Simulation of Attacks and Corresponding Driver Behavior in Vehicular Ad hoc Networks with VSimRTI

Norbert Bißmeyer
Fraunhofer Institute for
Secure Information
Technology (SIT)
Secure Mobile Systems
(SIMS)
Rheinstraße 75
Darmstadt, Germany
norbert.bissmeyer@
sit.fraunhofer.de

Björn Schünemann,
Ilja Radusch
Fraunhofer Institute for
Open Communication
Systems (FOKUS)
Automotive Services and
Communication Technologies
(ASCT)
Kaiserin-Augusta-Allee 31
Berlin, Germany
[bjoern.schuenemann,
ilja.radusch]@
fokus.fraunhofer.de

Christian Schmidt
Deutsche Telekom AG
Hochschule für
Telekommunikation Leipzig
(HfTL)
University of Applied Sciences
Gustav-Freytag-Str. 43-45
Leipzig, Germany
christian.schmidt@hft-
leipzig.de

ABSTRACT

A malicious attack in which bogus information is distributed in a vehicular ad hoc network may have notably effect on the traffic efficiency. The reliability and trustworthiness of a VANET is very important, especially in the deployment phase. As long as the density of vehicles on the road, equipped with a VANET communication system, is relatively low, the introduction of bogus traffic information by attackers may have substantial impact due to the lack of vehicles that are able to disprove such faked information. As result, vehicle drivers may react corresponding to a displayed danger warning and therewith thwart the road traffic unnecessarily.

We present possible ways to simulate stationary and moving attackers in order to show their effect on the traffic efficiency by considering appropriate driver behavior. In order to have realistic traffic and communication behavior, the simulation runtime infrastructure VSimRTI is used.

1. INTRODUCTION

In future vehicular ad hoc networks (VANETs), wireless communication opens up promising possibilities to enhance traffic safety on the roads, improve its efficiency and may provide additional infotainment services to the driver. In order to realize such applications, information is exchanged between vehicles or between vehicles and roadside units (RSUs). Whereas this Vehicular-to-X (V2X) communication is definitely an enrichment for the road traffic, an attacker that distributes bogus information may neutralize the positive effect or worse, may downgrade traffic efficiency. Hence, the exclusion of attackers from the network by applying cryptographic security mechanism, as summarized in the Trail-Use standard IEEE 1609.2 [1], is very important. Nevertheless, internal attackers in the possession of valid credentials are still a risk due to the decentralized character of VANETs and the wireless communication links. Therefore, reactive security mechanisms [18] are necessary that detect attackers in the V2X communication and avoid negative influences to the VANET subsequently.

For information exchange by V2X communication, two basic message types are considered by standardization efforts in Europe. Cooperative Awareness Messages (CAMs) are used to distribute regularly vehicle or RSU positions periodically. These beacons are broadcasted in the direct communication range and basically contain data of the sender such as the current timestamp and the position including latitude, longitude, heading and speed [3]. The second message type, a Decentralized Environmental Notification Message (DENM), is used to inform adjacent network nodes via broadcast or distant nodes via multi hop forwarding mechanisms about unexpected events (e.g. congested areas or hazards on the road) [4]. Vehicles equipped with a V2X communication system display relevant information to the driver by a Human Maschine Interface (HMI) that may be combined with a navigation system.

1.1 Motivation

As previously argued, attackers may be available in VANETs despite cryptographic security mechanisms applied. Hence, detecting attackers with various malicious behavior is important to impede their negative influence. In the context of intrusion detection, it is well known that estimating the behavior of attackers is challenging, especially, if no practical experience from a real network is available.

As result, the simulation of attack behavior is an important tool for adjusting security systems that detect misbehavior in V2X communication. With a realistic simulation framework, presented in section 3, a detailed analysis of possible attack outcome is enabled. Based on attack models that can relatively easy be implemented and adjusted in a simulation,

SIMUTOOLS 2011, March 21-25, Barcelona, Spain
Copyright © 2011 ICST 978-1-936968-00-8
DOI 10.4108/icst.simutools.2011.245577

further endangerments to a VANET can be identified. We focus in this paper on attacks that may have an noteworthy impact to traffic efficiency.

