Accurate Accident Reconstruction in VANET

Yuliya Kopylova, Csilla Farkas, Wenyuan Xu

Accurate Accident Reconstruction in VANET

Yuliya Kopylova, Csilla Farkas, Wenyuan Xu

Dept. of CSE, University of South Carolina
{kopylova,farkas,wyxu}@cse.sc.edu

Abstract. We propose a forensic VANET application to aid an accurate accident reconstruction. Our application provides a new source of objective real-time data impossible to collect using existing methods. By leveraging inter-vehicle communications, we compile digital evidence describing events before, during, and after an accident in its entirety. In addition to sensors data and major components status, we provide relative positions of all vehicles involved in an accident. This data is corroborated by observations provided by witness vehicles to rectify inconsistencies. Our application utilizes the mandatory form of VANET communication (beacons), making it non-obtrusive in terms of resource and bandwidth consumption.

Keywords: Accident reconstruction, EDR, in-vehicle applications, VANET.

1 Introduction

One of the most active research areas of mobile ad-hoc networks is the Vehicular Ad-hoc NETworks (VANET). The dramatic increase in the number of vehicles equipped with computing and wireless technologies enabled new applications previously infeasible. These applications fall into safety and comfort categories. Safety VANET applications include imminent collision warning, obstacle detection/avoidance, emergency message dissemination, intersection decision support, cooperative driving etc. Comfort VANET applications include traffic congestion advisories, route updates, automated toll and parking services, etc. [5, 2]. While safety applications have been in the focus of academic and industrial research, the topic of forensic applications using VANET data has been under-explored. In this paper we propose a forensic application that harvests inter-vehicle communication for the purpose of post accident analysis. Our objective is to collect data sufficient for establishing the chain of events associated with the accident.

The contributions of this work include the following: (1) we identify desirable properties of data collection process for accurate accident reconstruction,(2) we propose a viable solution that achieves these properties based on vehicular communications, (3) we provide some details on application logic, architecture, and integration of the proposed application, (4) we discuss mechanisms to protect confidentiality of the data collected by our application

The rest of the paper is organized as follows. Section 2 overviews data collection practices for accident reconstruction. Section 3 presents the proposed solution. Section 4 provides a limited discussion on security and privacy issues associated with our solution. Section 5 concludes the paper.

2 Accident Reconstruction Overview

Conducted by law enforcement agencies, accident reconstruction is defined as a process of determining the cause and the circumstances of a collision from available evidence [9]. The data of interest involves movement, relative positions, and interaction of the involved vehicles. Accident reconstruction is usually conducted in two steps: (1) data collection and (2) data fitting. Data collection involves measurements of parameters relevant to trajectory and impact reconstruction, such as speed, position, acceleration, point of impact, etc. Data fitting is accomplished through trajectory modeling based on the data collected in the first step. Supplying accurate data to the modeling software is the key to the successful reconstruction especially in complicated incidents [7].

The data gathered through conventional means (close-ups of skid marks, tire prints, evidence of the area of impact, collision debris distribution, etc.) is often incomplete and occasionally misleading [9]. More reliable crash data is collected by Event Data Recorders (EDR). The main purpose of EDR is to verify proper functioning of the safety systems in place. Even though EDR data was not originally intended for accident reconstruction, its use in post-accident analysis is becoming a more accepted practice [11, 1]. However, information collected from a single EDR is often insufficient for obtaining accurate reconstruction of an accident. This is especially true in multi-vehicle collisions, hit-and-run scenarios, and accidents that span multiple events [6, 7, 12].

Shortcomings of the existing data collection practices are summarized below:

1. Insufficiency of data in scope and duration:
   - Triggered exclusively via airbag deployment. A near rollover event, skidding off the road, etc. do not trigger EDR recording [6, 7];
   - Insufficient history of recording especially pre-crash. In more than half of the cases investigated with the help of EDR, insufficient recording history renders EDR data inadequate for accident reconstruction [7].
2. Insufficiency of relevant data:
   - Geared towards assessing functionality of safety systems (airbags, seatbelts and mechanical parts), not trajectory reconstruction;
   - Limited to a single event; subsequent events, even if caused most of the injury or fatality are not recorded [6];
   - No existing means of recording data related to other vehicles trajectories.
3. Inaccuracy of data:
   - Inaccuracy of values due to indirect measurements;
   - Inaccuracy of values due to error propagation through accident phases;
   - No existing means to counter sensor malfunction/miscalibration [7, 12].

