Preventing Traffic Jams by Secure and Efficient Beaconing

Mohd. Amir Siddiqui 1, Jeetendra Kumar Mishra 2, Saurabh Gupta 3
Department of Computer Science and Engineering
1,2MNNIT Allahabad, Allahabad, India
3Al-Falah School of Engg. and Tech., New Delhi, India
amrsiddiqui.786@gmail.com, jeet9065@gmail.com, ensaurabhgupta@gmail.com

Abstract - Traffic Jam has become a very big problem of today's world. It not only stresses the commuters but also wastes fuel and productive hours of Human Resource. Many times in dense but free flowing traffic, jams arise spontaneously, triggered by minor events such as an abrupt steering maneuver by a single motorist. This paper talks about resolving such type of traffic jams with the help of VANET communication. When it comes to communication, two new words security and efficiency comes into the picture. To perform well in real time scenario the communications between the entities has to be secure as well as efficient. Beacons are the mode of communication in VANET. We used asymmetric key cryptographic mechanism with some changes to reduce protocol overhead as well computational overhead, due to entities has to be secure as well as efficient. Beacons are the mode of communication in VANET. We used asymmetric key cryptographic mechanism with some changes to reduce protocol overhead as well computational overhead, due to exchange of key, signature and certificate and to verify signatures, without any significant compromise with security. Extensive simulations have been performed to show the effectiveness of the proposed mechanisms.

Keywords – Comfortable driving model, Traffic Jam, Beacon, VANET

I. INTRODUCTION

The given paper discusses the two, said, issues separately in two different sections and finally aggregate them to complete the whole picture. The first section talks about resolving “Phantom” traffic jams where as in the second section the subject of discussion is securing beacons.

Facing traffic congestion has become a part of daily routine for commuters around the globe. Comparing the change from Indian point of view in between 1951 to 2007[1].

- Increase in Road Length (kms.) 837 to 1900 (2.27%)
- Increase in Population (lacs) 29.9 to 160 (5.35%)
- Increase in No. of Vehicles 35000 to 15.03 lacs (42.94%)

This problem will grows with the ever growing traffic on the roads.

Many times a freely flowing traffic becomes congested all of sudden despite of the fact that the road system is still adequate to serve higher traffic. Such traffic breakdowns are due of perturbations caused by human drivers. Increasing and extending the road network is not a suitable solution to cure congestion because of spatial, financial, and environmental constraints. Development in the Information Technology and Communication, however, can lend a helping hand to make today's transportation system not only more efficient but also safer, more reliable and more convenient. VANET comes as an appropriate tool to serve the purpose. As there is no need of any underlying infrastructure and latency time is low for message exchange.

VANET-based traffic state estimation is explored previously also. But previous studies focused on the congestion detection with respect to dynamic route choice or radio channel analysis. Our approach tries to identify “critical"
Preventing Traffic Jams by Secure and Efficient Beaconing

road segments and to prevent a traffic jam before it actually occurs. Most of the times, a breakdown spontaneously occurs without an obvious cause such as a construction site or an accident. It is actually caused by misbehavior of human drivers in dense traffic. Therefore, we suggest using periodically emitted beacons to analyze the current traffic state. Communicating vehicles change their driving behavior in dense traffic and inform following vehicles about the discovery of dense traffic. After a vehicle has changed its driving behavior, it is expected to be less likely the trigger of traffic breakdown. This makes given method different from many other approaches which direct vehicles to an less-congested alternate routes in order to resolve the congestion.

Periodic beacons that we use for message exchange are essential for most safety applications [2] and have therefore been extensively studied. Hence, this paper will focus on the aspects related to traffic dynamics, although we have to admit that more innovative beacon schemes are the object of current research.

The basis for many VANET applications is beacon. The issues regarding security of beacon message communication are discussed in a section of this paper. With beaconing we denote the periodic transmission of packets containing a vehicle's position and other information as a single-hop broadcast to all neighboring vehicles or road-side units. Implemented in an insecure way, beaconing open opportunities for abuse. To address these problems, many security solutions suggest, using signatures based on asymmetric cryptographic mechanisms like ECDSA together with more mechanisms [3]. In order to reduce the significant communication and computational overhead created by this, we propose to skip signatures or certificate in certain situations.

