

Modeling Roadside Attacker Behavior in VANETs

Tim Leinmüller[§], Robert K. Schmidt[§], Elmar Schoch[¶], Albert Held* and Günter Schäfer[‡]

[§]DENSO AUTOMOTIVE Deutschland GmbH, Germany, {t.leinmueller|r.schmidt}@denso-auto.de

[¶]Institute of Media Informatics, Ulm University, Germany, elmar.schoch@uni-ulm.de

*Daimler AG, Research and Development, Ulm, Germany, albert.held@daimler.com

[‡]Telematics/Computer Networks Research Group, Technische Universität Ilmenau, Germany, guenter.schaefer@tu-ilmenau.de

Abstract—Communication using VANETs is commonly seen as the next milestone for improving traffic safety. Vehicles will be enabled to exchange any kind of information that helps to detect and mitigate dangerous situations. Security research in the past years has shown that VANETs are endangered by a plethora of severe security risk.

Subject of this work is the modeling of attackers that target active safety applications in VANETs. Through a risk analysis, this work identifies assets, threats and potential attacks in inter-vehicle communication. The risk analysis shows that the most serious threat arises from a quasi-stationary (road-side) attacker that distributed forged warning messages. This attacker is discussed more deeply. We show the degrees of freedom that are available for position forging and find thereby two attacks that demand attention: single position forging having low effort compared to sophisticated movement path forging having a potentially high influence on road traffic safety.

I. INTRODUCTION

Vehicular Ad-Hoc Networks (VANETs) describe the technology of direct communication among vehicles themselves as well as among vehicles and (roadside) infrastructure. They enable vehicles to exchange information in order to increase vehicle passenger safety and road safety, traffic efficiency and driver convenience. Such information are enhancing autonomous in-vehicle safety systems as well as they are informing the driver of relevant events where his reaction or attention is required. Thus, the information received by a vehicle must be secure and reliable, meaning that information security is a crucial part of such a system.

Information security and hence drivers' safety is endangered once there is a vulnerability in the system attracting attackers who exploit the vulnerability according to their motivation. For example, the open system character of VANETs might motivate attackers to interfere with the system. This interference may even provoke wrong driving maneuvers leading to an accident in the worst case.

Attacks on VANETs have been summarized generally in previous work [1]. Several solutions have been proposed to secure the system against a variety of these attacks. What is missing so far is an in-depth discussion and analysis of attackers and the modeling of attacker behavior to analyze and to help to improve the proposed security solutions.

The early stage of development of VANETs does not allow for a meaningful attack analysis. Currently, there are still too many options with respect to protocols and applications. Modeling all possible attacker behaviors and attacks on these would be impossible. Therefore, we reduce the options by

specifying a simplistic model of a VANET first. Based on this model, we conduct a risk analysis, identifying assets, threats, vulnerabilities and attackers leading to a quantification of the respective risks.

Following the risk analysis, we take a detailed look on the attacks and attackers that pose high risk to the system. The outcome of this evaluation is that position information is a crucial and endangered subpart of the system. Hence, we focus on modeling attacks on position information and elaborate on potential attack implementations used by attackers. Finally, we discuss effort and impact of these concrete attacks serving as a knowledge basis for security system designers. Furthermore, we highlight the most significant attacks.

The remainder of the paper is as follows. In Section II we summarize related attack classifications as well as security systems that are coping with malicious data. After defining our basic system assumptions in Section III, we examine the security issues of the system by an in-detail risk analysis in Section IV followed by the attack analysis in Section V. There, we discuss and motivate for a consideration of the most imminent risk of a roadside attacker which is then modeled and evaluated in Section VI. The results of the risk analysis as well as the attacker model are then summarized in Section VII.

II. RELATED WORK

Besides our work in [1] and in more detail in [2] a description about attacker capabilities in vehicular ad-hoc networks has been given by Raya et al. in [3]. However, previous work did not specifically discuss attacker capabilities with respect to position forging. For the development of concrete attacks an understanding of potential countermeasures is needed. Thus, in the following we summarize existing security approaches detecting malicious or at least inconsistent data in VANETs.

Golle et al. propose to assess the plausibility of information upon reception in general. In [4] they provide a framework to detect and correct false information. Their approach envisions nodes to search for possible explanations for received data. Acceptance of data is then encouraged by scoring explanations and selecting the explanation with the highest score being consistent with the VANET model.

Raya et al. [5] formulate a detection system for misbehavior as a means to exclude vehicles from the communication system. Upon detection of misbehavior, the cryptographic key belonging to the respective vehicle is revoked. The basic idea behind the misbehavior detection approach is to evaluate

deviation from normal behavior of vehicles. By using a basic clustering algorithm, they are able to differ between normal and abnormal behavior, and hence detecting attackers. As a prerequisite for the algorithm, the authors assume the presence of an honest majority.

In our previous work in [6] we propose a basic position verification system designated to evaluate the cooperativeness of vehicles regarding geographic routing in VANETs. The idea is to inspect the consistency of position data. This includes analyzing changes in movement and density of vehicles, map-based verification as well as considering radio limitations.

In summary, several reactive security mechanisms for VANETs have been discussed in the literature. However, the detailed study of attacks and attackers has been neglected so far. Previous work employed basic attacker models to show the effectiveness of the respective security system. Static attacks have been applied and the reaction of the respective mechanisms (attacker(s) detected or not) has been shown.

