Attacks on Inter Vehicle Communication Systems - an Analysis

Amer Aijaz[1], Bernd Bochow[2], Florian Dötzer[3], Andreas Festag[4],
Matthias Gerlach[2], Rainer Kroh[5] and Tim Leinmüller[5]

[1]Volkswagen AG, Konzernforschung Elektroniksysteme, Amer.Aijaz@volkswagen.de

[2]Fraunhofer Institute for Open Communication Systems (FOKUS), {Bernd.Bochow|Matthias.Gerlach}@fokus.fraunhofer.de,

[3] BMW Group Research and Technology, Florian.Doetzer@bmw.de,

[4]NEC Europe, Andreas.Festag@netlab.nec.de,

[5]DaimlerChrysler AG, Research Vehicle IT and Services, {Rainer.Kroh|Tim.Leinmueller}@DaimlerChrysler.com.

Abstract— **Inter-vehicle communication systems are a new paradigm of networking. Largely related to mobile ad hoc networks and their distributed, self-organizing structure, they also introduce new threats. In order to assess these threats we introduce a model of attacks on an inter-vehicle communication system in this paper. This model is used to refine the system model of the NoW communication system and to find potential weaknesses during the specification phase of the NoW communication system.**

Our work shows that there are several interesting new challenges requiring novel solutions, some of which are outlined at the end of this paper. Although this is still work in progress, it is the foundation for analysis and assessment of future work.

As one of the main results of this paper, we identified several difficult to detect attacks on the hard- and software, and on the sensor input. We further point out system requirements to thwart such attacks.

I. Introduction

Inter-vehicle communication (IVC) and vehicle to infrastructure communication are amongst the most promising applications of mobile ad hoc networks. Therefore these mobile ad hoc networks, sometimes also referred to as vehicular ad hoc networks (VANETs), are studied in several research projects. Many applications are discussed in this context, but road traffic related messaging and local danger warning remain the most prominent ones for car-to-car communications, while car-to-home and car-to-infrastructure are the scenarios that will support the deployment of such systems.

Especially safety related applications require a secure and reliable system. Therefore, in this work we present an overview on the various possible attacks and countermeasures that have to be studied intensively. This work is considered as base for future development and analysis of security related functionalities within the NoW system model.

The remainder of this paper is organized as follows. In the next section, we discuss related work, followed by the introduction of the generic NoW system model. Then we provide background information on threat modeling and attack trees in general (Section IV) and apply these techniques in the context of vehicular ad hoc networks and the NoW system (Section V) in particular. In Section VI we discuss the results of the previous section and the resulting impact on the security system that has to be developed. Finally, Section VII concludes the paper and provides an outline of future work.

II. Related Work

Security issues have not been a major issue in past inter-vehicle communication research projects. Among past projects, significant work has been done in VSC [1], while currently there are security working groups within the EU's 6 Framework Programme's Research Project Willwarn [2] and the German national research project NoW – Network on Wheels [3].

But inter-vehicle communications' (IVC) topics have seen rising research efforts in the past years. Contributions to security in this field have been general analyses, such as [4], [5], and [6].

Others presented approaches to solve specific problems or security objectives. Golle et al. introduced a scheme to detect malicious data in IVC [9]. Dötzer discussed privacy issues for vehicle communications in [10]. Gerlach presents a holistic approach to VANET security in [7]. Leinmueller et al. [8] analyzed the impact of falsified position information on geographic routing.

Many papers have been written about trust establishment and decentralized key management, such as [11], [12], [13] and [14], while Kargl wrote his Dissertation about general security in mobile ad hoc networks (MANETs) [15].

III. The NoW System Model

As mentioned above, the NoW system architecture is not yet specified and still under development. Yet, a generic model can be derived from the different attacks, each of which is usually targeted at a specific component. Figure 1 depicts these components representing the system model assumed by the Security Working Group in NoW.

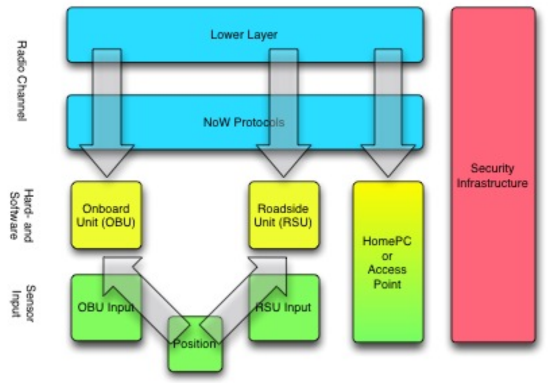

Fig. 1
A GENERIC SYSTEM MODEL.

Due to its generality, the model provides a basis for comparing and integrating previously found attacks into the attack model while establishing a common understanding of the system under discussion.

The model consists of four major aspects. First, the radio channel and the protocols employed over this channel. Using the radio channel, the lower layer protocols such as a physical transmission or the medium access protocol are exposed to an attacker, as are the NoW protocols, such as, e.g. routing. Attacks on the radio channel are the ones that can be carried out over the wireless interface.

Second, actual hardware and the software running thereon. Within the NoW project, we envision three major kinds of platforms. These are onboard units (OBU), which are installed in the vehicles, road side units (RSUs) as part of some road infrastructure (such as traffic lights, with or without access to the communication infrastructure)[1], and – to accommodate for deployment applications such as car to home media download (see below) – the HomePC or commercial Access Points providing content or Internet access. They all represent a processing platform similar to a current PC.

Third, the sensor input to the different processing units, which can be all kinds of physical sensors, like temperature, oil on the road, and the like. Note that in a broader definition, sensor input can even be communication to and from the OBUs not using NoW protocols. The importance of the position information in the NoW system is reflected in the separate component. As sensor information are not as important in the HomePC environment they are included in the block for the HomePC.

