COOPERATIVE POSITION VERIFICATION - DEFENDING AGAINST ROADSIDE ATTACKERS 2.0

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

ABSTRACT

Security analysis has shown that attacks from roadside attackers constitute the highest risk for vehicular ad-hoc networks (VANETs). Therefore, protecting them against these attackers is one of the primary goals of security engineering in VANETs.

In previous work, we introduced a defense mechanism that is able to defend against roadside attackers to a certain extend. The main weaknesses of this mechanism are solved by the additional mechanisms introduced in this work.

As in our previous work, vehicles build up trust relations to other vehicles that have been neighbors for a certain time and thus proofed their movement. Upon detection of new neighbors, information from already trusted neighbors is used to evaluate the new neighbor. The new approach shortens the evaluation time of new direct neighbors and defends against attackers that try to circumvent the previous defense mechanism by increasing their transmission range.

KEYWORDS

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

INTRODUCTION

Vehicular ad-hoc networks (VANETs) enable for applications aiming at increasing road safety. Periodic exchange of position information, referred to as beaconing, cooperative awareness message or heartbeat message broadcast, is the basic information that enables cooperative safety applications. In addition, event triggered messages are used to inform about specific events such as roadworks or the tail-end of a traffic jam. These applications have the potential to enlarge the drivers horizon and to reduce fatalities and injuries in road traffic.

Security engineering for VANETs and its applications is challenging (1, 2). For example, there is no means to protect against denial of service attacks like jamming the communication channel. Thus, the primary objective of security engineering is to ensure that things do net get worse than they are without VANETs. Appropriate security mechanisms should defend against attackers that send forged safety messages. 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.

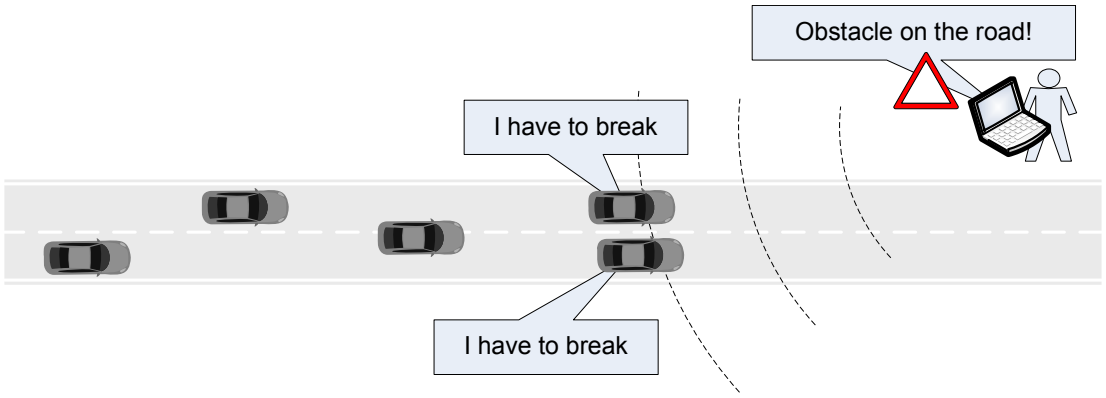

Fig. 1. Example: Roadside attacker distributing forged warning message.

Several security concepts have been proposed to address this problem. An overview on these approaches can be found in (3). Security analysis shows that roadside attackers constitute the highest risk to VANETs (4) under the assumptions above. These attackers are located next to a road and equipped for instance with a laptop. By a suitable radio interfaces he is able to send messages to passing vehicles in the VANET (Figure 1). He pretends to be a vehicle as his messages are not distinguishable from other vehicles' messages.

In previous work, we introduced an autonomous defense mechanism called Minimum Distance Moved (MDM) which specifically targets roadside attackers (5). It is based on the fact that roadside attackers can only move barely compared to vehicles. Vehicles build up trust relations to other vehicles that have been in the vicinity for a certain time/distance and thus proofed their movement. This property can not be achieved by a roadside attacker.

In (5), we also discussed the shortcomings of MDM . These are the required evaluation time, i.e. the trade off between fast evaluation of vehicles and secure evaluation of vehicles, and the vulnerability to attackers that increase their transmission range.

In order to solve these problems, we propose cooperative mechanisms that follow two basic ideas. First, "MDM passed" ratings are exchanged between neighbor vehicles (neighbors). The ratings are adopted in case the information is received from a neighbor that already passed MDM. Second, vehicles exchange identifiers (IDs) of and/or position information of their neighbors.

