International Journal of Computer Applications (0975 - 8887)
Volume 177 - No.10, October 2019

Intersection Safety through Traffic Violation Detection

Mükremin Özkul
Dept. of Computer Engineering, Epoka University
Tirana, Albania

ABSTRACT

This paper presents a violation detection and collision avoidance system to vehicles at road intersections. The system relies on secure messages to assist vehicles in a constant size neighborhood by detecting traffic rule violations and finding trajectory conflicts at intersections. Each vehicle is modeled as an automaton that, regardless of its visual range, can see the states of other vehicles through on-board sensors and/or by using wireless communications. Traffic rules are encoded in the program of a vehicle and guide the changing state of the vehicle in traffic. Each vehicle can autonomously decide if the vehicles in its neighborhood comply with the traffic rules by observing the movements of the vehicles on the road and then anonymously reporting the observed violations to a traffic authority be further processed. Each vehicle periodically generates shared secrets which are then used as part of messages it sends to achieve security and privacy. The location of these messages is not traceable by any single traffic authority in the system, including the authentication parties and the road infrastructure. Yet, the proposed system is able find the location and real identity of any vehicle whenever it commits a rule violation in traffic with a lightweight protocol. Further, the security analysis is provided and the performance simulation results show that the system allows no false positives.

Keywords

Vehicular ad hoc networks (VANETs),Dedicated Short Range Communications(DSRC), traffic violation and ticketing, traffic safety, location privacy

1. INTRODUCTION

Intersections constitute a large part of the urban road network. National Highway Traffic Safety Administration (NHTSA) [1] reports that nearly half of all road accident injuries occur at intersections. The majority of these accidents are caused due to human error such as traffic rule violations or misjudgment of a traffic situation. As a result, in recent research into systems for vehicle safety and driver assistance has been a primary focus of study in Vehicular Ad Hoc Network (VANET) systems. A VANET is a decentralized car-to-X communication type of wireless network that uses vehicles as nodes to create mobile network.

In VANETs, vehicles equipped with wireless communication devices disseminate periodic messages or ?beacons?, to report individual data such as location, speed, trajectories, and destinations in real-time. Such information allows a vehicle to perceive the surrounding environment beyond its visual range and provides the basis of acquiring the real-time traffic data for safety applications.

A key component in VANETs is to provide privacy and security guarantees for the vehicles in traffic. An adversary vehicle could try to gain the right of crossing at an intersection by broadcasting a false identity, such as pretending to be an emergency vehicle, thus jeopardizing the safety of others with the false information it disseminates. Therefore, each vehicle needs to be authenticated before it is allowed to participate and broadcast messages in traffic communications. On the other hand, the system should not allow the tracking of identities or the locations of vehicles at any time, even by legitimate authorities.

This paper presents a system to improve the safety of vehicles - human driver or autonomous - by detecting traffic rule violations with minimum infrastructure at intersections. The decisions of each vehicle are based solely on the secure messages of the others with a smaller amount of computational complexity for vehicle-to-vehicle communication and/or its on-board sensors information. Whenever the vehicles are in the neighborhood that is defined by the wireless communications, the system is active and produces valid results. The traffic rules, encoded in a vehicle's program and using a digital map, are used to compute the next states of neighboring vehicles and then to identify potential traffic violations and conflicts on roads and at intersections. These rule violations include speeding, failure to stop at red lights, or driving in the wrong direction in traffic.

In the system, each vehicle acts like a traffic police, observing and verifying the states of the neighboring vehicles to verify if they are in allowed states. Whenever a vehicle disobeys a traffic rule imposed at the current location, while moving or at a stop, it is considered a violator.

The system aims the following properties.

(1) **Privacy:** The real identity and the location of a vehicle u should be kept private including to traffic authorities at all times.

(2) **Security:** The communication infrastructure must be secure to avoid attacks from adversaries, i.e., a vehicle should be prevented from using multiple identities or fabricating false violations to the others.

(3) **Efficiency:** A vehicle adapts and maneuvers with little or no delay to changes in the traffic flow in real time.