1.2 Challenges

For identifying new attackers and their behavior, we use a simulation environment that allows easy and fast implementation of malicious node behavior. The estimation of possible attack scenarios is a challenging task due to the variety of traffic situations on the road. Another challenging task is the estimation of possible driver reactions caused by bogus information displayed on a virtual HMI. In [6], models about driving habits are proposed that primarily consider Post Crash Notifications (PCN). Based upon findings described in related work, we propose additional driving behavior models.

1.3 Structure

The paper is structured as follows. In section 2, we present related work that considers attack models which can be assumed to be realistic in VANETs and discusses attacker impact on the V2X communication system. Section 3 describes the simulation framework VSimRTI that is used to simulate the attacks described in section 4. In order to show the impact of our attacker models, section 5 describes the evaluation based on simulated driver behavior. Section 6 concludes this paper and describes future work.

2. RELATED WORK

As motivated in section 1.1, the analysis of attack scenarios is important for a vehicular Intrusion Detection System (IDS) to develop respective security mechanisms. Most IDS approaches proposed in [10], [11] and [21] base on restrictive attacker models. Additional models proposed in this work can be used to adjust such systems in order to get better detection results and reduce false positive detections. Attack behavior is discussed in several proposals, especially in the context of detecting misbehavior in V2X communication. In [17], a road side attacker is assumed to be most probable. Additional to this approach, we assume moving attackers which in our analysis are not restricted to a certain geographical area. Similar to [17], we focus on the distribution of bogus information.

In [16], the negative effects on multi hop message delivery is analyzed which is caused by faked position information sent by an attacker. In contrast to this work, we simulate driver behavior and analyze the effects on the traffic efficiency, i.e. effects on travel time. In [6], the effect on the driver behavior is analyzed in the case that an attacker broadcasts PCN messages. Additionally to this approach, we consider different attacker models combined with varying traffic situations and different driver behavior.

3. V2X SIMULATION FRAMEWORK

To show the effects of stationary and moving attackers on the traffic efficiency, it is necessary to actually test and evaluate the appropriate driver behavior. Running a real field test is highly complex and expensive. For this reason, we use software simulators to particularly examine certain scenarios, validate their findings, and prepare real tests. However, traffic simulation itself is a hard task as there is no mathematical model of traffic flow [8]. Moreover, in the field of V2X communication, traffic simulation itself does not suffice [19]. To validate an attacker, we also need a communication network simulation component and we have to be able to implement own applications that run on every vehicle. Therefore, we use a framework that provides the integration of several simulators. This framework is called *V2X Simulation Runtime Infrastructure* (VSimRTI) [14, 15]. In several studies, e.g. [22, 20], VSimRTI has been used to analyse the behaviour of V2X applications. Furthermore, VSimRTI was used in the PRE-DRIVE C2X project[1] to get an integrated simulation tool set.

In the next sections, we will introduce the main characteristics of VSimRTI and describe the integration of the attacker scenario implementation and its evaluation.

The VSimRTI system architecture is inspired by the IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) [7]. However, the complexity of the HLA standard and its implementation would have exceeded the scope of a V2X simulation framework. Instead, a subset of the standard and some of its fundamental concepts were used to realize the V2X Simulation Framework. So, a lightweight framework for simulation integration was created that facilitates the simulation of V2X communication scenarios. Communication among the simulators is enabled by the VSimRTI which is accessible by ambassadors similar to the HLA standard.

Figure 1 illustrates the FMC Model[2] of the general architecture of VSimRTI. One of the fundamental design principles of VSimRTI is that it creates a federation of simulators that is managed by services of a runtime infrastructure[15]. A federation of simulations is built by integrating each participating simulator into a designated federate (upper part of figure 1). The resulting set of federates is managed by the runtime that provides the required services. The federates themselves consist of the simulation system as well as of two ambassador components for the bidirectional communication between the runtime core and a federate: the VSimRTI Ambassador and the Federate Ambassador. The ambassador pattern allows to transparently connect arbitrary simulation systems that provide a remote control interface. Attaching a simulation federate only requires to implement the federate ambassador interface and to realize the commands specified within.

