DEFENDING AGAINST ROADSIDE ATTACKERS

Robert K. Schmidt*, **Tim Leinmüller*** **and Albert Held****
*DENSO AUTOMOTIVE Deutschland GmbH, Technical Research Department, Germany,
[r.schmidt|t.leinmueller]@denso-auto.de
**Daimler AG, Research and Development, Ulm, Germany, albert.held@daimler.com

ABSTRACT

Communication between vehicles is a very promising technology to reduce fatalities and injuries in road traffic. Vehicles spontaneously form communication networks where they exchange messages to warn surrounding vehicles. Theoretically, this system is open to any communication node that is equipped with the required communication technology. This openness demands appropriate security mechanisms in order to protect against attacks and misuse.

In this work, we present a mechanism to protect the system against a particular kind of attacker, the so-called roadside attacker. First, we explain the abilities of such an attacker. Then, we introduce a defense mechanism that is based on the fact that the roadside attacker can only move barely compared to a vehicle. The idea is to build up trust relations to vehicles that have been neighbors for a certain time and thus proofed their movement. This property can not be achieved by a roadside attacker. We show how to realize such a mechanism and discuss its limitations. We further show how to integrate such a mechanism into a security system that we refer to as vehicle behavior evaluation framework.

KEYWORDS

Vehicular ad hoc networks (VANETs), Security, Behavior analysis, Roadside attacker.

INTRODUCTION

In Vehicular Ad-Hoc Networks (VANETs), all equipped vehicles are enabled to spontaneously exchange relevant information with other vehicles. This information can be used for three classes of applications, namely, safety, traffic efficiency and (passengers') convenience. Especially applications from the safety class benefit from the abilities that direct communication between vehicles provides. Even time-critical operations can be realized, e.g. warning of a hazard on the road. The goal is obvious, vehicles warn each other in order to prevent accidents and injuries.

One of the biggest remaining challenges in VANET research and standardization is security [1, 2]. Once there is a forged warning message in the system, drivers might react on that by a maneuver or become distracted. As a consequence, such a system could cause accidents instead of preventing them.

Previous work has shown [3] that the highest risk for the system originates from a roadside attacker that is sending forged warning messages, as shown in the example in Figure 1. Basically, such an attacker places himself near a road. He somehow got the technology to appear as a legitimate node in the communication network by knowing of the communication protocols and packet contents. The packets he sends are valid and contain the information he selects.

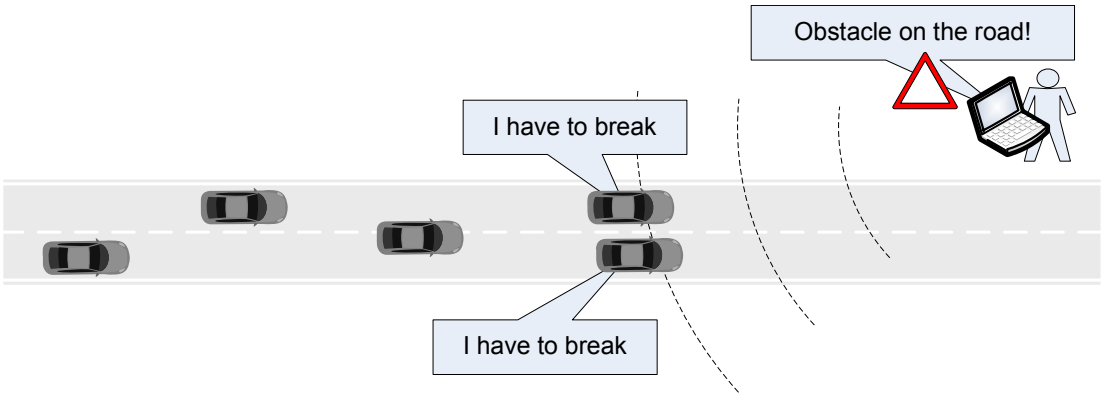

Fig. 1. Example: roadside attacker distributing forged warning message

To prevent or at least detect forged information in VANETs, a lot of approaches have been proposed. An overview on these approaches can be found in [4]. Independent of cryptographic means like digital signatures, consistency checks need to be applied. These checks can be used to determine which information does not fit to the current context.

As a framework for such checks, we have proposed the VEhicle Behavior Analysis and Evaluation Scheme (VEBAS) in [5]. The underlying hypothesis is that behavior analysis of vehicles indicates trustworthiness and untrustworthiness of messages they send. With behavior, we refer to all observable information on a vehicle, in particular its past, present and even future movements and its communication activities.