Finally, the Security Infrastructure behind the NoW system represents the organizational and technical aspects of distributing trust in the system. This includes the vehicle manufacturers, certification authorities, traffic authorities, and certified staff, to give some examples.

IV. Threat Modeling and Attack Trees

An essential part of the security engineering process is threat modeling. Most processes for threat modeling and risk analysis that have been described in the literature are focusing on existing system designs. In our case, however, the system design has not yet been specified and can in fact be influenced by security requirements. This in turn will generate new vulnerabilities and have an effect on the threat model. This is why we chose to use attack trees as a tool to assess the system's security. Attack trees are a top down approach, that allow us to improve our threat model with every iteration of the system's design.

A. *Security Engineering*

The process of security engineering has been described in [16], [17] and [18]. They all agree that before designing a security architecture, threats have to be assessed and the risks have to be analyzed. The analytical part of security engineering consists of following steps:

1) Describe the general system model and point out specific properties that affect the security.
2) Describe the general threats that affect the system and generate attack trees that reflect the various attacks accordingly[2].
3) After the generation of specific attack trees and the identification of vulnerabilities, apply a cost function in order to develop a proper risk analysis.

We described our system model in Section III and will point out specific properties in this section. The attack trees will be presented in Section V. The application of proper cost functions will be included in the final version of this paper.

B. *Attack Trees*

Attack trees as in [19] provide a structured and standardized means to classify and refine attacks on a system and they have been used before successfully (cf. [20]). The root of each tree represents a general attack on the system such as, e.g., Denial of Service. Attack trees specify attacks in terms of attack goals and their subgoals. The overall attack goal is then further refined in the tree structure using AND and OR logical connections.

Figure 2 depicts the graphical and textual representations of AND and OR connections. Usually, the textual representation is preferred over the graphical one, since the graphical representation becomes hard to read and quite space consuming for more complex attack scenarios.

As an example, consider the simple scenario that an attacker wants to steal a car. An attack tree could look like the one depicted in Figure 3; the attacker can shortcircuit the car to make it move or obtain a copy of the key . The aforementioned two attack goals can again be subdivided into sub-goals. For example, to short-circuit the car, the thief may need to break a car-window to access the car interior, and find the right ignition cables to shortcircuit them.

[1] Note the distinction of traffic infrastructure and communication infrastructure.

[2] Attack trees have been mentioned in the literature as threat trees as well.

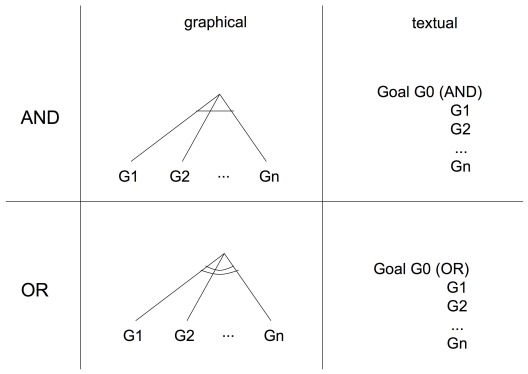

Fig. 2
GRAPHICAL AND TEXTUAL REPRESENTATION OF ATTACK TREES.

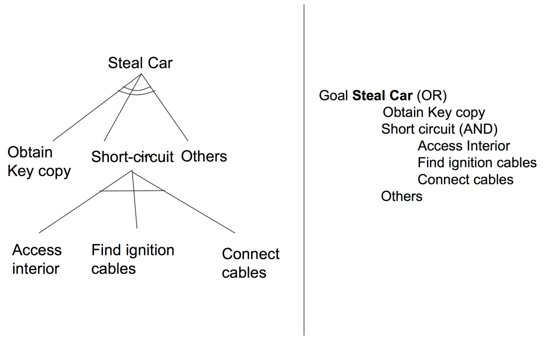

Fig. 3
AN EXAMPLE ATTACK TREE: STEAL A CAR.

C. *IVC Systems*

IVC systems have some properties that support security and others that hinder security.

Properties that have positive effects:

- No Energy Constraints: unlike mobile devices cars usually provide enough electric power to operate a communication system. The implication for security is that the incentive to deny cooperation is low.
- Known Time and Position: this information is required for most traffic related messages. This information can also be used to support security.
- Limited Physical Access: usually limited to the owner of a car or authorized personnel.
- Periodic Maintenance: in most cases cars receive periodic maintenance, which can be used for regular checks and updates.
- Secure Computing Platform: in a future automotive environment it seems inevitable that some kind of secure computing platform must be available. Such a platform may be used for IVC security to some extent.

Properties that have a negative effect:

- High Mobility: vehicle based networks will experience a high degree of mobility. The average speed of nodes will be very high, resulting in frequent topology changes and short average connection times. However, the high mobility can also be used to transport high-latency accepting information physically.
- Large Number of Nodes: IVC based networks will soon be among the largest ad hoc networks, requiring scalable solutions for adequate availability and sufficient performance.
- No Centralized Infrastructure: as we are dealing with a distributed ad hoc network, we have to assume that centralized infrastructure is only available at specific sitations. This affects fundamental security building blocks, such as trust management and key distribution and requires new concepts.
- Privacy Concerns: privacy is a major issue in a IVC system because cars are highly personal devices and they are kept for a long duration. System design approaches must therefore reflect the need for flexible addresses and/or identifiers.
- No User Interaction: in contrast to other distributed trust schemes, in our scenario there is no user interaction possible since this could distract drivers and would significantly reduce the popularity and usability of such a system.