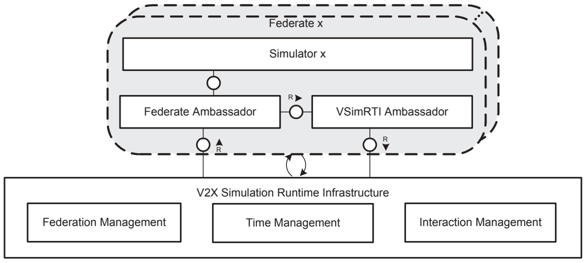

Figure 1: FMC Model of the general architecture of VSimRTI

[1] http://www.pre-drive-c2x.eu

[2] http://www.fmc-modeling.org/

The services, offered by the V2X Simulation Runtime Infrastructure (lower part of figure 1), include federation-, time-, and interaction-management [12]. The Federation Management is responsible for the lifecycle management of participating federates. This includes deploying, starting, stopping, and destroying federates in a distributed system. The exchange of data among federates is enabled by the Interaction Management that handles message publication. Message handling is realized by the interaction management using a publish/subscribe pattern based on the types of the message. Message types to exchange traffic, network, vehicle, and sensor data are predefined to realize a standardized communication behaviour. The Time Management is necessary for coordinating the simulation progress and for synchronizing participating federates. Conservative Time Management performs well under the assumption that a significant lookahead of a value greater than 0 can be provided by the simulators. However, many simulators that are common for V2X simulation scenarios, e.g. communication network simulation, may have zero lookahead values. A common algorithm for optimistic synchronization has been implemented in VSimRTI time management[12, 13]. In case of causality violations, a rollback to a correct simulation state is performed and the delivery of previously sent messages is undone. This algorithm was implemented in VSimRTI time management.

3.1 Traffic Simulator - SUMO

Simulation of Urban MObility (SUMO) is an open-source microscopic traffic simulator. It uses the Krauß car-following model [9], a collision-free vehicle movement model in which each vehicle is modelled individually [8]. Furthermore, it supports multilane roads allowing vehicles to change lanes and overtake other vehicles. SUMO is also able to model right-of-way rules at intersections of streets with equal or different priorities as well as traffic lights. According to [8], SUMO even models the drivers of vehicles which are assumed to eventually fail to always behave perfectly. Besides the actual simulation, SUMO comes with some tools to generate a network of streets and vehicle routes. Thus, it is possible to import a real map from e.g. OpenStreetMap and simulate the vehicle movements in a realistic scenario.

SUMO uses a time discrete and space continuous model which makes it suitable for the use with VSimRTI. The integration with VSimRTI has already been developed. The required ambassador converts the messages from VSimRTI and interacts with the external interface TraCI provided by SUMO [15].

3.2 Network Simulator - JiST/SWANS

The communication network simulator uses the movement data from the traffic simulator as an input to model the wireless ad hoc communication. This task is covered using the JiST/SWANS network simulator platform. Java in Simulation Time (JiST) is a general-purpose discrete event simulation engine aiming at virtual machine-based simulator construction [12, 2]. On top of JiST, the *Scalable Wireless Ad hoc Network Simulator* (SWANS) has been implemented. SWANS emulates several layers in the *Open Systems Interconnection* model (OSI model). It models the signal propagation including transmission power, reception sensitivity, antenna gain, bandwidth, error model, and more while taking mobility of nodes into account. The VANET extension by Ulm University[3] includes a new Routing Protocol for Geographic Routing, several bugfixes, and enhanced mobility models.

The performance and scalability of JiST/SWANS is high. The implemented models are partially adopted from ns-2 and GloMoSim and validated against both simulators. Although, at the Link layer, it does not implement the IEEE 802.11p standard completely as used in VANETs, the implementation of IEEE 802.11b for medium access suffices for our purpose. The Network layer implements IPv4, while at the Transport layer, both UDP and TCP are available.

3.3 Application Simulator - VSimRTI_App

The third main simulator required for the evaluation is the *Application Simulator* which is provided as a separate federate by the VSimRTI [12, 15]. This simulator provides the environment where the applications are executed in, e.g. on a vehicle, a RSU, or a traffic light. The individual applications influence the global simulated vehicle traffic. The Application Simulator contains the *Facilities Layer* which provides generic support facilities to applications. This layer is further composed of three main components according to the ETSI specifications[5]: information support for data management, e.g. the particular vehicle's movement data such as velocity, heading, and position; communication support, e.g. to achieve the various communication modes required by the applications; and application support for all common functions supporting the applications. While applications may exhibit some common requirements, their assigned use cases may also add some specific requirements.