II. Resolving Traffic Jams

VANET enables physical driving and communication system to work hand in hand, which requires considering the influence of both areas on each other. In this spirit, we discuss the application of reducing traffic jams to design a protocol for the behavior of vehicles. We exploited the information sent by regular periodic beaconing so that no additional communication protocol is required. Therefore, we forgo discussing security-related aspects of our approach and refer to the next section and corresponding literature (e.g. [4]).

Traffic state estimation, which we applied to determine when to change driving behavior, has already been investigated in the context of adaptive beaconing. Therefore, it was suggested to adapt either the transmission range [5] or the beacon interval, [6], depending on local vehicle density.

Applications aiming at easing congestion, however, require more information than knowledge about the local vehicle density. VANET is used to identify congested roads and to offer alternative and less congested routes because VANETs enable all actors in traffic (e.g., vehicles, traffic lights or road-side units) to exchange information and to coordinate their behaviour. In addition to the risk of causing congestion on the alternative routes, other strategies become effective only after a traffic breakdown has already occurred.

In this paper, we present a VANET-based strategy to reduce traffic jams, which explicitly accounts for human reaction time and becomes effective at low penetration rates. Simulations not only use realistic radio propagation and mobility models but also empirical traffic data from a German Autobahn, which makes this paper stand out from all aforementioned studies.

A. Warning for Congestion –

The approach proposed to prevent congestion is based on communicating beacon messages. Beacon messages are periodically broadcast status messages which contain a vehicle's position, velocity, acceleration, a unique vehicle identifier, and a time stamp. In our approach, we suggested to add two additional variables: a position c, and a time stamp c, marking a "critical" road segment. In this context, a road segment is called critical when a breakdown is likely to occur. Usually a beacon's payload size is around less than 100 B, but, in order to incorporate expected future demands, e.g., security, the beacon size is fixed to 500 B to show that the approach works with those beacon sizes also.

A vehicle may calculate the average velocity \( v_a(t) \) of all transmitting vehicles ahead from the beacon it receives during an interval \([t, t+\Delta t]\). When the average velocity drops below a given threshold \( T_v \) for two successive intervals \((v_a(t-\Delta t) < T_v \text{ AND } v_a(t) < T_v)\), it marks the segment as critical by setting \( c_t \leftarrow t \) and \( c_s \leftarrow x(t)+m \), where \( x(t) \) denotes...
the vehicle’s current position at time \( t \) and \( m \) denotes an average communication range. All the vehicles which receive a notification about such a critical condition add this information to their beacons [see Fig. 1(a)].

Vehicles use this information to decide whether to change their driving behavior. For this decision, a vehicle has to judge the relevance of the information. Information about a critical road segment is considered as relevant if the vehicle is close to the said segment, if it is approaching it, and if the information is sufficiently up-to-date [see fig. 1(b)]. By introducing a Boolean variable \( b \), which indicates whether to change driving behavior, and temporal and spatial thresholds \( T_t \) and \( T_s \), respectively, the aforementioned conditions can be written as

\[
b \leftarrow \text{false} \quad \text{if } (t - c_t < T_t \text{ AND } 0 < c_s - x(t) < T_s)
\]

\[
b \leftarrow \text{true}
\]

which a traffic condition is classified as “critical” below the threshold \( T_v = 81 \text{ km/h} \). This value is \( 10.8 \text{ km/h} (=3 \text{ m/s}) \) below the maximum velocity of trucks in simulation and demonstrates that vehicle interactions and perturbations are strong enough to make even slow vehicles (i.e., trucks) slow down. Finally, we set \( \Delta t = 1 \text{ s} \) and \( m = 150 \text{ m} \). The variable \( m \) is an estimate for the distance to the critical road segment.