D. *Application Classification*

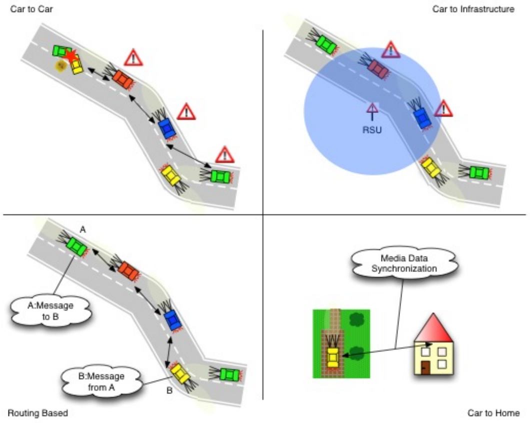

Fig. 4
FOUR MAJOR APPLICATIONS OF THE NOW SYSTEM.

To be able to look at attacks on the NoW system, we classify the applications into four groups covering the whole range of possible applications as depicted in Figure 4. These are

1) Car to Car Traffic Applications,
2) Car to Infrastructure Applications,
3) Car to Home Applications, and
4) Routing based Applications.

The applications cover single hop and multi hop communciations for the broadcast and unicast case and therefore the relevant range of applications for the NoW project. Car to car traffic applications include the transmission of traffic related information over multiple hops to a group of receivers, such as obstacles on the road, low friction, low visibility, etc. These examples have been discussed in the Willwarn project (cf. [2]) and are basically multi hop multicast/broadcast based applications.
Second, car to infrastructure applications represent the single hop broadcast case. An example application would be a low bridge warning application, where a bridge permanently broadcasts its height, or work zone warning, where cars are notified by the work-zone using radio beacons. Note that the name of these kind of applications may be misleading, as it is mostly the infrastructure that sends messages to cars[3].
Third, car to home applications, which are seen among the prominent deployment applications for the NoW system represent the single hop unicast case. For example a car to home media synchronization would be an application to be thought of.
Finally, as we assume that routing in VANETs will be an enabler for many applications, we include a rather general attack tree on routing based (multi hop unicast) applications. For the multi-hop applications, we assume both IP-based and position based routing mechanisms to be available.

V. Attack Modeling for the NoW System

A. Attacker Model

Our threat model is based on a generic attacker model with four groups of attackers:

1) Attackers with a programmable radio transmitter/receiver.
2) Attackers with access to an un-modified NoW unit who can therefore control the inputs, sensors, etc.
3) Attackers who have access to a modified NoW unit and who have obtained the keying material.
4) ”Inside” attackers who have access to records and equipment operated by the vehicle manufacturer or the NoW unit manufacturer.

B. Major Security Goals

In the system that we described in Section III, we identify four major security goals:

1) Information authenticity: receiving nodes can verify that the information contained in a received message is correct.
2) Message integrity and Source authentication: receiving nodes can verify that the messages have not been altered on their way and that the sender is a valid source.
3) Privacy: sending nodes cannot be tracked and the identity of the users is not revealed nor can it be linked to the identifiers used for communication.
4) Robustness: the system cannot be easily disturbed.

Or put differently, there are three major kinds of attacks on the system. The violation of the first two security goals may enable the injection of false messages, meaning that a user can inject syntactically valid messages with false content. Obtaining information to threaten the system's users' privacy means to violate the privacy goal. This information can be related to their movement patterns, their communication behavior, their communication partners or personal data. Finally, attacks on the system's robustness will affect the usability or performance of the system.

Based on these general attacks some more refined attack trees can be constructed for different applications in the system. Where applicable, application-independent attack trees are created for easy reuse. These general attack trees are one output of the collaborative effort to define the attacks on the system. Note that the more detailed the system is being specified, the more detailed the attack trees can become. In this paper, we will only provide a highlevel view on the attacks and detail them where we think they are of particular interest.

C. Reusable Attack Subtrees

During attack tree construction on the current high level of attacks it seemed necessary to create reusable (”general”) attack trees in order to avoid redundancy in the attack trees for each application. As the attack trees become more detailed, these general attack subtrees may turn out to be distinct as different applications introduce different kinds of vulnerabilities. In the current status of the work we stick to the general attack trees for the sake of compactness of the presentation of attacks. There are three major general subtrees:

- *Become Part of the Network* (Figure 5): once a malicious node is legitimate part of the network, it is easier for an attacker to insert malicious content or affect the network, this may be the basis for many attacks.
- *Manipulate OBU Input* (Figure 6), i.e. the component depicted in Figure 1. Manipulating this input has impact on the proper functioning of the NoW system, as many warnings are based on sensor input.
- *Violate Privacy* (Figure 7). The subtree on violating privacy summarizes the general attacks on privacy based on the NoW communication system.

1) Get Identifier
   a) Copy (NoW protocols/OBU/RSU)
   b) Steal (NoW protocols/OBU/RSU)
   c) Create (NoW protocols/OBU/RSU)
2) Have Identifier

Fig. 5

General Subtree B: Become Part of the Network.

1) Become Part of the Network: A node is part of the network once it obtained and is able use an identifier (cf.

[3] Infrastructure to car would be a better name.

Figure 5). The principle is similar to that in DHCP[4] networks, where a node can only take part in the networking, once it obtains a (valid) IP address from the DHCP server. In this attack tree, getting or having an identifier implies that only possession of this identifier authorizes a node to take part in the communciation. Usually, this requires some sort of certification for the nodes, an aspect which has not been included in the tree for the sake of simplicity.