4. ATTACKER SIMULATION

The proposed simulation environment is further used to implement attacks on the VANET with possible reactions of the driver. In the following scenarios, the attacker is distributing bogus information in order to effect the traffic efficiency negatively.

4.1 Single Lane Road

In the first scenario, the attacker has a fixed position at the road side as show in figure 2.

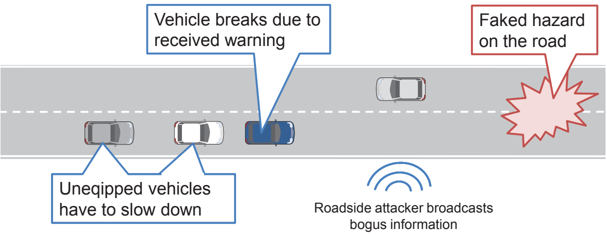
Vehicle breaks due to received warning
Faked hazard on the road
Uneqipped vehicles have to slow down
Roadside attacker broadcasts bogus information

Figure 2: Simulation of a hazard on a single lane road

It is imaginable that a laptop, a compromised RSU or a parked vehicle is used to broadcast messages with bogus content. Vehicles on the road segment can use only one lane per direction. Due to the mobility model used in the traffic

[3] http://vanet.info/jist-swans

simulator SUMO, vehicles are not able to overtake via lanes of the opposite driving direction. As result, slow vehicles will thwart following vehicles on the same lane. As proposed by [17], a fixed roadside attacker can be assumed as realistic due to minimal effort to the attacker which is broadcasting regularly bogus information about a hazard on the road via DENMs.

4.2 Multilane Highway

In the second scenario, the attacker is driving on a highway road segment where every direction consists of two lanes. In contrast to the first scenario, vehicles can overtake and, therefore, slow vehicles do not thwart faster vehicles. In [6], different approaches for changing the lane are implemented as reaction on a faked PCNs but in our implementation the lane change is initialized and controlled by the traffic simulator SUMO automatically.

In this scenario, the moving attacker, illustrated as vehicle in figure 3, is constantly broadcasting DENMs claiming a hazard directly in front of the attacker's vehicle. The intention of the attacker may be to have a free road in its driving direction. Vehicles approaching at the outer range of the attackers communication range receive the bogus information and would consequently not overtake the attackers vehicle.

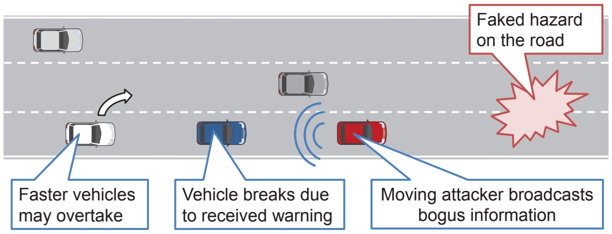
Faked hazard on the road
Faster vehicles may overtake
Vehicle breaks due to received warning
Moving attacker broadcasts bogus information

Figure 3: Simulation of a hazard on a multilane highway

4.3 Sybil Attack

In the third scenario, we are showing a Sybil attack that is executed by a roadside attacker similar to the first scenario described in section 4.1. With a Sybil attack, the attacker pretends to be different vehicles at the same time by broadcasting CAMs with forged identifiers and positions. In general, a Sybil attack may be used to simulate congested roads or it can be used to compromise security means based on a honest majority. In the latter case, several malicious nodes would be inserted into the VANET which distribute false information. In the Sybil attack presented in this paper, CAMs with faked identifiers and faked positions are broadcasted by a static attacker in order to simulate a congestion on a highway with 3 lanes for every direction. Vehicles equipped with a V2X communication system assume to detect a congestion if the speed of a vehicle in the transmission range is below a defined threshold and its distance to another vehicle is smaller than the usual safety zone. In this paper, we assume that vehicles driving slower than 10 m/sec and exhibit, additionally, a safety distance smaller than 9m are considered to be part of a congestion. Vehicles on the road detecting such a situation in front on the same road segment exhibit a reaction such as defined in section 5.

