the prevention of position forging is of great importance.

Furthermore, there has been academic work on the possibility of using distance bounding in secure location verification schemes for position-based routing - in [17] it is argued that accurate and reliable position information for vehicles is crucial to the operation of vehicular communications, and the authors devise an infrastructureless cooperative position verification scheme using distance bounding. This is particularly true in the move towards automated systems, in which location information may be used for lane changing and adaptive cruise control applications. In [18] the authors consider the cost and practical implementation challenges affecting the implementation of distance bounding protocols in ad-hoc wireless environments (not vehicular networks specifically).

In Section VII we propose a distance-based dynamic group protocol for vehicular communications. To the best of our knowledge, no distance-based dynamic group protocol has been proposed for vehicular networks. We now explore related work in the topics of dynamic group protocols and in distance bounding independently of one another.

The concept of distance bounding was first proposed by Brands and Chaum in [19]. There has been work on the use of radio frequency distance bounding protocols for securing Passive Keyless Entry and Start Systems (PKES) in vehicles, preventing relay attacks. In [20] distance bounding is proposed as a method of securing PKES systems. The authors of [20] highlight radio frequency (RF) distance bounding as the only feasible method of distance bounding for this application, since the other main type of distance bounding (ultrasonic distance bounding) is vulnerable to relay attacks.

Dynamic group protocols have been developed to enable the functioning of group protocols in groups in which members may join and leave. In [21], Camenisch and Stadler develop a group protocol in which new members may join the group, but in which leaving the group is not provided for. In [22], Camenisch and Lysyanskaya present a dynamic group protocol with both

group joining and leaving capabilities, but it is highly costly and is not secure against manipulation by its members.

A number of dynamic group protocols have been proposed in recent years, that enable both joining and leaving the group. In [23] is proposed a dynamic Diffie-Hellman group key exchange that is formally proved secure under the Decisional Diffie-Hellman (DDH) assumption. Kumar and Tripathi propose a tree-based dynamic group key agreement protocol in [24], and in [25] a pairing free anonymous certificateless group key agreement protocol for dynamic groups. This protocol from [24] forms part of the basis for our protocol proposal in VII

In government and industry, numerous projects have in recent years worked towards standardising, with the IEEE 802.11p standard in North America, and European Telecommunications Standards Institute (ETSI)-developed ITS-G5 standard in Europe, and made proposals for the implementation of vehicular communications. Recent projects and consortia - such as the Car-to-Car Communications Consortium (C2C CC), a European industrial consortium of vehicle manufacturers - have outlined use cases and applications for ITS, developed in line with these standardisations: the ETSI standard [3] for ITS defines a "Basic Set of Applications" for ITS. ISO (International Organisation for Standardisation) standards are also under development for proposed components of ITS, including cooperative awareness systems. The standardisations and proposed applications for ITS are summarised in [2] and [26].

III. System

A. System components and requirements

The proposed system has three components: on-board units (OBUs), roadside units (RSUs) and trusted authorities (TAs). A system comprising these three components is the model on which academic and industrial efforts have been based, and is detailed in the ISO standard CALM for C-ITS (Communications Access for Land Mobiles for Cooperative ITS)[27], the network architecture from which European projects and standards are derived.

TAs are trusted authorities: central service providers that oversee the operation of the vehicular communications network. OBUs are the processing and communication devices contained in the vehicles themselves, which handle communications sent from and received by the vehicle and interface with the OBUs of other vehicles and with RSUs. Typically, OBUs contain a tamper-proof hardware security module (HSM) for communications and storage, and have networking capabilities over Dedicated Short Range Communications channel (DSRC), GPS, 2G and local area network (LAN)[27].

RSUs are roadside infrastructure, which are integral to vehicular communications architectures, since they enable vehicle-to-infrastructure communications. RSUs have two main functions: to communicate with administrators and service providers using Internet, and to provide communication support for OBUs locally.

Some research has been conducted into the optimal placement of RSUs to ensure maximum coverage while minimising the cost of deployment ([28], [29], [30]). RSUs are expensive to install, fuelling the need for optimal solution of the deployment problem with regard to minimising cost. In [29], optimisation of the solution to the RSU deployment problem is considered: a trade-off between communication quality (coverage by RSUs) and cost of mounting RSUs. In [31], the authors consider the handover time between RSUs, and state the necessity that for deployment of vehicular networks to form ITS, to enable handovers of OBUs from one RSU to the next RSU, RSU coverage must be ubiquitous and the signals of adjacent RSUs overlapping. Suggestion has been made of installing cars as RSUs ([32], [33]). Furthermore, there has been extensive work on routing and multi-hopping protocols for vehicular communications applications to ensure complete coverage of RSU communications in more sparsely RSU-covered areas in which direct RSU coverage is not complete. Solutions for improving coverage in highway vehicular communications through routing are given in [34]. CALM C-ITS[27] gives single-hop and multi-hop communications as the two communication methods between ITS stations (OBU-OBU and OBU-RSU).

Given the necessity for the coverage of RSUs to be ubiquitous in areas in which ITS operate, we assume ubiquitous and overlapping RSU coverage to be the case in the system model. We model the road in "coverage areas" each under coverage of at least one RSU. In practice, this represents one of two cases: that an RSU has direct one-hop communications with all vehicles in their "coverage area"; or that an RSU has a "coverage area" comprising a combination of vehicles with which it has direct one-hop communcations, and of vehicles outside its immediate range, with which it has indirect multi-hop communications, routed through more nearby vehicles.

B. System model

The model to be considered for the system, in terms of OBU and RSU distribution, varies depending on the

environment. For example, the model for a city, with a mesh of roads in close proximity in multiple directions, is different to that of a highway, in which a single unidirectional flow of traffic can be considered. These two systems are illustrated in Figures 1 and 2. The system models presented are simple but sufficient. In the highway model, Figure 1, the "coverage area", as discussed, for *RSU 1* is *Zone 1*, for *RSU 2*, *Zone 2* and so on.

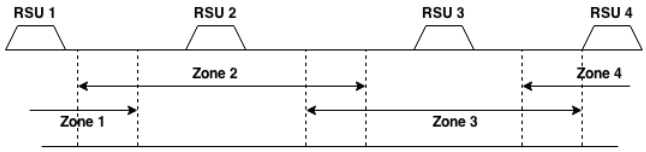

Figure 1. System model for highways

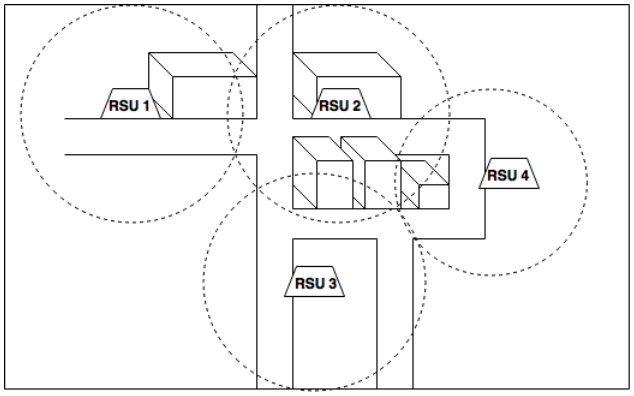

Figure 2. System model for urban areas

C. Communication

In the proposed system, vehicles communicate through OBUs with other vehicles' OBUs, as well as with RSUs, over wireless DSRC. The IEEE 802.11p specifies the WAVE (wireless access in vehicular environments) system for ITS support. In both ETSI ITS G5 and IEEE 802.11p, V2V and V2I communications are specified over DSRC to provide a network for vehicular communications. Over DSRC, the broadcast of one message every 300ms is specified for ITS, with a 75 MHz bandwidth in the 5.85-5.925 GHz spectrum [2]. ETSI standard ITS G5 specifies a 200-800m communication range for vehicles. RSUs have an Internet connection with TAs, through which they communicate.