Stealing an identifier is like copying it and making it unusable for the victim at the same time. Assuming some sort of binding of identifiers to nodes by using public key cryptography (e.g. using certificates or identity based cryptography) copying this identifier implies either breaking the respective cryptographic primitive on the basis of overheard messages or being able to access the private information on the victims platform itself. Stealing the identifier may be harder to do using the wireless interface, but possibly be done by stealing the physical device (e.g. SIM card) attached to the NoW unit. Creating an identifier implies either knowing secret information to actually create valid key pairs and valid bindings to a certain (malicious) node. To achieve this, an attacker must be able to intrude the security infrastructure, an attack we consider hard to carry out, if this infrastructure is well protected and thought out.

2) Manipulate OBU Input: As the on board units of the NoW system will probably be installed in a place that is not easy to access, altering the sensor readings is a straightforward way to attack a system. Like this, the attacker has an OBU with a valid identifier (and credentials) and can therefore attack the network from the inside.

Manipulations of the car – in other words, tuning it – is not uncommon. It will, however, require some skills to tamper with the car electronics directly, as these systems are becoming more and more complex, and will even include cryptography-based in-vehicle network protections (cf. [21]). One of the more probable attacks of this subtree would be stressing the components, as this probably goes undetected and rather leads to a faulty car.

Changing the sensor readings can be more effective, due to the following reasons. First, the in-vehicle system will probably not detect this kind of attack since no components are touched, when for example only the temperature sensor is put into ice water. Second, a receiving vehicle would still receive authorized, valid messages, only that their content is wrong.

3) Violate Privacy: In Figure 7, the attacks on the privacy of the users are listed. This subtree is a general view of attacks on privacy, and will be reused for the applications in this document. Some applications in themselves be a threat to the privacy of users, such as credit card payments; we will focus on privacy violations inherent to the communication system on NoW.

1) Manipulate a car
    a) Manipulate sensors
    b) Manipulate connections between components
    c) Replace OBU by own system/fake system
    d) Put system in ”service mode” und use the given (test-)functions
    e) Execute own code
    f) Stress components generating temporarily wrong outputs
2) Manipulate sensor readings
    a) Manipulate positioning system
    b) Manipulate time system
    c) Manipulate car sensors
3) Use an erroneous car
    a) Damage car
    b) Get erroneous car

Fig. 6
GENERAL SUBTREE A: MANIPULATE OBU INPUT.

Linking the identity of a user by observing his behavior is intuitively the easier and therefore more probable attack in subtree 1 in Figure 7. Observing somebody mounting his car and observing newly popping up nodes while the car is started is very easy in comparison to hacking a trusted third party (TTP) where security precautions will be high. Being that trusted third party is a completely different matter. Therefore note that a trusted third party should not be understood as a single entity, but a network of authorities.

A similar attack on privacy, i.e. revealing and tracking the location of a user requires either physical presence (at least in the radio propagation area) of the attacker or a networked grid of receivers and a database in the background. The first is an attack is feasible already by just observing a car (chasing a car by its color or number plate, or the like). The second-mentioned attack, however, would require a significant amount of money and organization to be implemented but should not be ignored. The VII (Vehicle Infrastructure Integration) project [22], currently underway in the United States could actually provide the infrastructure to deploy such a surveillance system even though its benefit for the deployment of vehicular communication is undisputed [23].

1) Link Person and (network-) Identifier
    a) Get access to TTP that links Person and Identifier (Security Infrastructure)
    b) Observe behavior (Side Channel)
2) Track a specific node
    a) Recognize a node (having seen it before) (AND)
    b) Generate traces by linking overheard messages (NoW Protocols, Lower Layer)

Fig. 7
GENERAL SUBTREE C: PRIVACY VIOLATIONS.

D. *Attacks on Car to Car Traffic Applications*

The attack trees shown in Figures 8 and 9 correspond to the specifics of car to car traffic applications. These applications exchange mainly traffic related information such as

[4] Dynamic Host Configuration Protocol

warnings of obstacles behind a curve, low visibility, etc. In addition to the general attack trees in Section V-C it can be thought of two attack subtrees: disseminate false messages and disturb system.

1) Generate new message (Lower Layer, NoW Protocols)
   a) Attack cryptographic system
   b) Become part of the Network (Subtree D) (AND)
   c) Inject directly
2) Replay message (Lower Layer, NoW Protocols)
   a) Attack cryptographic system
   b) Capture message (AND)
   c) Send out
3) Modify message (Lower Layer, NoW Protocols)
   a) Attack cryptographic system
   b) Capture message (AND)
   c) Break message integrity protection

Fig. 8
CAR TO CAR SUBTREE A: DISSEMINATE FALSE MESSAGES.

1) Disseminate False Messages: Figure 8 depicts the subtree for dissemination of false messages. A car to car traffic messaging system is relying on messages that are distributed by cars that experience a traffic relevant event. It is therefore critical that the messages about events are correct. An attacker can either try to generate new valid messages, replay existing messages or modify existing messages. One approach that could help to achieve either one of those goals is the to attack the cryptographic system by breaking cryptographic algorithms, attacking cryptographic protocols or force the system to use less secure algorithms or protocols. We placed it in every subtree, since the specific targets are different.

Another way of generating new messages than attacking the cryptographic system would be to become part of the network by manipulating the OBU input or use manipulated / dismantled hardware AND inject false messages directly.

In order to replay a message, an attacker must capture a message and send it out without getting caught by timing protocols.

A message modification would again require to capture a message and then finding a way to break the message integrity protection.

2) Disturb system: Figure 9 shows the attacks that lead to a crippled system. There are a couple of ways to disturb the system. Either an attackers tries to disable nodes remotely, suppresses wireless communications, exploits network vulnerabilities or abuses application level functionalities. The ultimate goal is to deny services, but even weaker forms that reduce the overall system performance may have significant effects.

