

University for Business and Technology in Kosovo

UBT Knowledge Center

UBT International Conference

2015 UBT International Conference

Nov 7th, 9:00 AM - 5:00 PM

A Policeless traffic ticketing system with autonomous vehicles

Mükremin Özkul
Epoka University

Ilir Çapuni
Epoka University

Follow this and additional works at: <https://knowledgecenter.ubt-uni.net/conference>



Part of the [Computer Sciences Commons](#), and the [Digital Communications and Networking Commons](#)

Recommended Citation

Özkul, Mükremin and Çapuni, Ilir, "A Policeless traffic ticketing system with autonomous vehicles" (2015). *UBT International Conference*. 95.

<https://knowledgecenter.ubt-uni.net/conference/2015/all-events/95>

This Event is brought to you for free and open access by the Publication and Journals at UBT Knowledge Center. It has been accepted for inclusion in UBT International Conference by an authorized administrator of UBT Knowledge Center. For more information, please contact knowledge.center@ubt-uni.net.

A Policeless traffic ticketing system with autonomous vehicles

Mükremin Özkul and Ilir Çapuni

Dept. of Computer Engineering, Epoka University, Tirana Albania

Abstract. Besides being expensive, traffic violation monitoring systems rely heavily on a huge infrastructure that incurs installation, operational, and maintenance costs.

Developing countries — where people do exhibit less traffic safety awareness — deployment of such systems becomes a daunting task. A police- men cannot be everywhere, and a policeman can also be bribed.

With the above goals in mind, in this paper we present an infrastructure- less and police-less traffic violation detection system that relies solely on the broadcast messages between the vehicles and secure communication of the vehicles with the transportation authority. Each vehicle should be equipped with a small board box (or a smartphone) with a wifi antenna and 3G capability and subscription. The system is highly scalable and can include pedestrians with smartphones. It is active and operational wherever and whenever there are two participants in the range of each other.

Each participant has two roles to bear simultaneously. The first one is to report and prove its location to the transportation authority. The second one is to report the presence of other vehicles in the neighborhood to the transportation authority and flag those that disobey the traffic rules acting as trustworthy and anonymous witnesses. This is a preliminary report on a still ongoing research project.

Keywords: Traffic violation system, traffic rules, faults, broadcast messages, V2V

1. Introduction

The traffic violation monitoring systems mostly rely on video detection based on real-time image processing that use fixed roadside units, RSU, such as radars, cameras, or mobile service patrol cars that is equipped with on board devices to identify the vehicles to report and to register for issuing violation tickets. Unfortunately, correct operation of such systems is often conditioned by good weather conditions. As a result are not efficient and accurate on rainy, snowy or in any conditions that restrict visual contact between the vehicles on the road. Furthermore, image and video computing algorithms are still costly and require a lot of computation power.

The coverage area of the video detection systems is limited by the visual coverage area. Because of the high installation, maintenance, and costs of such cameras, deployment of these systems are often limited to urban. In the US, most of the accidents resulting in bodily injuries [5] occur on the roads in the rural areas out of the scope of any traffic violation monitoring. Therefore, it is important to have an intelligent monitoring system with a wide coverage without just relying on such systems to enforce the traffic violations.

1.1 Our contribution

In this paper, we are introducing Traffic Violation Detection and Reporting System (TVDRS) that

1. makes no use of policemen (which could be bribed).
2. is everywhere where there is traffic
3. needs no costly infrastructure.

In particular, we are interested in detecting, witnessing, and issuing a valid traffic violation ticket for violations such as: speeding, moving on a wrong lane, parking on a forbidden place, driving in the opposite direction on a one-way road, traffic light violation, not stopping on the pedestrian

crossways etc. To capture the traffic behavior with most of its realities, we use the model and conventions presented in [1]. In short, in this model, a vehicle, a bike, a pedestrian . . . acts as “automaton on the wheels” that has communication capabilities with their neighborhood of finite size. From now on, we will call these objects vehicles, but with a clear intention that the definition scales up to pedestrians and other participants as well. Therefore, as an automaton, its transition function features the current traffic rules, whereas the local constraints (e.g. speed limit for a certain part of the road at certain time intervals) is stored on a map which is loaded on the unit. Each vehicle updates its state asynchronously. A violator is a vehicle that is not obeying to the rules that regulate the traffic in the position that the vehicle is positioned. The violation is detected and “witnessed” only by the vehicles in the space-time neighborhood of the violator and is reported by them to a transportation authority (TA) that acts as a trusted party and is in charge to collect violations and issue fines to the violators. A vehicle may be adversarial and may not co-operate. Witnesses need to remain anonymous to the violator. We assume that vehicles communicate with each other. Occasionally, a vehicle can communicate with the road side units (RSUs) and use 3G/4G or later network if the topology of the road is covered by it. These participants can communicate with the TA.