In [35], a comparison is made of the IEEE WAVE standard against ETSI ITS G5, with particular focus on performance in cooperative awareness situations in high-node density environments, and it is found that in both cases came a considerable drop in the number of received Cooperative Awareness Messages (CAMs) when the penetration rate of the channel increased. Given the high density of nodes at peak times on roads, it is crucial that messages are sent frequently to counteract this loss, so that key messages are received.

D. Assumptions

We make certain assumptions for the system; these are informed by current and proposed future directions in ITS architecture development, and are as follows:

- RSUs have ubiquitous and overlapping coverage of the road (all areas of the system are covered by at least one RSU, either through single- or multi-hop communications, and at all boundaries between RSU coverage areas there is some overlap). It follows that All OBUs are within communication range of at least one RSU at all times.
- RSUs may communicate with (at least) their neighbouring RSUs
- The system contains a mixture of connected and disconnected vehicles - some have OBUs with communication capabilities; some do not
- Cryptographic operations at OBUs are tamper-proof - they are performed within a tamper-resistant HSM which also stores the cryptographic keys
- All RSUs can communicate with at least one Trusted Authority (TA) at all times (over Internet)

IV. Security properties

The security properties identified in this section are derived from prior academic literature, and standards - in particular ETSI TR 102 893 V1.1.1 (2010-03) [3], which gives security requirements for ITS falling into five categories: confidentiality, integrity, availability, accountability and authenticity. Broadly, security properties for ITS safety messaging arise from two main high-level requirements - safety and privacy - which are in many ways conflicting in this context: for safety applications, overtaking warnings, for example, we require that messages are sent frequently, that their contents are accurate, unaltered and trustworthy, and that they are received by all those who require the information they contain. We therefore require that a message's sender is, and its contents are, trusted by its recipients. Privacy requirements, however, drive a requirement for recognition of message senders' true identities to be unobtainable from the safety messages, and for no opportunities for tracking vehicles to be given by safety messages.

For safety messages, we identify five main areas in which security requirements arise.

A. authentication and integrity of messages

B. conditional anonymity towards a set of entities
C. tracing and non-repudiation for a specific entity
D. limiting impact of misbehaving users to a time/space
E. linkability and unlinkability: continuous linkability for a set of nearby vehicles; long-term unlinkability; long-distance unlinkability

A. Authentication and integrity of messages

It is required that messages be authenticated - that a receiver can verify that the claimed sender is the real sender, and that that sender is a legitimate user of the network. It is also required that the integrity of the message content be verifiable: that a receiver may verify that the content of the message has not been altered in transmission.

Interestingly, the confidentiality of safety messages is not required: sensitive or private information will not be contained in the safety messages and so the contents of the message itself need not be hidden. In practice, this means the safety message may be sent as plaintext, without encryption required.

B. Conditional anonymity towards a set of entities

Conditional anonymity is the property that entities communicating on a vehicular network cannot be linked to their identity through their messages, but that some higher authority has the ability to trace the identity of the sender of a specific message. It is required that safety messages be anonymous to those receiving the safety messages (a set of entities S), to prevent linking of safety messages received to a specific driver or vehicle, enabling recognition of their vicinity in the area, which violates privacy. Privacy of drivers is a basic right, protected by law in many countries, and so any communication solution must preserve this; ETSI [3] states that "Details relating to the identity and service capabilities of an ITS user should not be revealed to any unauthorized 3rd party". Tracing by a higher authority, or combination of higher authorities, is required for dealing with misbehaviour or liability-related issues.

C. Tracing and non-repudiation for a specific entity

For cases in which vehicles misbehave (sending misleading messages, for example), or for liability-related issues, it is required that safety messages sent may be traced back to a particular vehicle by a specific entity - a higher authority, often termed a Tracing Manager (TM). This is why the anonymity described above is "conditional". Ideally, the tracing should be collaborative, so that no single entity can trace the identity of any vehicle alone. This prevents prevents any single point-of-failure from which it is possible to derive the identity of the network members and hence compromise the privacy of the network.

It is also required that the sender has nonrepudiation towards this specific entity: that given any message, there is some entity (a TM) who can trace its sender and can prove that the message was indeed sent by that particular sender.

D. Limiting impact of misbehaving users to a time/space

It is desirable, given a user who is in some way misbehaving on the network - sending out misinformation, for example, or flooding the network with messages to deny service - that its participation in the network be somehow withdrawn. This may mean participation in the network will be stopped within a given time, preventing its future participation in the network. It could also mean that its actions are blocked in a certain area or space.

E. Linkability and unlinkability

Studer et. al study the linkability properties in some depth in [9]. There are two higher-level concerns driving the requirements for linkability and unlinkability: safety and privacy. For the safety applications of vehicular communications, we require linkability for nearby vehicles: that nearby vehicles can continuously recognise that messages sent from the same sender were sent by the same sender (short-distance linkability).

For privacy, we require that opportunities for tracking are not given to attackers through the safety messages. ETSI[3] states that "it should not be possible for an unauthorized party to deduce the location or identity of an ITS user by analyzing communications traffic flows to and from the ITS user's vehicle"; and "it should not be possible for an unauthorized party to deduce the route taken by an ITS end-user by analyzing communications traffic flows to and from the ITS end-user's vehicle."

Fundamentally, we cannot achieve, using communication protocols, the prevention of tracking through physical tailing; it is therefore futile to include this prevention in the security requirements for the safety messages: it is always possible for a vehicle to be linked by a nearby party, within line of sight. It is therefore not required that two vehicles who remain nearby one another be unlinkable for that period of time since, trivially, the same tracking effect could be given in such a case by physical following of one vehicle by another. What we require is that parties that are not nearby a given vehicle V are unable to track V through its safety messages (long-distance unlinkability), while those in

some "nearby" vicinity are (short-distance linkability). Furthermore, we require that parties leaving the defined nearby vicinity of V for a given time cannot continue to link its safety messages on return to its vicinity to those it received before leaving its vicinity. Given these requirements, it appears that linkability properties based on distance may be more fitting than time-based ones, and this observation is further discussed in Section VI as a means of providing continuous linkability.