Two approaches lead to the incapacitation of a node from a remote place. One is to overload the electronics by generating a electromagnetic pulse. While this seems to be a military scenario in the times of frequent terrorist attacks this may cause additional trouble in case of a critical situation. Apart from this, we have to assume that attackers may find a way to shut down systems remotely exploiting vulnerabilites.

1) Remote Incapacitation of NOW components (OBU, RSU)
   a) Generate EMP
   b) Stimulate System Malfunction
2) Suppress Communication
   a) 802.11p jamming
   b) GPS jamming (OBU Input)
   c) Inhibiting physical environment (Lower Layer)
   d) 802.11p weaknesses and flaws abuse (lower layer)
3) NoW network misbehavior
   a) Overload nodes (NoW Protocols, OBU)
   b) Disturb routing (Now Protocols)
   c) Don't participate in message forwarding / routing (NoW Protocols)
4) Application layer misbehavior
   a) Generate many false messages (NoW Protocols, OBU)
   b) Generate corrupt messages (OBU)

Fig. 9
CAR TO CAR SUBTREE B: DISTURB SYSTEM.

Wireless communication is more susceptible to suppression than wired communication. In this Section by communication we mean all in- and outgoing wireless signals to and from a car that transport data packets of some kind. The most obvious way to achieve this is to jam the wireless channels, in our case either the 802.11p or the GPS system. Another variant is to set up a physical environment that hinders communication. Finally, some special weaknesses of the 802.11p protocols may be used to deny their operation.

The network's operation can be abused to overload nodes in such a way that they cannot respond as they should. Alternatively, the routing or message distribution protocols may be disturbed so that messages are not relayed properly. Some nodes may also deny to forward packets and behave in a selfish way. In a worst case this could be done in a coordinated way.

On application layer, many false messages can be produced in order to overload nodes that are busy checking these messages authenticity and integrity. Or corrupt messages may be generated that can be authenticated properly but whose content does not meet the actual situation.

E. Attacks on Car to Infrastructure Applications

The application specific attack trees on car to infrastructure applications are depicted in Figures 10 and 11. As road side units (RSUs) play an important role in car to infrastructure applications, they also contain attacks on the road side units as well. Road side units are different from a OBU in the way that they are more prone to vandalism, easier accessible and probably de-mountable. They may have access to a fixed access networks and/or be mains or battery powered.

1) Disturb System: To disturb the system, i.e. make it deny its service, an attacker can either try to paralyse the RSU, the OBU or jam the communication channel. In addition, the attacker could destroy the sensors, but that would rather lead to false messages and is therefore covered in Figure 11.

As the RSUs are freely accessible and will probably not be surveilled all the time, the easiest attack is to physi-

1) Paralyze RSU (RSU)
    a) Deplete RSU Battery
    b) Physically destroy RSU
    c) Use up computing resources on RSU
2) Paralyze OBU (OBU)
    a) Physically destroy / remove OBU
    b) Use up computing resources on OBU
    c) Damage communication equipment
3) Affect communication channel
    a) Physical jamming (lower layer)
    b) MAC jamming (lower layer)
    c) Attack NL mechanisms (NoW protocols)

Fig. 10
CAR TO INFRASTRUCTURE SUBTREE A: DISTURB SYSTEM.

cally destroy them (vandalism). This cannot be countered by technical means. As the RSUs are serving information to the passing vehicles, attacks on the road side units and the communication channel will be the most effective. In particular, if the roadside units are to issue warning messages they can be seen as a crucial part of the traffic infrastructure that must be protected (such as traffic lights, stop signs, etc.) only that it may be that physical damage to them may not be as obvious (simply no radio signal, no warning).

Depending on the energy supply of these units, an attacker can either cut the mains supply or try to deplete the battery by, e.g., sending lots of messages to the RSU, making it use up its battery faster.

The second class of effective attacks agains the NoW system may be attacks against the communication system. As is obvious, an attacker can attack on the three different network layers, physically jamming the channel with noise, using a dedicated (malicious or faulty) transceiver to attack on the medium access or the network layer. In [24], Bellardo and Savage list and explain attacks to the 802.11 standard and give some remedies. A detailed attack tree for the NoW routing protocols as can be projected to date will follow in Section V-G.

2) Disseminate False Messages: Figure 11 depicts the subtree to inject false messages in the system. The attack tree is based on the fact that for car to infrastructure applications, RSU send messages to OBUs. The subtrees 2) and 3) in Figure 11, i.e. altering and replaying messages will surely be prevented by using the appropriate cryptographic primitives.

Changing the location of a legitimate RSU may be fairly easy, leading to warning messages in the wrong places: this attack scenario calls for revocation of RSU certificates and even the possibility of switching them off remotely. It can even be imagined that an attacker obtains many RSUs, puts them in one place and overcrowds the medium. Changing the software on the RSU requires an attacker to install malicious software on these nodes. This can be done either when having physical access to the computing interfaces, which is rather improbable, or hacking the node, if it has some sort of Internet access. This is to be an attack that is to be accounted for, since in current systems these attacks are more than merely annoying.

1) Obtain legitimate RSU (RSU, Security Infrastructure)
    a) Obtain Identifier (cf. General Subtree B)
    b) Change location of legitimate RSU (Position)
    c) Change software on legitimate RSU (RSU)
2) Replay RSU messages (Lower layer, NoW Protocols) (AND)
    a) Capture message
    b) Send out
3) Alter message (Lower Layer, NoW Protocols) (AND)
    a) Capture message
    b) Break message integrity check algorithm
4) Create legitimate messages with wrong content (RSU Input)
5) Alter RSU sensor readings / send information (RSU)
    a) Physically access RSU sensors (RSU)
    b) Physically access RSU storage / computing (RSU)
6) Make OBU believe that it received legitimate messages without actually receiving one (OBU) (AND)
    a) Gain access to install malicious software
    b) Install malicious software
7) Make OBU interpret the message wrong
    a) Alter OBU-SW (OBU)
    b) Alter OBU-configuration (OBU)
    c) Alter OBU sensors (OBU-Input)

Fig. 11
CAR TO INFRASTRUCTURE SUBTREE B: DISSEMINATE FALSE MESSAGES.

