TECHNICAL CONCEPT AND PREREQUISITES OF CAR-TO-CAR COMMUNICATION

Timo Kosch
BMW Group Research and Technology
Hanauer Strasse 46, 80992 Munich, Germany
Tel. +49 - 89 - 382 - 41107 E-mail: Timo.Kosch@bmw.de

SUMMARY

In the past few years a development of wireless local information exchange between the vehicle and its environment from classic DSRC systems towards more general multi-hop ad-hoc networks could be observed [2, 13]. While the earlier DSRC systems were designed for electronic toll collection or platooning, the recent more general ad-hoc network approach is not specially tailored to a certain application area. It is based on now widely available components off the shelf like Wireless LAN radio technology, even though this technology needs some adaptation to meet the requirements of ITS applications, as addressed e.g. by the Vehicle Safety Communication (VSC) project in the US and by a number of research projects in Europe on a European and on a national level. This article provides an overview on the prerequisites of Car-to-Car Communication and interesting technical concepts identified by the Car-to-Car Communication Consortium.

INTRODUCTION

Connecting vehicles with their direct environment enables a new range of applications and improves existing applications by providing very precise information. The resulting vehicle ad-hoc network (VANET) poses many interesting technical challenges. After years of research, the fog around many of the underlying technologies and technical concepts has somewhat lifted. However, certain problems still need to be overcome in order to make wireless short range communication in the automotive world a reality. Among the most important is the need for standardization. Most of the applications need a certain penetration rate of vehicles participating in the network in order to work properly. Vehicles of different manufacturers need to exchange data in order to reach this penetration rate. The goal of the Car-to-Car Communication Consortium is to standardize the interfaces and protocols in order to make the vehicles of different manufacturers interoperable. This article describes the technical approach of the Car-to-Car Communication Consortium. It provides an overview of the state of the art in the field, pointing out concepts and technologies that have been developed or identified by the Consortium and assessed as necessary building blocks for a standard. Beginning with an overview of the very diverse requirements of a heterogeneous landscape of applications that become possible, the major technical elements are described.

SUPPORTING THE REQUIREMENTS OF HETEROGENEOUS APPLICATIONS

Short range communication based on Wireless LAN technology can support many different kinds of applications. Figure 1 shows a number of possible applications. Car-to-Home applications, that make use of a Wireless LAN connection between the vehicle and a home network to transfer for example MP3 files to the vehicle, can be realised regardless of whether any other vehicle is also equipped with communication technology. We classify these types of applications as *deployment applications* since they can support the deployment phase of Car2Car technology, providing customer benefit independent of the overall penetration rate of the technology in other vehicles. This, however, is not true for most of the other listed applications. Applications that provide *driver information based on car-to-car communication* require some low to medium penetration rate (simulation suggests that in many cases, around 10% penetration rate would be sufficient [17]).