In the following, we provide a basic VANET model to support the security discussions in this work. Then, we briefly summarize the MDM mechanism and discuss its limitations. In Section 3 we introduce the attacker model that contains the capability to circumvent MDM. In response, we present cooperative mechanisms that aim at detecting the attacker (Section 4). Finally, we summarize the achievements in the last section.

BASIC VANET MODEL

Communication System

VANETs use wireless communication according to the IEEE 802.11 protocol family (IEEE 802.11p). Our model assumes that all vehicles share a single communication channel. For the transmission range of every vehicle, a certain maximum value is assumed, e.g. $250m$. Warning messages are distributed via single hop broadcast. The system supports geo-message distribution and geo-routing for distribution of messages inside geographic areas. For more details on geo-routing and geo-message distribution please refer to (6) and (7).

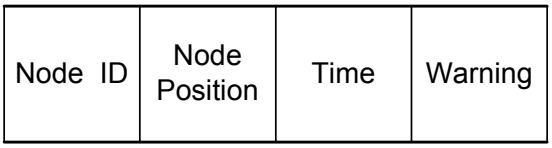

Fig. 2. Simplified warning message format

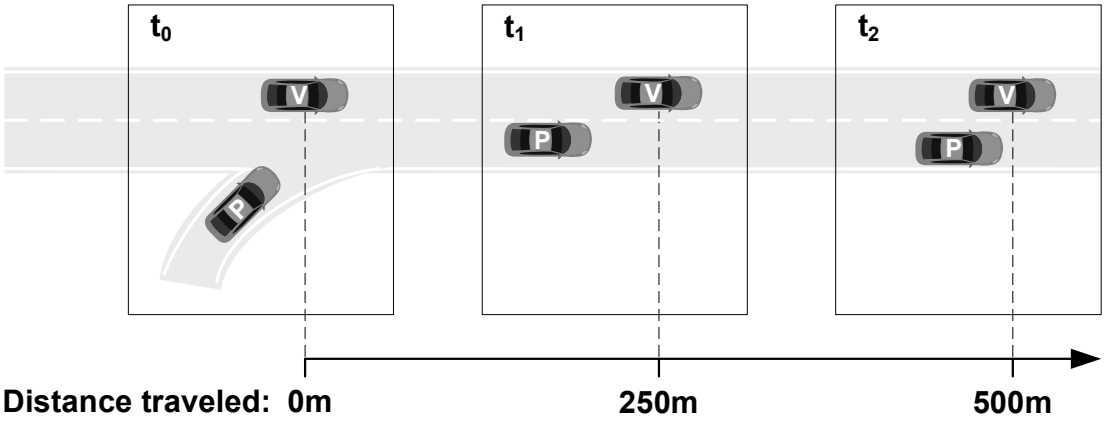

Fig. 3. MDM concept

Active Safety Applications and Message Format

Safety applications in VANETs can be divided into two categories (4):

- Event-driven applications
- Cooperative awareness applications.

For this work, the second category is of interest as it relies on the same information exchange that also provides the basis for our security mechanisms. Cooperative awareness applications determine dangerous situations based on the analysis of received position information from the surrounding vehicles. The information is collected from so called beacon messages that are broadcasted regularly (at least once per second) by every vehicle.

Beacon messages can be seen as an instance of the general message format shown in Figure 2 with an empty ”Warning” field. The ”Node ID” (temporarily) identifies the vehicle that sends this message. ”Node Position” determines the sending vehicle’s position, and ”Time” the time when the message was sent originally.

MINIMUM DISTANCE MOVED (MDM)

MDM at a Glance

The basic concept of the MDM mechanism is shown in Figure 3. MDM runs on the verifying vehicle V observing the vehicle’s own movement while being in contact with a vehicle under investigation (proband vehicle P). The higher the distance V has moved while staying in contact with P, the higher the probability of P being a moving vehicle as a roadside attacker can not cover an arbitrarily large communication area. In Figure 3, at time t_0 V encounters P for the first time. After traveling $250m$ (time t_1), P is still within radio range of V. Likewise, after $500m$ (time t_3). Assuming that V has defined the required distance to be $500m$, trust in P is established at time t_3.