The desiderata of the system are as follows.

1. A violation ticket to a vehicle x for violation v that occurred at time t at position p is generated only if a violation v at time t at position p was conducted by car x .
2. For a violation v of car x at time t at position p , at most one violation ticket is generated.
3. The above holds, regardless of the behaviour of the participants or non-deterministic nature of the environment.
4. Scales naturally so that other participants in the traffic (say, pedestrians or cyclists) can participate.

1.2 Related work

A video-analysis system for real-time traffic-violation detection systems using cameras located on the intersection in the urban areas is presented at [7]. The system model uses cameras with content-analysis capabilities by using image recognition to classify objects in traffic in order to detect and track violations on the road such as one-way driving, and illegal bus-lane driving. Radio Frequency Identification technology, RFID, enables automatic identification of vehicles. Many counties in Europe use RFID tag systems in electronic toll collection, ETC, in order to automatically charge passing vehicles at high-way toll booths, or bridges. In [8], an architecture of a traffic law enforcement system by using RFIDs is described.

1.3 The structure of the work

The rest of the paper is organized as follows. The following section starts with important –but somewhat tedious – description of the underlying model that is given [1]. We recommend the reader to skip the details on the first reading. Then, we proceed with giving the details of the protocol.

2. Our System

2.1 The System Model

Our model uses a two-dimensional triangular grid whose sides are equal to 1 (say, $l = 7.5$ meters), and we fix a coordinate system with two axes x and y as shown in Fig. 1. The main reason for this choice is geometric: we can easily lay down such a grid on all kind of roads, regardless of their curvature Fig. 2. For convenience we set $\vec{w} = -\vec{x} + \vec{y} = (-1, 1)$ which gives us the set of vectors

$$D = (\vec{x}, -\vec{x}, \vec{y}, -\vec{y}, \vec{w}, -\vec{w})$$

which denotes the set of unit vectors in the vector space. A site in a grid is defined by a vector $\vec{p} = (x, y)$.

An object is a pair $O = (s, P(O))$,

where s is its (internal) state (from a finite set of states) and

$$P(O) = (x, y) \in Z^2$$

determines its position on the grid, and it has 6 immediate neighbors in

$$I_N(O) = \{\vec{p} + \vec{u} \mid \vec{u} \in D\}.$$

A vehicle is an object that has its own propulsion and can move to one of the six immediate neighboring sites.

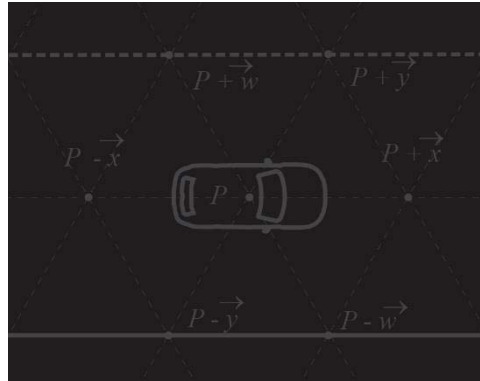


Fig. 1. A vehicle placed at position P in a traffic lane bounded by a full boundary on the right, and dashed on the left.

A part of the internal state of an object is its ID (say, based on a MAC address of the networking device). Other information defining the state of an object may include current and maximum allowed speed of the vehicle, direction, position of the vehicle on the road (in some other coordinate system, say GPS), vehicle length, a priority index (say some vehicles like ambulance are given higher priority), number and the identity of the passengers in the vehicle etc.