One basis for such a behavior analysis is the knowledge of the movement of the surrounding vehicles. This knowledge originates from periodically broadcasted status messages that every vehicle in the VANET is required to sent. These so-called beacons contain a vehicle identifier, the current position, velocity and heading of a vehicle. Thus, vehicles receiving a number of beacons from the same vehicle are provided with data that allows for a meaningful movement and behavior analysis. VEBAS consists of multiple *behavior analysis modules* that inspect the information on vehicle's movement for particular aspects like unreasonable position jumps. The result of this analysis leads to the per-vehicle behavior evaluation. Note that such an evaluation is only possible for vehicles which have sent some information on movement. This approach is not able to evaluate the trustworthiness of a single message sent by a newly discovered vehicle where no past information for that vehicle has been received.

With this paper, we go into detail with one behavior analysis module: Minimum Distance Moved (MDM). Its purpose is to analyze real physical movement of a vehicle. So, this module excludes non-moving entities as they do not pass this evaluation for becoming a trustworthy vehicle. MDM does not rely on the packet content on the vehicle's position or movement but only the identifier. Physical movement is verified by observing the own movement while receiving packets from the vehicle to be verified.

The remainder of this paper is organized as follows. The next section describes the attacker scenario that we address with our proposed security mechanism. The concept of this mechanism is given in the section entitled "Behavior Analysis Module: Minimum Distance Moved", followed by a discussion on implementation related issues highlighted in the section "Limitations and Implementation issues". With the last section, we summarize our findings and briefly describe follow-up work that addresses some remaining behavior analysis issues.

ROAD-SIDE ATTACKERS

The knowledge on different attackers and their behavior is essential for a proper design of countermeasures. In this section, we introduce and describe the potential attack behavior of a roadside attacker according to

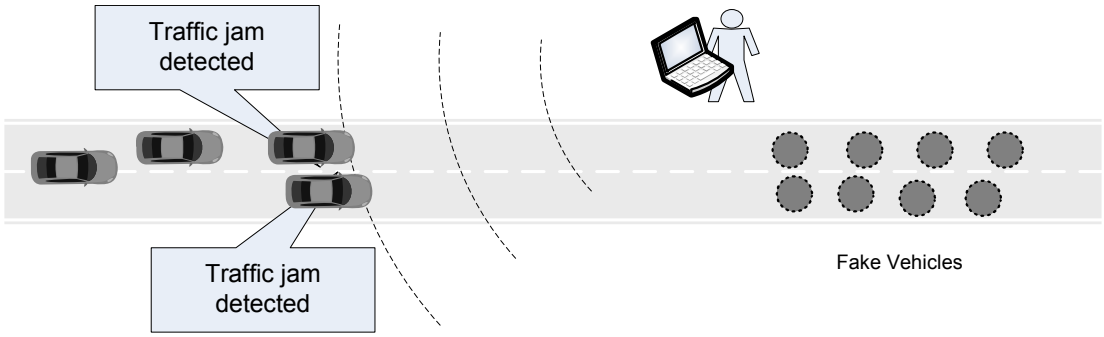

Fig. 2. Example: roadside forging traffic jam

common criteria in security engineering. The roadside attacker that focus on fulfills the following criteria.

- He is an insider, i.e. when sending messages, he appears to be a node with a legitimate communication system.
- He is acting intentionally and actively, which means that he deliberately distributes forged messages.
- His motivation can be both, malicious or profit oriented.
- He is acting alone and not in cooperation with other attackers.

As we have explained in [3], a roadside attacker has many possibilities to forge his position and resulting movement, i.e. his behavior. Summarized, theses possibilities include

- Random or calculated selection of positions (guessing)
- Replay of positions recorded from movements of other vehicles
- Digital map based selection of positions on roads.

With some of these possibilities, the attacker is even able to convince other vehicles of arbitrary traffic situations. An example for such an attack is shown in Figure 2 where an attacker forges multiple vehicle positions on a road to make follow up vehicles believe that there is a traffic jam ahead.

However, the roadside attacker can not overcome the fact that his physical position is fixed to a particular location. This limitation is the starting point for behavior analysis module that we explain in the following section.

BEHAVIOR ANALYSIS MODULE: MINIMUM DISTANCE MOVED

The basic idea of the MDM module running on the verifying vehicle V is to observe its own movement while being in contact with the vehicle under investigation (proband vehicle P). The longer the contact time, the higher the probability of P being a moving vehicle as a roadside attacker may not cover an arbitrarily large communication area. The size of this communication area also determines, how long V has to keep track of P. To verify if P has moved, its transmitter must have moved. This fact may be verified, if V travels through the whole (expected) communication area of P which translates to more than twice the communication radius. Then, if P is still within communication range, it must have moved its position. In the following, we will denote the distance to be traveled by the verifier as d_{min}.