**B. Comfortable Driving Model**

The Comfortable driving model [7] contains a probabilistic component \( p \) that causes minor fluctuations in a vehicle’s velocity reflecting drivers’ incapability to maintain a constant velocity. The original CDM distinguishes three cases when determining \( p \) for a vehicle labeled \( n \) as follows:

- In the first case \( (p = p_b) \), the vehicle \( n \), following the preceding car \( n+1 \) with time headway \( t_h \), reacts to the predecessor’s activated brake light \( (l_{n+1} = \text{true}) \) if it is within an interaction horizon \( t_c(t_h < t_s) \).
  - This case was introduced to correctly mimic driver’s tendency to overreact in dense traffic. This phenomenon, sometimes called “over-deceleration effect”, results from a driver’s finite response time to the preceding car’s brake lights. If the time headway is too small (i.e., \( t_h < t_s \)) the following driver performs an unnecessarily strong braking to avoid collision.

- The second case \( (p = p_0) \), known as the slow-to-start rule, effects a reduced acceleration rate for vehicles starting from rest provided that there are no obstructions ahead \( (l_{n+1} = \text{false or } t_h \geq t_c) \).
Preventing Traffic Jams by Secure and Efficient Beaconing

- The last case models the random fluctuations observed even in free traffic flow. From these explanations, we can already conclude the relation \( p_d < p_0 < p_b \).

In the modified model, we suggested vehicles which set \( b \leftarrow \text{true} \), to keep a larger gap to the preceding vehicle. This increased gap is created simply by not accelerating. An additional gap whose length we denote by \( g_{ap} \), is considered as sufficiently large if it is larger than the distance travelled during the driver’s reaction time \( \tau_r \) of 1s (\( \tau_r=1s \)). It is intuitive that a larger gap decreases the probability for the occurrence of an “over-deceleration effect”.

We modified the calculation of the randomization parameter \( p \) by introducing a fourth parameter \( p_c \) (\( p_0 < p_c < p_b \)) to model the situation described earlier:

\[
p = \begin{cases} 
  p_b, & \text{if } l_{n+1} = \text{true} \land t_h < t_s \land gap_n \leq v_n \tau_r \\
  p_c, & \text{if } l_{n+1} = \text{true} \land t_h < t_s \land gap_n \geq v_n \tau_r \\
  p_0, & \text{if } v_n = 0 \land \neg (l_{n+1} = \text{true} \land t_h < t_s) \\
  p_d, & \text{otherwise.}
\end{cases}
\]

For the simulations, We adopted the values for \( p_b = 0.94 \), \( p_0 = 0.5 \) and \( p_d = 0.1 \) from [7] and set \( p_c = 0.8 \times p_b \).

C. Implementation Model–

In order to show the effectiveness of the proposed approach we took dynamic highway scenario. Vehicles move on a 12-km-long two-lane highway segment with an on-ramp and off-ramp. This segment corresponds to a section of the German Autobahn A044 between the cities of Unna and Werl. Fig. 2 shows the geometry of the considered highway section.

![Figure 2. Schematic of the highway segment used for simulations. The locations of loop detectors are labelled as D01, . . . , D10.](image)

To model open boundary conditions, including the inflow and outflow via the two ramps, we used the detector data of November 4, 2010, which show a spontaneous breakdown in morning peak-hour traffic (see Fig. 3). The time series of detector D06 as depicted in Fig. 3(a) is exemplary for all detectors upstream the on-ramp. The detectors in the simulation measure the velocity of passing vehicles and return the average value aggregated over 1-min intervals in analogy with the real detectors. Both time series show a breakdown in the detected velocities during the morning peak hour from approximately 07:15 am to 9:00 am. The real detectors distinguish two types of vehicles, namely cars and trucks, which explain the two curves in the given figures: The time series of cars is plotted with a solid black line, whereas the corresponding time series of trucks is plotted with a solid gray line. We used two different vehicle types in our implementations to reflect this fact. As all vehicles of one type share an identical set of parameters, the fluctuations in free traffic flow are less pronounced in the simulations (b) than in real traffic (a)(shown in figure).
Similarly, entering vehicles are communicating according to the given penetration rate. The on-ramp increases the probability for a breakdown as vehicles entering the system are likely to provoke perturbations that are the cause of breakdown. For simplicity, we used identical vehicle rates to model traffic flow on the opposite driving direction where they omitted the on-ramp and the off-ramp. Lane width is set to 3.75 m with additional 2.5 m between opposite driving directions. we used two distinct vehicle types, namely “cars” and “trucks,” having vehicle length as 7.5 m and 15.0 m and maximum velocity as 33.0 m/sec and 25.5 m/sec both respectively.