V. Threat model

In general, the threat model is an attacker who wishes to in some way disrupt the intended function of the vehicular communications network. This could be by changing or deleting safety messages in, or inserting new messages into the network, causing potentially dangerous situations; or by using the message broadcast to track drivers' whereabouts, for example. An attacker may be mobile: a driver in a vehicle, tracking other vehicles, or disrupting the communications of a network. An attacker could also be immobile: one or more devices stationed at points to receive or broadcast network messages.

Numerous attacker capabilities are given for this context in prior literature; the threat model we consider is given below. We consider that there are three main classes of attacker:

A. A mobile attacker, located within a moving vehicle with reception of messages over some surrounding coverage radius r_1
B. An immobile attacker, positioned at a single location, with reception of messages over some surrounding coverage radius r_2
C. An attacker with widespread or global coverage, facilitated by a series of antennae positioned to give coverage of a large area

Each class of attacker has different capabilities, and the types of position, in relation to a targeted OBU, are illustrated in Figure 3.

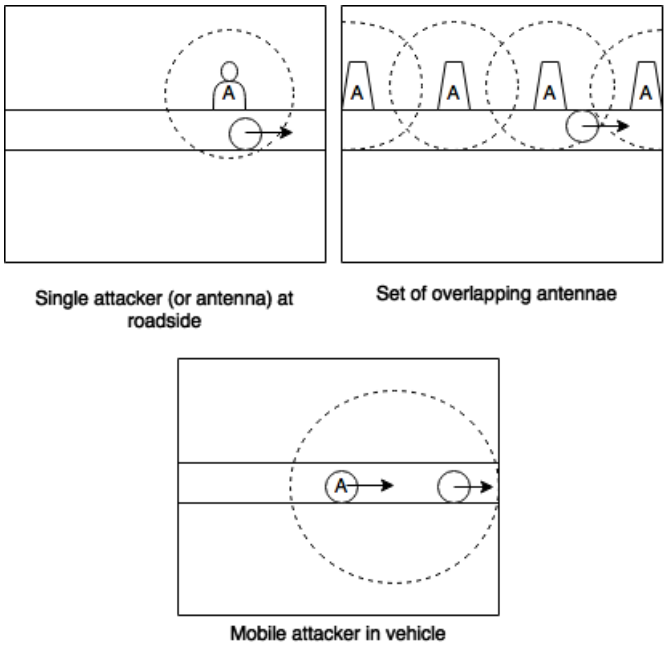

Figure 3. Attacker positions

Threat agents

There are numerous possible attackers in this context. On a smaller scale, the disruption of some vehicular communication represents an attractive target for hackers "messing around": kids with jamming devices, for example. In general, such an individual attacker is likely to target a single location: perhaps positioned at the roadside, or with a small set of antennae placed.

The potential for causing widespread harm also makes the disruption of the network communications a target for large-scale targeted or untargeted terrorist or hacktivist attacks. Advantage may be gained through network disruption by rival car companies and other road users, and so these are possible threats. There is a threat of tracking of a vehicle by any interested party, and by the government and authorities. A more resourceful attacker has additional capabilities over an individual, less capable one. Potential attacks are: the control or insertion of RSUs; a global or widespread antennae coverage for tracking purposes; a global or widespread manipulation of safety messages.

Active and passive attackers

Attackers may be active - disrupting the network; changing the message flow by deleting, changing or inserting messages - or passive - eavesdropping on network communications; in particular using this passively-obtained information to track vehicles.

An active attacker might have a number of motives for deleting, changing or inserting new messages:

- messing around
- causing general (untargeted) chaos
- causing general harm (to users in a specific location for example, in a terrorist act)
- causing targeted harm (targeted at a specific entity)
- altering safety information – traffic updates, traffic light waiting, for example – to gain an advantage for their own journey (eg. reducing the traffic on their preferred route, to the disadvantage of other road users)

With regard to tracking capabilities, the threat is a passive attacker who wishes to compromise a driver's

privacy by tracking their location and time without the need to remain in constant physical proximity to them (i.e. without actually following them physically). An attacker might be interested in capturing a message from a party they wish to track in such a way, in order to map their whereabouts generally, to find out when they are in a certain place, or to attack their communications with rogue messages, for example, without needing to remain nearby them. An extension to this is the threat of an attacker who, having driven nearby a vehicle, later rejoins its neighbourhood and is able to link it back to its previous messages. This capability would give the attacker some tracking opportunity without having to remain constantly in the vicinity of its target vehicle, and hence affords more tracking capability that physical tracking itself - detracting from the privacy we require.

A passive attacker's motives for tracking vehicles may be:

- to follow the movements of a specific vehicle
- to recognise the presence of a specific vehicle in a certain area
- to map the movements of vehicles within a certain area
- to learn the *identity* of a vehicle's driver. The threat here is a party that may learn the true identity of a vehicle's driver, or recognise a vehicle, from its safety messages. This has been a security property considered throughout the literature on this topic, with tracking through ID disclosure given as a threat in early works such as [4].

Insiders and outsiders to the network

An attacker may be an insider - an apparently legitimate member of the communications network (a party who knows the network secrets) - or an outsider - another vehicle or immobile attacker who is not part of the targeted network (does not know the network secrets). An inside attacker to a network could either be a moving vehicle - another road user - or an immobile attacker. An immobile attacker might, for example, position a series of large antennae in close proximity such that they could continuously authenticate to a network. Given the slow signal degradation of messages sent by OBUs [36], the requirement for an attacker to remain an insider to a network is a continuous proximity to that network.

Clearly, network members must be able to send messages over the network. Thus, an insider, as an apparently legitimate member of the network, may attack the network: by inserting messages communicating false information, or by flooding the network with messages in order to deny service. Furthermore, an insider to a network can view *who* is sending the messages over that network (although this should be a pseudo-identity only, not a true identity). If there is no tracing for any specific entity, such as a trusted authority, enabled by the communications protocols, misbehaving members of a network cannot be traced and therefore misbehaviour on the network can continue without action such as revocation being taken. The threat here is a party that continuously misbehaves on a network, sending bogus messages or flooding the network in order to deny service, for example, disrupting its intended function.

An outsider has more restricted capabilities towards a targeted network. An outsider to the network could, again, be a moving vehicle; an attacker with one or more antennae to receive messages; or an attacker positioned at a specific location near the network.

Without knowledge of the required communications secrets (usually a group key in this context), an outsider should be unable to insert, change or delete messages sent over the network. Furthermore, an outside attacker without the ability to decrypt network communications can only eavesdrop on information sent as plaintext: the choice of information to encrypt is therefore an important part of the security design; in particular, whether to encrypt pseudo-identities. However without adequate authentication mechanisms, an attacker may pose as a valid member of a network in order to insert messages, or masquerade as another OBU or multiple other OBUs. An appropriately-positioned outside attacker may be able to deny service to the network, with wireless jamming attacks for example.

Depending on the type of attack, attacks may be targeted at a specific entity; targeted at randomly-chosen single vehicles; targeted at a specifically-chosen group of vehicles; or targeted at a randomly-chosen group of vehicles. It is possible that an attacker may unintentionally disrupt the network: a signal jammer placed accidentally within range of a vehicular network, for example, could disrupt the message flow. However in this context, attacks are more likely to be intentional: the insertion of rogue messages; changing of network messages; and tracking of vehicles take some concerted effort on an attacker's part.

