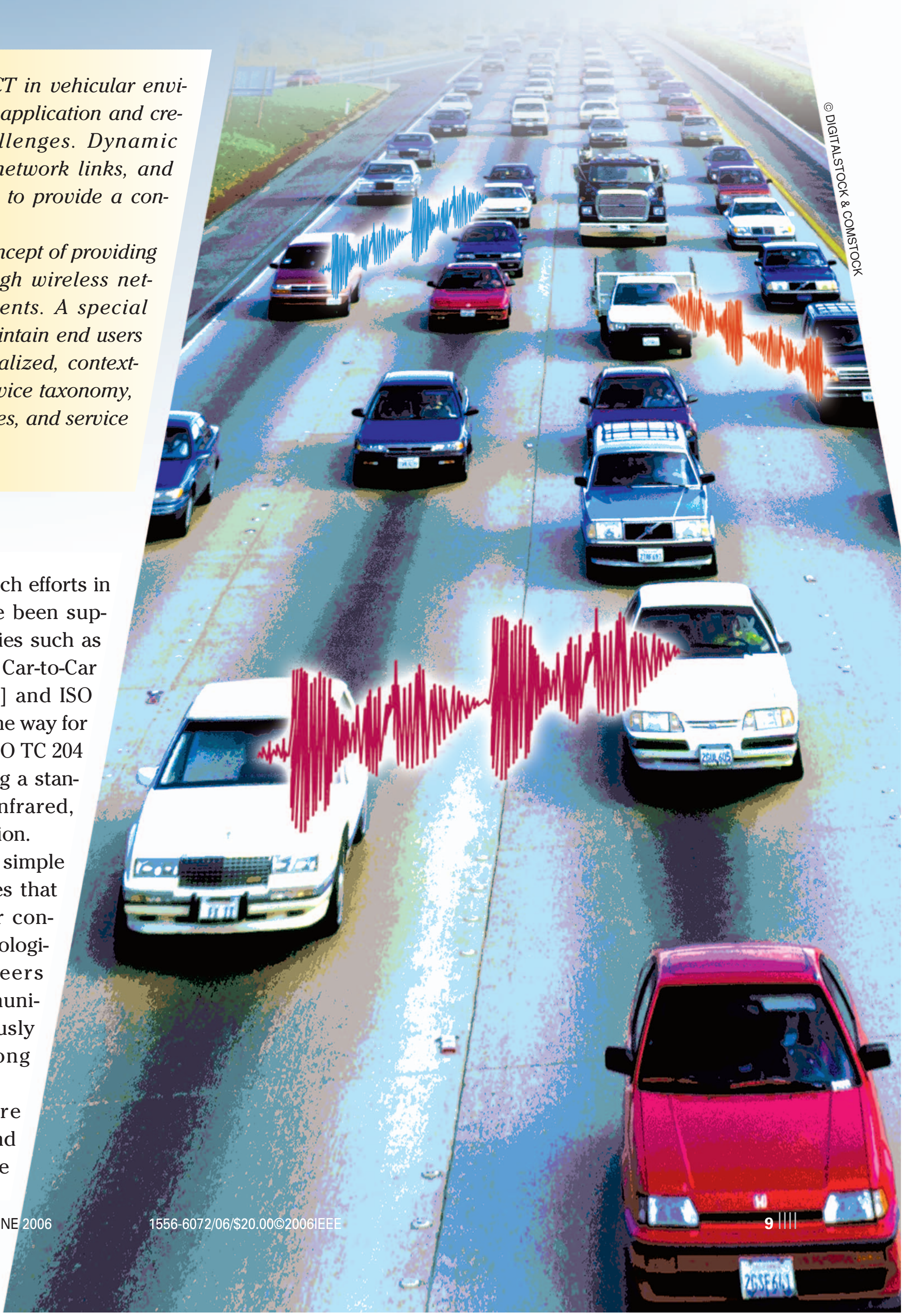
Trustworthy Applications for Vehicular Environments