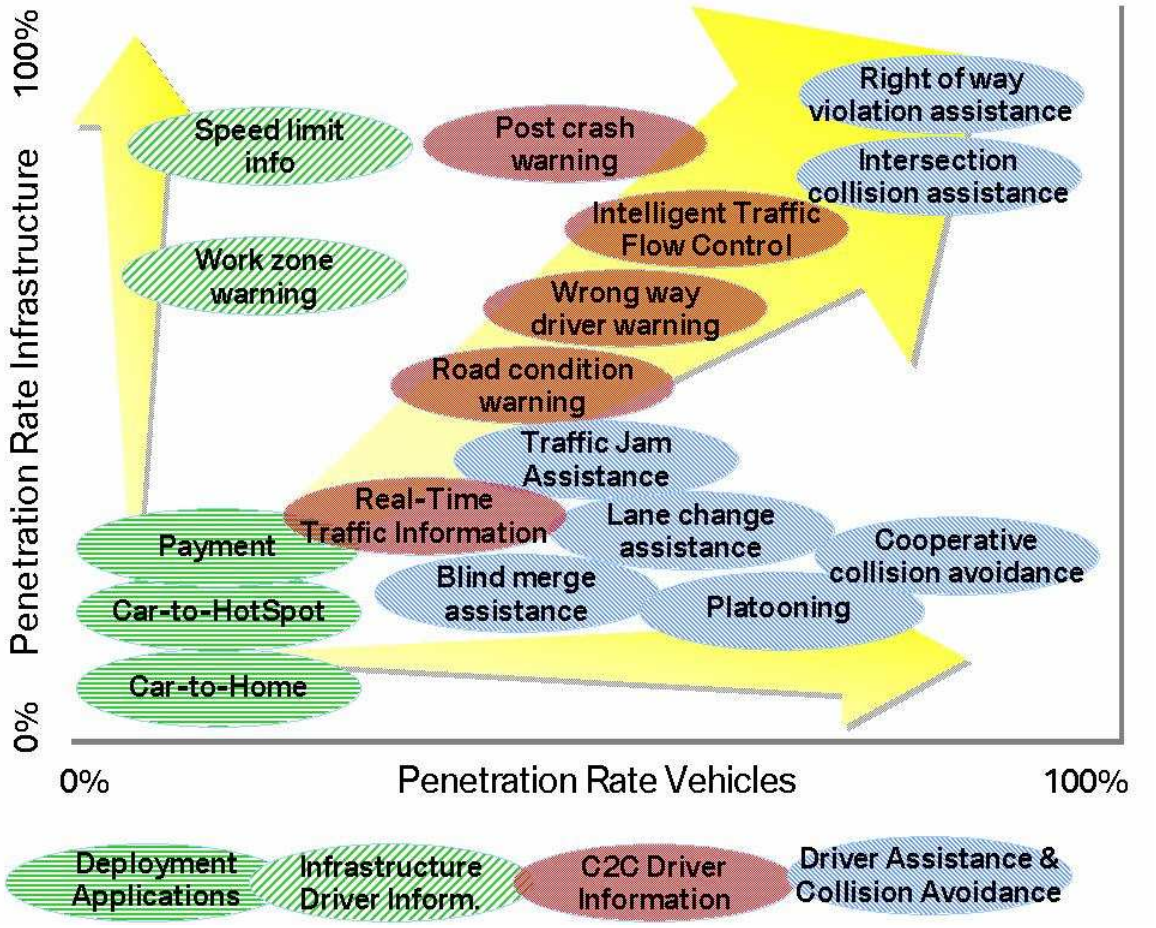

Figure 1: Necessary vehicle and infrastructure penetration rates for different kinds of applications

Driver information applications can also make use of information provided by road-side units. For these *infrastructure driver information* applications, a certain penetration of infrastructure units is necessary. Payment in parking lots for example requires at least a few parking lots to

extend their payment system by wireless communication. Collision avoidance in complex scenarios like intersections will most likely only be feasible with a combination of car-to-car and car-to-infrastructure communication and will require high penetration rates of both infrastructure units and on-board units. *Driver assistance and collision avoidance* applications generally require a high penetration rate, up to an almost full penetration.
The requirements of these four classes of applications[1] shown in Figure 1 are differing with respect to many technical issues. Deployment applications require Internet Protocol (TCP/IP) support and high data rates for bursty or streaming data traffic. Car-to-car driver information applications require the vehicles to send sensor data and the network to route this data. The information in the messages needs to be correct and trustworthy and the privacy of the participants needs to be ensured. Infrastructure-assisted warning and driver information applications require interoperability of infrastructure nodes with mobile ad-hoc nodes. Driver assistance and collision avoidance applications pose high requirements on allowable packet latency and packet loss. The network must be highly reliable, secure and support many nodes to access the channel with relatively small but frequent data packets at the same time.

THE APPROACH OF THE CAR-TO-CAR COMMUNICATION CONSORTIUM

The C2C-CC aims at standardizing a vehicle ad-hoc network, i.e. a decentralised communication system. Standardizing the way data is transmitted and forwarded ensures interoperability on the network side. This alone is not enough, however. C2C-CC nodes need to be cooperative, i.e. not only do they need to follow a specific protocol, but they must show cooperative behaviour. Additionally, C2C-CC nodes need to ensure a certain Quality of Service level, e.g. a minimum latency when sending or forwarding messages.

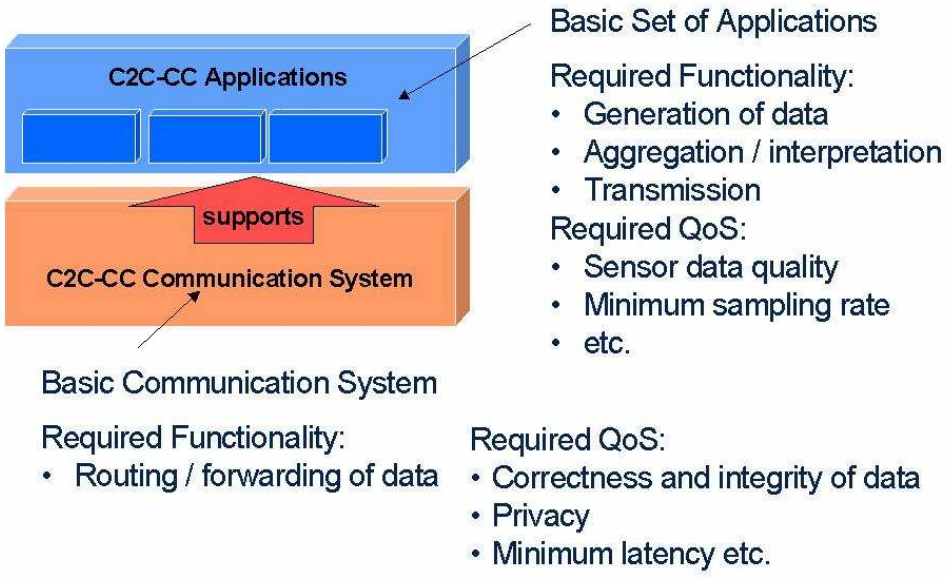

Figure 2: Standardization of the C2C-CC system: Basic Set of Applications, Basic Communication System and necessary QoS

[1] the ones denoted by italic letters in the previous paragraphs and shown under the application matrix in Fig. 1..