III. MINIMALISTIC VANET MODEL

A. Communication System

The communication system is a wireless communication system of the IEEE 802.11 family (e.g. 802.11p). We assume a single communication channel that is shared by all nodes. The transmission range of every node is limited to an average value, e.g. 250 m. Messages are distributed via single hop broadcast, the system does not make use of routing.

Note that those simplifications do not limit our work to non-routing scenarios but merely reduces the number of potential system vulnerabilities. Our findings are also valid for systems that make use of position based routing and message distribution (see [7] and [8]), under the condition that the analysis is extended with additional vulnerabilities resulting from such protocols.

B. Active Safety Applications

In principle, safety applications can be divided into two categories:

- *Event-Driven Applications*: They send and receive messages about events that may be interesting to the driver, the in-vehicle safety systems or both, for a certain time in a certain area [9]. Examples are a post-crash warning or a warning of a dangerous road condition. Simplified, respective warning messages comprise the four fields as shown in Figure 1.
- *Cooperative Awareness Applications*: This category summarizes applications that determine dangerous situations based on the analysis of received position information from the surrounding vehicles. This information is collected from so called beacon messages that are broadcasted regularly by every vehicle. An example application for this category would be a forward collision warning or warning of a vehicle driving in the opposite direction. The beacon message can be seen as an instance of the message format in Figure 1 with an empty "Warning" field.

Node ID	Node Position	Time	Warning
---------	---------------	------	---------

Fig. 1. Simplified Warning Message Format

Both kinds of applications rely on accurate position information. However, the event-driven applications send messages whereas cooperative awareness applications use the position information from regularly exchanged beacons.

C. Security Functionalities

Our minimalistic system does not make use of certificates. As discussed in previous work (see [10]), certificates mainly restrict access to the system (more precisely, restrict contribution of certified messages), but do not prevent a node that has valid certificates from attacking. Note that if the system would make use of certificates, our analysis would be the same, with the exception that the attacker would have to get access to valid certificates.

The other assumption with respect to security is that the system employs reactive security mechanisms such as consistency checks or plausibility checks. The basic mechanisms we assume to be in place are checks regarding position and checks regarding the time the message was sent. With respect to the Time field of a message, messages are discarded if they contain a time in the future, or if they are older than a threshold to be defined. The Node Position field must contain a position within the receiver's radio range otherwise, the message is ignored.

Step by step, we add more advanced checks in the progress of the attacker modeling. These checks comprise validation of subsequent positions/time tuples, i.e. the vehicle's velocity and heading, acceleration and heading change. They can also verify if these values fit to the current traffic situation, e.g. traffic jam or free flow. The most complex check is finally the validation of the movement of the vehicles relative to each other. This includes checks on the logical order and its development over time. For example, it is an untypical behavior of two vehicles switching their logic position frequently. Multi-lane roads require mechanisms that can distinguish different movement pattern for different lanes.

IV. RISK ANALYSIS

In this section we conduct a risk analysis that is based on the introduced simplified VANET model. The selected risk analysis process that we employ is based on commonly used risk analysis procedures (see for example [11]).

We chose to conduct a qualitative risk analysis approach because it is the only type of approach that can be applied to systems that are still in development and thus there is no statistical data available yet with respect to conducted attacks or abused vulnerabilities.

Our risk analysis is separated into five steps.

- 1) Identification of the system's assets
- 2) Determination of threats to the system
- 3) Identification of system vulnerabilities that enable the threats
- 4) Identification of attackers that could exploit one of the vulnerabilities to instantiate a threat
- 5) Determination of risk

We use the outcome of the last step to motivate our choice to look into a subset of possible attacks in more detail and to model a specific attacker.

A. Assets

The identification of assets in an inter-vehicle communication based safety system is rather straightforward. We chose to value the assets relatively to each other in order to be able to determine the relative risk to the system in the last subsection of this section.

- 1) *Safety messages*
- 2) *Privacy*
- 3) *Communication system*

We rated the safety messages to be the highest asset of the system, followed by privacy and the communication system as such. Note that by privacy, we denote the problem that the system distributes privacy relevant data. This in turn requires the system to guarantee that the data originator (vehicle and vehicle driver) is able to remain anonymous. The last asset, the communication system, describes everything that is related to the communication part, i.e. the communication hardware, the protocols, and the communication media.

B. Threats

In active safety systems there are essentially two obvious situations that result in security threats to the systems. The first one is loss of warning messages and the second one is the distribution of modified, bogus, or wrong data in warning messages. Both situations result in different threats, which will be discussed in this section. As a starting point in this discussion we chose threats towards the classic security goals for information systems (confidentiality, integrity and availability). Not all of these threats do obviously apply to safety related communication in VANETs. Thus, we explain which of the threats apply and extend the list by these threats that are typical for safety communication in VANETs.

- *Confidentiality*: In a vehicular safety messaging system confidentiality is not an important issue, since messages distributed in the system are normally not confidential but meant to be received by all nodes, or at least by all nodes within a certain area.
- *Integrity*: Regarding integrity, there are three immanent threats. All of these three concern the content of distributed safety messages. The first of these threats is having wrong or forged messages in the system. The second threat are messages being modified during distribution and the third are replayed messages. The threats have in common that they might lead to inappropriate warning

messages being displayed to the driver and thereby in the worst case even provoke accidents.

