# A Witness System for Vehicular Ad Hoc Networks

Nasir Ali, Björn Scheuermann, and Martin Mauve

Computer Networks Research Group
Heinrich Heine University, Duesseldorf, Germany
{ali, scheuermann, mauve}@cs.uni-duesseldorf.de

***Abstract*—Searching for witnesses in case of road accidents is a challenging task for the police and involved persons. In this paper, we propose a mechanism that helps to find witnesses. Our solution preserves the potential witnesses' anonymity and gives them a free hand to decide whether to step forward as a witness or not. We analyze the performance of our application using a realistic model of a German city.**

## I. Introduction

There are a number of situations in road traffic where witnesses can be very helpful. For example, a witness might be able to describe the events that led to an accident. Currently, it is often hard to identify suitable witnesses: a person might not be aware that she observed something of importance, or she might not know that witnesses are sought at all for an incident she observed.

We propose to use car-to-car communication to identify potential witnesses and thereby solve this problem. A very important aspect of our solution is that the potential witness remains in full control of the decision whether to step forward or not. As a technical basis we rely on vehicular ad hoc networks (VANETs) for direct communication between vehicles.

Our system operates in three phases. In the first phase, users register with a Central Authority (CA), e. g., the police. When witnesses are required, vehicles will broadcast a *Witness Request Message (WRM)*. This might either be triggered explicitly by the driver or automatically by crash sensors, for instance when an airbag fires. A receiving vehicle notifies its driver and logs the information. In order to protect the privacy of the potential witnesses and to withhold their identitiy from all other parties before they have actually decided to testify, we use one-way communication only. There is no acknowledgment from the receiving nodes. In the third phase, a person that is willing to testify may contact a central authority by using the information supplied in the request. The central authority will then be able to question the witness.

The main contributions of this paper are the identification of a novel application for VANETs, the design of the application in a fashion that leaves the users in control of the decision whether or not to step forward as a witness, and the evaluation of the application in the context of a realistic simulation environment.

The rest of the paper is organized as follows. Section II describes the application. Section III shows the evaluation results of the system. Finally, concluding remarks are given in Section IV.

## II. Witness System

The witness system, as proposed here, consists of three parts: user registration, transmitting requests for witnesses, and feedback from the witness. During the registration the user will receive a set of Event Identifiers (EIDs). Whenever a request for witnesses is broadcasted, it includes one of these EIDs. A potential witness then uses the EID to identify the event when contacting the central authority.

### A. Registration

In a first step, a user registers with a Central Authority (CA), e. g., the police. The CA issues a set of random but unique *Event Identifiers (EID)*, and for each EID a certificate (CT-EID) binding that EID to the public key of the user.

### B. Transmitting Requests for Witnesses

At the time of an event for which a user needs (or might need) witnesses, the user's car broadcasts a Witness Request Message (WRM), which includes

*< EID, CT-EID, Timestamp, Location, SigUser >.*

Here, Timestamp indicates the current time and date, Location shows the current location, and SigUser is the signature of the user over the transmitted message. One of the EIDs from the set of EIDs is used. Each EID is used only once and identifies the specific event. The Event Data Recorder (EDR) [1] of the sending vehicle stores the transmitted message.

When receiving a WRM, the Timestamp and Location field are checked. If they match the time and location of the receiver, then the driver is notified and the message is stored for future use. The receiver doesn't acknowledge or send back any information, thus maintaining full anonymity.

### C. Feedback from the Witnesses

The person looking for a witness submits the information about the event to the CA. The CA extracts the event information from the car's EDR (if not damaged), which includes the original Witness Request Message as well as any additional information, such as a description of the event and uploads it on a central website along with contact information of the concerned authority. It also provides the user with new EIDs and accompanying certificates if necessary.

We suppose that there is an application that compares the stored events in the EDR on the base of EIDs with the events published by the CA. If any two EIDs match, then

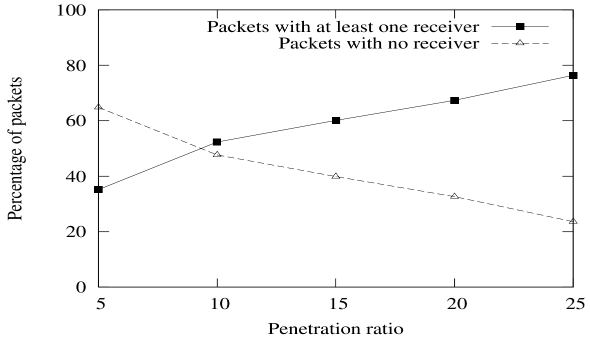

Fig. 1: Penetration ratio vs. success probability within a range of 250 m.