Further, to account for the constantly changing nature of viruses, worms and other malicious code, some update mechanism is favorable, which in turn may introduce additional vulnerabilities. As has been mentioned before with the general attack tree in Figure 5, once an attacker is able to create or obtain valid identities, it will be fairly easy to insert any (false) message he wishes. Last not least, if the RSU uses or propagates sensor information, it may be easy to insert false messages by simply changing the sensor readings. This attack is similar to the attack mentioned in the attack tree in Figure 6.

There is another side to car to infrastructure applications, which is the OBU. Even though improbable, an attacker, instead of altering messages themselves or sending faked messages around, may simply lead the OBU to issuing false messages by installing malicious software or altering the sensed environment of the OBU such that it assesses the situation wrongly.

F. Attacks on Car to Home Applications

The car to home applications are applications that may be deployed in the near future. With respect to the assumptions that hold, this application is different to the other applications mentioned in this paper which have been *safety applications*, i.e. applications common for all equipped vehicles and crucial for the safety of the driver.

Due to this reason, we name and group the attacks slightly different. Instead of concentrating on the communication and peers, we now take a system-centric approach. The assets of this system are the data transferred and the availability of the peers resources (such as that the vehicle is operational at all time).

One particular difference to the safety applications is that the vehicle engine may not be on during operation of this application. Further, the vehicle owner may not be in the car at the time the application is executed. This can lead to attacks at the vehicle that render it useless (see Attack Tree in Figure 12). Further attacks may be to obtain or change valuable information, or access either of the peer systems, i.e. the HomePC or the vehicle OBU, we summarize these attacks as *Unauthorized Data and System Access*. These attacks are covered in Figure 13. Attacks on the privacy of the user can be mainly by means of accessing the data rather than using information inherent to the communications interface and will be located in the same tree.

1) Disturb System: To disturb the system an attacker must gain access to either data or the system itself. From a higher level perspective taken for the analysis of this application, this boils down to the attacks shown in Figure 13. To disturb the system, there is an attack stemming from the assumption that we are dealing with a battery powered system, namely the sleep deprivation attack. Assuming a typical car battery has a capacity of 80Ah at 12 V, and the OBU will consume as much power as an average Laptop, i.e. 20W (1.6 A at 12 V) we can calculate the time after which the battery is exhausted as $\frac{80Ah}{1.6A} = 50h$.

1) Unauthorized Data and System Access (cf. Subtree B in Figure 13).
2) Paralyze OBU (cf. Subtree 2 in Figure 10.)
3) Affect Communication Channel (cf. Subtree 3 in Figure 10.)
   a) Deplete Vehicle Battery (Sleep deprivation) (NoW Protocols, OBU).

Fig. 12

CAR TO HOME SUBTREE A: DISTURB SYSTEM.

2) Unauthorized Data and System Access: As has been seen in the previous sections, unauthorized access to a system is usually based on weak protection of the system, a knowledgeable attacker and physical or remote access to the vehicle OBU or the communication partners of the vehicle. As in this application, a HomePC, i.e. the user's PC, which is probably connected to the Internet, a plethora of attacks using the HomePC can be carried out. Thus, first the application running within the HomePC must be protected, as must be the vehicle side peer of the application, to prevent hackers from altering crucial data in the vehicle by way of the HomePC. Hence it will be crucial to devise means to protect the communicating peers from attacks. On the other hand, attacks on the communication system will probably be prevented by using secure standard protocols to protect the data transmitted over the air. It is possible that these protocols will be employed on top of the existing NoW protections.

G. Attacks on Routing based Applications

Most attacks on the routing can be seen as attacks on the NoW Protocols component unless otherwise stated, therefore unlike in the previous paragraphs, no components are indicated in the subtrees. Note that we assume that the routing protocol of the NoW system will use geographical locations.

1) Eavesdrop on or insert messages into communication (NoW Protocols, Lower Layer)
   a) Gain physical control of the communication channel
   b) Guess the code for deciphering the encrypted data exchanged
   c) Break cryptographic protection
2) Gain system access on at least one of the communication partners
   a) Gain physical control of the car (OBU)
   b) Gain physical control of the communication partner (PDA, Home LAN, etc.)
   c) Gain remote system access on car by exploiting security holes (OBU)
   d) Gain remote system access on the communication peer by exploiting security holes (PDA, Home LAN, etc.)

Fig. 13

CAR TO HOME SUBTREE B: UNAUTHORIZED DATA AND SYSTEM ACCESS.

1) Waste/exhaust resources (Overload wireless channel and nodes)
   a) Waste/exhaust of bandwidth of wireless channels (pertains all neighbors)
   b) Create false location table entries in nodes
   c) Overload selected node (OBU)
   d) Overload all neighbor nodes (OBU)
2) Deter nodes from packet reception
   a) Create routing black holes
   b) Create routing loops
   c) Partition Network

Fig. 14

ROUTING: SUBTREE DOS.

1) Disturb System: Here, the attacker's idea is to abuse regular routing functionalities in order to overload other nodes or even the entire reachable system partition. The impact of the attacker's actions reaches from service degradation (e.g. increased delays) to entire network failure.