Redesigning EDR to expand data collection can only partially these limitations. However, this task is not straightforward from architectural standpoint due to intra-vehicle communication constraints [10]. We propose a solution that addresses all limitations without the need of redesigning EDR.

3 Proposed Solution

Our solution addresses the above limitations in the following manner:

1. We improve the log recording triggering mechanisms by integrating our application into existing in-vehicle applications (access to rollover sensor, diagnostic module, etc.) in section 3.1;
2. We expand the scope of the data through recording positions and dynamics of all nearby vehicles (VANET communication data) in section 3.2;
3. We provide a mechanism to rectify GPS sensor malfunction/mal-calibration through submitting corroborating witness data in section 3.3;
4. We provide sufficiency of data duration by the means of rotating log centered around the accident event in section 3.4.

3.1 Architecture Philosophy

The application we propose derives data from two sources: sensory data obtained locally on the vehicle and external communication data arrived from vehicles nearby. On the one hand, our application needs to fit and benefit from sensor data collection mechanisms in place for in-vehicle applications; on the other hand, our application needs to be able to process significant volumes of data and share this data across multiple VANET applications that base their decisions on a similar subset of data to ensure consistency of decisions made across safety applications. We approach this challenge from the architectural standpoint.

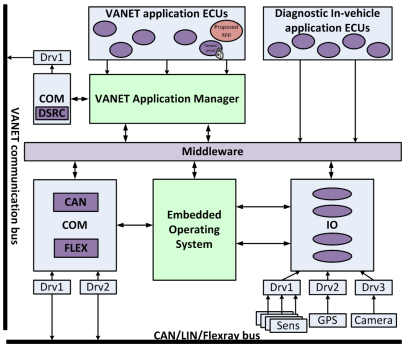

Fig. 1. Proposed architecture

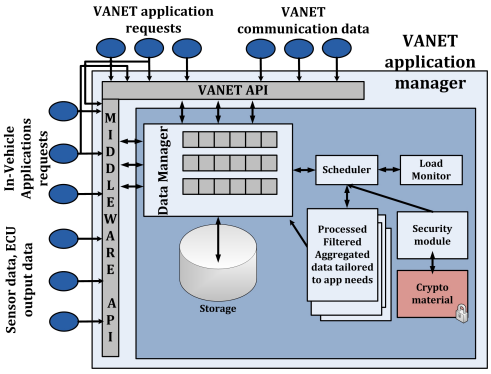

Fig. 2. VANET Application Manager

Many VANET applications are proposed as standalone applications: they assume (1) direct access to sensor data and (2) autonomy from other VANET applications. Designing a standalone application might lead to either impractical (sensor data belongs to different functional domains) or inefficient application (redundancy in data processing, competing for resources). To avoid this pitfall, we discuss in a follow up paper how to fit our application into the framework of both existing in-vehicle applications (Figure 1) and future VANET applications (Figure 2). Fitting our application into the framework of existing in-vehicle applications allows for expanding log recording triggering mechanisms to include

rollover sensor data and output from Diagnostic Module. Fitting our application into the framework of VANET applications promotes applications cooperation.

3.2 VANET Communication Data

To obtain data related to other vehicles, we propose to use beacons already being exchanged by the VANET vehicles. A fundamental aspect of VANET communication is periodic beaconing; that is transmission of position, heading, status, along with additional parameters. Beacons contain the most relevant pieces of information necessary for accident reconstruction such as GPS position, heading, current speed, lateral and longitudinal acceleration, engine rpm, break status, etc. They are required for normal operation irrespectively of number and types of applications. According to [4, 13], for operation of a typical traffic safety application in VANET beacons are assumed to have the following characteristics:

Generation Rate	Dissemination Latency	Communication Type	Communication Range	Size
10 beacons/sec	up to 100 ms	one hop broadcast	up to 300 m	80 bytes

3.3 Accident Reconstruction Application Data

To provide a complete suite of data necessary for accurate accident reconstruction including mechanisms to counter sensor malfunctions, we propose to create a two-piece digital evidence:

1. **Primary evidence:** the first piece contains data necessary for trajectory reconstruction of *all vehicles* in the proximity of an accident. This data is stored on the vehicle directly involved in the accident and can be retrieved through explicit permission of the owner or court decision. Primary evidence consist of three parts:
   (a) History of vehicle's own **sensor data.** This allows trajectory reconstruction of the vehicle collecting the data (directly involved in the accident). This data represents how the vehicle perceives itself.
   (b) History of overheard **beacon data** from the vehicles nearby augmented with correctional data. This allows trajectory reconstruction of all vehicles in the vicinity. This data represents how the vehicle perceives its neighbors.
   (c) List of neighbors at the time of the accidents along with the **encryption keys** submitted to them. This allows retrieval of corroborative evidence at the time of investigation, i.e. after access to the primary evidence is granted.
2. **Corroborative evidence:** The second piece consists of witness data obtained from the vehicles nearby. It contains information necessary for verification of the data included in the primary evidence file. This data corresponds to how witness vehicles perceive each other. The goal of this piece is to counter falsified/mal-calibrated GPS data submitted by other witnesses; offset missing data due to path obstruction and out-of-range scenarios; protect against dishonest vehicles directly involved in the accident (owners of

the primary evidence). Corroborative evidence submitted by a witness vehicle v_i is beacon log augmented with correctional data (vehicle v_i would store this log as a part of its own primary evidence should v_i itself get into an accident). Corroborative evidence is submitted to a road side unit (RSU), a trusted and impartial party. This data is encrypted with a key stored in the primary evidence file to prevent power abuse by investigating authorities.

Correctional data in the beacon log is used for cross referencing evidence. The same data can be utilized by routing protocols for position verification in VANET. There are many ways to accomplish this task. The most common approach is to rely on additional functionality of wireless antennas such as capability of assessing Time Difference of Arrival (TDoA), Time of Arrival (ToA), or Angle of Arrival (AoA). A method proposed in [15] is suitable for our application. It is resilient to node collaboration and does not rely on RSU for verification. Thus, the beacon log in both the primary and corroborative evidence files is augmented with three measures of TDoA, ToA and AoA per every entry.

Table 1 summarizing proposed digital evidence uses the following notation: Δt is sampling interval,$(b_i)_{t_j}$ stands for beacons received from vehicle i within time $t_j + \Delta t$, $(\delta_{v_i v_k})_{t_j}$ stands for correctional data on vehicle v_i regarding vehicle v_k with respect to GPS data in beacon received within time $t_j + \Delta t$.

Table 1. Digital Evidence Summary

Primary evidence on V_0		
Sensor Data	$((s_1, s_2, \ldots, s_n)_{t_0}, (s_1, s_2, \ldots, s_n)_{t_1}, \ldots, (s_1, s_2, \ldots, s_n)_{t_k}$	self perception
Beacon Log	$((b_{v_1}, \delta_{v_0 v_1})_{t_0}, (b_{v_1}, \delta_{v_0 v_1})_{t_1}, \ldots, (b_{v_1}, \delta_{v_0 v_1})_{t_k})$, $(b_{v_2}, \delta_{v_0 v_2})_{t_0}, (b_{v_2}, \delta_{v_0 v_2})_{t_1}, \ldots, (b_{v_2}, \delta_{v_0 v_2})_{t_k})$, $\ldots$ $(b_{v_n}, \delta_{v_0 v_n})_{t_0}, (b_{v_n}, \delta_{v_0 v_n})_{t_1}, \ldots, (b_{v_n}, \delta_{v_0 v_n})_{t_k}))$	v_0 perceives v_1 v_0 perceives v_2 v_0 perceives v_n
Set of Keys	$(E_{v_0 v_1}, E_{v_0 v_2}, \ldots, E_{v_0 v_n})$	encryption keys
Corroborative Evidence on RSU		
Witness Data	$[((b_{v_0}, \delta_{v_1 v_0})_{t_0}, (b_{v_0}, \delta_{v_1 v_0})_{t_1}, \ldots, (b_{v_0}, \delta_{v_1 v_0})_{t_k})$, $((b_{v_2}, \delta_{v_1 v_2})_{t_0}, (b_{v_2}, \delta_{v_1 v_2})_{t_1}, \ldots, (b_{v_2}, \delta_{v_1 v_2})_{t_k})$, $\ldots$ $((b_{v_n}, \delta_{v_1 v_n})_{t_0}, (b_{v_n}, \delta_{v_1 v_n})_{t_1}, \ldots, (b_{v_n}, \delta_{v_1 v_n})_{t_k})]_{E_{v_0 v_1}}$ $\ldots$ $[((b_{v_0}, \delta_{v_i v_0})_{t_0}, (b_{v_0}, \delta_{v_i v_0})_{t_1}, \ldots, (b_{v_0}, \delta_{v_i v_0})_{t_k})$, $((b_{v_1}, \delta_{v_i v_1})_{t_0}, (b_{v_1}, \delta_{v_i v_1})_{t_1}, \ldots, (b_{v_1}, \delta_{v_i v_1})_{t_k})$, $\ldots$ $((b_{v_n}, \delta_{v_i v_n})_{t_0}, (b_{v_n}, \delta_{v_i v_n})_{t_1}, \ldots, (b_{v_n}, \delta_{v_i v_n})_{t_k})]_{E_{v_0 v_i}}$	v_1 perceives $(v_0, v_2, \ldots, v_n)$ v_i perceives $(v_0, v_2, \ldots, v_n)$