- *Availability*: Threats against the availability of the warning system are either the loss of single or multiple messages, or the system being not usable due to, for instance, a denial of service attack.
- *Authenticity / Authentication*: Authenticity of safety messages in VANETs is not required. For a node receiving a warning message, it is not of interest to determine the identity of the message sender, but only that the message content is reliable.
- *Controlled Access / Authorization*: The general idea of safety applications in VANETs is to provide free access to information for everyone. So from this point of view, controlled access is not a security goal. On the other hand, only vehicles and road side units are intended to create and distribute warning messages in the network. Clearly, there is no problem in a laptop user receiving warning messages, however he should not be able to create warning messages.
- *Accountability / Non-Repudiation*: Accountability and non-repudiation are also no direct security goals in VANETs. Only if liability of message senders would be considered as relevant, these goals would be of interest and could be endangered by attacks.
- *Privacy*: Privacy is one of the major security aims in inter-vehicle communication. Since most of the distributed information in active safety system is related to the driver and the respective vehicle, there is the threat of correlation of this data and driver identities by arbitrary third parties. This is due to the fact that data distributed in warning messages or beacons contains personal data such as speed and position, which could for instance be abused for driver profiling.
- *Anonymity*: At a first glance anonymity seems not to be a security goal that can be threatened in VANETs. Every node is able to submit information anonymously to other nodes. However, in case anonymity is seen as a means to circumvent problems with respect to privacy then it becomes vulnerable to the same threats as privacy. I.e. if privacy is not achievable, anonymity could be a means to leverage the problem of distribution of privacy relevant information. A good example is position information in beacons. A receiving node can not be prevented to track a node that regularly sends beacons, but the sender can anonymize its beacons. Thus, anonymity is a major security goal in VANETs, especially as "replacement" for privacy.

From this analysis of threats, we can briefly summarize the threats as

- Distribution of wrong or forged messages
- Disturbance or unavailability of communication system
- Tracking and profiling of vehicles or vehicle drivers

C. Vulnerabilities

The determination of vulnerabilities of a safety communication system according to our model differs significantly from the usual approach in information systems. Usually, there are at least some controls in place that restrict access to the system or limit abuse of the system. Since this contradicts the philosophy of VANETs, where all information is meant to be publicly available, such kind of controls are not in place. Consequently, the vulnerabilities of the system originate from the system's nature as such.

The vulnerabilities can be summarized as

- *Unprotected wireless communication channel*: This denotes the fact that everyone has free access to the communication media. It is not protected against physical disturbance.
- *Plaintext information exchange*: Since all data is exchanged unencrypted (i.e. in plaintext), everyone can understand anything that is transmitted in the VANET. Likewise, everyone is free to send messages with any kind of content.

D. Attackers

When it comes to naming attackers in a VANET scenario, usually three types of attackers are mentioned:

- *Road-side attacker*: The attacker that is using a laptop to transmit forged warning messages to vehicles to make them react in a certain way, e.g. to make them brake.
- *Vehicle (driver)*: The attacker that uses forged warning messages to obtain free road on his itinerary.
- *Infrastructure-based attacker*: The attacker that collects large amount of transmitted data to obtain vehicle (driver) movement patterns.

More generic attacker models for VANETs have been introduced in [3] and [12]. According to our system model definition, we only look at a subset of attackers from the above mentioned models. In accordance with those models, we classify the attacker's role in a VANET communication system according to the following criteria:

- 1) *Mobility*: Mobile or stationary, which means the attacker is either moving within the network, e.g. like a normal vehicle, or he is staying quasi stationary at the same position, e.g. on a bridge over the highway.
- 2) *Affiliation*: Insider or outsider, which means that the attacker is either part of the network, i.e. a legitimate node, or an outsider, e.g. a laptop user. The distinction between insider and outsider does only make sense in case there are criteria that distinguish a legitimate node from an outsider. Examples for these criteria are sensor information, position information or other data that is available on in-vehicle communication buses. Note that in our simplistic model, security credentials are not a criteria for this distinction since we assume a system without security credentials. If used, security credentials would be another criteria for the distinction between insider and outsider.

- 3) *Intention*: Intentional or unintentional, i.e. either the attacker is deliberately acting against common rules in the network/system or not. The unintentional attacker classification covers basically the case where a system is violating the rules due to malfunctioning.
- 4) *Motivation*: Malicious/destructive/"just for fun" or profit oriented, meaning the intention of the attacker is either to disturb the network and its services in order to cause for instance harm, or his intention is to gain personal profit out of his actions. Personal profit might be monetary profit but also profit in terms having less road traffic on the own route. In most cases, an attacker that has personal profit in mind tries to minimize attack cost and will limit his efforts to succeed.
- 5) *Activity*: Active or passive, which means the attacker is either actively participating in the network in order to reach his goals or just passively listening to the communication.
- 6) *Cooperation*: Cooperative or single determines, whether it is a group of two or more attackers that cooperate in an attack, or whether it is a single autonomous attacker.