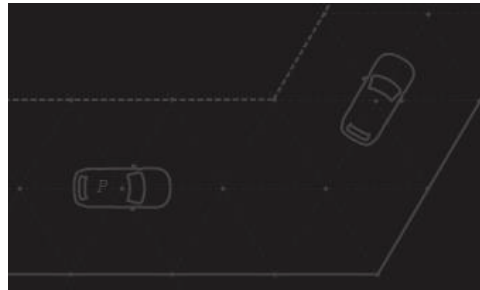


Fig. 2. A curve on the grid. A curve or upheaval on the grid easily can be draw and represented by using the triangular grid model.

There is a distinguished state called disabled to mark objects that cannot move or bond. We also distinguish boundary objects that form boundaries. Boundary objects can be dashed or full. Any site of the grid can hold at most one object that can span one or more consecutive sites at the same time, except if one of them is of a dashed boundary type. In the illustrations, the boundaries of the roads are marked as bold lines, like in Fig. 1. A site has its direction which is determined by the direction of the boundary objects in its immediate vicinity. A lane is a list of consecutive sites having the same direction between two boundaries. A vehicle object constantly updates its state by applying a rule from the rule set. Additionally, the position of the same vehicle at time t may be different from the time $t - 1$ after the rule application.

A motion rule of an object is a function

$$\delta : (s, P(O)) \rightarrow (s0, R)$$

where $R = P(O) + \vec{u}$ for some unit vector $\vec{u} = \vec{0}$.

The rule set prohibits a vehicle object from moving out of the road boundaries. Communication and state synchronization of objects is defined as a bonding process. Each object can see the state of objects of a constant size neighborhood around it. Together, two objects may form either a flexible bond or a synchronization bond, or form no bond at all. However, the objects that only move in the same direction can form bonds between each other. We can make use of non-vehicle objects with a specific direction placed strategically on the grid to mark a road and its lanes, its boundaries, its directions, maximum allowed speeds etc. The distance $d(V_i, V_j)$ denotes the Euclidean distance between the two vehicles V_i and V_j . We extend this to define the distance between sites in a natural way. System Evolution A configuration is a finite set of objects with bonds between them. The switch from one configuration C_1 to another one C_2 is done by applying of a single rule which defines motion of the vehicles as well. Whenever configuration C_1 transitions to configuration C_2 using some rule $r \in R$, we will write $C_1 \xrightarrow{r} C_2$. Within one unit of time, a vehicle moves at least c_1 cells and at most c_2 cells, where c_1 and c_2 are two non-zero integer constants defined by the traffic rules, such that $c_1 < c_2$. Whenever a configuration is obtained from a previous by not applying an appropriate rule, we say that a violation occurred. For example, if a site contains more than one vehicle at the same time, then a violation of a rule has occurred.

A trajectory is a finite sequence of configurations C_1, C_2, \dots, C_n , such that $C_i \xrightarrow{r} C_{i+1}$ for $1 \leq i < n$. The whole system evolves as a continuous time Markov process, defined on a finite state space.

2.2 Protocol

The computation effort in our system is spread on the TA and on the vehicles using an optimal ratio. We now describe the program of the vehicles and of the TA.

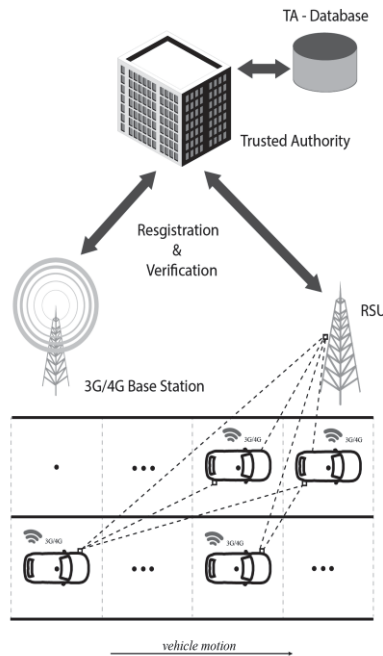


Fig. 3. Network

In the detecting part of the protocol, while beaconing, vehicles can detect that a vehicle is violating the traffic rules. In order to witness that vehicle x has conducted a violation v at time t in position p , a witness must prove that at time $[t - \tau, t + \tau]$ it was in the constant ball $B(p, \pi)$, where τ

and π are two parameters whose value depends on the implementation. For this, vehicles need to be able to prove their location to the TA, but in a way that does not intrude to its privacy: vehicles should not know the IDs of the neighbors. The backbone of the system is the A-VIP protocol (see [4]) devised to verify and infer positions of vehicles in vehicular network using anonymous beaconing. The protocol is efficient (in terms of computational complexity) and robust against common attacks. It also clearly identifies the cars that are not consistent in their proofs.