Matthias Gerlach, Stephan Steglich, and Stefan Arbanowski, Fraunhofer FOKUS
Maarten Wegdam and Harold Teunissen, Bell Labs, Alcatel-Lucent

Abstract: *The integration of ICT in vehicular environments enables new kinds of application and creates new technological challenges. Dynamic network topology, unreliable network links, and moving terminals make it hard to provide a convincing end user experience.*

This article introduces the concept of providing trustworthy applications through wireless networks in vehicular environments. A special emphasis will be on how to maintain end users privacy when providing personalized, context-aware services. Therefore, a service taxonomy, enabling middleware technologies, and service enablers are introduced.



© DIGITALSTOCK & COMSTOCK

In the last couple of years, research efforts in vehicular ad hoc networks have been supported by standardization activities such as IEEE 802.11p and WAVE [1] the Car-to-Car Communication Consortium [2] and ISO CALM [3]. These activities pave the way for mobile applications in vehicles. ISO TC 204 CALM (CEN TC 278) is developing a standard which will merge Active Infrared, Microwave and GSM communication.

Available services range from simple voice communications to services that adapt to the location and other context of the user. The same technological developments let engineers combine intelligence and communication into cars that autonomously communicate on demand among each other.

Increasing congestion, more casualties, the increasing demand for information while on the

1556-6072/06/$20.00©2006IEEE

move, and the availability of wireless communication fostered activity to incorporate communication capabilities to vehicles.

At the same time, nomadic devices, such as PDAs (Personal Digital Assistants) and Smart Phones are becoming more powerful and include more powerful means of communication, like WLAN and cellular (e.g., CDMA2000 and GPRS/UMTS).

These developments will enable new applications that will integrate fixed and mobile services to increase both safety and comfort of drivers and passengers. This article focuses on trustworthy, privacy-sensitive, convenient and personalized applications, which will be crucial for the deployment and adoption of communications to and from vehicles in the near future.

Applications for Vehicular Environments

Developers of applications for mobile personalized environments can consider cars as increasingly intelligent:

- They *communicate*, either by means of cellular technologies, other infrastructure or ad hoc networks. Current initiatives in North America, Europe and Asia pursuit the deployment of communication facilities in cars.
- They *think*, because the capabilities of the in-vehicle computing systems are increasingly powerful, and make possible handling more complex algorithms.
- They *sense*, using the many sensors both on board of the vehicle and external ones. These sensors include positioning (such as GPS and eventually Galileo), temperature, velocity, and other on board sensors.
- They *act*. The different actuators can be classified as convenience actuators or safety-related actuators. Convenience actuators include the seat position, preferred radio station, air condition setting, and one day the interior look itself. Safety-related actuators are brakes, steering wheel, and the airbag trigger, for example. In-car networks make these actuators easily accessible to the applications.

As there are different applications that can be developed for vehicular environments, we provide a brief taxonomy of applications in the following sections.

Taxonomy

In contrast to the many existing transportation service centric classification, we provide a communication-oriented one. This way, applications can be developed/assessed with the respective constraints in mind.

Application Types

Applications in vehicular environments come from two directions: first the *transportation-related applications*. These are meant to increase the safety of the passengers while driving or cover other transportation-related aspects such as tolling or traffic management. One main class consists of (enhanced) safety applications. For example, some enhance the view of the driver by means of communication in order to avoid accidents.

Examples of safety applications are Cooperative Forward Collision Warning, Intersection Assistance, Extended Electronic Brake Lights. Many of these applications are currently developed worldwide.

Safety applications usually need many vehicles equipped with the communication system to work. Obviously, vehicle-based safety applications are most useful if every car has a communication device on board. This makes a deployment strategy necessary.

One strategy is by introducing vehicle-to-infrastructure based safety applications and installing the infrastructure at the same time. The VII (Vehicle Infrastructure Integration) initiative, a public private partnership [4], launched last year in the U.S. follows this approach.