According to this attacker classification, motivations of attackers are either malicious/destructive/"just for fun" or profit oriented. Malicious motivations would for instance be to provoke accidents, to provoke traffic jams or to bother other drivers. In general the effort that an attacker is willing to spend for such kind of attacks can be estimated to be rather low. However, combined with the motivation of e.g. becoming a famous hacker or selling repair services to damaged vehicles, these motivations would turn into profit oriented ones where the willingness to spend effort is higher. Clearly profit oriented motivations are freeing the road or a single lane along the own route, reroute road traffic for the same purpose, making drivers use a specific gas station or simply rerouting traffic around selected premises.

With these motivations in mind and in combination with the attacker classification, in conclusion, we can classify the above mentioned three types of attackers as follows.

- *Road-side attacker*: He is either an insider (e.g. with a legitimate communication system from an old car) or an outsider (laptop user) and he is acting intentional. The attacker is usually active in case he distributes forged messages. The attacker's motivation can also be both, malicious or profit oriented and he can act on his own or in collaboration with other attackers.
- *Vehicle (driver)*: This represents clearly the case of an insider that is acting intentional or unintentional (e.g. vehicle with a defective warning system). He is active, malicious or profit oriented.
- *Infrastructure-based attacker*: He can be both, insider or outsider, and he is acting intentional. He is passive and profit motivated.

E. Risks

The final step in the risk analysis procedure is the determination of risks of the system. In the qualitative risk analysis,

a risk is determined based on the identified asset value, the extent of the threat, and the likelihood of the threat exploiting an existing vulnerability.

From the previous subsection, we derive the risk statements in table I.

As classifications for our risk analysis we use commonly used metric triples (see for example [11]). The likelihoods for attempt (i.e. how likely it is that someone will try exploit the vulnerability) are Likely, Conceivable and Improbable. The likelihoods for exploit (i.e. how difficult or easy it is to exploit the vulnerability) are Easy, Moderate and Difficult. Finally, to express the overall risk, we use the classic risk levels High, Medium and Low.

We attributed those values to the risk statements in a process that is based on various discussions, common sense and well educated guess. Clearly speaking, there is no mathematical or statistical model behind a qualitative risk analysis.

The following reasoning motivates our classification. Laptop attacks are in general simpler to mount than attacks that require vehicle modification. Sending forged messages (and to see the reaction of other drivers) provides higher satisfaction (and thus motivation) than disabling communication. With this in mind, we come up with the classifications for Roadside Attackers and Vehicle Drivers.

The last risk statement, containing the Infrastructure-based Attacker, is not comparable to the previous ones. Although, we consider it likely to occur and easy to exploit, we only rate the risk moderate. The reason for this choice is the weighting of assets from Section IV-A.

The overall result from our risk analysis is that essentially, the highest threat to the system originates from the Roadside Attacker that tries to distribute wrong warning messages. Therefore, the next section will provide an overview on attacks that could be used to achieve this goal.

V. ATTACK ANALYSIS

A detailed attack analysis for VANETs is presented in [1]. In this work, we focus on a subset of these attacks that aim to manifest the previously identified threat that results in high risk to the system. Thus, we look into attacks that aim at realizing the "Distribute wrong or forged messages" threat and can be realized by a roadside attacker. The different attack possibilities are enumerated and grouped by using a so called attack tree [13]. The resulting attack tree is shown in Figure 2.

In order to disseminate a false message, the attacker can either create a new message, replay an existing message or modify a message. The creation of a new message can either be done by the attacker himself or the attacker can try to make another vehicle create a false message, for example by stimulating the other vehicle's safety system sensors. Message replay and message modification are quite similar attacks. In both cases, the attacker has to receive or capture a message first. The difference between receiving a message and capturing a message is that in the first case, the attacker is the legitimate receiver of the message, whereas in the second case, the attacker captures the message in transit. Once the attacker

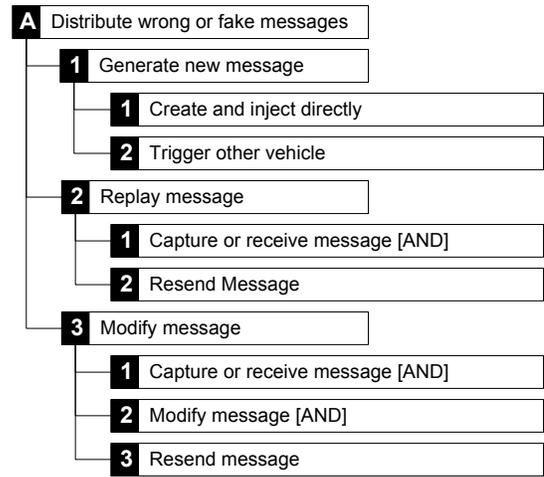


Fig. 2. Attack Tree A: Distribute Wrong or Forged Messages

knows the message, for the replay attack he directly resends the message, for the modify message attack, he modifies the message and resends it afterwards.

In the attacks that comprise the creation or modification of a message all fields of the warning message can be set or changed by the attacker. In our minimalistic model these fields are Node ID, Node Position, Time and Warning (Figure 1). The attacker has to use meaningful data in the message fields, otherwise the messages would fail the basic plausibility and consistency checks from Section III-C. Depending on the fields, this requires different effort.