(4) **Adaptability:** The system should be scalable to any participants with a mobile computational unit, e.g. pedestrians or cyclists, or to any increase in the number of participants.

(5) **Veracity:** An observed violation by a vehicle u for a vehicle x is to be traceable to the x and easily verified by a trusted authority.

2. RELATED WORK

Significant research has been carried out in the context of traffic safety systems.
Video image processing techniques are used to identify distinctive facial expressions; such as eye movements-signs of drooping eyelids, and yawning; to detect drowsy driving [2–5]. Some systems use on board sensors; such as speed and orientation sensors, GPS, and two-axis accelerometer; to extract information of the vehicle state and detect unsafe driving styles in order to provide feedback with recommended actions [6–8].
In [9] , the authors introduce a vehicle localization system by integrating data acquired by on-board sensors, i.e. Global Positioning System(GPS), inertial measurement unit, wheel odometer, and from Light Detection and Ranging (LIDAR) data to generate high-resolution maps and thus maintain a location accuracy to less than 30 cm errors. Other localization systems propose techniques such as computer vision and integrating vehicle and lane tracking in order to achieve high accuracy and consistency for vehicle localization.
In [10] , authors propose a simulation framework to analyze intersection safety applications and their communication requirements, e.g., transmission power, and authentication mechanisms. In the simulations, accidents are injected into the traffic at intersections in various scenarios. Then, the responses taken by drivers are modeled to predict vehicle collisions in order to give a warning to drivers in time to prevent a potential collision. The results show that for light vehicle traffic situations, a majority of accidents at intersections could be prevented by using vehicular safety applications. In the system, it is assumed that a relatively accurate position for a vehicle's location at any given intersection can be obtained and is available for every vehicle (or participant).
Multi-agent-based autonomous protocols [11–13] are proposed to manage the speed profiles and trajectories of autonomous vehicles at intersections. In, each vehicle is an autonomous agent, moving through intersections following preset parameters agreed upon by vehicles and a central intersection manager located at the intersection. All vehicles interact and send requests to the intersection manager to reserve space and time for them to pass through the intersection. It is then up to the intersection manager to decide whether or not a request can be met by simulating the vehicles' trajectories on a grid of $n \times n$ tiles. At each time step of the simulation, any tile required by a vehicle is reserved and no other vehicle occupies the same tiles. Afterward, the intersection manager informs the respective vehicles whether their requests were accepted or denied.
In [14], the authors propose a decision-making framework for autonomous vehicles to identify potential trajectory conflicts and traffic violations at intersections. Each vehicle is equipped with on-board sensors, enabling them to predict potential future pathways of vehicles and allowing them to determine appropriate maneuvers to navigate the intersection.
Although the aforementioned systems are efficient in terms of managing traffic flow at intersections, the assumptions of such systems is that the participants are trustworthy in their communications, thus inherently presenting security and privacy issues.
Pseudo-identity-based authentication using multiple certificates has been well-adapted as a method for managing vehicular networks as presented in [15–17]. The aim of the pseudonym-based authentication protocols is to protect the privacy of the individual vehicles, verifying their movement by the signature of the sender, while still hiding their real identities. Most of these methods violate the location privacy requirement by allowing an authorized authority to reveal the real identity of a vehicle during identity disputes. Moreover, the vehicle may be able to be tracked by other vehicles in the communication range by linking the vehicle with the pseudonym it uses.
This paper presents a safety system that detects violations at intersections both for vehicles with human drivers and autonomous vehicles. Each vehicle broadcasts its location through secure beacons and can see the states and trajectories of the vehicles in a constant size neighborhood on the road. So long as a vehicle obeys the traffic rules, neither the infrastructure nor the traffic authorities can find out the real identity of a vehicle or track its movements. Yet, the system provides irrefutable proof of a violation and can trace the location and the identity of violators to issue traffic tickets wherever and whenever there are enough participants or *"witnesses"* in the system in traffic to verify the violation.