The following example depicts the concept of MDM. Figure 3 shows three events that concern the verifier V and the proband P. At t_0 vehicle P enters the highway. V firstly receives a message from P. V then determines the distance it travels while having contact to P. At t_1, V receives another message from P. However, as we assume a communication range of 200 meters, the MDM criterion is not fulfilled yet: The traveled distance of V since the first contact to P is still smaller than twice the communication range,

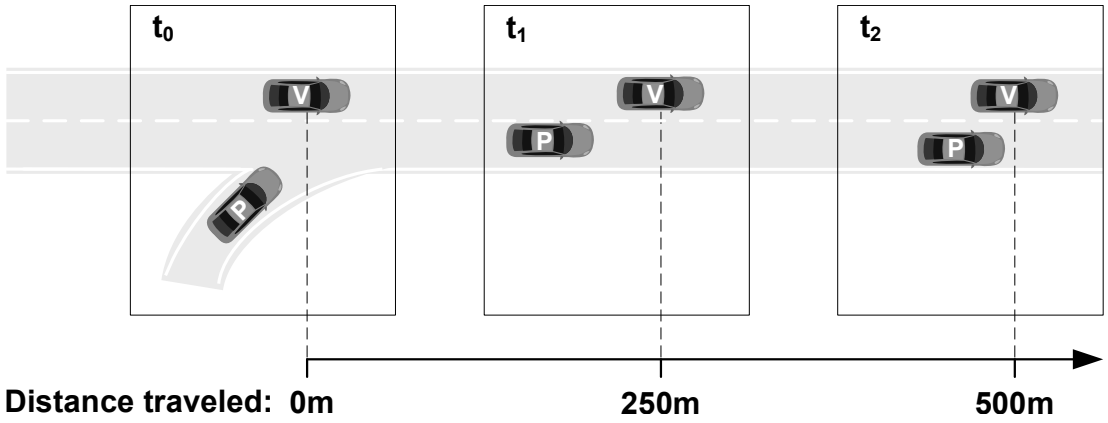

Fig. 3. Verifier vehicle V evaluates the proband vehicle P.

i.e. 400 meters. After receiving the next beacon at time t_2 this criterion is fulfilled. V has traveled 500 meters and is in communication range to P. Under the assumption of 200 meters communication range, vehicle P has now evidently moved.

LIMITATIONS AND IMPLEMENTATION ISSUES

The proper exclusion of stationary attackers in VANETs depends on a well-designed implementation. In the following we describe several aspects of the MDM module implementation. First, we discuss the basic MDM implementation concept with a flow chart. Next, we describe the crucial parameter d_{min} and criteria that have to be considered to verify movement. Then, we discuss the possibility to extended the modules output, followed by a discussion on additional consistency checks. Finally, we elaborate on the robustness of the mechanism in case of message loss.

Flow Chart - The program flow of MDM as shown in Figure 4 starts with the reception of a beacon message whose sender was newly discovered. The output of MDM is initialized with $MDM(ID) := not\ passed$. The vehicle's position at the discovery of the new vehicle is stored in $firstSeenAt(ID)$. Then, the vehicle waits for the next beacon. Receiving a beacon message from a known vehicle ID updates $distance(ID)$ according to the current air-line distance to $firstSeenAt(ID)$. In case $distance(ID)$ is above the minimum distance threshold d_{min}, the MDM returns that the evaluation for this vehicle has been passed with $MDM(ID) := passed$. If not, the output value is not changed and the vehicle waits for the reception of the next beacon to continue the evaluation.

d_{min} - The security of MDM is strongly dependent on this parameter which describes the evaluation scope. Vehicle V has to pass the distance d_{min} to provide an evaluation of a proband. How to set this threshold is not a trivial task as it results in a trade off between short evaluation time versus high attacker exclusion probability. d_{min} should be at least the doubled expected communication range which can be roughly obtained from signal propagation models, like the free space formula. It is important that the choice of the expected communication range must reflect the attacker's signal propagation and not the vehicle's signal propagation. d_{min} should be determined based on a model for ideal signal propagation or even consider mechanisms to increase the communication range. For instance, the attacker may place himself in an elevated position. On top of a bridge or a hill, he may have a line-of-sight relation to all vehicles within his range. Or, the attacker could be able to increase the transmit power or attaches advanced (directional) antennas. Figure 5 displays an example on how to set the minimum distance d_{min}. The upper figure shows a false negative decision of the MDM, where vehicle V falsely assumes movement of the attacker claiming to be vehicle X. Hence, he has not been excluded due to setting d_{min} too low. Setting this distance higher is shown in the lower part of Figure 5. After discovering the attacker (X), the