Consequently, in addition to the communication system, a basic set of applications and their corresponding protocols need to be standardized, too (see Figure 2). Local hazard warning, for instance, will only work if a high number of nodes participate. These kinds of applications need to be supported by every C2C-CC node. C2C-CC will define a basic set of applications that must be implemented in any participating node. Additionally, a certain Quality of Service must also be guaranteed by the applications, e.g. all nodes need to send specific sensor data at a minimum sampling rate and quality level. Vehicle integration per se is not addressed by the C2C-CC and is up to the individual car manufacturer. However, a certain set of preconditions must be fulfilled in order to install a C2C-CC system into a vehicle. This mainly involves the availability of a basic set of sensor data, quality and security issues.

SYSTEM ARCHITECTURE FOR CAR-TO-CAR COMMUNICATION

The overall structure of the C2C-CC system is shown in Figure 3. Directly reflecting the differing requirements of two of the main application types – comfort and safety applications - are two separate networking protocol stacks in the network layer which are supported in parallel by the C2C-CC architecture: TCP/IP addressing and routing and geographical addressing and routing. In order to support comfort and entertainment applications that either require Internet access or use components that build upon Internet technology and protocols, a TCP/IP stack is supported by the C2C-CC system. Safety applications on the other hand are usually broadcast type of applications. They neither need the addressing mechanisms of IP nor are the Internet routing protocols suitable for them. Thus, safety applications are directly supported by specific C2C-CC network protocols.

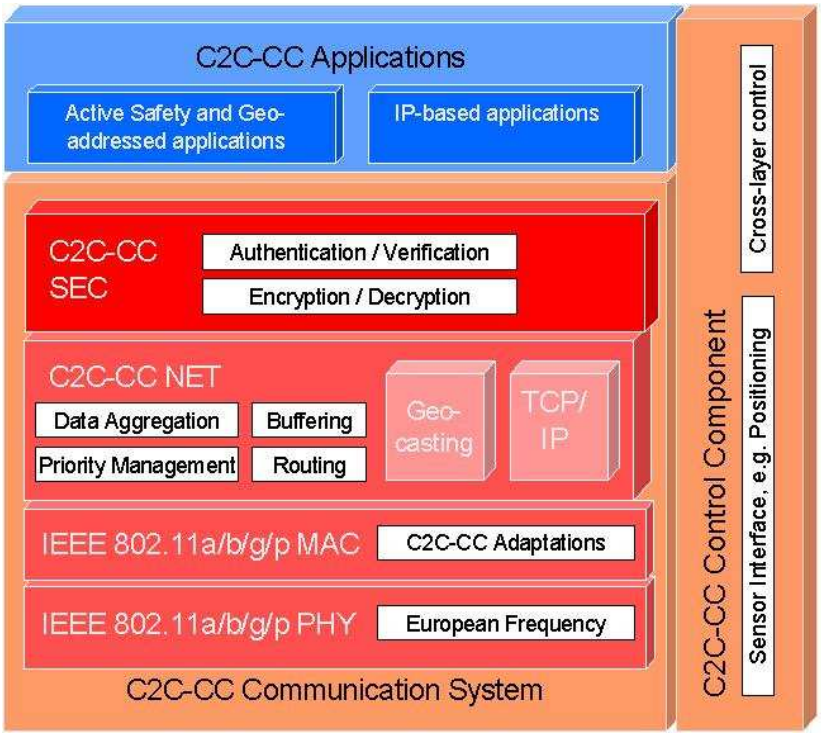

Figure 3: C2C-CC System Components and Functionality

NETWORKING

The ad-hoc network formed by car-to-car communication needs special routing mechanisms both for IP and non-IP traffic as well as for both point-to-point and point-to-multipoint communication. C2C-CC will support specific routing and forwarding schemes. The according functionality is provided by a routing component which is located underneath the IP layer. The task of the C2C-CC network layer is to deliver packets to recipients addressed according to the C2C-CC addressing scheme, supporting IP addressing and geographical addressing. From the IP layer's point of view, the C2C-CC network layer is an IP subnet.

For deployment applications and C2C personal communications and entertainment, the TCP/IP protocol will be supported, both in a single-hop and in a multi-hop fashion. For this point-to-point multi-hop communication, nodes are addressed by their C2C ID or IP address, respectively. Since C2C nodes are mobile, a lookup service is necessary in order to locate the addressed node. Such a lookup service will be supported by the C2C Network Layer [7, 8].