The data in the primary evidence file allows detailed reconstruction of relative trajectories of all vehicles before, during and after the accident; the data submitted by witness vehicles allows to corroborate the story and counter falsified/malcalibrated GPS data submitted by other witnesses.

3.4 Application Operation

A threaded approach as shown in Fig. 3 can be adopted if memory space is not a concern. In the absence of abnormal sensor readings, the accident reconstruction application monitors sensor data and updates rotating data log via Monitoring thread and Logging thread. Abnormal events of crash and witness type are processed by launching Accident thread and Witness thread respectively.

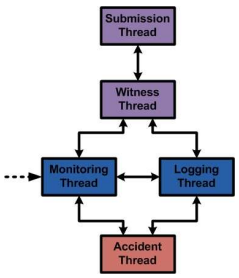

Fig. 3. App. threads

Logging thread is responsible for data recording within $t_{accident} \pm \tau$ interval. Threaded approach allows a vehicle to be a witness to multiple accidents while being itself involved in a crash. Abnormal events are triggered by two kinds of input: internal (e.g., sensor readings, output of in-vehicle applications) and external (e.g., witness request from other vehicles, receipt from RSU when witness data is received). A crash type event is generated based on internal input. In addition to airbag sensor reading (current EDR), we allow for readings from rollover sensor, lateral acceleration sensor, crash impact sensor, and output from the DM. Monitoring thread maintains a list of neighbors (witnesses) within communication range and analyzes data for suspicious events:

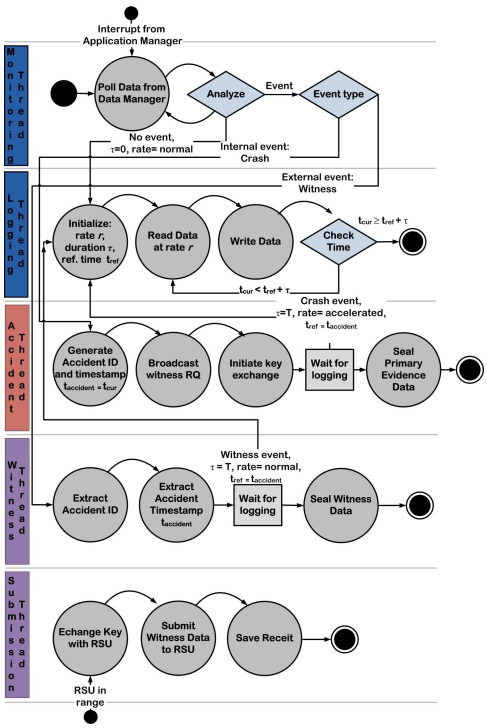

Fig. 4. Application State Diagram

Algorithm 1: Logging Thread

input : calling thread from,
recording duration tau,
time of event tref

if called from accident thread **then**
  tau ← T
  rate ← *accelerated*
  scope ← *alldata*
else if called from witness thread **then**
  tau ← T
  rate ← *normal*
  scope ← *beaconsonly*
else
  tau ← 0
  rate ← *normal*
  scope ← *alldata*
end
repeat
  tcur = `now()`
  record data of scope scope at rate rate
until tcur ≤ tref + tau;

Fig. 5. Logging Thread Algorithm

Sensor data is obtained through the AM by polling; events, generated by the DM or cooperative driving applications, are delivered by the AM via asynchronous notification. A crash type event is processed when digital evidence is compiled and sealed. A witness type event is triggered by the reception of a request to submit corroborating evidence originated on another vehicle. A witness type event is processed when evidence data is successfully delivered to the nearest RSU. Fig. 3 illustrates thread interaction; Fig. 4 details individual threads; Fig. 5 presents Logging thread pseudocode.

4 Security and Privacy

In this section we present a brief summary of the security and privacy concerns of our application.

Authenticity, Integrity, Non-repudiation: Since our application only harvests VANET communication data, authenticity, integrity, and non-repudiation of individual entries in the evidence file are predicated on correct and secure implementation of the communication protocol. These mechanisms are provided in 1609.2 standard.