As we will see later, if we assume that a vehicle is equipped with a tamper resistant unit and stipulate that not participating in the protocol is a violation itself, all the desired properties of the system are fulfilled.

2.3 Vehicle rules

Now we describe the rules that run on each vehicle independently. Signup Each time a vehicle is turned on, it will sign up to TA. This signup will be valid for a certain amount of time and is obtained by communicating with the TA over a secured channel using 3G/4G or RSU.

Suppose that a vehicle v sends a signup request to the TA at time t_0 . The TA saves the request and responds to it by sending the triplet (K_v, r_v, o_v) , where K_v is a short-term 128-bit AES symmetric key, and r_v and o_v are two random integers.

Using these, both parties can compute a time dependent secret $sv(t)$ and serves for the TA to verify the identity of v and last time when it has issued a beacon. The $sv(t)$ is computed as follows. Both sides initialize a counter to the value r_v and increment it by o_v at every beacon. Then, the value of the counter is encrypted using AES in counter mode.

Beaconing Once signed up, at every t_b seconds, each vehicle broadcasts a beacon as follows. Suppose that i is even. Then, the i -th beacon consists of the following.

1. Shared secret for the particular time instant $sv(i)$.
2. Encrypted location information obtained by encrypting the string consisting of the location padded with some flag bit¹ z_{i-1} which is XOR'ed with the value $(r_v + i o_v)$.
3. Plain location.
4. Current time.

Suppose that i is odd.

Now, we form a beacon using the shared secret $sv(i-1)$ from the previous time instant. The rest is done the same as for even case.

Reporting Reporting is a second task performed by a vehicle. When a beacon is received, a vehicle processes it using as detailed below.

Recall that a fault occurs whenever the transition between two configurations is not done according to the transition function. For this, we define the $OughtTo(v, sv, t)$ to be a set of possible states that vehicle v can get to at time $t + t_b$ from state sv while obeying the rules. Now, for each beacon that is received at some time instant, we compute its $OughtTo$. On the next beacon, we check if the current state of the vehicle –

identified by the same shared secret (for two consecutive time instants), is in $OughtTo$. If not, then clearly this vehicle has performed a violation of one of the rules.

Here are the details of the above. Suppose that a vehicle u receives a beacon of v .

On the next beacon, we compare if the state of the vehicle is in the $OughtTo(x, sx, t)$. If not, then a violation must have occurred.

Then, in a specific local table, vehicle u stores the beacon it received from v along with

1. the time when the beacon was received
2. its own position when the beacon was received
3. an optional field $Q_u(v)$ that carries the signal power of v computed by u

¹ The role of this bit will be clear later.

4. violation flag with the id of the type of the violation. If the violation flag is 0, then the violation id is null.

Furthermore, every τ seconds, u forms a message to TA containing all the recent beacons from its neighbourhood. This message is sent through a secure channel after a successful authentication. The very same beacon may be reported by many vehicles that are in the proximity of the vehicle that generated it. Below we will show how the transcript of these reports will be combined to produce a valid violation ticket.

Reporter u				
time	position	beacon	violation	Q(signal power)
t_{u1}	l_{u1}	$X^n n$	f1	Q^n_1
...
t_{ui}	l_{ui}	$X^n n$	f0	Q^n
...
t_{uk}	l_{uk}	$X^n n$	f0	Q^n

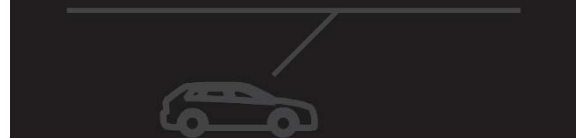


Fig. 4. A Reporter with the local table

2.4 Transportation Authority

Whenever a TA receives a report, it processes them in order to (i) determine the location of the vehicles that have announced their location through the beacons, (ii) verify the locations and the violations, (iii) compute the actual position and violation flag of the vehicles that may have advertised an incorrect location. Let S be the set of the positions and V be the set of vehicles that need to be verified. Suppose that TA receives a report from vehicle $u \in V$. It then processes entry-by-entry as follows.