In order to support multi-hop routing, the C2C-CC networking makes use of positioning capabilities inside the nodes. All C2C nodes are able to determine their position. Based on this position, a greedy forwarding scheme is used to forward a packet to its destination, i.e. of all nodes within communication range of a sender, the C2C node which is closest to the destination is chosen to forward a packet. The behaviour is similar to the greedy perimeter stateless ad-hoc routing protocol (GPSR) which also chooses the node closest to a destination node to route packets [14]. This greedy technique is also useful for C2C communication [10]. However, in real C2C networks, packets routed in a purely greedy fashion can be lost. Especially city scenarios with obstructions by buildings are complex. Research has provided a number of ideas how to tackle this problem [15, 18].

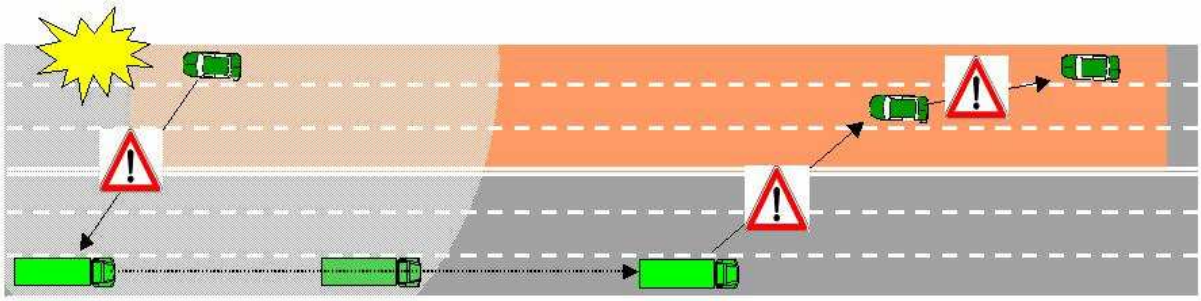

Figure 4: Geocasting and store & forward mechanisms

In order to know their network neighbours, C2C-CC nodes periodically transmit beacons. Those beacons are primarily used for routing and forwarding purposes. For this, a specific frequency of beacon sending in the order of approximately one second seems reasonable. The spatial resolution of vehicle positions that can be reached by this sample rate, however, is not fine grained enough for many safety applications. Every node implements a neighbour table that reflects the information received by beacon messages. Additionally, contention-based forwarding mechanisms are under consideration [3, 9].

Multi-hop point-to-point communication supports a number of interesting applications. For driver information, assistance and collision avoidance applications, which are the one's with the most

expected traffic efficiency and safety effect, usually more than one single car is interested in the information. Group communication techniques are needed to route the information from those vehicles or infrastructure nodes that can provide useful information to those for which it is valuable. Infrastructure and C2C driver information applications usually address vehicles in specific regions. Therefore, the C2C-CC network supports geobased addressing [6]. Figure 4 visualizes the concepts of geographical addressing and store & forward of messages on the road. In general, it is possible to address all vehicles in a specific area (Geocasting [19]), one particular vehicle in the area (Geounicast) or some but at least one vehicle (geoanycast). For data packets to potentially be forwarded to all of the addressed vehicles, a multihop forwarding mechanism is needed and supported. This multihop forwarding also makes use of the greedy forwarding approach in order to avoid flooding of the network. In this case, however, instead of the remaining distance to a destination node, the distance from the last forwarder is taken as a measure for re-broadcasting a packet. In order to allow for a 2D dissemination, more than one node re-broadcasts a packet. Based on the availability of additional information from a map or beaconing, different strategies can be used by the nodes to decide whether to forward a given packet [16]. The effect of this efficient forwarding approach is shown in Figure 5. In sparse networks and in order to support a message to sustain in an area for a certain time, store and forward schemes are used. The data packets can contain explicit lifetime information. As long as a packet is still valid, it will be delivered to vehicles in the addressed area. If no neighbour vehicle is available, which is a likely event especially in the introduction phase of the C2C-CC system, a packet is stored and forwarded as soon as a new vehicle gets into reach which is detected by the beaconing mechanism.