- *Node ID*: The Node ID can be set any non-zero number within the maximum number of available node IDs.
- *Node Position*: This is the most difficult field to set. At first, it needs to fit in the area where the attacker wants to distribute the message. In addition, it might also show a certain movement pattern in case the attacker wants to trigger one of the cooperative awareness applications in another car. To obtain such positions, the attacker can choose from a variety of sources, as we will discuss in the next section. The simplest way for an attacker to obtain a single position is to use a GPS receiver.
- *Time*: The Time field must be set to a point in time that matches the time frame of our previously outlined consistency check. Messages that are too old or have a Time value in the future will be discarded. The simplest and most convenient choice is to use current time when sending the message, which is usually available on every computer.
- *Warning*: The field must either be empty to send a beacon, or contain the desired warning the attacker wants to distribute.

This analysis shows that using the correct position information in combination with suitable time value is a key factor for the success of an attacker, or, vice versa a key component in the defense against attackers.

Attacker	Vulnerability	Threat	Exposed Asset	Likelihood		Risk
				Attempt	Exploit	
Roadside Attacker	Unprotected wireless communication channel	Disturbance or unavailability of communication system	Communication system	Improbable	Difficult	Low
Roadside Attacker	Plaintext information exchange	Distribution of wrong or forged messages	Safety messages	Likely	Easy	High
Vehicle (Driver)	Unprotected wireless communication channel	Disturbance or unavailability of communication system	Communication system	Remote	Difficult	Low
Vehicle (Driver)	Plaintext information exchange	Distribution of wrong or forged messages	Safety messages	Conceivable	Difficult	Moderate
Infrastructure-based attacker	Plaintext information exchange	Tracking and profiling of vehicles or vehicle drivers	Privacy	Likely	Easy	Moderate

TABLE I
RISK STATEMENTS

VI. MODELING POSITION FORGING ATTACKER BEHAVIOR

In this section we provide an overview and discussion on the attacker’s possibilities regarding position forging. We define basic assumptions for both, the safety applications and the attacker. Then, we identify different kinds of position forging which are used to compose concrete attacks. We start with a very basic attack, single position forging. Subsequently, we develop more complex attacks to conclude with highly sophisticated attacks, including construction of consistent movement paths. The idea behind this approach is to take two different viewpoints on the system, the one from the attacker and the one from the defender. The attacker carries out an attack, the defender tries to prevent the success of this attack by an appropriate countermeasure. However, during design of countermeasures one has to anticipate that the attacker may know about the countermeasures and try to circumvent or even abuse it for his purposes.

A. Attacker’s degrees of freedom

As stated before, our analysis of attacks on position information in safety messages is focused on attacks conducted by roadside attackers. Such an attacker can for instance be located next to the road or on a bridge. By forging position information (and thus messages) the attacker aims at misleading vehicle safety systems to display warnings to their drivers. The attacker’s options to conduct such attacks range from forging the location of a single event (single warning message, e.g. broken down vehicle) to sophisticated attacks that require forging of a complex movement pattern or driving profile. The aim of these sophisticated attacks is to trigger the cooperative awareness applications, which analyze movement patterns from received beacon messages. Another purpose of these sophisticated attacks is to override security mechanisms, i.e. consistency checks.

We divide the attacker’s degrees of freedom into three dimensions. These are the attack category, the accuracy of the forged position(s) and the scope of the position forging.

1) *Attack Category*: The attack category basically depends on two criteria, the number of forged positions and the number of entities (i.e. node IDs) the attacker uses at a certain time.

He can choose to continuously forge a single position or to forge an entire movement path. He can pretend to be a single entity or assume multiple identities at a time.

Those two criteria allow for the following categories of attacks:

- 1) Forge single position
- 2) Forge multiple positions with different node IDs
- 3) Forge movement path of a single node
- 4) Forge multiple movement paths with different node IDs

In our analysis we consider forging single positions as ”basic attack”. We think that the simplest thing an attacker could do is to forge one or more position(s) not having an intended relation to each other. He can enhance this attack by either establishing a path and/or by increasing the number of forged positions by forging multiple entities.

Forging multiple positions with different node identities is similar to the basic attack. The attacker’s effort increases marginally, the only additional aspect he has to consider is that two nodes should not be at the same position at the same time.

The difference between position forging and path forging are the restrictions that are obliged to the movement that is depicted by the path. The movement is limited to vehicles’ physical capabilities. When forging the movement, the attacker has to assure staying within these limitations. Hence, his effort increases and the attacker’s options for selecting subsequent positions are limited. Depending on the attacker’s desired level of forging detail, he has to consider speed, acceleration, heading, lanes and position change in relation to other vehicles on the road.

The last category describes an attacker that creates multiple moving entities. The attacker goal is to forge entire driving situations. In this case, he wants to try to convince vehicles from a different traffic condition by forging a majority of vehicles on the road. Note that this kind of attack demands the greatest effort compared to the other categories.

2) *Attacker’s Position Material*: The second dimension of the attacker’s degrees of freedom is the the quality of the forge position information and the quantity of position data that is available to the attacker. Quality does not only concern the

Quantity Quality	Position material			
	Limited		Unlimited	
	Inaccurate	Accurate	Inaccurate	Accurate
Position Material	<i>Static</i>	not discussed explicitly	<i>Dynamic</i>	

TABLE II
CLASSIFICATION OF POSITION MATERIAL SOURCES

accuracy of the positions on the road, but also the consistent connection to the former position in case of an attacker sending multiple messages with different positions.