The size of this required distance depends on the assumed communication range (it determines how long V has to keep track of P if traveling at a certain speed). V is able to confirm that P is moving if V travels through the whole (expected) maximum communication area of P, which translates to more than twice the maximum communication radius. Then, if P is still within communication range, it must have moved. We denote the distance to be traveled by the verifier as d_{min}.

Limitations of MDM

As mentioned previously, the limitations of MDM are the

- Required evaluation time
- Vulnerability to attackers with capability to increase transmission range

By design, MDM requires a minimum time $t_{min} = d_{min}/v_V$ (with v_V denoting the average speed of vehicle V) to provide an evaluation for proband vehicle P. Since neither reduction of d_{min} nor increase of v_V are acceptable to solve this limitation other mechanism are required.

Secure evaluation (i.e. attacker exclusions) is strongly dependent on d_{min}. It should be at least twice the expected maximum communication range. This range can roughly be obtained from signal propagation models, like the free space formula. In consequence, an attacker that is aware of MDM (d_{min}) will increase his communication range. From this point of view, the higher d_{min}, the better. This in turn results in even longer evaluation times, which are not acceptable.

ATTACKER MODEL

The assumed attacker model for a roadside attacker is the same as in our previous work (see for example (4)).

- The attacker is stationary
- 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.
- He is acting alone and not in cooperation with other attackers.

Since the attacker is aware of the possibility that other vehicles employ the MDM mechanism, he has to take additional efforts to be classified as a moving vehicle. To pass MDM although he does not move, the attacker has to:

- Forge movement paths
- Increase his transmission range.

Note that forging movement paths is not a requirement that originates from MDM. However, it is quite obvious that vehicles employing MDM will also employ simple mechanisms verifying movement continuity.

Movement Path Forging

A detailed description of how the attacker can obtain forged position material and movement paths can be found in (4). In summary, possible options to obtain movement paths are:

- Random or calculated selection of positions (guessing)

- Replay of positions recorded from movements of other vehicles
- Digital map based selection of positions on roads.

For this work, there is no difference in which option the attacker is using.

Increase of Transmission Range

To increase his transmission range, the attacker can:

- Increase transmit power
- Increase antenna gain through directional antennas.

Other means to increase the transmission range, e.g. cooperation with other nodes to use multiple spatially separated coordinated transmitters are out of scope for this paper. It can be assumed that it would be much simpler to overcome the mobility restriction by using a vehicle.

COOPERATIVE POSITION VERIFICATION

There are two principles for cooperative position verification that can be used to address the aforementioned shortcomings of MDM. These principles are:

- Transitive trust
- Exchange of neighbor information.

Obviously, the basic requirement for cooperative position verification is that there is a certain minimum penetration rate. Otherwise, the security systems are limited to autonomous verification. We assume that vehicles are always having at least two other communicating vehicles in communication range, one in front and one behind.

The general drawback of cooperative mechanisms is that they introduce communication overhead and might even enable new attack vectors. Therefore, the introduced mechanisms are trying to keep the overhead as small as possible. Different strategies are planned to be compared by means of simulation in future work. Additional attack vectors that are of interest for potential attackers are excluded by design as we explain in the following.

Transitive Trust

Transitive trust relations are used to reduce the time required to have a positive evaluation (”MDM passed”). Every vehicle informs its neighbors once it rates another vehicle as ”MDM passed” because it has moved d_{min}. The neighbors accept this rating in case the informing vehicle has the status ”MDM passed” from their point of view. The ratings are not passed on by the receiving vehicles. To ensure that new neighbors are informed about recent ratings, every vehicle repeats its ratings either periodically or triggered by detection of new neighbors.

Figure 4 shows an example where transitive trust is used. At time t_0 V and C have already been traveling together for a certain time/distance and thus trust each other (MDM passed). P enters the road and V starts MDM verification for P. C and P are not within communication range of each other. At time t_1 P passes the MDM for node V. V communicates this event to C. If now, C and P get into communication range (e.g. because of C braking hard), C instantaneously is able to trust P.