Another strategy is to provide applications that are an incentive for the user to buy the communication system to speed up the deployment process. Such a strategy is followed by European projects such as the Network on Wheels [5] project.

This leads to the second category: the *convenience and personalized applications*. These applications are there to increase the comfort of the driver and the passengers. These applications do not rely on a certain market penetration of a particular communication system. This can be by means of enhanced information services, navigation system or personalized vehicle settings. Examples are Internet access, personalized information on the road, and the like. Convenience applications extend the reach of mobile services to the vehicles. In addition, new services can be created based on the context information available in vehicular environments, such group navigation (follow me), gaming (for the passengers), or location-based promotions.

Communication Types

Applications for vehicular environments can be classified according to the types of communication they use. The main efforts currently focus on IEEE 802.11-based communications in vehicular environments (the 802.11p standard, see [1]). The following main types of communications are foreseen to exist in vehicular environments.

- *Safety Communications* are typically small broadcast messages (less than 100 bytes) with low latency. They use a dedicated royalty free channel providing low latency communication, which has a higher priority than the other channels. Some types of safety communication also include geographic addressing as a main feature.
- *Cellular and Fixed Wireless Access (FWA) based Communications* like CDMA2000, GPRS/UMTS and upcoming WiMax/WiBro. These will probably provide the most reliable, yet currently the most expensive means of

communication. In many applications that do not rely on direct vehicle-to-vehicle communication to work, cellular based communication is seen as some kind of backup communication technology for deployment.

- *Multi-hop Communications* provide communication over unlicensed bands (e.g., ISM). Note that due to the dynamic nature of vehicular environments, multi-hop communication may be quite unreliable.

The availability of these different communication types, facilitates the integration vehicular environments with the surrounding infrastructure and makes possible many new applications as we will describe below.

Integration of Vehicular Environments

Depending on which domain you work in, you can look at vehicular applications in two different ways: first, you see the car as a moving multi-sensor device and as a part of a large-scale sensor network. Second you will see the vehicle as a "device" that is part of the mobile communication environment of the user. Both fit together perfectly. The latter makes use of the sensor network by requesting certain information. This context information might be provided by a single sensor or by a group of sensors that represent, e.g., the external temperature, the general traffic situation, or the temperature at the destination gathered by another vehicle.

The examples above illustrate why this kind of information is to be used for location-based and context-aware services. If available, context information is used to augment any kind of personal communication system. The challenges are: how to gather certain sensor values, even from (groups of) other vehicles, how to derive useful context information out of a set of gathered sensor values (fusion), and how to propagate derived context information to interested services and applications while ensuring security and privacy.

Middleware supporting Mobile Environments

Like many other business domains, the automotive domain is nowadays characterized by heterogeneous, distributed technologies. When building applications and services for the vehicular environment, a lot of effort usually goes into the integration of legacy technologies. Middleware technologies, as known from the IT-sector since the mid 90s, start to be applied to vehicular environments as well. Middleware tries to hide the peculiarities of underling legacy technologies to ease the service and application development by providing well defined standardized interfaces (APIs). There are some middleware technologies that are currently being deployed in vehicular environments such as the Open Services Gateway initiative (OSGi), Web Services/SOAP, pure http based protocols, and advanced vehicular busses like FlexRay, CAN, or MOST. These APIs simplify the development of advanced application and services supporting the different communication types and providing suitable access to the car's resources including sensors and actuators. The compatibility of the deployed technologies with existing Internet and telecommunication standards also opens new opportunities to a much broader community of developers and hence will foster the development of innovative applications. Still, the main challenge today is the implementation of trustworthy security and privacy mechanisms. Today there are several suitable middleware platforms for cars commercially available. The most important one is OSGi.