VI. Continuous Linkability

Problem formulation

In this section, we focus specifically on the linkability property, justifying the linkability required according to proposed use cases, and presenting the most appropriate means of providing the identified linkability requirements. We argue as follows: for several of the safety

applications proposed for ITS, continuous and seamless communications for nearby vehicles are desirable. Previously-proposed short-term linkability of safety messages, achieved through unlinkable transitions at time intervals, appears disruptive of the foreseen applications, and the privacy it achieves is not an exact fit for the privacy guarantees we require from safety messages: that an attacker gains no tracking advantage through the reception of safety messages. Distance-based linkability is a fitting and viable alternative property that enables continuity.

Further to its introduction in Section I, we clarify the ETSI-proposed safety applications of ITS that suggest a requirement for continuous linkability. These are the use cases that are based on "cooperative awareness", and the most prominent are as follows:

- overtaking vehicle warning
- lane change assistance
- cooperative merging assistance
- cooperative forward collision warning

ETSI have given further information on these proposed applications. For the overtaking vehicle warning application, for example, "An overtaking (passing) vehicle signals its action to other local vehicles to secure the overtaking situation" [37]. In this way, vehicles may coordinate their overtaking actions in order to avoid collision. Clearly, vehicles executing such procedures require a highly reliable, efficient, frequent and continuously identifiable communications link between them ([37] specifies a critical latency time of less than 100ms).

Similarly, for the lane change application, [37] specifies the required "capability for this vehicle to co-operate in some manner with other vehicles involved in a lane change situation"; and for the collision risk warning application the requirement is specified for "a vehicle which will be turning left to broadcast its status in V2X co-operative awareness messages" and for "concerned vehicles to receive and process V2X co-operative awareness messages", where V2X is vehicle-to-entity (to another vehicle, or to infrastructure). For cooperative merging assistance, it is required "for vehicles being involved in a lane merging to establish and maintain as long as necessary unicast peer to peer sessions with other vehicles involved in the lane merging assistance process". C2C CC states Cooperative Forward Collision Warning as a safety use case of vehicular communications, in which vehicles must share information with one another in order to monitor the behaviour of nearby vehicles.

Given these foreseen safety-critical applications in ITS for vehicles to cooperate, sharing their intended actions and information on their states, it is required that the vehicle-to-vehicle (V2V) channels through which such communications are made enable the clearest possible picture of the exact situation surrounding each vehicle. An effective "dialogue" - a continuously-identifiable flow of information - between two cooperating vehicles is required, and as part of this it is desirable that communications between any two vehicles operating in such a way be continuously *linkable*.

Safety messaging is suited to this application and gives additional advantage over a purely sensor-based scheme since it allows vehicles to broadcast their directional *intention*: their intention to change lane, perhaps, to other vehicles. If, as the case could feasibly arise in the TACK protocol of [9], an OBU communicating with another OBU while performing a lane changing operation were to suddenly lose the linkability of its previous messages with that OBU to its new ones, this would reduce the safety of the application. The inefficiency of having non-continuous linkability for nearby vehicles, such that upon key updates, the linkability of messages between two vehicles is broken, reduces the appropriateness of the architecture for such safety-critical applications as those given. In a cooperative ITS in which safety relies on the timely and accurate communication of knowledge between nearby vehicles, continuity is desirable and fitting.

Furthermore, such sudden loss of linkability does not make sense in the context of vehicles driving nearby one another, since physical recognition remains continuous in such a case and so trivially, the updating cannot give any kind of additional privacy. In the context, it makes sense for the privacy given by the protocol to be shaped around the physical aspects: neighbouring vehicles can be continuously linked to their messages and location since any entity wishing to use this information for tracking in this case would have to remain in physical proximity - in particular, within line-of-sight - of the vehicle, which is akin to physical tracking and cannot be prevented cryptographically.

As discussed, the problem with providing such continuous linkability comes from an opposing requirement: the prevention of the tracking by all vehicles not included in a defined "nearby" set. Trivially, we cannot prevent using protocols any tracking capabilities that correspond to a physical tailing of a given vehicle. The ideal, therefore, would be an architecture that gave linkability only in exactly those cases corresponding to a physical tailing. In reality, in order to physically tail a vehicle V_1, it is required that an attacker keep V_1 almost continuously in his line of sight. A perfect representation of the real-world scenario would, therefore, be an architecture in which the safety messages of a vehicle V_1 were

unlinkable for all those excluded from a set of vehicles S, in which S comprises all those vehicles who have a near-continuous line-of-sight connection with V_1.

Such a design is highly ambitious: possibly a laser-based line-of-sight solution, in which vehicles check whether other vehicles are in their line-of-sight "most of the time" (corresponding to physical tailing) might be a way of achieving this. However, such a solution is less responsive than a real-world attacker physically tailing a vehicle and could not discern between, for example, a lorry continuously blocking a line-of-sight (an obstacle that could be circumvented by a real-world attacker) and a line of buildings blocking the line of sight (if, for example, the attacker and the target vehicle were not even driving on the same road). Such complexity would, without very careful engineering, produce a highly difficult balance of false negatives and false positives; in the former case, very nearby vehicles whose view was somewhat obstructed might not be linkable; in the latter, vehicles out of sight might be linked is obstructions were misinterpreted. In this work, therefore, we leave this linkability based on line-of-sight as an impossibility assumption.

The next-closest representation of this linkability of a vehicle V_1 allowed only for vehicles whose positioning corresponds to a physical tailing is a distance-based one, in which a defined set of continuously "nearby" vehicles can link the safety messages of V_1. This better provides the required properties than a time-based linkability, which, as discussed, does not correspond sensibly to the problem we have defined. In a model in which we seek unlinkability for all those not in a position to physically track V_1, such sudden time-based updates correspond to a nonsensical physical situation in which after set intervals of time the vehicle V_1 becomes suddenly unrecognisable (through a change in appearance) to all those vehicles surrounding it.

This time-based linkability is therefore not what is truly required. Furthermore, it does not, as it is presented in prior work, give *continuous* linkability. The current state-of-the-art makes a trade-off in which continuity is disrupted in order to enable a time-based update. However, the foreseen safety messaging applications for ITS mean that this disruption is unsuitable, as explained above. *Distance*-based linkability does give this continuity for nearby vehicles and, importantly, distance-based linkability is achievable as a security property, as we show in Section VII.

Linkability: distance- against time-based approach

Given the threat model identified for an attacker wishing to track an entity, we evaluate the differences in the *distance* rather than *time*-based approach to linkability.

By studying the system model set out, we can derive an exact description of the linkability requirements. The requirements for linkability for an OBU OBU_1 are that:

a) nearby vehicles to OBU_1 can continuously link messages to their sender OBU_1: two nearby vehicles must have the capability to hold a continuous "dialogue"
b) vehicles that are not, or do not remain, nearby OBU_1 cannot link the messages sent to the sender OBU_1

a) is a practical requirement for linkability, required for safety; b) is a security requirement required for privacy and tracking prevention. The two requirements must be considered in conjunction in the consideration of appropriate an appropriate linkability definition for the system.