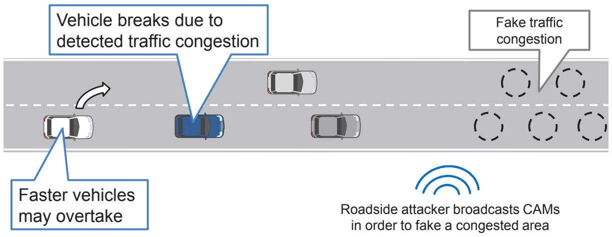
Vehicle breaks due to detected traffic congestion
Fake traffic congestion
Faster vehicles may overtake
Roadside attacker broadcasts CAMs in order to fake a congested area

Figure 4: Simulation of a faked traffic congestion on a multilane highway

5. EVALUATION

One of the major problems in the evaluation of attacks is the definition of appropriate driver behavior. The behavior can not be statically defined due to the fact that different drivers may have different perceptions. As result, we estimate two probable behavior schemes of the driver in order to evaluate the impact of the attacks presented in section 4.

In the first scheme, the driver reduce its speed permanently down to 8 m/sec until the end of the simulated road segment as soon as a danger warning is received. This simulation may reflect cautious drivers that reduce their speed for a longer time period because no real danger can be identified on the road. The red bar in the figure 5 and 6 represents this permanent reduction of the vehicle's velocity.

In the second scheme, the speed of the vehicle is reduced for 31.25 seconds down to 8 m/sec as soon as the transmission range of the attacker is entered and an appropriate message is received. In the communication simulation of JiST/SWANS, a communication radius of 300 m was used. As result, vehicles approaching the attackers communication range are immediately informed about the hazard on the road and reduce their speed for 250 m. This simulation can be assumed to be a normal behavior because vehicle drivers in the real world, approaching a faked danger spot, would see that no real danger exists and would accelerate to normal speed until they passed this area. The green bar in figure 5 and 6 represents this temporary reduction of the vehicle's velocity.

The evaluations in the following subsections 5.1 and 5.2 are generated by independent simulation runs with one attack, mentioned in section 4, and one previously mentioned driver behavior. We analyzed, further, the effect on the overall traffic by varying the number of reacting vehicles. Figure 5 and 6 show the average of driving time over all vehicles that is required between the starting point A and the destination B. If no vehicle is equipped with a V2X communication system, then this trip time is used as reference for the evaluations with reacting vehicles. We consider a vehicle equipment rate of 20 %, 40 %, 60 %, 80 % and 100 % in independent simulation runs. Unequipped vehicles do not reduce their speed and may overtake other vehicles with lower velocity if there is a free lane available.

Every simulation with an attacker and an appropriate reaction scheme is executed five times in order to get an averaged value for the evaluation. In every independent run, the equipped vehicles are selected randomly. The results of all runs are collected in order to compare the different driver behavior schemes with the different equipment rates.

5.1 Attack Impact on Single Lane Roads

In the single lane scenario, the impact of a roadside attacker, such as described in section 4.1, was analyzed. As displayed in figure 5, the impact on the overall road traffic is already immense if only 20 % of all vehicles are equipped with a V2X communication system and, therefore, able to react on the bogus information. Due to missing opportunities to overtake, drivers that assuming a hazard on the road block out all following vehicles on the road segment. As result, unequipped vehicles may also be influenced by the attacker if they are blocked out by other vehicles. This impact is similar for both reaction types as distinct by the different bars in figure 5.

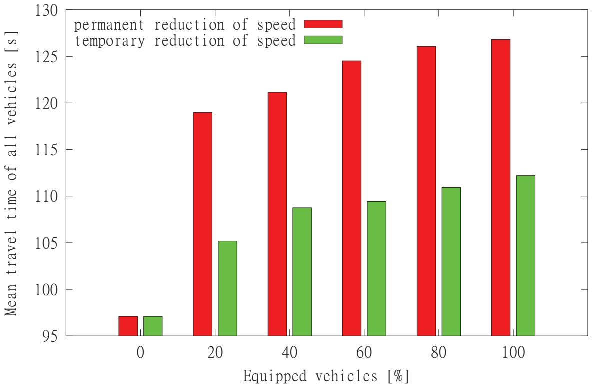

Figure 5: Impact of a roadside attacker on a single lane road

For the single lane road segment, the minimal mean travel time for all vehicles is 97 seconds, as displayed in figure 5 in the first bar. With two equipped vehicles, the mean travel time increases up to 18 % in case of permanent speed reduction and 7 % in case of particular speed reduction. The maximum delay exceeds 23 % and 13 % if all vehicles react on received messages respectively to permanent and particular reduction of speed.