3. SYSTEM LAYOUT

The system architecture is represented as seen in Fig. 1. A Trusted Authority (TA) which is located in a cloud platform maintains the private information of participants in a database and communicates via a 3G/4G network with the vehicles and through the Internet to the other servers. A Verification Server (VS) validates the veracity of beacons sent by the vehicles on the road. The VS is also located in a cloud platform. TA holds the real identity of vehicle x and the VS has the location information of the vehicle x in real-time, but no servers have both pieces of information at the same time. Traffic Controllers (TC) are physically centered at intersections to receive beacons from the vehicles, detect their presence, determine their location on the digital map, and control the traffic flow through lights at the intersection. TCs relay received beacons from vehicles to the VS which verifies together with the TA without revealing the real identities of the vehicles.
At every time step, say 0.1 s, TCs broadcast a beacon which includes intersection information, i.e. the time remaining for the current light time and the light sequence, to the vehicles within the communication range. Based on the beacon of a TC, vehicles can decide whether to cross an intersection or stop and wait until signaled to do so by a green light.

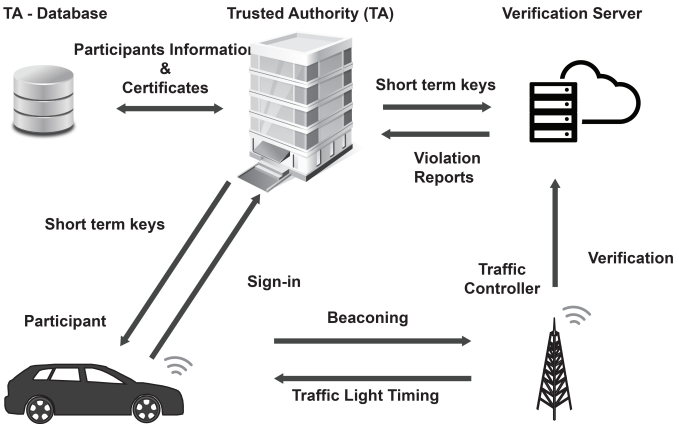

Fig. 1. The system layout.

The road model is based on a two-dimensional triangular grid with a fixed-coordinate system presented in the prior work in [18]. Each point defined as $\overrightarrow{p} = (x, y)$ of this system is called a *site* and a vehicle is considered an automaton which in its transition function features the traffic rules, whereas the local constraints, including speed limit for a movement between the two state updates, traffic direction, and reserved sites like bus lanes, are stored on a digital map, which is loaded on the unit. In addition, every vehicle has a wireless communication unit, such as Dedicated Short-Range Communications (DSRC), is equipped with a Global Positioning System receiver (GPS), and has 3G/4G/5G capability.

3.1 Detecting Rule Violations

Before a state update, a vehicle v computes all of the unoccupied sites on the road in the neighborhood, *Movable set* set M_v, which directs the sites to allow a movement system update from its current site to the next one on the road. The vehicle then determines from a finite set of trajectories the one which is chosen for the next movement update. Each vehicle is also able to compute its neighbors' movable sets in the commutation distance. By using movable sets, a vehicle can determine if any conflicts or the potential for collisions exist between the two vehicles' trajectories.
The *Ought-To set* $\mathrm{OughtTo}(v, s, t)$ gives all the possible next states that a vehicle v can be at time t after applying a state update at the time $t-1$ from state $s-1$. A vehicle is obeying the traffic rules as long as its state remains in its $\mathrm{OughtTo}$, and if not, a traffic rule violation is committed by the vehicle.