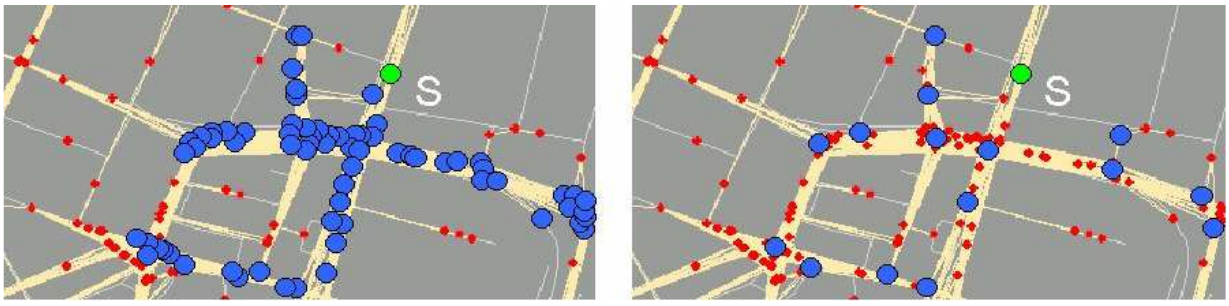

Figure 5: Efficient Message Propagation

C2C-CC standardizes the network protocols, the rules of behaviour required to be followed by each C2C-CC network node and the interfaces of each C2C-CC communication layer as its Service Access Point(s). Figure 6 shows the two Service Access Points of the C2C-CC network layer providing the interface to send and receive geoaddressed data or IP addressed data. The network layer uses the services of the MAC to transmit these IP and non-IP packets as well as additional control packets like beacons, needed to fulfill the network layer's routing and forwarding tasks.

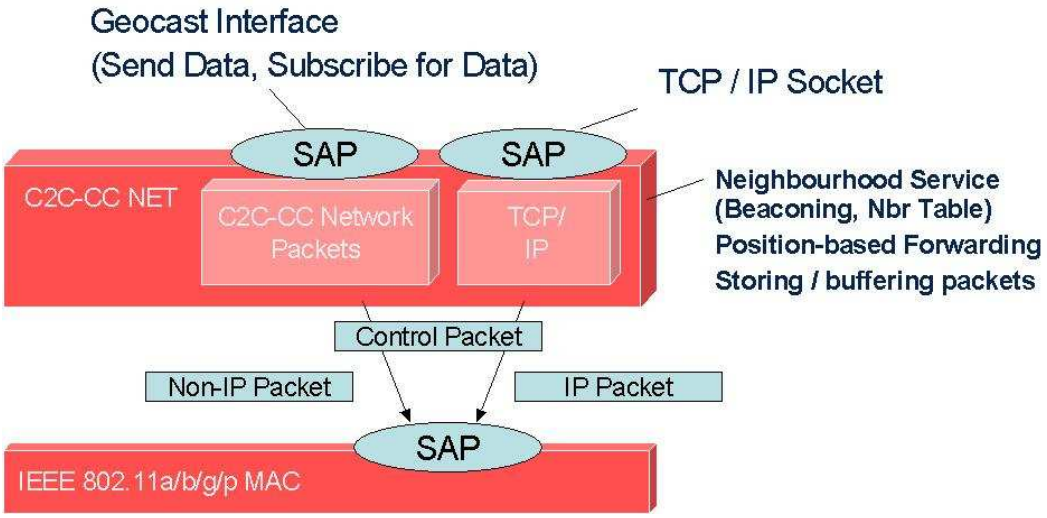

Figure 6: NET and MAC Interfaces as Service Access Points

RADIO TECHNOLOGY

The allocation of the 5.9 GHz spectrum for DSRC applications by the US FCC initiated intensified research on a decentralized medium access control for DSRC. Early on, the activities were heading towards standardization, facilitated by the choice to build upon existing WLAN technology following the 802.11a standard. The former WAVE study group within 802.11, meanwhile better known as the 802.11p working group to which it officially became in November 2004, has discussed DSRC specific adaptations of IEEE802.11a. The C2C-CC has decided to build upon this technology for several reasons:

1 tests have shown suitability for automotive domain
2 802.11 WLAN is a relatively mature technology
3 compatibility with existing hardware and infrastructure
4 international harmonization

Safety applications are based on 802.11p and will need an exclusive frequency in Europe, as well. In order to support home and Hot Spot access, the modems will need to also support at least one other WLAN technology (802.11a/b/g or else). This means that a switching between frequencies needs to take place or the modems must be able to support both modes in parallel.

For driver assistance and collision avoidance applications, it is important to have very precise information about the direct surroundings of a vehicle. Compared to driver information, these kinds of applications usually need information from a closer environment, but with much higher precision and reliability. In order to achieve this, the beaconing which is basis for the multihop network needs to be much more frequent. Vehicles need to report their positions, headings, velocities and possibly other sensor data more often than every second (seeFigure 7). the main challenge is the scalability of the medium access control layer. This is a major challenge for the medium access.