5.2 Attack Impact on Multilane Highways

As described in section 4.2 and 4.3, two different attacks are simulated on a multi lane highway segment. In the first case, the attacker broadcasts DENMs from a moving vehicle claiming that there is a hazard on the road. Vehicles equipped with a V2X communication system react as soon as they receive such bogus DENM by reducing their speed constantly or temporarily equivalent to the single land road scenario described in section 5.1. But, in contrast to the single lane road segment, faster vehicles that are not equipped can overtake the slow vehicles in this evaluation. As result, figure 6 shows an linear increasing of driving time for both reaction types.

The roadside attacker described in section 4.3 broadcasts bogus CAMs also on a multi lane highway in order to create the illusion of a traffic congestion on the road. The results for this attack are very similar to the previously mentioned outcome, depicted in figure 6, because in both cases faster vehicles are able to overtake slower vehicles. The minimal mean travel time for all vehicles is 116 seconds from the start point to the destination. Depending on the time, equipped vehicles follow the attacker vehicle, the delay of mean travel time exceeds 41 % and 22 % respectively to permanent and particular reduction of speed. But, if only a subset of vehicles react on bogus information, attacks on multi lane roads have a limited impact on the overall traffic efficiency because uninvolved vehicles are not blocked out.

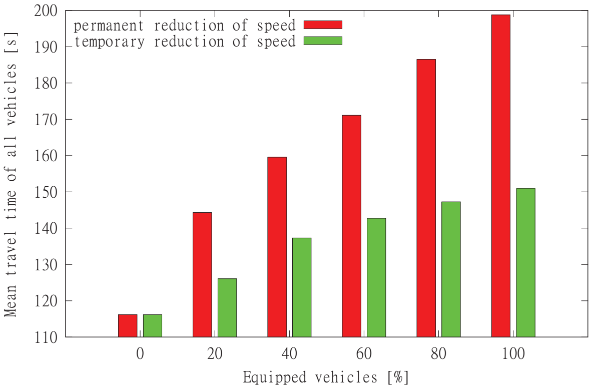

Figure 6: Impact of an attack on a multi lane highway

Nevertheless, both attacks may have larger impact on the traffic if warning messages are forwarded via multi hop communication to distant vehicles which take another route to their destination. In this case, the attacker may be able to reroute other vehicles in order to have a free road for itself.

6. CONCLUSIONS AND OUTLOOK

As presented in section 5, different attacks have different impact on the road traffic, but most determining is the road situation. Especially single lane road segments and urban environments can be considered to be most effected by malicious attackers, because already a few vehicle drivers reacting on bogus information, may disturb the traffic efficiency of a larger area. As result, it would be reasonable for an attacker to wisely choose the environment in order to broadcast bogus information. It has be shown in section 4 that attackers may have different motivations to distribute different kind of messages.

The simulation infrastructure VSimRTI offers great opportunities to implement varies kinds of attack behavior and appropriate driver reactions. Due to the integration of the traffic simulator SUMO and the network simulator JiST/SWANS, realistic vehicle movement and data transmission can be assumed. With VSimRTI, stationary and mobile attackers can easily be simulated that distribute different kind of predefined messages. Such kind of attackers can be used to test and adjust applications that have high requirements on robustness against bogus information.

In future work, the proposed attacker models and driver behavior models will be enhanced in order to provide a realistic basis for a vehicular IDS. Based on the simulation framework presented in section 3, more sophisticated attackers can be created that may be able to circumvent basic vehicular attack detection mechanisms as proposed in [18] and [11]. We will analyze with VSimRTI, among other things, the impact of inserting contradicting mobility information in order to make misbehavior detection systems more robust against blackmailing attacks.

Additionally, the set of possible driver behavior will be enhanced by implementing the re-routing of vehicles in case of congested areas. Furthermore, multi-hop routing mechanisms should be used in our ongoing work in order to identify the impact to more distant traffic. Finally, the proposed attacker simulations and driver reactions should be implemented in larger traffic simulations with random route selection. Based on these further simulations, threats introduced by malicious attackers should be used to adjust and evaluate an vehicular IDS.

7. REFERENCES

[1] *IEEE 1609.2 Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*, July 2006.