3.2 Sign-in

Initially, a vehicle registers with the Trusted Authority (TA) which maintains a database containing the identity information of all the participating vehicles, distributes digital certificates, manages the sign-in process, receives violation reports, and issues tickets to the vehicles.
In the system, it is assumed that privacy is maintained at all times by the system protocols in place and that the TA and VS do not collude or claim false violations. All the time that the vehicle is in the system, its true identity is kept private from both the TA and the VS. Therefore, TCs are not designed to communicate with eachother, and only share information with the VS. This communication strategy preserves the identity and location privacy of each vehicle at each instant of time.
Only the TA holds the right to disclose the real identity and location of vehicles in the case of a valid violation as reported by the witnesses in the system. Trust in the TA and the VS is limited, that is in the case of issuing a violation to a vehicle, both parties are needed to validate the violation. To achieve such goal, the TA and the VS must cooperate. The vehicles are not trusted by default and could be malicious, disseminate false information, impersonate others, and collude to fabricate false reports about the others.
Upon start-up, the vehicle establishes a symmetric key with the TA by initiating a sign-in process via secure communication channels, e.g. a wireless or 3G/4G network. After the sign-in, the vehicles communicate with the TCs to report violations.
In order to verify if the vehicle possesses valid credentials, a registration request is first sent from vehicle v at time t^0 to the TA which verifies if the vehicle possesses the valid credentials, i.e. a long term id of v. After the TA returns the quadruplet $(K_v; r_v; o_v; t_s)$ to the vehicle v, where K_v is a short-term symmetric key, and r_v, o_v, and t_s are three random integers. Both parties initialize a counter n to the value r_v and increment it by o_v at every message sent by the v.

In order for messages the vehicle sends to be validated and trustworthy, a time dependent secret $s_v(t)$ is used. This time dependent secret is only used once to prevent replay attacks by the others in the system. The $s_v(t)$ is computed and encrypted as follows
First,

$$s_v(t) = E_{K_v}\{r_v + no_v\}.$$

Second, a randomized ID $P_v(t)$ is computed as follows

$$PID_v = E_{K_v}\{S_{ID} + t_s o_v\}.$$

where S_{ID} is the session identity of the vehicle, and t_s is a short-time period at which $P_v(t)$ is re-computed and updated.

3.3 Beaconing

The vehicle v periodically broadcasts a beacon every τ_b seconds, say 10 per second, in which it shares a randomized ID, its type, and location on the road with others in the communication range using the IEEE 802.11p [19] standard. The vehicle v forms the beacon as follows

$$B_v = \langle PID_v, l, t_{stamp}, \sigma, s_v(t), E_{K_v}\{l(t)\}\rangle,$$

where PID_v is the randomized ID v, l is the is the location information in plain text, time-stamp t_{stamp} to provide beaconing time, the encoded location information $E_{K_v}\{l(t)\}$, and the σ is the beacon digest obtained by using the hash function $H()$, say SHA-1.

$$\sigma \leftarrow H(PID_v, l, t_{stamp}, s_v(t), E_{K_v}\{l(t)\}).$$

3.4 Beacon authentication

A beacon needs to be authenticated to confirm that it is from an authenticated vehicle and is not unaltered. One way that is used is to verify the *"freshness"* of a received beacon is by checking the t_{stamp} to ensure it is in the window of τ_b. As soon as a beacon is received, a vehicle u first verifies the freshness of the beacon by making sure that the t_{stamp} is in the window of τ_b. Then, the message integrity is computed and then verified by comparison with the beacon digest value σ in the received beacon. If the two values are the same, then the beacon is valid and unaltered with a third party, otherwise it is discarded. A neighborhood table in the vehicle u keeps a record of beacons that have been received for a fixed amount of time.
A beacon received by TC from u, is first verified for its integrity before being submitted to the VS which first checks whether the PID_u exists in its database. If not, the VS extracts the information PID_u , $s_u(t)$, and the time stamp t_u from the beacon and relays a request to the TA to authenticate the legitimacy of the vehicle.
Verification requests received by the TA are processed as follows:
Let $\mathcal{V}$ represent the set of vehicles that needs to be authenticated for the VS. For each request of the VS, the TA proceeds as follows:

(1) reads the time stamp t_u in the request entry;
(2) for each $w \in \mathcal{V}$ computes

$$j = \lfloor \frac{t_{uw} - t_w^0}{\tau_b} \rfloor,$$

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

(3) using j, it retrieves the pre-computed secret value s_w^j that matches s_v^j and the randomized ID PID_v.

The authenticity of the beacon is verifiable by the TA and vehicle v can be identified as the vehicle in the report entry. The report entry is invalidated and discarded if the time stamp t_u does not match any time-dependent secret.
To complete the process, the TA sends the $P_v(t)$ and the set valid shared secret $s_v(t)$ associated with the $P_v(t)$ to the VS. Thus, the VS is able to verify the authenticity of beacons from v for a time period t_s. If the vehicle u is not authenticated, the TC broadcasts the randomized ID $P_u(t)$ of the intersection.