1. read the time t_{uv} when vehicle u has received the beacon from v ,
2. for each $w \in V$ computes

$$i = b \frac{t_{uw} - t_w^0}{\tau b}$$

where t_w^0 is the time when TA has received the signup request from w ;

3. using i , it retrieves the precomputed secret value x_i that matches x_i .

Suppose that such a match is found. Then, TA identifies v to be the vehicle that sent the beacon. It extracts the quadruple associated to it in the report and performs the following operations.

1. Decrypt the location l^i that v has advertised via a beacon received by u at time i and the flag z^{i-1} .
2. If the flag $z^{i-1} = 1$, the entry is discarded.
3. If the flag $z^{i-1} = 0$, the TA stores the position l_i in v in v in its own report table, together with the violation flag, violation ID, and the power indicator $Q_i(v)$ if present. The role of z^{i-1} is to notify the TA that the $i - 1$ -th beacon was affected by replay attack. Now the TA performs the verification of position claims as in the plain vanilla A-VIP protocol given in [4]. It is easy to see that our protocol inherits all the security properties of the aforementioned protocol. Namely, the same arguments as for A-VIP show that our protocol is robust against various attacks. However, we emphasize that violations can be detected only if there are cars witnessing it. A special treatment is needed for the transmit-power attack and detecting a car moving on a wrong direction. Namely, the protocol is devised to work assuming that all the vehicles do not maliciously increase or decrease the transmission power. In such a case, a vehicle that is moving on a wrong way (see Figure 5) may appear to be stationary to the vehicles behind. If there are no other vehicles in front of the vehicles violating the one-way road in the figure, this violation remains undetected.

3. Speeding tickets

For the remaining of the paper, we focus on a specific fault of exceeding the maximum allowed speed on a grid segment. A lane or more neighbouring lanes having the same speed limitations, and directions are divided as a grid segments, roads, each with a unique identifier on the digital map of a vehicle. A vehicle's speed over a site is the ratio of the length of unit vector \vec{u} , over the time $t_i \rightarrow t_{i+1}$.

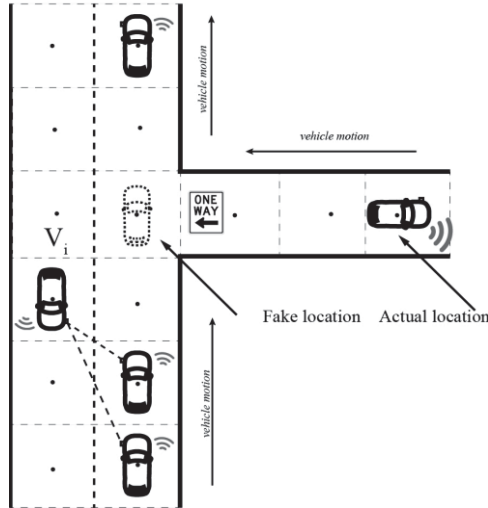


Fig. 5. Power attack by a vehicle. V_i broadcasting with more power value than of the system standard. Thus, it is observed by the other vehicles at a closer location on the grid.

Recall that when the vehicle V_i is located inside one of the sites defined by OughtTo after applying a movement rule, the vehicle is said to be obeying the traffic rules. Whenever the vehicle exceeds the maximum speed boundary over a state update period of itself, that will cause the vehicle to be inside a site location other than outside the OughtTo, than we a speed fault is committed by the vehicle. The violations happen in an empty neighborhood is not monitored nor registered because the lack of any reporters.