Broadly, the practical requirement from which b) is derived can be expressed as follows: that no attacker may gain any tracking advantage through the reception of safety messages, that is greater than his tracking capabilities through a physical tailing of the vehicle.

It follows that any party that travels continuously within a defined "close" distance of OBU_1 (which is the attacker model equivalent to physical tailing of OBU_1) may continuously link the messages sent by OBU_1. Conversely, any party that does not travel continuously within the defined "close" distance of OBU_1 must not be able to continuously link the messages sent by OBU_1. This is a natural fit for the real-world problem at hand.

A distance-based linkability provides security against threats that are not prevented by time-based linkability. In particular, the case of an attacker who sets up two antennae with large and overlapping (or at least immediately adjacent) message reception range, as in Figure 4. If linkability were time-based, then the attacker could track the movements of an OBU by strategically positioning its antennae so that the tracked OBU would only leave their range for a certain amount of time. The attacker would therefore gain advantage through this method additional to his tracking capabilties through physical tailing. If, however, linkability were distance-based, then an attacker could only track the movements of an OBU by ensuring that its antennae were sufficiently close that at each point in the OBU's travel at least one antennae fell into its specified "close" distance, as in Figure 5. This is equivalent to physical tailing and cannot be prevented; it also requires huge resources from an attacker, and is unrealistic as an attack in general. The distance-based approach therefore provides greater security against a stationary receiver-based attack.

In a protocol providing distance-based linkability, we identify three main linkability requirements:

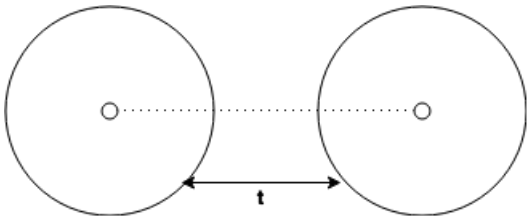

Figure 4. Attack on time-based linkability

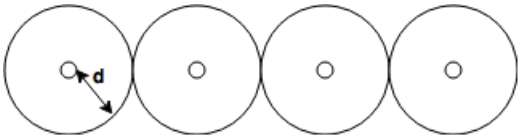

Figure 5. Attack on distance-based linkability

1) Continuous linkability for a set of nearby vehicles, S
2) Long-term unlinkability for any vehicles not remaining in S
3) Long-distance unlinkability for vehicles outside S

In practice, 1) means that vehicles remaining in S for a certain time period t should be able to continuously link two different messages sent by V_1 to the sender V_1 during t. 2) means that any vehicle that does not belong to, or that leaves, the set S should not be able to link two different messages sent by V_1 to the sender V_1. 3) extends this: any vehicle that leaves and then rejoins, after a defined "long" period of time, the set S, should not be able to link messages sent by V_1 during its first membership to the set to those sent by V_1 during its second membership to the set - only those OBUs that remain *continuously* in the set S should have continuous linkability for V_1.

This is a natural refinement of the linkability property given in [9]. In [9] the requirement is stated that in order to achieve long-term unlinkability it is important that two TACKs used by the same vehicle cannot be linked to each other. The difference between the linkability of [9] and our linkability is our exclusion of the fundamentally unpreventable case in which an attacker tracks an OBU by remaining in its vicinity. The exclusion of this case in the refinement opens the possibility of providing architectures in which linkability is continuous for vehicles nearby one another, and this continuity has important practical applications.

VII. Achieving Continuous Linkability

We outline both a solution for providing *continuous* linkability in existing time-based architectures, and one for providing continuous linkability in a new distance-based protocol. These solutions are sketches; we leave their detailing to further work.

Solutions for providing continuity in existing architectures (time-based)

The first solution is the outline of an architecture to be incorporated into the temporary anonymous key framework (the TACK protocol, [9]), which is presented in [9], and in which long-term unlinkability is preserved through the regular updating of the key of each vehicle. This updating process creates a break in linkability, which, as discussed, in not ideal for some proposed safety applications. Our solution enables the linking of the current key to the new key at the same vehicle, providing continuity of short-term linkability. However, there are flaws in the solution which point to the requirement for distance verification, as will be explained.

In the TACK protocol, OBUs update their key pairs on entering a new region. This works as follows: OBUs pick a random public/private key pair and send it to a Regional Authority for the new region, signed with a group key which vouches for the validity of the OBU. The RSU verifies the validity of the OBU and signs a certificate for its new TACK public key; this certificate is then sent back to the OBU, which continues communications in the region using its newly-certified TACK key pair. For the short time duration over which a single TACK key pair is used by an OBU for signing messages, the messages sent by that OBU can be linked to each other. However, messages sent before and after a TACK key pair update cannot be linked to each other: there is a break in linkability in the transition.

Our concept for providing continuous linkability in this architecture is as follows: on updating to a new key, an OBU sends a "linking certificate" broadcast, which notifies nearby vehicles of the link between its previous key and its newly updated key.

1) Let $K_O = (K_O^+, K_O^-)$ be the currently used key pair of the OBU, composed of public key K_O^+ and private key K_O^-. Similarly, let $K_N = (K_N^+, K_N^-)$ be the next key pair for the OBU, composed of public key K_N^+ and private key K_N^-.
2) OBU certifies its link with RSU:
   OBU $\rightarrow$ RSU: $((K_N^+, K_O^+)_{sigK_O^-})_{sigK_{RSU}^+}$
   RSU $\rightarrow$ OBU: $cert_{RSU}(K_N^+, K_O^+)$
3) On receiving this "linking certificate" from the RSU, the OBU broadcasts its two public keys, old and new, along with the certificate for them:
   OBU: $(PK_O^+, PK_N^+, Cert_{RSU}(K_N^+, K_O^+))$.
4) Receiving OBUs link K_N^+ to K_O^+ and replace it in their records.

An issue with this concept is its reliance on signal degradation: in [36], wireless path loss in four different environments – highway, rural, urban and suburban – is given. The results in all environments give estimated low path loss exponents, leading to the conclusion that vehicle-to-vehicle systems should be "robust to interference from other users". In particular, this low path loss exponent for V2V signals means that signal degradation cannot be relied on to create a group of nearby message receivers, and drives a requirement for some other form of distance verification.

In our solution, an OBU's "linking certificate" may be received by anyone within range of its broadcast; this does not necessarily mean only those vehicles nearby - an attacker with one or more large antennae, for example, may pick up these broadcasts from a distance greater than the anticipated broadcast range, and with multiple antennae positioned within range of a route may continuously track a vehicle in this way. This issue could be solved through the encryption of the linking certificate with a group key, such that only group members within a verified distance of the broadcasting OBU could decrypt its linking certificate. Such a solution would require a distance-verified group formation, which is the basis of our second solution presented below.