3.5 Issuing Tickets

A violation report from a vehicle u is sent to the TA through the VS, then is processed and decrypted. Each report consists of two consecutive beacons for the time instants t and $t+1$ of a violation. First, each beacon in the report undergoes the authentication process as provided in the previous section. A violation of The TA is vested with the legitimate power to reveal the real identities and the location of vehicles whenever valid violations are reported by the witnesses in the system v. As the report entries for the consecutive time instants t and $t+1$ are validated to the same v, the TA extracts the location information l at the t and $t+1$. After that, TA checks $\mathrm{OughtTo}(v, s, t)$, and determines what violation has been committed.
Given that during the process the TA is only able to compute the reports from the VS, the real identity and the location privacy of a vehicle remains anonymous at all times to others, including to the VS and TCs.

4. SECURITY ANALYSIS

In this section, we analyze the proposed model from a security perspective. The two aspects of security that the most attention must be directed towards are replay attacks and unforgeability of false tickets.

4.1 Privacy

The model guarantees full privacy to protect the real identity of the user to keep them anonymous and impossible to trace. The other vehicles cannot link different shared secrets to the same vehicle at any time.
Although, a TC is able to generate the secrets of a vehicle in a time-space ball defined by the communication distance, as the vehicle v moves outside the wireless distance or makes a change to its short-term private key, TC cannot decrypt beacons anymore and hence cannot track the vehicle outside the intersection.
The TA, on the other hand, is unable to trace the trajectory of any vehicle since the queries of a TC to the TA do not include any location information.

4.2 Traceability

Upon a violation report, TC and TA are collaboratively able to reveal the identity and the location of a violator vehicle. Identity tracing is not used without a valid violation claim, and the obeying vehicles' identities remain hidden at all times in the system. Therefore, the system achieves the seemingly-conflicting requirement of anonymity for the legitimate users as well as traceability for the violators.

4.3 Unforgeability

Several adversaries can collude to report and forge a false violation to a vehicle. However, a violation report needs to include a unique time dependent secret s_v to claim any violation of v.
Recall that, the TA keeps the shared secrets of v to itself, and a shared secret is used once, so the only way for an adversary to claim a false violation for an obeying vehicle is to exploit the randomized shared secrets. Moreover, the uniqueness of a beacon is easily verifiable by the TA. Each vehicle v broadcasts a unique beacon whose keys an adversary does not have access to.

4.4 Replay attacks

An adversary replays an old beacon of the vehicle v in a replay attack at a later time and location than the original beacon in order to fabricate a false violation. To ensure no two beacons are the same, each encrypted beacon contains a t_{stamp} and a time dependent secret s_v two consecutive time instants t and $t+1$. This ensures the freshness of a beacon in the system. The TC ensures a beacon is legitimate by checking the t_{stamp} information in a beacon to determine whether the time is in the allowable window of τ_b until the receiving time. If the beacon does not fall within that window of time, it is disregarded and discarded by the TC.

5. SIMULATION

To simulate the traffic environment, a microscopic open source traffic simulation, Simulation of Urban Mobility (SUMO) [20], is employed. In particular, the OMNET++ [21] simulator is used to develop the computational framework. This is an event-based network simulator is based on C++, and employs the IEEE 802.11 protocol stack for wireless communications. VEINS [22] is a vehicle-to-vehicle (V2V) communication platform that can exchange data and information with SUMO, and using TraCI [23], is able to map the vehicles as a mobile network node in OMNET++.

5.1 Simulation settings

A four-leg isolated intersection with a traffic light controller is used upon which to base the simulation map. In the map, there is no source of interference, e.g high buildings or energy lines, to the wireless communications. The simulation assumes that all the roads have two lanes in the same traffic direction, including a total length of 500 m. upstream and downstream of the intersection. Each vehicle periodically broadcasts beacons at intervals of 0.1 seconds. The main simulation parameters are summarized in Table 1.

Table 1. The simulation parameters.