The my ID is	location is 6223.17 5709.38 ***** neighbor 9	location 6143.20 5671.35 no violation
The my ID is	location is 6223.84 5709.70 ***** neighbor 6	location 6090.26 5642.51 speed violation 29.00
The my ID is	location is 6224.51 5710.02 ***** neighbor 2	location 6246.38 5716.77 speed violation 30.00
The my ID is	location is 6225.18 5710.34 ***** neighbor 7	location 6164.63 5681.54 no violation
The my ID is	location is 6228.54 5711.94 ***** neighbor 5	location 6188.50 5692.90 no violation
The my ID is	location is 6229.21 5712.26 ***** neighbor 3	location 6209.31 5702.79 no violation
The my ID is	location is 6229.21 5712.26 ***** neighbor 10	location 5974.47 5591.08 speed violation 30.00
The my ID is	location is 6229.89 5712.58 ***** neighbor 12	location 5843.83 5528.94 speed violation 30.00
The my ID is	location is 6229.89 5712.58 ***** neighbor 9	location 6149.91 5674.54 no violation
The my ID is	location is 6230.55 5712.90 ***** neighbor 6	location 6117.28 5655.36 speed violation 30.00
The my ID is	location is 6231.22 5713.22 ***** neighbor 2	location 6273.40 5729.63 speed violation 30.00

Fig. 6. The list of the witnessed violations delivered by a reporter vehicle to TA

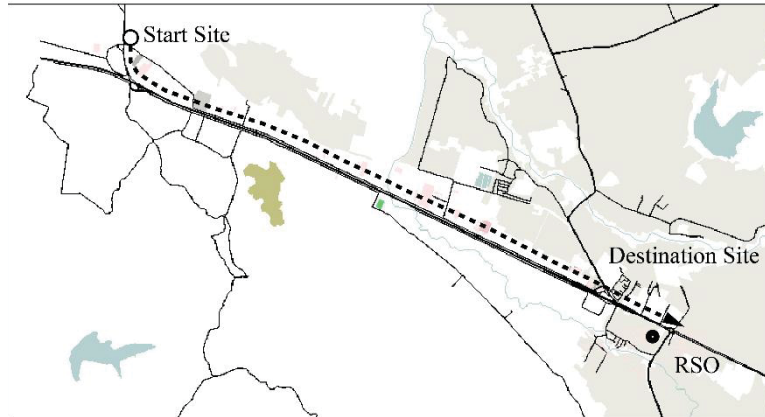


Fig. 7. The grid map that is used for the simulation. The RSO is positioned near the destination site.

First, the location information is processed and mapped on the vehicle map. Then, the state information of speed, location, and lane of the violator vehicle is compared with the site properties information on the map. Whenever the information matches, the violation event is validated as committed violation and a candidate ticket is issued and stored in the candidate ticket list for the violator vehicle. If there exists a synchronization bond between the reporter and the violator vehicles, the sync bond breaks and a flexible bond forms. The bonding change would prevent any vehicle in a cluster commit the same violation with the violator vehicle.

When a reporter vehicle enters in the communication distance of a RSO, the witnessed violations are delivered to the TA and the reporter vehicle clears its list.

4. Simulation

In order to evaluate our proposed model, we have used OMNET++, Network Simulation, and SUMO 0.22 an open source micro-traffic traffic simulator. VEINS 3.0 vehicular network simulation framework establishes communication between OMNET++ and SUMO. OMNET implements the IEEE 802.11p protocol stack at both the physical and the MAC layers. The state updates and information exchange between the vehicles, i.e channel access and wireless communication is implemented by using OMNET++ and VEINS. SUMO is used to simulate the movement updates, and to obtain the environmental details of each individual vehicle on the grid. We use a portion of the Tirana Durres highway, and a part of the urban area of Tirana as seen in Fig. 7.

Table 1. Simulation parameters for the simulation scenario

Parameter	Value
Transmission power	1.6mW.
Transmission range	$\cong 150m$.
Bit rate	18M bit/s
Grid length	11 km.
Data message size	512 Byte
Speed of vehicles	27 km, 81 km, and 108 km.

A RSO is positioned 100 meters away from the starting site at the beginning of the Tirana Durres highway on Tirana side. The RSO transmits periodic information beacons to notify the reporter vehicles and gather the local tables from the vehicles in the communication distance. A reporter

vehicle only delivers the information in the local list to the Trusted Authorities (RSOs). to ensure the privacy of the vehicles. The length of the highway grid is approximately 8 km. and has two lanes, and the speed violations take place in the highway section of the grid.