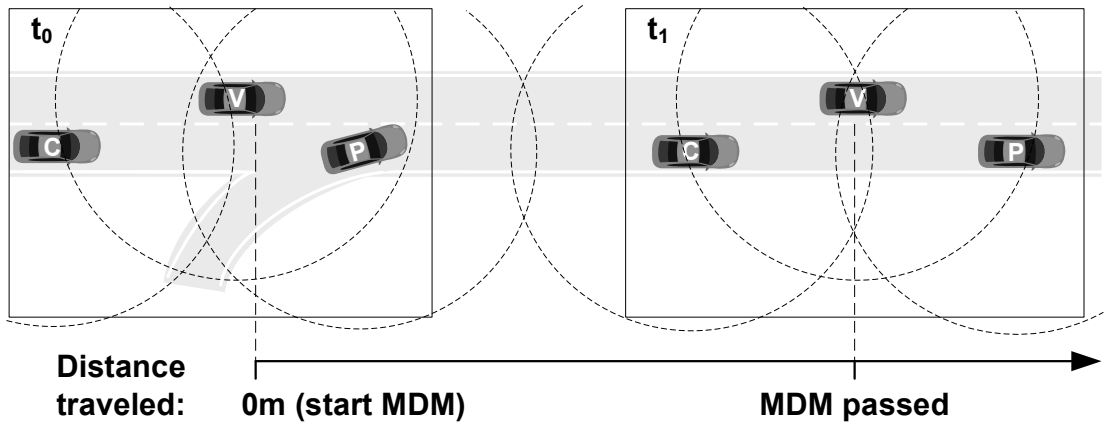

Fig. 4. Example: Transitive trust based mechanism.

This example shows, ideally, the time required to rate a newly detected vehicle reduces to 0 seconds. It is difficult to give an estimation on the reduction on average since it depends on unpredictable factors like the traffic scenario (city, rural road, or highway), road traffic flow, or (equipped) vehicle density. By nature of the mechanism, highest reductions are expected in scenarios where vehicles move in the same direction with similar velocities for a long(er) time. This means, the mechanism is expected to work best in highway scenarios or rural road scenarios.

Note that this transitive trust based mechanisms does not create additional attack vectors that are interesting from an attackers point of view. The reason is that if an attacker is able to get a ”MDM passed” rating (which is the prerequisite to report other vehicles as ”MDM passed”), there is no point in reporting another node as ”MDM passed” to conduct an attack. The attacker can directly use the node that achieved ”MDM passed”.

Exchange of Neighbor Information

The exchange of neighbor information addresses the problem of an attacker increasing his transmission range and forging movement paths. The vehicles use proactive or reactive exchange of neighboring node IDs to detect that the attacker is forging position information (as introduced in (8)). For the remainder of this work we simply assume proactive exchange. The difference between proactive and reactive exchange in terms of communication overhead is subject to future work.

In contrast to the MDM mechanism, the analysis of exchanged neighbor information includes the analysis of position information from and movement data of the proband vehicle P. Every vehicle determines which of its neighbors should be within communication range of P. The results are compared with the received neighbor information. Inconsistencies in the movement of P indicate that P could be an attacker. As a result, the ”MDM passed” threshold d_{min} for the assumed attacker is increased (at least doubled, for a detailed discussion on the increase see below). The potential threat is communicated to all other vehicles within the increased d_{min} distance. These vehicles will increase their d_{min} accordingly.

Figure 5 shows an example scenario in which an attacker A is extending his communication range and placing himself virtually at position A_1. His intention is to virtually move together with vehicle D to pass D’s (and the other vehicles’) MDM threshold. If the exchange of neighbor information mechanism is not in place, A succeeds after the vehicles moved for at least d_{min}. With the mechanism in place, vehicle C will determine if A_1 should be seen by B and D. According to the assumption of a limited communication range $r = d_{min}/2$ C assumes that A_1 should be seen by D but it should not be seen by B. Through the exchange of neighbor information, C knows that B is seeing A_1. Therefore, C increases