Parameter	Value
Traffic flow	600 - 800 per hour in each direction
Beacon transmission rate	.1 x per second
Transmission range	$\cong 200m.$
Road length	500 m. at each approach
Simulation duration	60 min.

5.2 Speeding

Recall that, $\mathrm{OughtTo}$, with site and traffic rules, determines whether a vehicle obeys or violates the traffic rules. Whenever a vehicle positions after applying two consecutive movement updates in a site other than the $\mathrm{OughtTo}$, the vehicle is said to have committed a speeding violation. The system relies on the reports of the

witness vehicles, therefore any violations in an empty neighborhood are neither detected nor visible to the traffic authorities.
A witness vehicle u computes the speed of a vehicle v as follows. First, it stores the received beacon from a vehicle v in its state. At the next beacon from v, it extracts the location information in the beacons and computes the distance d_v covered by v between the time of beacons. Then, $v_{speed} = \frac{d_v}{\tau_b}$ calculates the speed of v to determine if the speed follows the rules of that section as shown on the digital map. If v is found to be outside the OughtTo, this irregularity is recorded in the report table of u. The traffic controller is then given a report list within a time period set by the TA.
All the vehicles are injected into the simulation according to the Poisson distribution at 800 vehicles per hour in the east-to-west traffic flow, and 600 vehicles in the north-to-south direction. A random distribution of speed, varying from 20 km/h to 40 km/h, with a maximum of 50 km/h is set for the obeying vehicles. 2% of the traffic are speed violators travelling at up to 80 km/h, and exceeding the speed limit, who are injected into the east-to-west traffic flow vehicles.

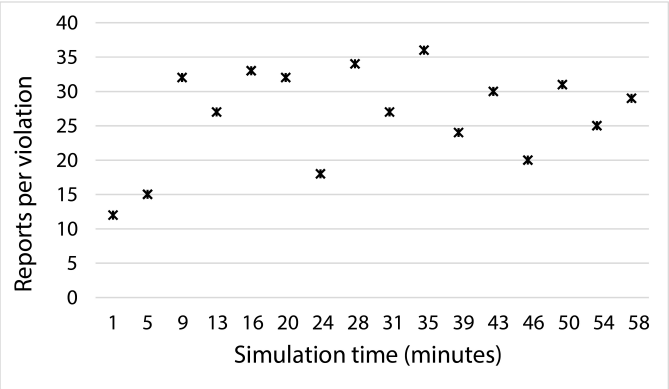

Fig. 2. Speed violations with the number of reports for each issued ticket.

It is important to emphasize that the system relies on the participants playing the roles of witness and reporter simultaneously. The Fig. 2 shows the number of reports for each of the tickets issued. It is evident that some of the violations have a larger number of reports on them than the other violations. This is because whenever a speed violation occurs close to the intersection, a large number of reports are produced because of the waiting vehicles at the stop line of the intersection.
The Fig. 3 presents the effects of the participation rate, or the penetration rate, of the witness vehicles on the number of issued tickets. The results show that even at the lower penetration rates, the TA is able to issue tickets to the violators since a single valid report is enough to process a violation.
Clearly, the simulation conditions are ideal here, and there is no signal interference, e.g. high buildings and power lines. However, as the penetration rate drops below 15%, some violations are never witnessed in the first place and no tickets are issued to the violator. This is because the violator is not in the communication range of the others. Since the system relies on the number of witnesses, which is based on the higher number of reporting vehicles, a better performance is obtained at higher penetration rates.
The Fig. 4 reflects the effect traffic density has on the number of reports and issued tickets. Predictably, as the percentage of the vehicles increases, the detect rate of a violation increases proportionally, and hence the TA is able to issue more tickets at higher traffic densities than at lower traffic densities.