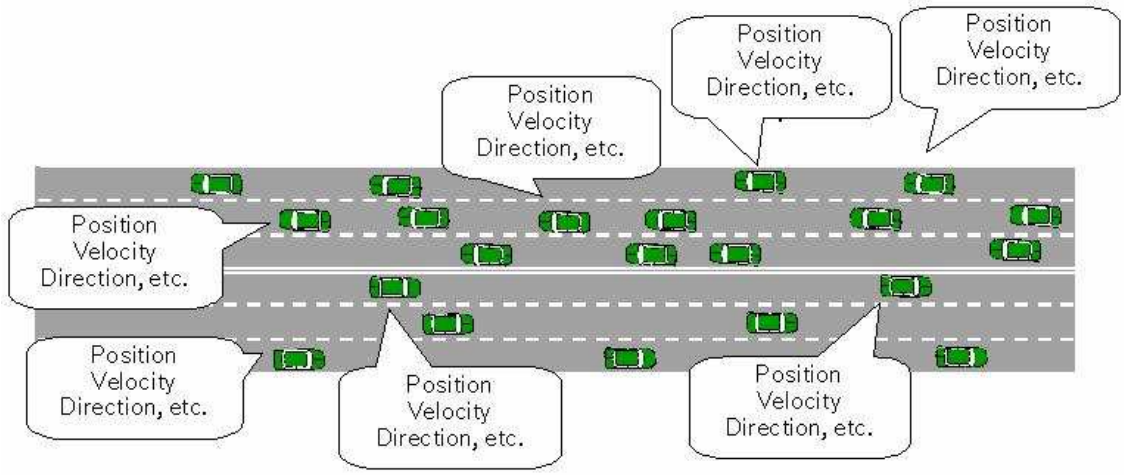

Figure 7: C2C-CC Decentralized Traffic and Safety Communication

SECURITY

Securing car-to-car communication is an indispensable prerequisite for its deployment and real-world use. Three major goals need to be achieved:

1. All information communicated in the network needs to be correct and trustworthy.
2. The C2C-CC system must be extremely robust and must not fail to work.
3. The C2C-CC system participants' privacy must be ensured.[2]

In order to achieve the first two of these goals, the C2C-CC network must be protected against different kinds of attacks. Analysing the threats for this special kind of network, Denial of Service attacks, generating fake messages or tampering with messages need special consideration. It is extremely important to ensure message integrity - a risky driving manoeuver based on false message information might be fatal - while sender authentication is not needed in many cases.

For the assistance and collision avoidance types of applications, the C2C-CC security solution must still allow low latency communication. This is an important requirement since applying cryptographic methods can create considerable computing overhead. Hence, it is not possible to adopt security protocols involving strenuous verification or interaction processes.

For the C2C-CC system, we aim at building upon existing concepts, methods and algorithms. Necessary extensions and adaptations are considered within research projects. Some of the promising approaches considered by the C2C-CC [22] are briefly outlined in the following paragraphs.

Certificate-based schemes are promising candidates. A PKI Certificate is a document that could be issued to any C2C-CC node by a Trusted Third Party. It carries a Public Key acting as a logical identity for the node it is issued to. It is not required for all nodes to maintain connectivity with the Trusted Third Party, yet it is required that nodes in the network establish connectivity to the Trusted Third Party from time to time in order to receive certificate updates as well as information about black-listed certificates (certificate

[2] In many cases, VANET applications communicate personal data, such as current location or current speed, which could be used for vehicle / driver profiling.

revocation list).

When authenticating itself to other nodes, a trust candidate node submits its PKI Certficate. The node receiving this certificate trusts the Trusted Third Party which created this certificate and therefore is able to verify that this certificate is indeed created by the Trusted Third Party. If yes, then the node could be confident that any cryptographically signed message it receives from the trust candidate that can be decrypted with the public key mentioned within the certificate could only be sent by the trust candidate. Encrypting messages with private keys does not usually protect privacy. However, anonymous certificates can be created by certificate issuers using blind signatures [4]. Blind signatures allow a certificate issuer to digitally sign a certificate without knowing the content of the certficate.

The US VSC Consortium introduced another approach [21], granting a higher degree of unlinkability than in the sole anonymous certificate approach. In this system, each on-board unit (OBU) *Ui* has it's own long term symmetric key *K*i. The Trusted Third Party which acts as a Certificate Signing Authority (CA) maintains a global mapping of OBU identity to *K*i. In order to get a certificate, an OBU must engage in an interactive protocol with the CA.
Logically, this protocol has four stages:

1. *Ui* demonstrates possession of *Ki* to the CA, perhaps by signing an initial challenge.
2. *Ui* generates *k* key pairs *I1, I2,. . ., Ik* .
3. The CA blind-signs certificates for all *k* keys. Each key has a one day validity window.
4. *Ui* un-blinds the certificates.

After this exchange, *Ui* has *k* days worth of certificates. It uses one certificate per day until all the certificates have expired, at which point it must re-run the protocol to get a new batch of certificates.