As a starting point, we have a look at the data sources where position data originates from. For example, an attacker can guess positions, replay them from passing by vehicles, or he can derive positions from digital maps.

With *guessing*, we denote the random selection of position. This can be manually guessing by the attacker or even automated approximation by some algorithm that is computing positions by knowing his position.

Replaying positions from vehicles requires that the attacker is able to receive messages, extract the position and create a forged packet attaching the extracted position. In that way, he is able to get valid road positions (assuming that he does not get invalid positions from another attacker that is guessing positions). However, the attacker is limited to the positions he receives (which might be detectable by a reactive security system). In order to bypass this limitation, he can apply an artificial error model to variate positions.

A more sophisticated and elegant way to select positions is to use *digital maps*. The attacker can select arbitrary positions on roads. However, he might need to select positions close to his own current position in order to avoid sending messages that will not be taken into account by bypassing vehicles.

In Table II, we summarize this position material discussion with a scheme for the classification of position data sources by quantity and quality. The amount of position information the attacker possess can be limited by having pre-defined or recorded positions. Or, it can be unlimited when the attacker has the ability to generate positions. These two cases can be further distinguished by the quality of the position information. Quality covers the positions' character of being on valid a road and, with respect to the history, being in a valid lane, with a consistent difference to the last position.

For the position forging attacker model only two cases for the combination of quantity and quality of position data are of interest. The attacker has either a limited amount of positions with limited quality, or an unlimited number of positions with high quality. In our discussion of attacks we denote these two cases as *static* and *dynamic* position material, indicating the ability of the attacker to react to the current traffic situation.

Of course, there are many combinations in-between resulting from different kinds of data sources. However, we believe that the identified strategies fit best to the two categories of applications the attacker aims at (event driven applications and cooperative awareness applications). The remaining two strategies do not improve the attacks significantly. They either

increase only the attacker's effort (Limited Quantity/Accurate Quality), or they increase the probability of attack detection (Unlimited Quantity/Inaccurate Quality).

3) *Scope of Position Forging*: In the last dimension, we distinguish the scope of the forged position, i.e. the distance between the physical attacker position and the forged position.

- Unlimited, i.e. ∞
- Distance-bounded, i.e. []

Unlimited means that the attacker forges arbitrary positions without respecting a maximum distance between the forged position and his own position.

Distance-bounded means that the attacker only forges positions with a maximum distance to his own physical position. Bounding this distance one the hand decreases the probability of the attack being detected but on the other hand decreases also the influence of the attacker.

With those three dimensions in mind, we can combine the outlined degrees of freedom to establish concrete attacks. As a next step, we proceed with a discussion of the attacks by introduction an effort-impact-analysis. Effort comprises both hardware and software capabilities as well as knowledge on correct usage of the communication protocols. The impact describes the quantity and quality of the influence on passing by vehicles.

B. Attack Compositions

The combination of the above stated degrees of freedom will be discussed in the following. We point out the most significant combinations serving the attacker to reach his goal, i.e. to trigger an event-driven application or a cooperative awareness application as defined in Section III-B. Table III provides an overview on all possible combinations, i.e. the concrete attack composition. We will now go through each category.

The first category of attacks on position information is very basic. Here, an attacker only uses one ID at a time and does not care for the consistency of subsequent positions. We assume that he aims at forging an event. In order to do so, he needs one or few more positions. According to this motivation of the attacker, it is sufficient to have static position data. He only has to find a suitable position, depending on the event forging location, and may then proceed with sending the message. Hence, the attacks 1a) and 1b) are of further interest. For 1c) and 1d) the effort to carry out this attack is higher, but we think there is no increase in the probability of success of this attack. The main reason is that there is no consistent relation between positions transmitted in subsequent messages. Hence, this may be detected regardless whether the position is accurately on the road or not. Nonetheless, this strategy is suitable as event driven messages occur less frequently than beacon messages and require only one position. Summarizing this category, for an attacker that wants to influence many vehicles by means of a forged safety message for example, the most interesting choice in terms of position information is to use single ID position forging with static distance-bounded positions.

Figure 3 illustrates an example of attack 1b). Attacker A is shown by the black circle. He uses random position data

Attack Position Data Scope	1) Single Position		2) Multiple Positions				3) Single Path				4) Multiple Paths					
	Static	Dynamic	Static	Dynamic	Static	Dynamic	Static	Dynamic	Static	Dynamic	Static	Dynamic	Static	Dynamic		
	∞	[]	∞	[]	∞	[]	∞	[]	∞	[]	∞	[]	∞	[]		
Attack ID	1a)	1b)	1c)	1d)	2a)	2b)	2c)	2d)	3a)	3b)	3c)	3d)	4a)	4b)	4c)	4d)