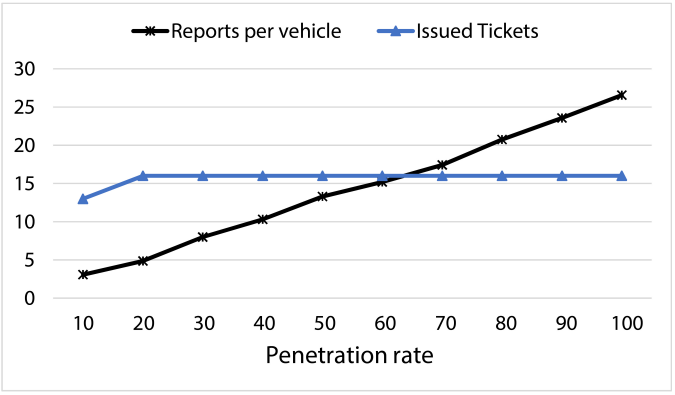

Fig. 3. The effects penetration level on the number of issued tickets.

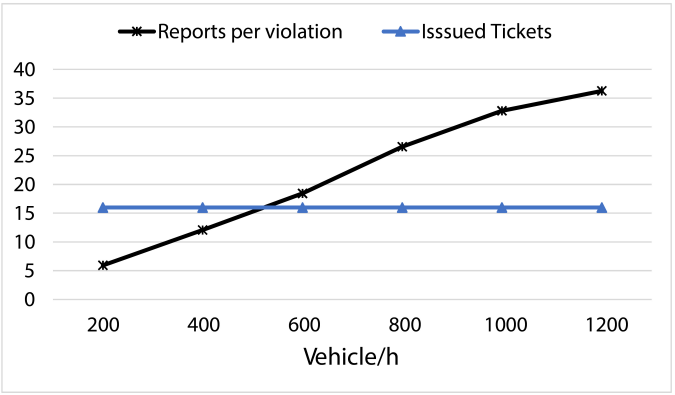

Fig. 4. The effects of vehicle density on the number of issued tickets.

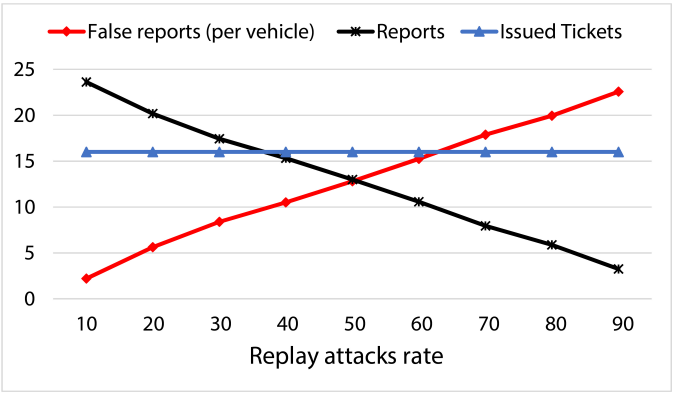

Fig. 5. The effect of replay attacks and false reports on the issued tickets.

In a replay attack scenario, the adversary vehicles replay the messages of other vehicles in its communication rang. To model this, the ratio of the attackers is set at levels between 5% to 90% during the simulations.
The Fig. 5, shows that the number of false violation rise in direct proportion to the number of replay messages in the system. How-

ever, the system does not produce any false positive results tickets, even at the higher number of false violation reports.

6. CONCLUSION

This paper presents a system able to detect and verify traffic violations at intersections. The system works based on the periodic and secure messages of vehicles. The verification and decision process ensures that at all times the identities of the participants, both as witnesses or as violators, are not disclosed, even to the traffic authorities. According to the simulation results, the proposed system correctly identifies traffic rule violations in real time. Of an even greater concern is the potential for a security attack or a vehicle being falsely accused of a traffic violation. This system guards against these dangers as well as holding potential to help participants resolve legal or insurance issues.

7. REFERENCES

[1] National Highway Traffic Safety Administration. Traffic safety facts 2014.a compilation of motor vehicle crash data from the fatality analysis reporting system and the general estimates system. 2014.

[2] Nawal Aliou, Aouatif Amine, and Mohammed Rziza. Drivers fatigue detection based on yawning extraction. *International Journal of Vehicular Technology*, 2014, 2014.

[3] Martin Eriksson and Nikolaos P Papanikolopoulos. Driver fatigue: a vision-based approach to automatic diagnosis. *Transportation Research Part C: Emerging Technologies*, 9(6):399 – 413, 2001.