Every radio-equipped vehicle shares an identical set of physical parameters that are summarized in Table. As data rate, we chose the minimum of the mandatory rates 3, 6, and 12 Mbits/sec.

<table>
<thead>
<tr>
<th>TABLE 1</th>
<th>PROPERTIES OF RADIO DEVICES AND RADIO CHANNEL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PHY</strong></td>
<td></td>
</tr>
<tr>
<td>fading</td>
<td>Nakagami-m</td>
</tr>
<tr>
<td>interference</td>
<td>cumulative noise &amp; capture effect</td>
</tr>
<tr>
<td>transmission power</td>
<td>-17 dBm</td>
</tr>
<tr>
<td>reception threshold</td>
<td>-81 dBm</td>
</tr>
<tr>
<td>sensitivity threshold</td>
<td>-91 dBm</td>
</tr>
<tr>
<td>noise</td>
<td>-99 dBm</td>
</tr>
<tr>
<td>antenna gain</td>
<td>0 dBm</td>
</tr>
<tr>
<td>SINR</td>
<td>10</td>
</tr>
<tr>
<td>data rate</td>
<td>5 Mbits/sec</td>
</tr>
<tr>
<td><strong>MAC</strong></td>
<td></td>
</tr>
<tr>
<td>beacon size</td>
<td>500 B</td>
</tr>
<tr>
<td>beacon interval</td>
<td>250 ms</td>
</tr>
<tr>
<td>jitter</td>
<td>4%</td>
</tr>
</tbody>
</table>

For communication distances of 80 m and above, we set $m = 0.75$. For smaller distances, however, we set $m = 1.5$ as for short distances a clear line of sight is likely to exist. Status messages have a constant size of 500 B and are broadcast with a frequency of 4 Hz. Note that both message size and frequency fulfills the communication requirements for safety applications presented in [2].

III. SECURING BEACON COMMUNICATION

To secure beacons, they need to be signed and also carry a certificate to attest validity of network participants. To serve the purpose the vehicles need to be equipped with asymmetric cryptographic key pairs (VK,SK) and certificates (Cert) issued by a trusted certification authority (CA). Then all beacons get signed using the vehicle’s signature key.
SK. Receivers verify the signature using the verification key VK. Signature and certificate containing VK are attached to the beacon. The said mechanism brings two problems in the picture:

1. Incorporating signatures and certificates to the beacons introduces a significant protocol overhead. When we use a solution based on ECC, which incurs small overhead, even then certificate and signature need at least 150-160 bytes [3].
2. Signatures Creation and Verification causes notable computational overhead. Every sent beacon needs one signature generation and two verifications (certificate and signature).

Taking a max 200 neighbour vehicles and 10Hz as beaconing rate, a vehicle needs to generate 10 signatures and verify 4000 signatures per second, which is more than the capacity of normal vehicle on-board units. As cost constraints, on-board units need to be cheap, that is why this cannot be resolve only by using more powerful hardware. In order to reduce the significant communication and computational overhead created by this, we propose to skip signatures or certificates in certain situations.

A. Excluding Certificates and Certificate Verifications

Verification of validity of a certificate corresponds to one signature verification. If certificates (already verified) are stored locally, it will cost some more memory, but the subsequent beacons having the same certificate can be verified without cryptographic operation which reduces the computational costs of handling received packets almost by half.

Additionally, when certificates are stored locally, it gives the opportunity to remove the certificate in subsequent packets from the same node. In summary, one needs not to attach certificates to every packet without affecting security level if once the communication partners have exchanged their certificates.

Removing certificates from beacons may result in a situation that a node gets a packet from a neighbor without already receiving a certificate previously. In such case, that packet must be taken as invalid or signature verification will be delayed until the verification key VK is received. But because the certificate omission banks more than 100 bytes per packet, it is suggested to analyze strategies where certificates can be skipped.