Another interesting approach is is the use of zero-knowledge mechanisms. Zero-knowledge proofs (ZKPs) are proofs that convince a verifier of the truth of an assertion and yet yield nothing beyond the validity of it (also refer to [11]). ZKPs were firstly introduced by Goldwasser, Micali and Rockoff [12]. Thus, the zero-knowledge protocols require parties to provide zero-knowledge proofs of the correctness of their secret-based actions, without revealing these secrets.
Traditional simple zero-knowledge proofs have three main characteristics:

1. *Interaction*: The prover and the verifier talk back and forth
2. *Hidden Randomization*: The verifier tosses coins that are hidden from the prover and thus unpredictable to him
3. *Computational Difficulty*: The prover embeds in his proofs the computational difficulty of some other problem

If the prover is not malicious and really knows the secret, he will always be able to answer the randomization based questions of the verifier. So-called simulators are used in ZKPs to provide "real" zero-knowledge protocols without the possession of the secret. The cryptographic strengths of ZKPs is based on some hard-to-solve problems like solving the discrete logarithm for large numbers, the problem of factoring large numbers that are products of two or more large primes, etc. Non-Interactive zero-knowledge proofs (NIZKPs) [1] differ from the traditional ZKPs in the following aspect: public randomness. That is, the prover and the verifier both have access to the same, short, random string and the interactive process in ZKPs is prevented (mono-directional interaction from prover to verifier only).
With a NIZKP approach, senders of messages show that they are trustworthy by proving that they know a secret. Knowing the secret can be regarded as equivalent to possessing a certificate. The secret, however, is not revealed, neither is the identity of the sender, thus ensuring privacy. The non-interactive variant is important for C2C messaging since the interactive approach imposes too much communication overhead and is not feasible in low latency scenarios. The application of NIZKP to securing intersection communication is described in [5].

Additionally to the cryptographic approaches, plausibility checks can be used to trust the contents of a message. If many nodes report a certain situation, the existence of this situation is highly likely. If, however, a message is received that does not fit with what is known from the values of local sensors and from other messages, it is disregarded. In order to be able to do so, it is necessary that redundant messages are sent.

EVALUATION

To ensure proper behaviour of the C2C-CC system and protocols, it is important to validate the specifications. This is mainly done by simulation [20]. It is necessary to simulate the wireless network, the vehicle movements, the driver behaviour and the application behaviour. A combined simulation environment is needed to model the interdependability of e.g. traffic behaviour and wireless network. The dissemination of messages depends on the topology of the network which is determined by the positions of the vehicles. If the drivers of these vehicles now receive additional information, they may change their movement. Therefore, the positions of the vehicles also depend on the message dissemination and thus on the network. Simulation must take this kind of interdependability into account. Figure 8 shows the visualization of one of the used simulators.

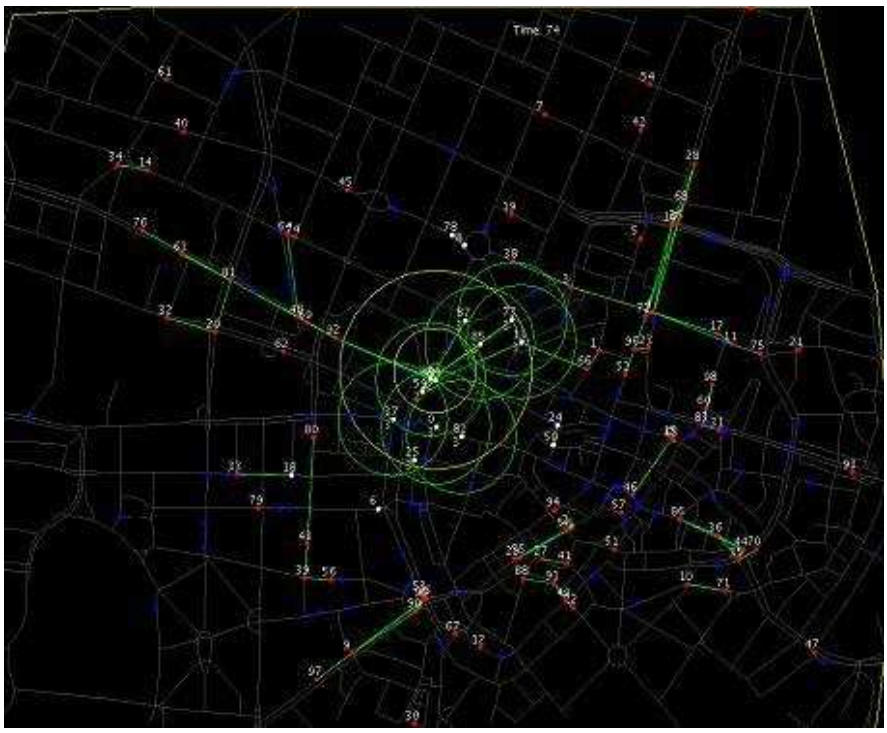

Figure 8: VANET simulation snapshot

SUMMARY AND DISCUSSION

This article provided a brief overview of the technologies that need to be standardized to enable interoperable car-to-car communication. The overall architecture and the necessary building blocks have been described. While many of the necessary technologies have been developed, some of them still need further evaluation and some research issues still remain to be solved. Also, even though many technologies work fine in demonstrators, some may still need improvement in order to be used in the real-world. The C2C-CC fosters the further development of existing technologies and presses on the solution for remaining problems by cooperation with research projects in the field and by providing information and guidelines for new research projects.