[4] Qiang Ji, Zhiwei Zhu, and P. Lan. Real-time nonintrusive monitoring and prediction of driver fatigue. *IEEE Transactions on Vehicular Technology*, 53(4):1052–1068, July 2004.

[5] Nidhi Sharma and V. K. Banga. Drowsiness warning system using artificial intelligence, 2010.

[6] S. Boonmee and P. Tangamchit. Portable reckless driving detection system. In *2009 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, volume 01, pages 412–415, May 2009.

[7] Cheol Oh, Eunbi Jung, Heesub Rim, Kyungpyo Kang, and Younsoo Kang. Intervehicle safety warning information system for unsafe driving events. *Transportation Research Record: Journal of the Transportation Research Board*, 2324:1–10, 2012.

[8] Rui Sun, Washington Yotto Ochieng, and Shaojun Feng. An integrated solution for lane level irregular driving detection on highways. *Transportation Research Part C: Emerging Technologies*, 56:61 – 79, 2015.

[9] Jesse Levinson, Michael Montemerlo, and Sebastian Thrun. Map-based precision vehicle localization in urban environments. In *Robotics: Science and Systems*, 2007.

[10] Jason J. Haas and Yih-Chun Hu. Communication requirements for crash avoidance. In *Proceedings of the Seventh ACM International Workshop on VehiculAr InterNETworking*, VANET '10, pages 1–10. ACM, 2010.

[11] Kurt Dresner and Peter Stone. Multiagent traffic management: An improved intersection control mechanism. In Frank Dignum, Virginia Dignum, Sven Koenig, Sarit Kraus, Munindar P. Singh, and Michael Wooldridge, editors, *The Fourth International Joint Conference on Autonomous Agents and Multiagent Systems*, New York, NY, July 2005. ACM Press.

[12] Q. Jin, G. Wu, K. Boriboonsomsin, and M. Barth. Advanced intersection management for connected vehicles using a multi-agent systems approach. In *2012 IEEE Intelligent Vehicles Symposium*, pages 932–937, June 2012.

[13] Matteo Vasirani and Sascha Ossowski. Learning and coordination for autonomous intersection control. *Applied Artificial Intelligence*, 25(3):193–216, 2011.

[14] S. Noh. Decision-making framework for autonomous driving at road intersections: Safeguarding against collision, overly conservative behavior, and violation vehicles. *IEEE Transactions on Industrial Electronics*, 66(4):3275–3286, April 2019.

[15] K. Shim. CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. *IEEE Transactions on Vehicular Technology*, 61(4):1874–1883, May 2012.

[16] C. Zhang, R. Lu, X. Lin, P. . Ho, and X. Shen. An efficient identity-based batch verification scheme for vehicular sensor networks. In *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, pages 246–250, April 2008.

[17] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *IEEE Transactions on Vehicular Technology*, 59(7):3589–3603, Sep. 2010.

[18] M. Ozkul and I. Capuni. An autonomous driving framework with self-configurable vehicle clusters. In *2014 International Conference on Connected Vehicles and Expo (ICCVE)*, pages 463–468, 2014.

[19] Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments. *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)*, pages 1–51, July 2010.

[20] Michael Behrisch, Laura Bieker, Jakob Erdmann, and Daniel Krajzewicz. Sumo - simulation of urban mobility: An overview. In *in SIMUL 2011, The Third International Conference on Advances in System Simulation*, pages 63–68, 2011.

[21] András Varga and Rudolf Hornig. An overview of the omnet++ simulation environment. In *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*, pages 60:1–60:10, 2008.

[22] C. Sommer, R. German, and F. Dressler. Bidirectionally coupled network and road traffic simulation for improved ivc analysis. *IEEE Transactions on Mobile Computing*, 10(1):3–15, 2011.

[23] Axel Wegener, MichałPiórkowski, Maxim Raya, Horst Hellbrück, Stefan Fischer, and Jean-Pierre Hubaux. Traci: An interface for coupling road traffic and network simulators. In *Proceedings of the 11th Communications and Networking Simulation Symposium*, CNS '08, pages 155–163, New York, NY, USA, 2008. ACM.