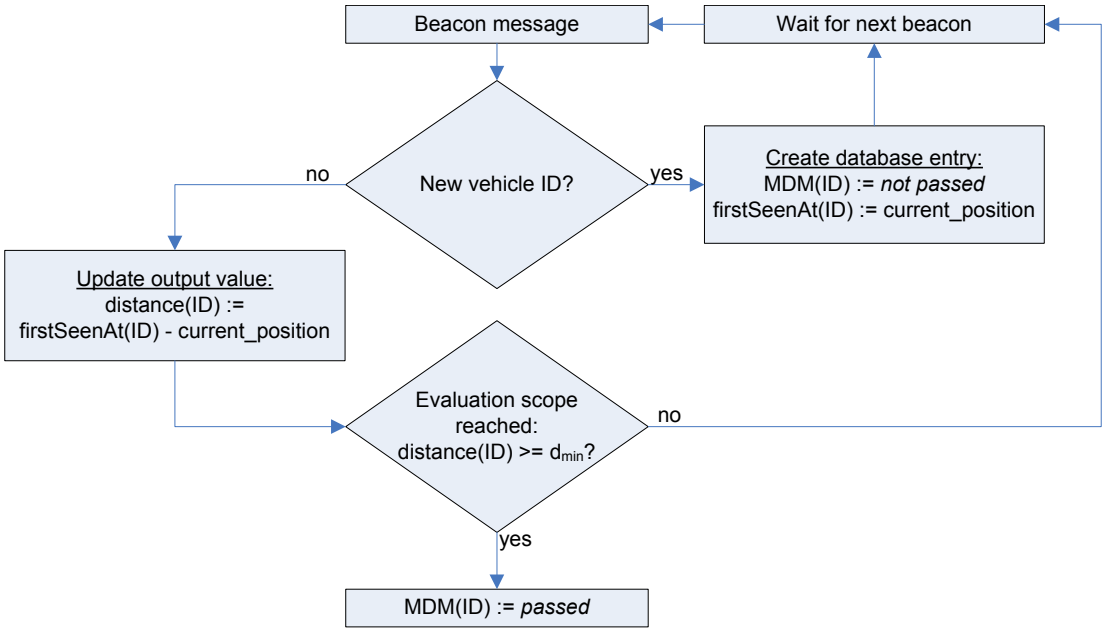

Fig. 4. Flow chart of behavior analysis of MDM.

minimum distance d_{min} is never reached as this threshold has been set much higher than the attacker's communication range.

Extended output - If we think of highway scenarios, a vehicle quickly travels a distance of 1 or 2 kilometers compared to urban areas with frequent intersections. This shows that a binary decision of MDM may not provide an evaluation within reasonable time constraints in some road scenarios. Instead of returning a true or false for a given vehicle ID, the MDM may also return a percentage of the distance traveled in relation to the minimum distance threshold. The requesting application itself may then decide if this vehicle is trustworthy enough or not. So, the interface of MDM may be extended to output $distance(ID)$.

Consistency checks - The entire received movement trajectory of the proband has to be checked for consistency. For example, changes in velocity and heading must be reasonable. If access to a digital map is available, reported positions may be verified for being valid positions on a road. These consistency checks inspect each successive beacon from the proband. In the VEBAS framework, this essential task will be done by other analysis modules and is out of scope for the MDM module. Therefore, MDM is also made robust against forged packet content as it only relies on the (digitally secured) identifier but not the data like position or velocity.

Message loss - MDM is basically tolerant against message loss as it calculates the airline distance to the first known position each time a beacon is received. It is not dependent on receiving updates frequently. However, for reasons of limited memory, the respective database entries for a vehicle should expire at some point in time. This expiry is the only point where message loss is to consider. The expiry time must be selected sufficiently high, in case the proband's messages experience high message loss or if the proband is temporarily out of communication range.