LIKE MANY OTHER BUSINESS DOMAINS, THE AUTOMOTIVE DOMAIN IS NOWADAYS CHARACTERIZED BY HETEROGENEOUS, DISTRIBUTED TECHNOLOGIES.

The OSGi specifications define a "standardized, component oriented, computing environment for networked services" [7]. Most important in OSGi is the framework, which specifies a runtime environment for service bundles. Life cycle management, dynamic loading and unloading of service bundles, dynamic service registration and deregistration are main features of OSGi. OSGi is being used in telematics platforms on vehicles for lifecycle management. Further, the current specification of OSGi, Release 4 targets mobile devices as well, thus spreading the availability of a standard platform for mobile services even more. It also supports state-of-the-art technologies such as http, UPnP, SOAP, and other services necessary for networking devices.

Personalization and Context-Awareness in a Mobile Environment

In the previous sections, we have described different type of car applications. In this section, the focus will be on personalized applications. These applications are able to provide services to users that are 'on the move [8]'. For example, at breakfast a user watches the news on the television. When he leaves for work, the news is seamlessly transferred to the in-car multimedia system where the news is continued (audio-only of course). More advanced are context-aware applications that exploit the user's (or car's for that matter) context to adapt the timing, quality and functionality of their services to the user situation and resource availability. Proactive applications are applications that provide services not in response to end-users' requests, but on their own initiative, based on context-dependent conditions that become or are predicted to become true. For example, the car starts to slow down because cars on the opposite site of the highway indicate an accident 1 mile forward. The combination of mobility, context-awareness and proactiveness enables a new class of personalized applications.

Providing Context Awareness

We follow the well known definition of context from Dey and Aboyd [9] that states that context is any information that can be used to characterize the situation of an entity. Examples of context information are location of the car, number of persons in the car, temperature in and outside the car, number of neighboring cars, etc.

In fact, a large number of context information sources can be identified, where only a limited number really make sense to realize deterministic context-aware applications. Therefore we consider two important aspects: context distribution and context reasoning. Security and privacy issues will be covered in a separate section.

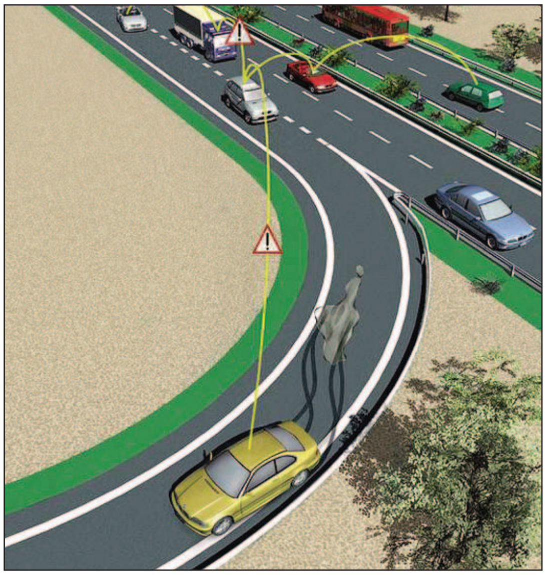


FIGURE 1 Example of a Pro-active application [2].

Context Distribution

Context sources are highly distributed and typically have a very dynamic behavior. The question is how to gather context information while limiting communication, and how to deal with the scalability and dynamicity characteristics.

Context sources include sensors in and around the car, navigation system, the user's mobile device, application servers (e.g., enterprise calendar, traffic service), and network servers.

Based on the context information needs of the applications, appropriate context sources needs to be discovered, and collected context information needs to be distributed to these applications so that they can adapt their behavior accordingly.

Context Reasoning

The raw context data is often too low-level and needs therefore to be interpreted to determine a certain state of the user or car. For example, higher-level context information like "accident ahead" or "driving home" can be derived from raw context information. This information can then be used by safety applications, e.g., slowing down the car, or can be used for convenience applications, e.g., informing the driver on the quickest alternative route home.