1) Inject beacon message
   a) Inject beacon message with falsified position information and/or timestamp
   b) Inject beacon message with falsified node ID
2) Inject location query message
   a) Inject location query message with falsified piggybacked source node ID, position, and/or timestamp
   b) Inject location query message with falsified piggybacked sender node ID, position, and/or timestamp
3) Inject data message
   a) Inject data message with falsified piggybacked source node ID, position, and/or timestamp
   b) Inject data message with falsified piggybacked sender node ID, position, and/or timestamp

Fig. 15

ROUTING: SUBTREE INJECT FALSE MESSAGES.

2) Inject False Messages: The attack goal in this subtree is the manipulation of location tables of other nodes. This can be achieved by falsification of information in data and signaling messages and results in misdirection of data message. After a certain threshold of false information is reached the system becomes dysfunctional.

3) Privacy Violation: The goal in this subtree is to infringe a user's privacy, either by eavesdropping of data message or by revealing and tracking a node's position. If

1) Eavesdropping
   a) Eavesdropping of forwarded data message
   b) Inject beacon message with falsified node ID, position information and/or timestamp
   c) Inject location reply with falsified node ID, position, and/or timestamp
   d) Inject data message with falsified piggybacked information
2) Revealing/tracking a node's position
   a) Analyzing/tracking the node ID, position, timestamp in a beacon
   b) (Frequently) sending a location query
   c) Analyzing/tracking the node ID, position, timestamp of the source node in a data message
   d) Analyzing/tracking the node ID, position, timestamp of the sender node in a data message

Fig. 16
ROUTING: PRIVACY VIOLATION.

multi-hop forwarding is used and the eavesdropper is one of the forwarders, an attacker does not need any specific actions for eavesdropping. However, the attacker might actively manipulate other nodes' location tables. By such a manipulation, the attacker might be selected as a forwarder and can eavesdrop any messages sent to the attacked node. For revealing and tracking a node's position, an attacker might misuse the existing protocol mechanisms of the routing protocol.

VI. EVALUATION AND LESSONS LEARNED

In Section V, different attacks on different applications and components of the NoW system have been outlined. From these attacks, important characteristics of and requirements on the NoW system can be derived. A summary of those requirements is given in Table I. A more detailed discussion can be found in the following sections.

Applications	*Components*	*Requirement*
All	OBU, RSU	Trusted platform
All	OBU, RSU, HomePC	Firewall
All	Security infrastructure	Trust establishment and control for applications
Car to car, Car to infrastructure	OBU, RSU, NoW Protocols	Plausibility checks
Car to home	OBU, HomePC, NoW Protocols	Secure wakeup of the OBU
Car to infrastructure, Car to car	RSU	Tamper evidence mechanisms
Routing	OBU, RSU, NoW protocols	Trust establishment for NoW protocols

TABLE I
SECURITY REQUIREMENTS, COMPONENTS AND APPLICATIONS DEDUCED FROM THE ATTACK TREES.

A. Plausibility Checks

As discussed in the attacks for Manipulating OBU (and RSU) input depicted in Figure 6, altering the physical environment around the sensor for just that sensor may be hard to detect while easy to do. It may therefore be a quite probable attack to such kinds of systems. Note that in the case of manipulated sensor input malicious nodes are hard to distinguish from faulty ones. It would therefore be a good idea to introduce some sort of plausibility checks for sensor readings into the system. For instance, receiving an icy road warning while the own external temperature sensor indicates temperatures sufficiently above 0 deg C, would be a good indication that the message might have been send by a malicious or malfunctioning node.

B. Trusted Platform

From the short analysis of the attack tree in Figure 5, it becomes clear that choosing a platform that protects private information is among the prominent design issues of NoW system implementations in addition to choosing strong cryptographic primitives.

C. Trust Establishment for Communication

Trust establishment for the communication system, in particular for the routing in the NoW system is important, as can be seen in the attack tree in Section V-G. Even though there already are existing solutions on intrusion detection systems and distributed trust establishment techniques, there are currently few solutions tailored to IVC networks.

Trust establishment will probably both rely on some trusted infrastructure (e.g. for initial identity management) but also on completely distributed mechanisms when the ad hoc network has no connection to the fixed security infrastructure.

Note that there may be different providers of trust, i.e. those who provide for trust in the communication interface and those - and possibly many different ones thereof - who provide trust in the different application instances.

D. Secure Wakeup

As has been pointed out in Section V-F, battery draining attacks against parked vehicles should be prevented as they may become a serious threat to vehicle functionality and hence to deployment of the application. Users would probably not buy an application which can be used to make their car be dead after two days of parking.

As the OBU must not run all the time the vehicle is parked, a wake-up mechanism is sought. This mechanism could be subject to attack if too simple or insecure. In [26] an approach to secure the wake-up mechanism based on hash chains or WiFi Protected Access of car to home applications is discussed which deals with such attacks.

E. Privacy Protection

Privacy has been identified as one major security goal in Section V. The attack trees, in particular the attack tree in Figure 7 stress that to detect the user's privacy, a holistic approach is necessary. This includes that first the communication system can provide for anonymous communications.

Second, it will not be sufficient to only have one identifier which is detached from the user's identity, because a system will then be recognizable and therefore easier to trace; in addition the act of mapping a system identifier to a real world identity is easy for a men with a transceiver, as has been pointed out above. Therefore, pseudonyms are a promising solutions to be used in the communication system even though their extensive use will be detrimental to system functionality and performance. In a nutshell, the system must provide for the untraceability of its users.

Finally, infrastructure, both communication wise and traffic related should be designed or integrated into such systems carefully considering the possibility of privacy violations due to centralized collection of massive amounts of user data.