Confidentiality: We consider four distinct situations with different confidentiality requirements:

1. *Beacon exchange: no confidentiality.* Beacon messages do not contain confidential information: they are transmitted in the clear but digitally signed for integrity protection and proper attribute authentication [8].
2. *Primary Evidence: confidentiality against all but authorized parties.* Digital evidence on the vehicle directly involved in the accident is encrypted and stored in a tamper proof location. To prevent involvement of non-governmental institutions (issuers of secure VANET communication keys as per 1609.2) in law-enforcement mechanisms, a separate set of keys for digital evidence is issued by the law-enforcement authorities (preloads and replenish scheme [14]). Thus, the evidence can be decrypted only by the law enforcement authorities. Other interested parties (insurance companies) would have to legally obtain the decryption key from the police.
3. *Corroborative evidence request-response sequence: confidentiality against all except direct communication partners.* These are safety messages encrypted as required by 1609.2. During this step, another key is generated: the encryption key for corroborative evidence (simple Diffie-Hellman key exchange after mutual authentication will suffice).
4. *Witness data: confidentiality against authorities with too much power.* The secret key obtained in the previous step insures witness protection. Corroborative evidence submitted by witness vehicles to a RSU is encrypted with the key stored in the digital evidence file on the vehicle directly involved in an accident. Corrupt, overzealous or curious authorities can access witness statements (submitted to RSU), but unable to decrypt them without obtaining a subpoena of the vehicle under investigation.

Non-frameability: Intention of corroborative evidence is twofold: (1) to protect against misbehaving nodes by submitting correctional data to the vehicle involved in an accident (perceived position history from other witness vehicles) and (2) to protects against dishonest nodes directly involved in an accident by submitting witness package to the nearest RSU.
Privacy: The privacy goal of our application is to ensure that access to the digital evidence"does not enable one to learn anything about individual that could not be learned without access to some other external data"[3]. External data includes physical evidence from the scene, EDR data, eye witness statements, cameras along public roads, etc. The advantage we provide is completeness and relevance of the data compared to traditional means. If proper investigation procedures are followed, no impact on privacy of individuals is expected.

5 Conclusions and Discussion

We propose a forensic application for accurate accident reconstruction. It leverages VANET communication to create a two-piece digital evidence. The data in the primary evidence (stored on a vehicle) allows detailed reconstruction of relative trajectories of all vehicles before, during and after the accident; witness data (stored on RSU) corroborates the story. Our ongoing work includes evaluation/simulation studies and technical details for individual components.

References

1. Croft, A.: Sensing Diagnostic Module: The modern motor vehicle's "black box"
2. Dotzer, F., et al.: Secure Communication for Intersection Assistance. In: 2nd International Workshop on Intelligent Transportation (2005)
3. Dwork, C.: Differential privacy. In: ICALP. pp. 1–12. Springer (2006)
4. van Eenennaam, E., et al.: Exploring the Solution Space of Beaconing in VANETs. In: 1st IEEE Vehicular Networking Conference (2009)
5. Elbatt, T., et al.: Cooperative Collision Warning Using Dedicated Short Range Wireless Communications. In: 3rd IW on VANET. pp. 1–9. ACM Press (2006)
6. Gabler, H., Hampton, C.: Estimating Crash Severity: Can event data recorders replace crash reconstruction? Accident Analysis & Prevention 40, 548–558 (2008)
7. Haight, W.: Automobile Event Data Recorder (EDR) Technology - Evolution, Data, and Reliability. Tech. rep., Collision Safety Institute (2001)
8. Hartenstein, H., Laberteaux, K.: VANET Vehicular Applications and Inter-Networking Technologies. John Wiley & Sons (January 2010)
9. Lofgren, M.: Handbook for the Accident Reconstructionist. IPTM (1983)
10. Navet, N., et al.: Trends in Automotive Communication Systems. IEEE 93, 1024–1223 (2005)
11. NHTSA: Final Rule: Event Data Recorders (2006)
12. Niehoff, P., et al.: Evaluation of Event Data Recorderss in Full Systems Crash Tests. Tech. rep., NHTSA (2006)
13. project, C..D.: C&D WP-1 Requirements Document. Tech. rep. (2009)
14. Raya, M., Hubaux, J.P.: Security Aspects of Inter-Vehicle Communications. In: 5th Swiss Transport Research Conference (2005)
15. Shmatikov, V., Wang, M.H.: Secure Verification of Location Claims with Simultaneous Distance Modification. 12th IC ASIAN'07 (2007)