Solution for providing continuous distance-based linkability

We propose a distance-based solution to providing continuous linkability for nearby vehicles. We outline the architecture in this work, and develop the protocol details in future work. The solution we propose is a distance-based dynamic group protocol. More specifically, this is a dynamic group protocol whose initialisation, join and leave decisions are made according to a distance verification made through a distance-bounding protocol. The basis is as follows: distance-verified nearby vehicles share a group key, with which they encrypt safety messages between themselves, encrypt their pseudo-identities, and encrypt broadcasts of their pseudo-identity updates.

In the dynamic group protocol, groups are initiated using a ternary tree structure, and key exchange is based on elliptic curve Diffie-Hellman (ECDH). The protocol is derived from prior proposals for dynamic group protocols based on ECDH key exchange.

The protocol design varies according to whether the RSUs themselves have distance bounding capabilities. We provide a design for both cases: that in which both RSUs and OBUs are able to take part in distance bounding protocols; and that in which only OBUs, and not RSUs, can take part in distance bounding protocols.

As well as providing the discussed linkability requirements, other protocol design aspects are required in order to meet the other security requirements discussed in Section IV:

- Distributed tracing mechanism - requiring cooperation from RSU and TA for tracing such that no single party is able to perform tracing alone
- Revocation procedure for revoking misbehaving users
- Conditional anonymity through assignment of pseudo-identities

We leave the cryptographic specification of the protocol to future work, recognising the requirement for the provision of the above-listed properties, as in prior work. Here, we outline an architecture for a distance-based dynamic group protocol.

Preliminaries

Before giving the protocol outline, some preliminaries are required. We describe the two-party and three-party ECDH key exchange protocols from which the ternary tree-based group key generation protocol of [24] is built, and give details of the protocol from [24]. We then give an overview of the use, and proposals for use, of distance bounding in vehicles.

Two-party elliptic curve Diffie-Hellman key exchange (ECDH): Let A and B be two parties. Let E be an elliptic curve, P be a point on E, and p be a prime, where parties A and B share knowledge of E, P and p. Then A and B may establish a shared key using ECDH as follows.

1) A selects random $x \in \mathcal{Z}_p^*$ as private key
2) A calculates $X = xP$ as public key
3) B selects random $y \in \mathcal{Z}_p^*$ as private key
4) B calculates $Y = yP$ as public key
5) $A \rightarrow B$: X
6) $B \rightarrow A$: Y
7) A and B each calculate shared key $K = xY = yX = xyP$

Three-party ECDH: Let A, B and C be three parties. Let E be an elliptic curve, P be a point on E, and p be a prime, where parties A, B and C share knowledge of E, P and p. Then A,B and C may establish a shared key using ECDH as follows.

1) A selects random $x \in \mathcal{Z}_p^*$ as private key
2) A calculates $X = xP$ as public key
3) $A \rightarrow B$: X
4) B selects random $y \in \mathcal{Z}_p^*$ as private key
5) B calculates $Y_1 = yP$, $Y_2 = yX$
6) $B \rightarrow C$: X, Y_1, Y_2
7) C selects random $z \in \mathcal{Z}_p^*$ as private key

8) C calculates $K = zY_2$, $Z_1 = zY_1$, $Z_2 = zX$
9) $C \rightarrow A, B$: Z_1, Z_2
10) A calculates: $K = xZ_1$
11) B calculates: $K = yZ_2$
12) A, B and C all now share the key $K = xyzP$

Ternary tree-based dynamic group protocol: A ternary tree-based group key protocol is proposed in [24] over elliptic curves. We adapt this protocol to include distance verification and to provide the security requirements outlined; the use of ECDH key exchange provides greater efficiency than the standard Diffie-Hellman key exchange (proposed in [23], for example). In particular, we introduce a distance verification-based decision process for the initialisation, join and leave processes of the protocol.

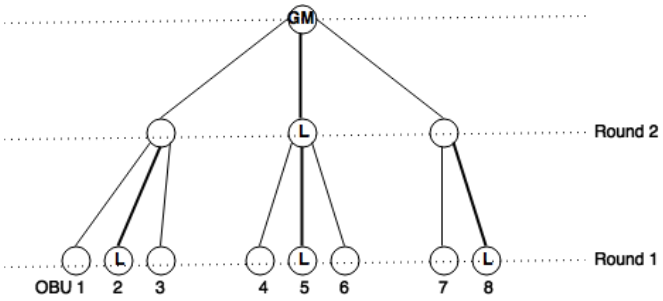

Figure 6. Ternary tree structure for group key generation

Figure 6 shows the structure of the ternary tree on which the group key generation protocol is based. The concept of the group key generation is as follows. The process is based on a combination of two-party and three-party elliptic curve Diffie-Hellman (ECDH) key exchange. At Round 1, nodes (individual OBUs) form subgroups of two or three parties, and each subgroup at Round 1 establishes a shared key using either two- or three- party ECDH key exchange as appropriate. One OBU from each subgroup then represents their subgroup at Round 2 (labelled L, these subgroup-representative OBUs are the nodes shown at Round 2 in Figure 6. These nodes at Round 2 again form subgroups of two or three parties, and each subgroup at Round 2 establishes a shared key using ECDH key exchange. The process continues until a single shared key is established for the entire tree.

1) Nodes form subgroups of two or three
2) Each subgroup establish shared key using two- or three-party ECDH
3) One node from each subgroup becomes the representative node at the next Round
4) Proceed to next Round. If more than one node remains: repeat steps 1)-3). Else: group shared key K is established and the single remaining node at the last round is the Group Manager GM.

Distance bounding verification: Distance bounding protocols enable mutual establishment, between two parties, in which one party represents a *verifier* and one a *prover* of an upper bound on their distance from each other. This means that both parties are assured that they are no closer to each other than the distance given by the distance bounding.

In vehicular communications, distance bounding would enable two vehicles to establish a mutually-trusted upper bound on their distance from each other, such that an attacker could not make any two vehicles appear closer together than they really were (snce no lower bound is established, an attacker could still make two vehicles appear further apart than they really were, but this is irrelevant to the security requirements we are examining).

With regard to proposals for integrating distance bounding hardware into vehicles, there has been work on the use of radio frequency distance bounding protocols for securing Passive Keyless Entry and Start Systems (PKES) in vehicles, preventing relay attacks. In [20] distance bounding is proposed as a method of securing PKES systems. The authors of [20] highlight radio frequency (RF) distance bounding as the only feasible method of distance bounding for this application, since the other main type of distance bounding (ultrasonic distance bounding) is vulnerable to relay attacks. Furthermore, there has been academic work on the possibility of using distance bounding in secure location verification schemes for position-based routing - in [17] it is argued that accurate and reliable position information for vehicles is crucial to the operation of ITS and an an infrastructureless cooperative position verification scheme using distance bounding is devised.

Distance-based dynamic group protocol

The dynamic group protocol will have three main stages:

1) **Initialisation:** this will consist of a ternary tree-based formation of a new group
2) **Join:** this will be executed to allow one or more parties to join an existing group
3) **Leave:** this will be executed to allow one or more parties to leave a group

The **Join** and **Leave** decisions will be made according to distance.

Broadly, the outline of the protocol steps are as follows.