REFERENCES

[1] M. Blum, P. Feldman, S. Micali: Non-interactive zero-knowledge and its applications. In: Proceedings of the twentieth annual ACM symposium on Theory of computing, ACM Press (1988) 103–112.

[2] R. Bogenberger and T. Kosch. Ad-hoc Peer-to-Peer Communication-Webs on the Street. 9th World Congress on Intelligent Transport Systems (ITS 2002). Chicago, USA, 2002

[3] L. Briesemeister, L. Schäfers and G. Hommel. Disseminating Messages among Highly Mobile Hosts based on Inter-Vehicle Communication. In Proceedings of the IEEE Intelligent Vehicles Symposium, October 2000.

[4] Chaum, D.: Blind signature system. In: Proceedings of Crypto ’83., 1983

[5] F. Dötzer, F. Kohlmayer, T. Kosch und M. Strassberger. Secure Communication for Intersection Assistance. 2nd International Workshop on Intelligent Transportation (WIT 2005). Hamburg, Germany, March 2005.

[6] W. Franz: Network Layer Elements.C2C-CC Internal Document. 2004

[7] W. Franz: Location Table.C2C-CC Internal Document. 2004

[8] H. Füßler, H. Hartenstein, M. Käsemann and M. Mauve: Analysis of a Location Service for Position-Based Routing in Mobile Ad Hoc Networks. Tagungsband 1. Deutscher Workshop über Mobile Ad Hoc Netze (WMAN), Ulm, Germany, March 2002.

[9] H. Füßler, J. Widmer, M. Mauve, and H. Hartenstein: A Novel Forwarding Paradigm for Position-Based Routing (with Implicit Addressing). Proceedings of IEEE 18th Annual Workshop on Computer Communications (CCW 2003), Dana Point, USA 2003.

[10] H. Füßler, M. Mauve, H. Hartenstein, M. Käsemann and D. Vollmer. Location-based Routing for Vehicular Ad-hoc Networks. ACM Mobile Computing and Communications Review (MC2R), vol. 7, no. 1, January 2003, pp. 47 – 49.

[11] Goldreich, O.: Zero-knowledge twenty years after its invention. 2002.

[12] S. Goldwasser, S. Micali, C. Racko: The knowledge complexity of interactive proof-systems. In: Proceedings of the seventeenth annual ACM symposium on Theory of computing, ACM Press (1985) 291–304.

[13] H. Hartenstein, B. Bochow, A. Ebner, M. Lott, M. Radimirsch and D. Vollmer. Position-Aware Ad Hoc Wireless Networks for Inter-Vehicle Communications: the Fleetnet Project. Proceedings of The 2001 ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc), Long Beach, USA 2001.

[14] B. Karp and H.T. Kung: GPSR: greedy perimeter stateless routing for wireless networks. Proceedings of the 6th annual international conference on Mobile computing and networking. Boston, Massachusetts, USA 2000.

[15] T. Kosch and C. Schwingenschloegl. Geocast Enhancements for AODV in Vehicular Networks. ACM Sigmobile Mobile Computing and Communications Review, July 2002.

[16] T. Kosch. Efficient Message Dissemination in Vehicle Ad-hoc Networks. 11th World Congress on Intelligent Transportation Systems (ITS). Nagoya, Japan, October 2004.

[17] T. Kosch. Local Danger Warning based on Vehicle Ad-hoc Networks: Prototype and Simulation. 1st International Workshop on Intelligent Transportation (WIT 2004), Hamburg, Germany, March 2004.

[18] C. Lochert, H. Hartenstein, J. Tian, H. Füßler, D. Herrmann, M. Mauve. A Routing Strategy for Vehicular Ad-Hoc Networks in City Environments. 58th IEEE Semiannual Vehicular Technology Conference VTC 2003-Fall, pp. 156-161, Orlando, FL, USA, October 2003

[19] J. C. Navas und T. Imielinski: Geocast - Geographic Addressing and Routing. Proceedings of the Third ACM/IEEE Annual International Conference on Mobile Computing and Networking (MobiCom), Budapest, Ungarn, September 1997.

[20] C. Schroth, F. Dötzer, T. Kosch, B. Ostermaier and M. Strassberger. Simulating the traffic effects of vehicle-to-vehicle messaging systems. ITS Telecommunications. Brest, 2005.

[21] VSC: VSC Security Architecture, March 2004.

[22] P. Wex, F. Dötzer and A. Ajaz: State of the Art: Trust Establishment. C2C-CC Security Group, Internal Document. 2003