CONCLUSIONS

Safety related communication in VANETs should be as reliable and secure as possible. Wrong or forged information pose high risks to drivers' and passengers' safety. However, the history of ICT security shows that there is no such thing as a system that prevents all attacks. Consequently, recovery mechanism need to be in place to assure system operation even in the case of attacks. In VANETs, amongst others, this

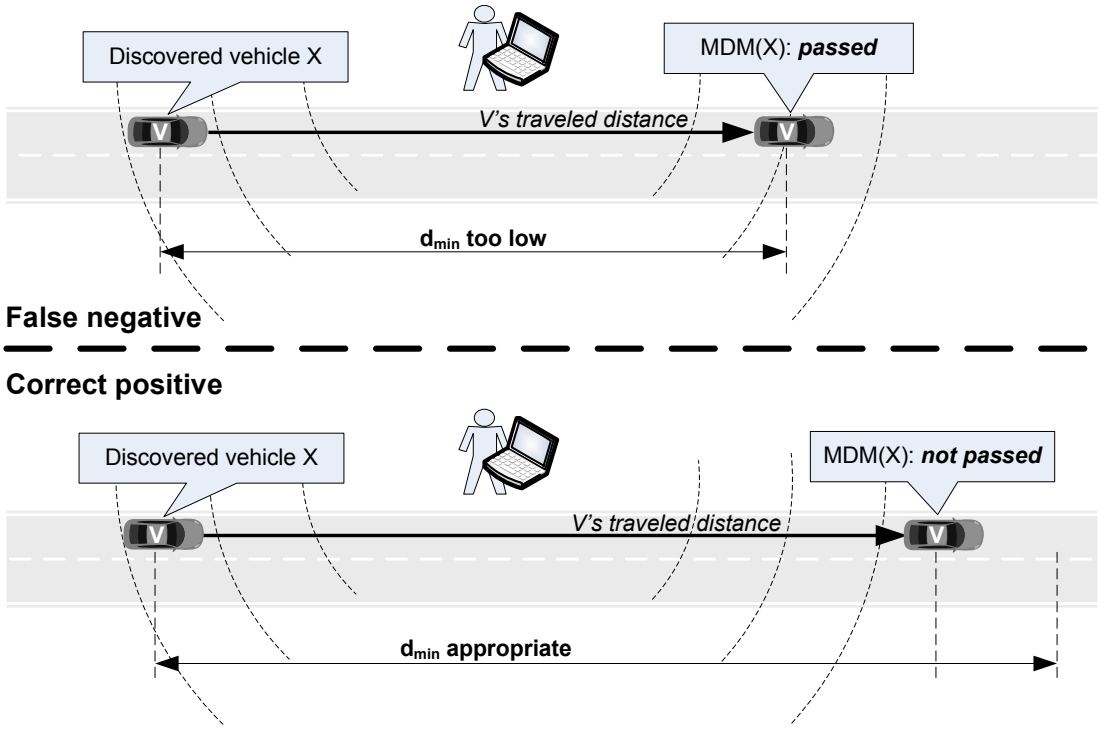

Fig. 5. False negative: MDM does not exclude the roadside attacker - Correct positive: MDM excludes the attacker.

translates to the requirement for mechanisms that detect wrong or forged information and ignore it within or exclude it from the system.

Security research in VANETs has identified and analyzed many attack scenarios. One of the most dangerous ones was determined to be the situation in which a roadside attacker is sending forged warning messages. In this paper, we have quickly summarized the abilities of such an attacker and highlighted one of his key weaknesses, the attacker's immobility. To make use of this weakness, we introduced the MDM module, a behavior analysis module that increases trust in vehicles that have been within communication range for a particular driving distance. We further discussed reasonable values for this distance. The concept is meant to be used as module for our VEhicle Behavior Analysis and Evaluation Scheme (VEBAS) framework [5].

The effectiveness of the presented module relies on proper setup. We have identified a trade off between fast vehicle evaluation and secure vehicle evaluation. For example, the setup has to consider the attacker's ability to place himself at an optimal position.

In the next step, the attacker's knowledge of the MDM module has to be considered. He may be able to increase his communication range to bypass the MDM checks, for instance by increasing the transmit power, installation of power amplifiers or directional antennas. This means that the setup of the presented module has to be adapted at the expense of an increased evaluation duration.

REFERENCES

[1] J.-P. Hubaux, S. Čapkun, and J. Luo, "The Security and Privacy of Smart Vehicles," *IEEE Security and Privacy*, vol. 4, no. 3, pp. 49–55, 2004. [Online]. Available: http://lcawww.epfl.ch/Publications/luo/HubauxCL04.pdf

[2] T. Leinmüller, L. Buttyan, J.-P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch, "Sevecom - secure vehicle communication," in *Proceedings of IST Mobile Summit 2006*, 2006. [Online]. Available: http://www.leinmueller.de

[3] T. Leinmüller, R. K. Schmidt, E. Schoch, A. Held, and G. Schäfer, “Modeling roadside attacker behavior in vanets,” in *Proceedings of 3rd IEEE Workshop on Automotive Networking and Applications (AutoNet 2008)*, 2008. [Online]. Available: http://leinmueller.de

[4] 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

[5] 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://www.leinmueller.de/