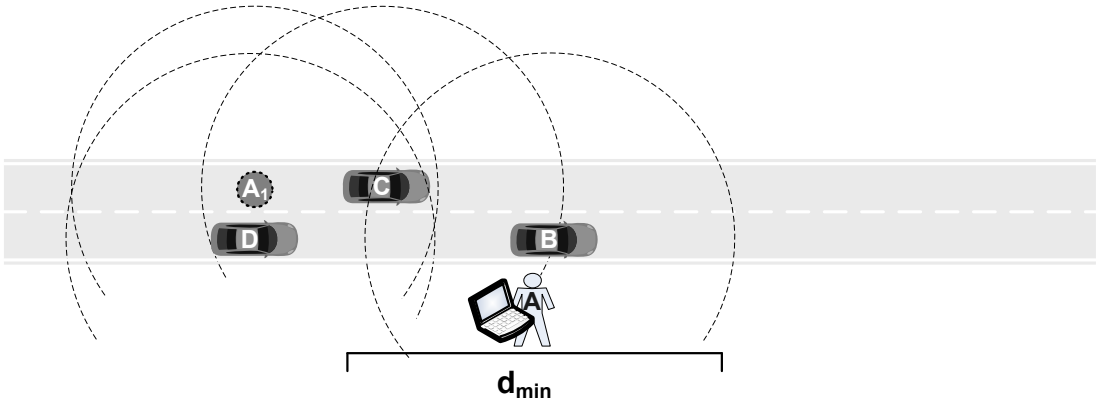

Fig. 5. Example: Exchange of neighbor information based mechanism.

(e.g. doubles) d_{min} for A_1 and notifies D and B to do the same. In consequence, A_1 is not able to obtain the "MDM passed" status because he is unable to cover the increased d_{min} distance.

As shown in the example, the selection of the increased value for d_{min} is crucial. Selecting a very high value results in unnecessary delays for the MDM validation. Setting the value too low bares the risk that the attacker's increase of the communication range is large enough to bypass the increased d_{min}. Ideally, d_{min} should be increased by the distance the attacker is enlarging his communication range. Since this distance is difficult to predict, d_{min} should be at least doubled, in case the detection mechanism provides indication that the enlarged communication range is between d_{min} and $2 * d_{min}$. In case the detection mechanism indicates that the attacker increased his communication range more than $2 * d_{min}$, d_{min} should be be increased to $4 * d_{min}$. Following our reasoning in Section , we consider a communication range increase of more than $4 * d_{min}$ less attractive than using a vehicle.

The increase to up to $4 * d_{min}$ is also the rationale behind communicating the potential threat not only to direct neighbors but to all nodes within the increased $4 * d_{min}$ range. Otherwise, nodes that are not within communication range of the detecting node might not be informed about potential threats. Furthermore, the information about the threat should be kept alive in this area for a certain time, e.g. by using Abiding Geocast (9).

It is important to note that the neighbors providing their neighboring nodes's IDs do not have to have the status "MDM passed" in order to be taken into account. The reason is that the mechanism can barely be abused (e.g. by an attacker trying to discredit a vehicle) The consequences of a vehicle falsely being classified as threat are at worst that it needs to move four times the normal distance it would have to move to prove that it is a vehicle. An attacker in a certain area could at most cause a general increase of d_{min} for all nodes in this area. Given the nature of the wireless communication channel there are much more attractive possibilities to disturb VANET communication.

CONCLUSIONS

Cooperative safety applications in VANETs should be as reliable and as secure as possible. Wrong or forged information pose high risks to drivers' safety and passengers' safety. Security research in VANETs has identified roadside attackers as a likely source of such forged information and hence is one the highest threats.

This paper continues our previous work and enhances the autonomous Minimum Distance Moved defense mechanism (MDM). MDM is enhanced through cooperative position verification using transitive trust relations and exchange of neighbor information. Both mechanisms compensate for the major shortcomings

of MDM. They reduce the time required by MDM to determine that a neighbor is a moving vehicle and they enable the detection of attackers that increase their transmission range. The combination of both mechanisms provides a solution to the trade off between fast vehicle evaluation and secure vehicle evaluation.

In future work we will analyze the communication overhead originating from different options. Furthermore we plan to conduct simulations studies on the effectiveness of our mechanisms in terms of time reduction and detection rate of different increases of the transmission range. For this purpose, we will also integrate the mechanisms in our VEhicle Behavior Analysis and Evaluation Scheme (VEBAS) framework (10).

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, 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

(4) 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://www.leinmueller.de

(5) R. Schmidt, T. Leinmüller, and A. Held, "Defending against roadside attackers," in *In proceedings of 16th World Congress on Intelligent Transport Systems*, 2009. [Online]. Available: http://www.leinmueller.de

(6) 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

(7) 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.

(8) T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Decentralized position verification in geographic ad hoc routing," *SECURITY AND COMMUNICATION NETWORKS*, vol. -, pp. –, 2008. [Online]. Available: http://www.leinmueller.de

(9) C. Maihöfer, T. Leinmüller, , and E. Schoch, "Abiding geocast: time–stable geocast for ad hoc networks," in *VANET '05: Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*. New York, NY, USA: ACM Press, 2005, pp. 20–29.

(10) 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