Gathering and reasoning about context information can violate the user's privacy, e.g., when this information is stored after usage or is associated to the user's identity. Another issue is the trustworthiness of the information that is derived.

Security and Privacy Issues

Users of applications for vehicular networks will only use a system they trust. From the users' point of view, the system can be trusted if it is available and reliable, protects the communication against modification and impersonation and guards the users' privacy.

Availability and reliability subsume the fact that a system works when needed. Privacy is the concept that the users have control over how their information is used, or as defined in 1890 the US Supreme Court Justice Louis Brandeis privacy as "the right to be left alone."

From these requirements, three fundamental security services can be identified. These are

- *Cryptographic Services*, using cryptographic algorithms that provide encryption integrity checking and signature functionality given the appropriate key material. Cryptographic services protect the integrity, authenticity and if necessary confidentiality and non-repudiation of given data.
- *Trust Establishment Services*, which includes managing trust relationships to peers, key management, certificate management, and checking the plausibility of messages, to name the most important.
- *Privacy Services*, i.e., measures to protect the information privacy of users within the network. Information privacy protects the fact of communication between two peers and the contents of communication. Of particular importance in vehicular networks is location privacy, which we will look at below.

The following sections describe the security services that should be provided by a middleware for vehicular environments.

Cryptographic Services

Given a properly installed and protected key, or a key pair, cryptographic services can provide integrity protection, authenticity, confidentiality, and non-repudiation. They are protective measures.

Cryptographic protection of payload can be done in virtually any layer of the protocol stack. Choosing the appropriate service depends on the level of interoperability, the requirements on the cryptographic algorithms concerning performance and overhead, and the types of communication supported.

For the higher layers, protocols, such as IPsec and https are available. For the lower layers, and specifically for vehicular environments, IEEE 1609.2 [1] defines certificate and message formats for signing and encrypting messages. Further, the standard mandates elliptic curve cryptography, which is efficient in terms of bandwidth and computation as the default asymmetric cryptographic primitive. As symmetric primitive, the advanced encryption standard (AES) is supported.

Trust Establishment Services

For cooperative applications, trust establishment between the peers is vital. Trust quantifies the expectation of a node on another's future behavior.

In this section, only the major possibilities for trust establishment are outlined. Trust refers to a specific expected action, with the consequence that the trust establishment mechanisms vary between the different layers in the protocol stack. Therefore, we focus on general aspects of trust establishment in this section.

Most protective measures in trust establishment are based on *certificates*. A node possessing a valid certificate signed by the trusted authority is automatically trusted. Certification can be centralized or distributed within the network. Certificates can also model centralized or distributed trust relations such as in PGP. The advantage of certification is the straightforward approach to trust management. The disadvantage is that a centralized infrastructure is usually required and that the approach stays and falls with the trust in the trusted third party. For vehicular environments, the IEEE 1609.2 standard defines a certificate-based framework for trust management. In addition, Hubaux et al. proposed different certificate based solutions for vehicular ad hoc networks in [10].

In ad hoc and peer-to-peer networks, *reputation systems*, where a node rates other nodes based on previous encounters can also be used to establish a trust relationship. A typical example for cooperative trust establishment is the eBay rating system. Unfortunately, these systems get better, the more ratings there are and may not work in the dynamic environments as found in vehicular networks. Reputation systems in vehicular networks have been looked at in [11].

Another way to detect malicious or faulty data coming from a peer node uses *plausibility checks*. Based on a-priory knowledge, a node can assess if the data it just got seem plausible or not. Similar to intrusion detection systems, this can be seen as a detection method, a typical reaction could then be to ignore these data. Plausibility can be based on quorums; if there is a dispute, the value backed by the majority of senders counts; alternatively a node can always assess a value based on its own measurements. One of the first papers proposing this for vehicular networks is due to Golle et al. [12].