TABLE III
ATTACK COMPOSITION

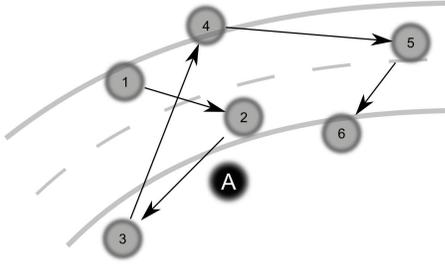


Fig. 3. Sample set of forged positions, Category 1

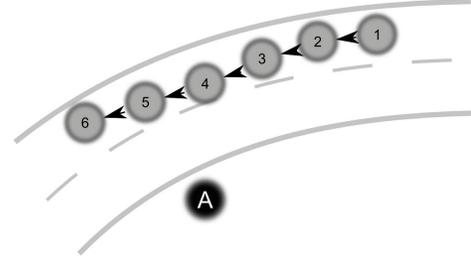


Fig. 5. Sample forged path, Category 3

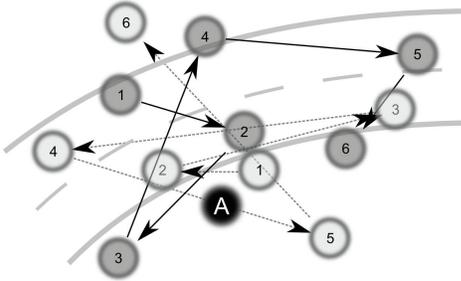


Fig. 4. Sample set of forged positions using two IDs, Category 2

which is limited to a small region around him. The successive locations he claims to be at are indicated by the grey circles with increasing numbers. The numbers, in turn, show the order, i.e. the point in time at which the position information is broadcasted. The arrows that connect each location represent the difference in the position. With respect to time, this difference is equal to the (forged) movement. By observing this movement compared to the course of the road there is obviously an inconsistency. From a more abstract point of view, if we treat the arrows as vectors, we can inspect their similarity. This includes their orientation and length. As we have seen, based on random position forging, the similarity is very limited and hence can be detected. This basic flaw of such kind of attacks does not improve when using multiple IDs as we discuss in the following.

The second category in Table III provides an overview on possible attack strategies for an attacker using multiple IDs. The additional usage of multiple IDs might help the attacker to convince vehicles of an upcoming event. Compared to attack case 1, the attacker might consider unlimited position forging. The attacker could combine attack 2a) and 2b). In other words, he can forge positions very far away, which might be detected by some vehicles but also forge positions within a limited

scope. The benefit of that combined attack is to have the influence on vehicles by distance bounded forging in parallel with possibilities of far-distance position forging. Figure 4 shows an example scenario for attack 2b). Summarizing for this kind of position forging, the basic problem of inconsistency of successive positions remains. Using multiple IDs does not improve this situation. Hence in the following, we will look into consistent path forging.

As stated before, if the attacker is motivated to pass plausibility checks or even wants to influence applications based on frequent position information, he has to apply forging of entire movement paths. Category 3 in Table III shows the relevant attacks. At the first glance, static position data is sufficient in order to forge a movement path. For instance, the concrete attack could use a sequence of positions received from messages of a passing by vehicle or a set of pre-determined positions which may have been gained from Google Earth. We think that this kind of attack will only work successfully when the traffic situation does not change. If it changes, the inconsistent movement path may be detected with respect to other movement paths. In other words, the attacker is limited to the current movement pattern of the vehicle.

In order to react on the current traffic situation and to be flexible in movement forging, dynamic data is essential. Dynamic data increases the effort for the attack but it also increases his abilities significantly. Having the ability to determine any valid position allows the attacker to forge any kind of vehicle behavior, like for instance acceleration or emergency braking. Such an attack aims at deceiving cooperative awareness applications that consider positions and movement.

In Figure 5 an example for attack 3d) is shown. The attacker is able to create a consistent movement path. The difference between the positions, again indicated by arrows, shows a particular pattern. Velocity and heading only change slightly and smoothly. Other vehicles within transmission range would suppose this entity as a normal vehicle driving on the road.

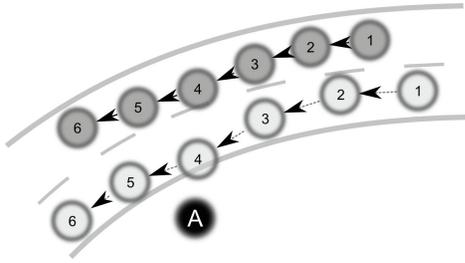


Fig. 6. Sample set of two forged paths using two IDs, Category 4

The next logical step is to carry out multiple path forging simultaneously, as shown in Table III for Category 4. The effort for this kind of attack increases linearly with the number of paths to be forged. Depending on the intelligence of consistency checks, the attacker has to be even more careful with the construction of the forged paths. However, if he is performing path forging inaccurately for one entity this does not necessarily enable the detection of other forged paths that are accurately forged. So, this attack is even more attractive as the probability of success increases. The attacker may succeed in forging a whole traffic situation by simulating a majority of vehicles, i.e. their positions, movement and relation to each other as well as their communication. The relevant attack cases are 4c) and 4d) where the latter one has the highest probability of passing consistency checks. Here, the same as for attack category 2) holds, the attacker may also combine 4c) and 4d).

Multiple path forging is exemplarily shown in Figure 6. The attacker transmits two sets of movement paths along the road. The arrows illustrating the movement have significant similarity which can be interpreted as a consistent movement pattern of a vehicle. By doing so, the attacker is able to create a forged view on the current traffic situation. In case of our example, surrounding vehicles would conclude that the left lane allows higher speed than right lane due to a slow vehicle on the right lane.