OBUs, if not part of a group, broadcast their GPS location and their current public key to the RSU. RSUs map the movement of groups and of external OBUs in

their area, and decide whether to perform **initalisation** and, in the join and leave cases using infrastructure (presented below are both infrastructureless join and leave designs, and join and leave designs which use infrastructure), whether to initiate **join** or **leave**.

Initialisation

There are two possibilities for the initialisation stage: that RSUs have the ability to perform distance bounding protocols with OBUs, or that they do not and the distance bounding can only be between OBUs, and not performed by RSUs. We present the initialisation process for these two cases.

With RSU distance bounding:

1) RSU recognises need for new group and sets a group leader C, who is the OBU closest to the center of the new group space
2) RSU executes distance bounding verification with all member of new group, to verify their GPS broadcast and that they are indeed in the group space
3) If distance bounding for an OBU shows that it is not in the group space, it is excluded from the initialisation process. For the OBUs whose distance is verified as being in the group space, the RSU calculates the tree division for the ternary tree architecture
4) RSU sends to each OBU in the group space the group parameters
5) RSU sends to each OBU individually (using its current public key - left over from last group) its tree instructions (see separate section) and the public keys of those with which it must communicate
6) OBUs execute the ternary tree group key generation to generate the group key

Without RSU distance bounding:

1) RSU recognises need for new group and sets a group leader C, who is the OBU closest to the center of the new group space
2) RSU calculates tree division for the ternary tree architecture
3) RSU sends to each OBU individually (using its current public key - left over from last group) its tree instructions (see separate section) and the public keys of those with which its must communicate
4) RSU also sends to each OBU individually its distance bounding instructions: the distance within which its neighbour nodes claim to be
5) OBUs perform distance bounding with the nodes they share with in the tree architecture (see diagram and instructions) and report back their verification of the distance
6) If all OBU distances are verified, RSU sends to each OBU in the group space the group parametersOBUs continue to execute ternary tree group key generation to generate the group key
7) If one or more nodes fall outside the distance bound, RSU excludes these nodes from the group space and recalculates the tree architecture. Then proceed to step 3) followed by step 6).

Join

Using infrastructure:

1) If not part of a group, and OBU issues a request to its nearest RSU to join a group, including its GPS location and its current public key (left over from last group)
2) RSU calculates group to join and node to join at
3) RSU sends to OBU and its first node members join request with the public keys and GPS of the first node members
4) RSU sends to first node group manager distance bounding instructions: distance to verify
5) If distance verified, join operation performed
6) If distance not verified, RSU makes request for new GPS signal or cancels request

Infrastructureless:

1) OBU broadcasts join request including GPS and public key
2) receiving (nearby) OBUs forward request to their group manager
3) group manager performs distance bounding with new joiner to verify distance
4) If distance verified, join operation performed
5) If distance not verified, request dropped, OBU must broadcast new join request

It is important to note that in the above infrastructureless case, the group manager must keep a mapping of the location of its group members using GPS and periodic distance bounding checks, so that is can calculate the required distance for new group members (see ...)

Leave

Using infrastructure:

1) OBUs periocally perform distance bounding checks, given instructions by RSU
2) If at a check an OBU falls outside the required distance, reported back to RSU
3) RSU recalculates existing group join or new group formation for fallen OBU

4) If existing group join, RSU performs steps 2) to 6) of group join procedure using infrastructure above
5) If new group formation, RSU performs initialisation procedure above
6) Once existing group join or new group formation is completed for OBU, RSU initiates leave procedure for current group; tree updates without fallen node

Infrastructureless:

1) OBUs periodically perform distance bounding checks
2) If at a check an OBU falls outside the required distance, the group manager issues a command to it to broadcast a new join request, to be picked up in its new group space (or, by an RSU to form a new group in the absence of a new group space - as in the initialisation procedure)
3) Once OBU has successfully joined new group it reports back to group manager, and group manager initiates leave procedure; tree updates without the fallen node

The infrastructureless join and leave procedures require substantial extra work from the group manager OBU.

Note: The RSU must share the group key with any group it oversees. Either the RSU can be part of the tree-based group key generation scheme, being initialised into it, or joining it, as appropriate; or, the group manager can set up a secure channel using key exchange with RSU in order to send the group shared key to the RSU.

Sending messages

Messages must contain the pseudo-ID of the sender - this provides linkability - and pseudo-IDs must be updated periodically by RSUs (with a record of updates kept for tracing back to ID jointly with TA) and updates confirmed to the rest of the group under encryption of the current group key, so that the previous and new pseudo-IDs are linked and linkability is continuous for all those continuously in the group. This means that if an OBU were to leave the group and return to it later following a pseudo-ID update, it could not recognise the pseudo-IDs of any remaining group members since it would not have received the group key-encrypted pseudo-ID linking information while it was not a member of the group (i.e. had left the distance bound).

Safety messages take the form $(M, \{M\}_K, \{RID\}_K)$, where M is the information; K is the group key and RID is the pseudo-ID of the sender. In other words, the safety message is sent both as plaintext and under randomised encryption with the shared group key, and the pseudo-ID of the sender is sent under randomised encryption with the group key.

Pseudo-ID updates

In order to preserve unlinkability for vehicles who leave and then later return to the group the pseudo-IDs used for linking messages within the group must be periodically updated - this could be an update made on reaching a new RSU area. The current and new pseudo-IDs must be broadcast to the group, signed with the group shared key so that only members who remain in the group can link changing pseudo-IDs within the group. This retains the long-term unlinkability property: if two vehicles were to meet (and be part of the same group) twice, having separated in between, more than this time threshold for the updating apart, then one could not recognise the other from its pseudo-ID.

This procedure is given in further detail:

1) RSU sends new pseudo-ID to each OBU in the group simultaneously
2) Each OBU broadcasts $\{RID_1, RID_2\}_{GK}$ where RID_1 is their current pseudo-ID, RID_2 is their new pseudo-ID, and GK is the shared group key
3) Each OBU updates to its new pseudo-ID

VIII. Conclusions and further work

Continuous linkability gives a seamless flow of communication between vehicles, which is a better match for certain safety applications than previously-proposed linkability with broken transitions. Prior work in the area of linkability in vehicular communications protocols gives little consideration to the provision of such continuity. Distance-based linkability fits the safety and privacy requirements for the vehicular communications context more closely than time-based linkability, provides a more natural continuity of linkability for nearby vehicles than other time-based solutions, and is achievable using distance verification.

In this paper, we explained the need for continuity of linkability; explored approaches to defining the most fitting linkability properties for the context; and thus formulated a distance-based linkability with three components: short-distance linkability, long-distance linkability, and distance-based long-term linkability. We outlined two architectures for achieving continuous linkability in Section VII - one an extension of a previously-proposed protocol, and one a new protocol for providing the identified distance-based linkability properties.

As further work, we plan to give a formal definition of the three newly-proposed distance-based linkability properties, and to develop the outlined distance-based dynamic group protocol for use in vehicular safety messaging; providing the required linkability properties, as well as collaborative tracing, revocation and other required properties, as given in Section VII.