For vehicular networks, in particular for the communication systems in these networks, there are still a lot of challenges: first, there is yet no approach to establishing some kind of certification infrastructure for vehicular networks. In particular, the different roles of the stakeholders in the process—the vendors of convenience applications, developers of transport related applications, the car manufacturers, and more—still have to be clarified.

IN VEHICULAR ENVIRONMENTS, WITH READILY AVAILABLE LOCATION TECHNOLOGY, LOCATION CAN BE USED IN A PLETHORA OF APPLICATIONS.

Second, security requirements for different applications are so diverse that it is difficult to specify these at the current point in time. In order to alleviate this problem, it may be prudent to design a security middleware providing the general functionalities defined in this section as services within the OSGi framework. A modular approach, however introduces a more complex system, which may be harder to design securely.

Finally, detection mechanism, and reactive measures, be it revocation of certificates, ignoring their data are still at their infancy—for static networks such as the Internet. Clearly, these mechanisms may be harder to develop for the highly dynamic and large networks found in vehicular environments.

Privacy Services

The offering of personalized applications that take the location and other context into account brings inherent privacy issues to vehicular networks and applications.

There are three aspects of information privacy: in the first place the protection of the fact of communication, which is often denoted as *unobservabilty* [13].

Second, the identities of the communicating peers and the link between the peers. This is often referred to as *sender anonymity*, *receiver anonymity*, and *unlinkability* between sender and receiver. Unlinkability sometimes also refers to linking messages from the same sender depending on the context.

Thirdly, the protection of the contents of communication. While this is easily achieved when all communication peers are known and trusted, it becomes a problem in open and untrusted environments such as found for vehicular applications. Worse yet, some parts of the system rely on publicly disclose d data. All these information can easily be used to build profiles of people without their consent. One of the main concerns in this context is the notion of *location privacy*, defined as the "ability to prevent other parties from learning one's current and past location" [14].

In vehicular environments, due to the readily available location technology, the location is used in a plethora of applications.

For example, geo-based routing protocols for vehicular ad hoc networks periodically send out messages containing

LOCATION PRIVACY MEANS INHIBITING UNCONTROLLED PERMANENT IDENTIFICATION AND RE-RECOGNITION OF SENDERS AND TRACING OF MOVEMENTS USING PUBLIC INFORMATION.

their position information [15]. Further, location-based applications such as point of interest notification may rely on interest profiles sent out by the vehicles.

The question may be raised about the difference vis-à-vis currently employed technologies and how low their privacy provisions are—and why people will care about privacy in vehicular environments. Most of the technologies mentioned in this context, like Customer Cards, mobile phones, RFID tags, can be controlled by the user. It is still possible to switch off your mobile phone, not to use your Customer Card, or not to buy at the store which uses RFIDs. In future vehicular environments, communication will be an always-on feature.

Also existing systems are mainly incompatible and hence prevent large-scale data mining; that will certainly change with the increasing use of standardized technologies.

In addition, the unprecedented accuracy of location technologies in combination with ubiquitous communication mechanisms facilitates seamless surveillance opportunities.

In a nutshell, to protect the privacy of the users we must ensure *location privacy* and *user controlled information disclosure*.

Note that privacy measures can conflict with the objective of a smoothly working system; hence, often a trade-off must be found between functionality and privacy.

User Controlled Information Disclosure

For user acceptance, users need to be in control of the release of privacy sensitive information to other parties [16]. Others can be other users or service providers such as point-of-interest providers. Willingness to share privacy-sensitive information depends on the amount of trust the user has in the inquirer of the data, how privacy sensitive the user considers the data and the usefulness of the application [17]. Appropriate trust establishment measures as part of cryptographic services can be used to establish the trust relationship. How privacy-sensitive the privacy-sensitive information is, is different for different users, but in all cases the privacy-sensitive information should be made less privacy-sensitive if possible for the specific application. This means that the data should be disassociated from the user by the use of pseudonyms or by providing complete anonymity, and that the context information should be made less privacy-sensitive by reducing it in quality. For example, a location-based application that warns drivers of upcoming bad weather should receive the location of the car at region-level accuracy even though it is available with GPS accuracy. Since location privacy is especially important and difficult to realize, we discuss this separately below.