[2] R. Barr. *SWANS - Scalable Wireless Ad hoc Network Simulator: User Guide*, 2004.

[3] ETSI - European Telecommunications Standards Institute. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. Technical report, ETSI, 2010.

[4] ETSI - European Telecommunications Standards Institute. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service. Technical report, ETSI, 2010.

[5] European Telecommunications Standards Institute. *ETSI TS 102 637-1 V1.1.1 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements*, September 2010.

[6] M. Ghosh, A. Varghese, A. Kherani, and A. Gupta. Distributed Misbehavior Detection in VANETs. In *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE*, pages 1–6, 5-8 2009.

[7] Institute of Electrical and Electronics Engineers. *IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)–Federate Interface Specification. IEEE Standard 1516.1.* IEEE, New York, NY, USA, 2000.

[8] D. Krajzewicz, G. Hertkorn, C. Rössel, and P. Wagner. SUMO (Simulation of Urban MObility); An open-source traffic simulation. In *Proceedings of the 4th Middle East Symposium on Simulation and Modelling (MESM2002)*, pages 183–187, Sept. 2002.

[9] S. Krauß, P. Wagner, and C. Gawron. Metastable States in a Microscopic Model of Traffic Flow. *Physical Review E*, 55(304):5597, May 1997.

[10] T. Leinmüller, A. Held, G. Schäfer, and A. Wolisz. Intrusion Detection in VANETs. In *In proceedings of 12th IEEE International Conference on Network Protocols (ICNP 2004) Student Poster Session*, 2004.

[11] T. Leinmüller, E. Schoch, and F. Kargl. Position Verficiation Approaches for Vehicular Ad hoc Networks. *Wireless Communications, IEEE*, 13(5):16 –21, october 2006.

[12] N. Naumann, B. Schünemann, and I. Radusch. Vsimrti - simulation runtime infrastructure for v2x communication scenarios. In *Proceedings of the 16th World Congress and Exhibition on Intelligent Transport Systems and Services (ITS Stockholm 2009)*. ITS Stockholm 2009, September 2009.

[13] N. Naumann, B. Schünemann, I. Radusch, and C. Meinel. Improving v2x simulation performance with optimistic synchronization. In *Services Computing Conference, 2009. APSCC 2009. IEEE Asia-Pacific*, pages 52–57, Dec. 2009.

[14] T. Queck, B. Schünemann, and I. Radusch. Runtime infrastructure for simulating vehicle-2-x communication scenarios. In *VANET '08: Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, pages 78–79, New York, NY, USA, 2008. ACM.

[15] T. Queck, B. Schünemann, I. Radusch, and C. Meinel. Realistic simulation of v2x communication scenarios. In *APSCC '08: Proceedings of the 2008 IEEE Asia-Pacific Services Computing Conference*, pages 1623–1627, Washington, DC, USA, 2008. IEEE Computer Society.

[16] Z. Ren, W. Li, Q. Yang, S. Wu, and L. Chen. Location Security in Geographic Ad hoc Routing for VANETs. In *Ultra Modern Telecommunications Workshops, 2009. ICUMT '09. International Conference on*, pages 1 –6, 12-14 2009.

[17] R. Schmidt, T. Leinmüller, and A. Held. Defending Against Roadside Attackers. In *In proceedings of 16th World Congress on Intelligent Transport Systems*, 2009.

[18] R. K. Schmidt, T. Leinmueller, E. Schoch, A. Held, and G. Schaefer. Vehicle Behavior Analysis to Enhance Security in VANETs. In *Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008)*, 2008.

[19] B. Schünemann, K. Massow, and I. Radusch. A novel approach for realistic emulation of vehicle-2-x communication applications. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2709–2713, May 2008.

[20] B. Schünemann, J. W. Wedel, and I. Radusch. V2x-based traffic congestion recognition and avoidance. *Tamkang Journal of Science and Engineering*, 13(1):63–70, March 2010.

[21] H. Stuebing, A. Jaeger, N. Bißmeyer, C. Schmidt, and S. A. Huss. Verifying Mobility Data under Privacy Considerations in Car-To-X Communication. *ITS World Congress*, October 2010.

[22] J. W. Wedel, B. Schünemann, and I. Radusch. V2x-based traffic congestion recognition and avoidance. *Parallel Architectures, Algorithms, and Networks, International Symposium on*, 0:637–641, 2009.