REFERENCES

[1] C. Sommer and F. Dressler. *Vehicular Networking*. Vehicular Networking. Cambridge University Press, 2014.

[2] Georgios Karagiannis, Onur Altintas, Eylem Ekici, Geert Heijenk, Boangoat Jarupan, Kenneth Lin, and Timothy Weil. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *Communications Surveys & Tutorials, IEEE*, 13(4):584–616, 2011.

[3] ETSI. Etsi tr 102 893 v1.1.1 (2010-03), technical report, intelligent transport systems (its); security; threat, vulnerability and risk analysis (tvra). 2010.

[4] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[5] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen. GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE T. Vehicular Technology*, 56(6):3442–3456, 2007.

[6] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, pages 41–55, 2004.

[7] Dan Boneh and Hovav Shacham. Group signatures with verifier-local revocation. In *Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004, Washington, DC, USA, October 25-29, 2004*, pages 168–177, 2004.

[8] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Pin-Han Ho, and Xuemin Shen. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. In *INFOCOM 2008. 27th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 13-18 April 2008, Phoenix, AZ, USA*, pages 1229–1237, 2008.

[9] Ahren Studer, Elaine Shi, Fan Bai, and Adrian Perrig. Tacking together efficient authentication, revocation, and privacy in vanets. In *Proceedings of the Sixth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON 2009, June 22-26, 2009, Rome, Italy*, pages 1–9, 2009.

[10] Albert Wasef and Xuemin (Sherman) Shen. EMAP: expedite message authentication protocol for vehicular ad hoc networks. *IEEE Trans. Mob. Comput.*, 12(1):78–89, 2013.

[11] Karim Emara, Wolfgang Woerndl, and Johann Schlichter. On evaluation of location privacy preserving schemes for vanet safety applications. *Computer Communications*, 63:11–23, 2015.

[12] Julien Freudiger, Maxim Raya, Márk Félegyházi, Panos Papadimitratos, et al. Mix-zones for location privacy in vehicular networks. 2007.

[13] Leping Huang, Kanta Matsuura, Hiroshi Yamane, and Kaoru Sezaki. Enhancing wireless location privacy using silent period. In *Wireless Communications and Networking Conference, 2005 IEEE*, volume 2, pages 1187–1192. IEEE, 2005.

[14] Chia-Ho Ou. A roadside unit-based localization scheme for vehicular ad hoc networks. *International Journal of Communication Systems*, 27(1):135–150, 2014.

[15] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo. The security and privacy of smart vehicles. *IEEE Security & Privacy*, (3):49–55, 2004.

[16] Network on wheels (now) german project website, http://www.network-on-wheels.de/about.html, (visited june 2015).

[17] Joo-Han Song, Victor WS Wong, and Vincent CM Leung. Secure location verification for vehicular ad-hoc networks. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5. IEEE, 2008.

[18] Adnan Abu-Mahfouz and Gerhard P Hancke. Distance bounding: A practical security solution for real-time location systems. *Industrial Informatics, IEEE Transactions on*, 9(1):16–27, 2013.

[19] Stefan Brands and David Chaum. Distance-bounding protocols. In *Advances in Cryptology—EUROCRYPT'93*, pages 344–359. Springer, 1994.

[20] Aurélien Francillon, Boris Danev, Srdjan Capkun, Srdjan Capkun, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *NDSS*, 2011.

[21] Jan Camenisch and Markus Stadler. Efficient group signature schemes for large groups (extended abstract). In *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, pages 410–424, 1997.

[22] Jan Camenisch and Anna Lysyanskaya. An identity escrow scheme with appointed verifiers. In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, pages 388–407, 2001.

[23] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Dynamic group diffie-hellman key exchange under standard assumptions. In *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, pages 321–336, 2002.

[24] Abhimanyu Kumar and Sachin Tripathi. Ternary tree based group key agreement protocol over elliptic curve for dynamic group. *International Journal of Computer Applications*, 86(7):17–25, 2014.

[25] Abhimanyu Kumar and Sachin Tripathi. A pairing free anonymous certificateless group key agreement protocol for dynamic group. *Wireless Personal Communications*, 82(2):1027–1045, 2015.

[26] Panos Papadimitratos, A La Fortelle, Knut Evenssen, Roberto Brignolo, and Stefano Cosenza. Vehicular communication systems: Enabling technologies, applications,

and future outlook on intelligent transportation. *Communications Magazine, IEEE*, 47(11):84–95, 2009.

[27] Communications in cooperative intelligent transport systems - calm for c-its, http://calm.its-standards.info, (visited june 2015).

[28] Evellyn S Cavalcante, André LL Aquino, Gisele L Pappa, and Antonio AF Loureiro. Roadside unit deployment for information dissemination in a vanet: An evolutionary approach. In *Proceedings of the 14th annual conference companion on Genetic and evolutionary computation*, pages 27–34. ACM, 2012.

[29] Po-Chiang Lin. Optimal roadside unit deployment in vehicle-to-infrastructure communications. In *12th International Conference on ITS Telecommunications, ITST 2012, Taipei, Taiwan, November 5-8, 2012*, pages 796–800, 2012.

[30] Javier Barrachina, Piedad Garrido, Manuel Fogue, Francisco J Martinez, J-C Cano, Carlos T Calafate, and Pietro Manzoni. Road side unit deployment: A density-based approach. *Intelligent Transportation Systems Magazine, IEEE*, 5(3):30–39, 2013.

[31] Arindam Ghosh, Vishnu Vardhan, Glenford Mapp, Orhan Gemikonakli, and Jonathan Loo. Providing ubiquitous communication using road-side units in vanet systems: Unveiling the challenges. In *ITS Telecommunications (ITST), 2013 13th International Conference on*, pages 74–79. IEEE, 2013.

[32] Ozan K Tonguz and Wantanee Viriyasitavat. Cars as roadside units: a self-organizing network solution. *Communications Magazine, IEEE*, 51(12):112–120, 2013.

[33] Wantanee Viriyasitavat and Ozan K Tonguz. Cars as roadside units: A cooperative solution. In *Vehicular Technology Conference (VTC Fall), 2012 IEEE*, pages 1–5. IEEE, 2012.

[34] Sok-Ian Sou and Ozan K Tonguz. Enhancing vanet connectivity through roadside units on highways. *Vehicular Technology, IEEE Transactions on*, 60(8):3586–3602, 2011.

[35] David Eckhoff, Nikoletta Sofra, and Reinhard German. A performance study of cooperative awareness in etsi its g5 and ieee wave. In *Wireless On-demand Network Systems and Services (WONS), 2013 10th Annual Conference on*, pages 196–200. IEEE, 2013.

[36] Johan Karedal, Nicolai Czink, Alexander Paier, Fredrik Tufvesson, and Andreas F Molisch. Path loss modeling for vehicle-to-vehicle communications. *Vehicular Technology, IEEE Transactions on*, 60(1):323–328, 2011.

[37] Etsi tr 102 638, “intelligent transport system (its); vehicular communications; basic set of applications; definition etsi specification tr 102 638, v.1.1.1, june 2009.