User controlled information disclose does not prevent the receiving party from using the data in a malicious way, but is gives the user the choice, as in the Customer Card example.

Location Privacy

Location information can be used to identify a user, or to track the user's movements. Tracking and re-recognition can be based on identifiers and addresses, or simply by correlating position and time information in messages when no identifiers are available.

Location privacy means inhibiting uncontrolled permanent identification and re-recognition of senders and tracing of movements using public information. This is often measured by stating the size of the anonymity set, which was first introduced by Chaum [18]. For example the sender anonymity set is the set of potential senders of a message. The bigger this set is, the harder it is for an attacker to determine who sent a message. This holds true as long as the properties of nodes as evenly distributed. For situations, where this is not the case, e.g., restricted movements on the road, a different metric has been proposed: entropy. Based on the probability distribution for users to assume a certain role in the system, entropy measures the degree of uncertainty of an attacker to assign a role to a user [19].

Different location privacy preserving techniques have been proposed. Pseudonym based solutions are used in systems, where addressability, liability, and accountability may be an issue. Doetzer [11] proposed a system where pseudonyms are changed frequently to avoid location tracking. A straightforward solution for changing pseudonyms may not yield appropriate anonymity, as pointed out by Beresford in [14]. The authors therefore propose mix-zones, where many nodes change their pseudonym at the same time.

MIX-based solutions require setting up a trusted entity as an anonymizer and encrypt all communication. Mixes are central instances, which act as a trusted proxy covering the real identity of a sender in the communication process. Huang et al. [19] proposed such a solution based on dynamic clustering. Their solution suffers from the problem that a cluster-head is not always easily found, and that it must be trusted but will probably be an ordinary node.

To make tracking and identification by means of additional information harder, Gruteser et al. propose to decrease the accuracy of time and location information for location based services [20]. Note that the authors assume a system, where no identifiers or addresses are used.

Summary

Providing trustworthy applications in vehicular environments is not as easy as one can think of. In this paper, we outlined the difficulties with respect to different application and communication types. A special emphasis has been given to personalization and context-awareness that add another dimension of complexity to the problem space. Applications using these aspects require a certain amount of information about end users.

This leads to the paradox where protecting the end users' privacy makes it harder to provide these convenient applications. The concept for creating trustworthy application is proposed that makes a compromise between these two extremes. Still, an application might provide other means to negotiate level of non-privacy with the end user for certain situations.

Acknowledgments

This work has been carried out within the Freeband Awareness project and the Network on Wheels project.

The Network on Wheels project is supported by the German Ministry for Education and Research (BMB+F) under Contract No. 01AK064F.

The Freeband AWARENESS project (http://awareness.freeband.nl) is sponsored by the Dutch government under contract BSIK 03025.

Author Information

Matthias Gerlach is working towards his Ph.D. at Fraunhofer FOKUS in the field of security in wireless ad hoc networks in vehicular environments. His particular interests are security solutions for constrained environments with a focus on privacy.

Stephan Steglich, Ph.D. is Assistant Professor at Technical University of Berlin and director of the Competence Centre Open Communications Systems at Fraunhofer FOKUS. His fields of interest include personalization, context-awareness, user-interaction, adaptive systems, and reflective middleware. Stephan is managing several international and national level research activities and has been an organizer and a member of program committees of several international conferences.

Maarten Wegdam, Ph.D., is senior member of technical staff at Bell Labs, Alcatel-Lucent in The Netherlands. His fields of interest include middleware, QoS in middleware, context-awareness and privacy aspects of context-awareness. Maarten is currently project manager of the Freeband AWARENESS project (http://awareness.freeband.nl). He has a part-time position as Assistant Professor at the University of Twente.