F. Tamper Evidence Mechanisms

Based on the attacks on RSUs given in Figure 11, it becomes clear that an RSU connected to some communication infrastructure can quickly detect attacks on its functionality. Protection of RSUs may consist of, e.g., a UMTS[5] transceiver, which can issue either alive-messages every now and then, or issue some sort of attack notification to a traffic center. Further, the RSU must detect tampering, vandalism or its unauthorized relocation and notify the responsible traffic information center. Referring to OBUs, it shall be possible to detect malicious changes to hard or software at least when the car is being inspected. For tamper evidence, again plausibility checks in connection with additional communication capabilities can be thought of.

VII. Conclusions and Future Work

During our work we found that attack trees provide a useful tool to assess the security of a system gradually. The top-down approach allows us to influence the system design at an early development phase regarding security considerations, while on the other hand being able to generate a more detailed analysis as soon as the system's specifications become more specific.

Looking at the attacks, we found that two procedures would enhance overall security essentially, doing local plausibility checks in cars and regular system checks on the nodes, most notably RSUs. Plausibility checks could include comparison of received information to internal sensor data, evaluating messages from different information sources about a single event and scenario building, where single traffic events are related using statistics. Simulations have shown that this greatly increases the effort of an attacker, but it requires proper models for every application. Regular system checks would verify the proper function of a unit and therefore reduce the number of malfunctioning units. This could also include the option to update the software.

[5] Universal Mobile Telecommunication Standard

VIII. Acknowledgements

This work has been carried out in the project "NoW: Network-on-Wheels" project supported by the German Ministry for Education and Research (BMB+F) under Contract No. 01AK064F.
We would like to thank Michael Schäfer, Elmar Schoch (both DaimlerChrysler), and Benedikt Ostermaier (BMW) for their valuable contributions and comments to this paper.

References

[1] "US Vehicle Safety Communication Consortium," http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm.

[2] The Willwarn Project, "The Willwarn project website," 2005, http://www.prevent-ip.org/willwarn.

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

[4] Albert Held and Rainer Kroh, "It-security and privacy for telematics services," in *Workshop on Requirements for Mobile Privacy & Security*, University of London, UK, September 2002.

[5] Jean-Pierre Hubaux, Srdjan Čapkun, and Jun Luo, "The security and privacy of smart vehicles," *IEEE Security and Privacy*, vol. 4, no. 3, pp. 49–55, 2004.

[6] Magda El Zarki, Sharad Mehrotra, Gene Tsudik, and Nalini Venkatasubramanian, "Security issues in a future vehicular network," in *Proceedings of EuroWireless 2002*, February 2002.

[7] Matthias Gerlach, "VaneSe - An approach to VANET security," in *Proceedings of V2VCOM 2005*, 2005.

[8] Tim Leinmüller, Elmar Schoch, Frank Kargl, and Christian Maihöfer, "Influence of falsified position data on geographic adhoc routing," in *ESAS 2005: Proceedings of the second European Workshop on Security and Privacy in Ad hoc and Sensor Networks*, jul 2005.

[9] Philippe Golle, Dan Greene, and Jessica Staddon, "Detecting and correcting malicious data in vanets," in *VANET '04: Proceedings of the first ACM workshop on Vehicular ad hoc networks*. 2004, pp. 29–37, ACM Press.

[10] Florian Dötzer, "Privacy issues in vehicular ad hoc networks," in *Workshop on Privacy Enhancing Technologies*, Cavtat, Croatia, May 2005.

[11] Matt Blaze, Joan Feigenbaum, and Jack Lacy, "Decentralized trust management," in *Proceedings of IEEE Symposium on Security and Privacy*, 1996, number 96-17, pp. 164–173.

[12] Lidong Zhou and Zygmunt J. Haas, "Securing ad hoc networks," *IEEE Network Magazine*, vol. 13, no. 6, pp. 24–30, 1999.

[13] Laurent Eschenauer, Virgil Gligor, and John Baras, "On trust establishment in mobile ad-hoc networks," in *Proceedings of the Security Protocols Workshop*, April 2002.

[14] Christian Schwingenschlögl and Marc-Philipp Horn, "Building blocks for secure communication in ad-hoc networks," in *Proceedings European Wireless*, 2002.

[15] Frank Kargl, *Sicherheit in Mobilen Ad hoc Netzwerken*, Ph.D. thesis, Universität Ulm, 2003.

[16] Claudia Eckert, *IT-Security: Konzepte, Verfahren, Protokolle*, R. Oldenbourg Verlag, 2003.

[17] Ross Anderson, *Security Engineering*, Wiley Computer Publishing, 2001.

[18] Matt Bishop, *Computer Security*, Pearson Education, 2002.

[19] Bruce Schneier, "Attack trees: Modeling security threats," 1999.

[20] Andrew P. Moore, Robert J. Ellison, and Richard C. Linger, "Attack modeling for information security and survivability," Tech. Rep. CMU/SEI-2001-TN-001, Carnegie Mellon University, 2001.

[21] Marko Wolf, André Weimerskirch, and Christof Paar, "Security in automotive bus systems," in *Proceedings of ESCAR 04*, 2004.

[22] U.S. Department of Transportation, "Vehicle infrastructure integration (vii)," http://www.its.dot.gov/vii/.

[23] Jerry Werner, "Details of the vii initiative's 'work in progress' provided at public meeting," http://www.ntoctalks.com/icdn/vii_pubmtg_v1.php.

[24] John Bellardo and Stefan Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *Proceedings of the USENIX Security Symposium*, 2003.

[25] IEEE, "IEEE standard 802.11p. draft amendement: Wireless access in vehicular environments (WAVE)," 2004, Draft 1.0.

[26] Matthias Gerlach, Jens Hünerberg, Bernd Bochow, Christian Maihöfer, and Carsten Tittel, "Secure wakeup on WLAN for car to home applications - MagicPackets for wireless," in *Proceedings of V2VCOM 2005*, 2005.