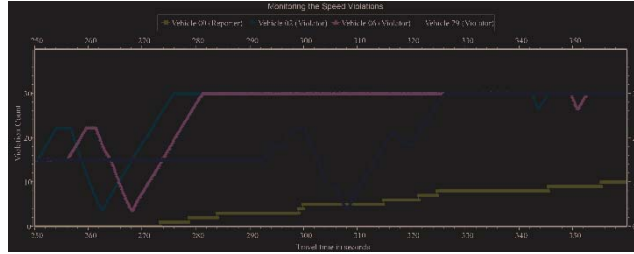


Fig. 8. The state of the local list of vehicle V0 during the simulation. The vehicles V2 and V6 start speeding up and exceeds the maximal speed of the lane as they have already flex-bonds to the V0 .

The vehicles of the same type assigned with different speeds of 80 km/h, 108 km/h, and 50 km/h. The speed of a vehicle at a time t is obtained from OT . The first groups of the vehicles are capable of reaching 80 km. and always maintain their speed under the inside the allowed speed boundary. Together with the second group of vehicles with the speed of 50 km/h, the vehicles report the vehicle’s violations. While the last group of the vehicles is capable of reaching 108 km/h, and violates the maximum allowed speed on the highway segment of the simulation. In order to ensure overtaking takes place, the violator vehicles enter into the simulation after the first mentioned vehicle groups start the simulation. The number of vehicles on the grid is fixed to 1000, 100, and 200, respectively for each vehicle group. The trajectory is the same for all vehicles. At the highway section of the map the maximum speed is bound at 90 km/h. Together with the violator group of 100 km/h speed, this group forms a close cluster of vehicles before the start of the highway to ensure to capture the first speed violation in the grid.

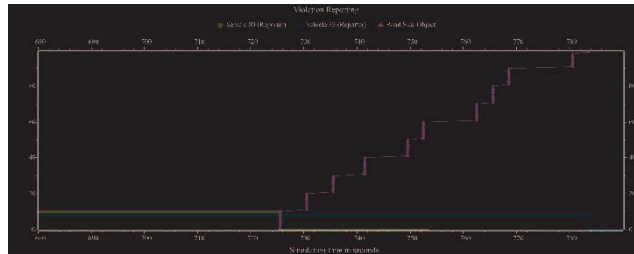


Fig. 9. The local lists are sent by the vehicles to the Road Side Object. After the transmissions is completed the vehicles clean their local list.

Conclusion and Future Work

In order to be able to compute the OughtTo set, we use a non-sophisticated method of repeating the same time dependent secret at two consecutive times. For the same reason, a vehicle releases information about its precise location in plaintext. The first open question would be if there is such a cryptographic tool that allows us to drop these –somewhat harsh – constraints. Second, a further validation of the result should be made using a real imple- mentation.

References

- 1 M. Ozkul, I. Capuni, "An Autonomous Driving Framework With Self-Configurable Vehicle Clusters" 2014 International Conference on Connected Vehicles and Expo, pp.463-468,3-7 Nov. 2014 DOI 10.1109/ICCVE.2014.57
- 2 World Health Organization. World report on road traffic injury prevention, 2004.
- 3 SWOV Fact sheet. Headway times and road safety, December 2012.
- 4 Malandrino, et al., "Verification and Inference of Positions in Vehicular Networks through Anonymous Beacons," in Mobile Computing, IEEE Transactions on , vol.13, no.10, pp.2415-2428, Oct. 2014 doi: 10.1109/TMC.2013.2297925
- 5 The Insurance Institute for Highway Safety (IIHS) General statistics.
- 6 <http://www.iihs.org/iihs/topics/t/general-statistics/fatalityfacts/state-by-state-overview#Rural-versus-urban>
- 7
- 8 K. Nagel and M. Schreckenberg, "A cellular automaton model for freeway traffic,"
- 9 in J. Physique I, 2:2221 (1992).
- 10 Vijverberg, et al., "High-Level Traffic-Violation Detection for Embedded Traffic Analysis," Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on , vol.2, no., pp.11-793,11-796, 15-20 April 2007 doi: 10.1109/ICASSP.2007.366355
- 11 Vishnevsky, et al., "Architecture of application platform for RFID-enabled traffic law enforcement system," Communication Technologies for Vehicles (Nets4Cars- Fall), 2014 7th International Workshop on pp.45,49, 6-8 Oct. 2014.