Harold Teunissen is Research Manager at Bell Labs, Alcatel-Lucent in The Netherlands. He received his M.Sc. in computer science from University of Twente. His field of interest includes wireless mesh networks, p2p services and next generation service lifecycle management. Harold is member of the WWRF steering board and participates in various European coordinated initiatives.

Stefan Arbanowski, Ph.D. is director of the Competence Centre Smart Environments at Fraunhofer FOKUS. He received his Ph.D. and M.Sc. in computer science from the Technical University Berlin. Beside telecommunications and related research areas, such as Distributed Computing and Middleware Technologies, he has extended knowledge in the fields of Intelligent Networks and Mobile and Personal Communications. He is active in the WWRF and chairman-elect of the WWRF Working Group 2 for 2004–2005.

References

[1] Wireless Access in Vehicular Environments. IEEE 802.11p and the 1609 suite of Draft standards: standards.ieee.org/catalog/olis/vehicular.html.

[2] The Car-to-Car Communication Consortium (C2CC). http://www.car-to-car.org.

[3] ISO TC 204 CALM (CEN TC 278): http://www.tc204wg16.de/Public/CALMintro.html.

[4] VII Home: www.its.dot.gov/vii.

[5] The Network on Wheels (NOW) Project. NOW website, 2004. http://www.net-on-wheels.de.

[6] W. Drytkiewicz, I. Radusch, S. Arbanowski, and R. Zeletin: pREST: A REST-based Protocol for Pervasive Systems, 1st IEEE International Conference on Mobile Ad-hoc and Sensor Systems, Oct. 24–27 2004, Ft. Lauderdale, USA.

[7] OSGi Home: www.osgi.org.

[8] Freeband AWARENESS project, D1.3v2, Overall architecture of the AWARENESS infrastructure, http://awareness.freeband.nl, Dec. 2005.

[9] A.K. Dey and G.D. Abowd, "Towards a Better Understanding of Context and Context-Awareness." In the Workshop on The What, Who, Where, When, and How of Context-Awareness, as part of the 2000 Conference on Human Factors in Computing Systems (CHI 2000), The Hague, The Netherlands, Apr. 3, 2000.

[10] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security and Privacy*, vol. 4, no. 3, pp. 49–55, 2004.

[11] F. Dötzer, L. Fischer, and P. Magiera. Vars, "A vehicle ad-hoc network reputation system," In *Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, 2005.

[12] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," In *Proceedings of the first ACM workshop on Vehicular ad hoc networks*, pages pp. 29–37, 2004.

[13] A. Pfitzmann and M. Hansen, "Anonymity, unobservability, and pseudonymity—a proposal for terminology," Technical report, TU Dresden, 2005.

[14] A.R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, pp. 46–55, 2003.

[15] M. Mauve, J. Widmer, and H. Hartenstein. A survey on position-based routing in mobile ad hoc networks, 2001

[16] S. Lederer, J.I. Hong, A.K. Dey, and J.A. Landay, "Personal Privacy through Understanding and Action: Five Pitfalls for Designers," *Personal and Ubiquitous Computing*, vol. 8, no. 6, pp. 440–54, Nov. 2004.

[17] L. Barkhuus and A.K. Dey, "Location-Based Services for Mobile Telephony: a study of users' privacy concerns," *Proceedings of Interact 2003*, Zurich, Switzerland.

[18] D. Chaum, "The dining cryptographers problem: unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, 1988.

[19] L. Huang, K. Sampigethaya, K. Matsuura, R. Poovendran, K. Sezaki, and M.L. Caravan, "Providing location privacy for vanet," In *Proceedings of Escar 2005*, 2005.

[20] M. Gruteser and D. Grunwald, "Anonymous usage of location based services through spatial and temporal cloaking," In *Proceedings of the ACM MobiSys*, 2003.

VT