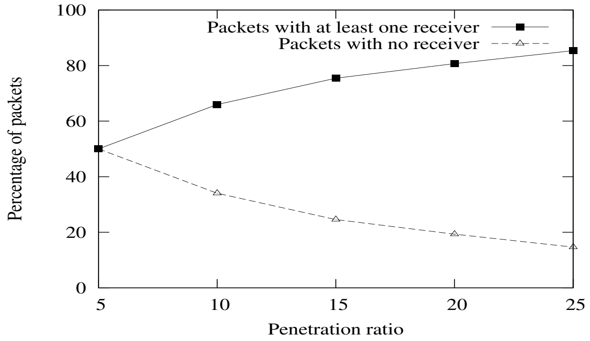

Fig. 2: Penetration ratio vs. success probability within a range of 500 m.

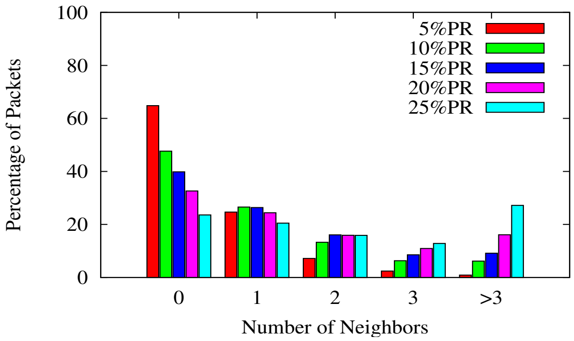

Fig. 3: Histogram of the number of neighbors for a radio range of 250 m.

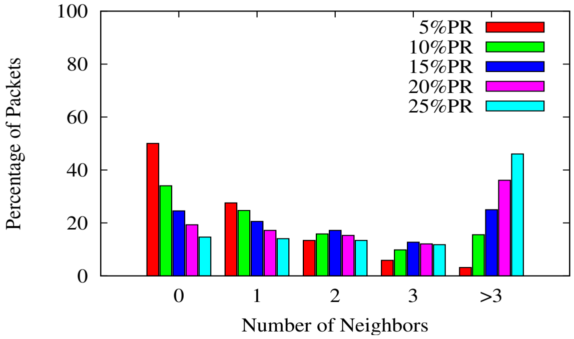

Fig. 4: Histogram of the number of neighbors for a radio range of 500 m.

it informs a potential user (e. g. via email) about the event information and authorities contact information. The witness now has two options: she may step forward and contact the concerned authorities, or she may remain anonymous. When a user reports to the CA as a witness, she will no longer be anonymous.

## III. Evaluation

In this section, we present the simulation experiments that were carried out to evaluate our system using the network simulator ns-2 [2]. Vehicular movements were generated by the microscopic traffic simulator VISSIM [3], connected to ns-2 as described in [4]. It includes, for example, multilane traffic, traffic lights, and different types of vehicles. It also takes driver-specific behavior into account. We use a traffic model of the extended downtown area of Brunswick, Germany, covering a geographical area of about 250 km$^2$, with more than 500 km of roads and up to 10 000 vehicles. In ns-2 we use the two-ray propagation model with different communication ranges of 250 or 500 meters. IEEE 802.11 is employed as the MAC protocol.

The main focus of these experiments is to determine the impact of the penetration ratio on a witness system as proposed here. The penetration ratio is defined as the number of vehicles equipped with the system divided by the total number of vehicles.

Figures 1 and 2 show the percentage of packets that have at least one receiver in relation to the penetration ratio and the communication range. It can be observed that a witness system requires 20 % to 25 % market penetration for reasonable performance. It will thus be a medium-term application for vehicle-to-vehicle communication.

Figures 3 and 4 show the distribution of the total number of receivers for the transmitted packes. Again, the results indicate that a penetration ratio of 20–25 % is required and that the communication range influences the success significantly.

## IV. Conclusion

In this paper, we presented a way to identify witnesses by using vehicle-to-vehicle communication. We ensure the privacy of potential witnesses—each potential witness is able to decide whether to step forward and act as a witness or to remain anonymous. Our results indicate clearly that the success of the system heavily depends upon the penetration ratio.

## References

[1] General Motors, “Event data recorder,” http://www.gm.com/corporate/responsibility/safety/event_data_recorders/index.jsp.

[2] “The Network Simulator ns-2,” http://www.isi.edu/nsnam/ns/.

[3] PTV AG, “Vissim,” http://www.ptv.de/cgi-bin/traffic/traf_vissim.pl.

[4] C. Lochert, B. Scheuermann, M. Caliskan, A. Barthels, A. Cervantes, and M. Mauve, “Multiple simulator interlinking environment for IVC,” in *VANET ’05: Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks*, Sep. 2005, pp. 87–88.