VII. CONCLUSIONS

Information security is an essential requirement for the effectiveness of inter-vehicle communication. In this work we conducted a security analysis to understand how attackers could endanger this requirement. We performed a risk analysis where we pointed out assets, threats, potential attacks and the final risk for the system. The outcome of this risk analysis is that (what was commonly assumed before) the highest risk for the system originates from roadside attackers that are sending forged warning messages. This finding motivates the more detailed investigation of attacks from roadside attackers.

In a first step, we discussed potential options for different attack strategies. From this overview we emphasized on position forging attacks which turned out to be a major vulnerability of the system. By bringing the applications into consideration, we identified the most promising attack on the each application. The result is that for event-driven applications single position forging is the best choice. For cooperative awareness applica-

tions the forging of multiple vehicle movement paths shows significant attraction for attackers.

The analysis also shows the different efforts needed to succeed in attacking the application. Low effort is needed to perform an attack on event-driven applications. Hence, we see the motivation must not be necessarily high, e.g. the just for fun-attack. For attacking cooperative awareness applications the effort is quite high. In other words, a high motivation is needed behind the attack, e.g. a profit-oriented or malicious attacker.

In future work, we will investigate mechanisms to detect the presented attacks. Moreover, currently proposed systems to distinguish between trustworthy and untrustworthy behavior will be analysed regarding false negative detections. Recently, we proposed our vehicle behavior evaluation framework VEBAS [14]. This one will also serve to enhance our attacker model with insights of a defense system like VEBAS system to allow the attacker to react on the countermeasures.

REFERENCES

- [1] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmüller, "Attacks on inter-vehicle communication systems - an analysis," in *Proceedings of Workshop on Intelligent Transportation (WIT 2006)*, 2006. [Online]. Available: <http://www.leinmueller.de/publications/wit2006-AttackModel.pdf>
- [2] —, "Attacks on intervehicle communication systems - an analysis," NOW-Project, Tech. Rep., 2005. [Online]. Available: http://www.network-on-wheels.de/downloads/NOW_TechReport_Attacks_on_Inter_Vehicle_Communications.pdf
- [3] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN'05)*, 2005. [Online]. Available: <http://lcawww.epfl.ch/Publications/raya/RayaH05C.pdf>
- [4] 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 (VANET)*. Philadelphia, USA: ACM Press, Oct. 2004. [Online]. Available: <http://crypto.stanford.edu/~pgolle/papers/vanet.html>
- [5] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks*, vol. n/a, p. n/a, 2007. [Online]. Available: <http://ivc.epfl.ch/>
- [6] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Improved security in geographic ad hoc routing through autonomous position verification," in *VANET '06: Proceedings of the 3rd international workshop on Vehicular ad hoc networks*. New York, NY, USA: ACM Press, 2006, pp. 57–66. [Online]. Available: <http://www.leinmueller.de/publications/vanet06-AutonomousPositionVerification.pdf>
- [7] W. Franz and C. Maihöfer, "Geographical Addressing and Forwarding in FleetNet," DaimlerChrysler / Fleetnet Whitepaper, 2003. [Online]. Available: <http://www.et2.tu-harburg.de/fleetnet/pdf/white%20paper%20on%20FleetNet%20addressing%20andforwarding.pdf>
- [8] C. Maihöfer, R. Eberhardt, and E. Schoch, "CGGC: Cached Greedy Geocast," in *Proceedings of 2nd Intl. Conference Wired/Wireless Internet Communications (WWIC 2004)*, ser. Lecture Notes in Computer Science, vol. 2957. Frankfurt (Oder), Germany: Springer Verlag, Feb. 2004.
- [9] C2C-CC Technical Committee, "CAR 2 CAR Communication Consortium Manifesto - Overview of the C2C-CC System, Version 1.1," CAR 2 CAR Communication Consortium, Tech. Rep., 2007. [Online]. Available: <http://www.car-2-car.org/index.php?id=570>
- [10] T. Leinmüller, E. Schoch, and C. Maihöfer, "Security issues and solution concepts in vehicular ad hoc networks," in *Proceedings of the Fourth Annual Conference on Wireless On demand Network Systems and Services (WONS 2007)*, Obergurgl, Austria, Jan. 2007. [Online]. Available: <http://www.leinmueller.de/publications/lsm07solutionconcepts.pdf>
- [11] D. J. Landoll, *The Security Risk Assessment Handbook*. Boca Raton, FL, USA: CRC Press, Inc., 2005.

- [12] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing Vehicular Communications - Assumptions, Requirements, and Principles," in *Workshop on Embedded Security in Cars (ESCAR) 2006*, 2006. [Online]. Available: <http://icapeople.epfl.ch/panos/escar-secure-vehicular-communications-fundamentals.pdf>
- [13] B. Schneier, "Attack Trees," *Dr. Dobbs's Journal*, vol. 24, pp. 21–29, Dec. 1999. [Online]. Available: <http://www.ddj.com/documents/s=896/ddj9912a/9912a.htm>
- [14] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in vanets," in *Proceedings of 4th Workshop on Vehicle to Vehicle Communications (V2VCOM 2008)*, 2008. [Online]. Available: <http://leinmueller.de/doku.php/publications:publications>