The approach in which a certificate is contained by only every nth beacon packet reduces a constant amount of bandwidth utilization, but the current vehicle context is not considered here. Therefore, we suggested a neighbor-based scheme that based on topology changes explicitly. The strategy is to use the fact that every node can recognize its neighbors in wireless transmission range via beaconing. Therefore, a node itself can monitor neighborhood changes and take the decision whether it should attach a certificate or not. For all new neighbors a certificate is attached, otherwise not.

B. Eliminating Signatures

Eliminating the certificates and also the signatures reduces communication overhead and computation overhead for some beacons to almost zero, but this leads to possibility of forging and modification attacks on beacons. The strategy to omit signatures is backed by the fact that not every beacon will trigger safety related applications but can be used in less safety critical use-cases. So it might be acceptable to selectively activate signatures, e.g., following a periodic schedule or depending on the situation. Different strategies for omitting signatures include periodic signing, where only every nth beacon is signed. This provides somewhat a reliable pattern of movement for each vehicle, having some extra unreliable info of the path with some secure steps.

The amount of trustworthy information on the basis of which a vehicle can take potentially safety critical decisions decreases to the rate of signed beacons available. To address this problem in a better way, it is proposed to use signature omission based on situation. All beacons are initially unsigned in this approach. Insecure beacons can be used for signaling potentially dangerous situations, but only if the sender of the previously unsigned beacons changes to secured beacons as well, the situation is checked by the safety applications. An alternate method is to predict potential collisions on the basis of current movement vectors.

C. Excluding Signature Verification

If it is assumed that all beacons are having signatures, it needs computationally expensive cryptographic verification. Signature generation costs about one third than verification. In dense traffic, a vehicle will get far more packets than it gives away. So it has to perform much less signature generations than verifications. The point of signature verification
omission is that receiver has to decide, it will verify signature of which packet. This has the benefit that According to the current load, the receiver can control its computational load. It also raises the drawback that an intruder might insert spoofed packets with invalid signatures and hope that receivers might not check them.

In order to omit verification of signature, the question arises that how to select packets to be verified. Strategies at hand are context-adaptive verification, periodic verification, and situation-aware verification. Context-adaptive verification: vehicles may use linear predictions to extrapolate different factors like positions, speed, etc. in the near future for each neighbor vehicle beacons. If future beacons from particular neighbor are enough close to the predictions, the vehicle called “behaves as expected” and verifications of signature may be skipped. If prediction and actual values are quite different, the verification enforced. Signatures will always be verified for all new neighbors.

IV. INTEGRATING THE STRATEGIES

In the first section discussed, we proposed an approach to reduce traffic jam before it actually occurs using the communications provided by VANETs. Traffic breakdown information gets broadcasted via vehicle to vehicles which informs the drivers following about the perturbation occurred and suggest them to change their driving behavior accordingly in order to avoid the jam. Beacons are used to share the information regarding traffic and it is the basis of the whole approach so it has to be legitimate information. Therefore the information has to be secured. Commonly stated solution to such a problem is asymmetric key cryptography. But Creating and verifying signatures and Adding signatures and certificates to the beacons causes a notable protocol overhead and significant computational overhead. In order to reduce the communication and computational overhead created by this, the paper proposes to skip signatures or certificates in certain situations.

To assess the impact of vehicle communication on traffic flow, we analyzed travel times for the considered highway segment and the given boundary conditions. Travel time is probably the most intuitive quality measure. Fig. 4 shows the average travel times for different penetration rates of communicating vehicles. Results were averaged over at least five independent simulation runs per penetration rate. The average travel time drops from 518 s without vehicle-to-vehicle communication to 440 s when 40% of all vehicles is equipped with communication devices.

This corresponds to a travel time reduction of more than 15%. Error bars mark the positions of the 0.1 and 0.9 quartiles, respectively, which means 80% of all vehicles were able to cross the highway segment within the error-bar indicated interval. The lower boundary is mainly delimited by the minimal travel time following from vehicles’ maximum velocity. The upper boundary, on the other hand, reflects the traffic dynamics and the existence of breakdowns. Here, the benefits of vehicle-to-vehicle communication become more obvious; with one fourth of all vehicles being able to communicate, the 0.9 quartile drops for more than 35% from 819 to 527 s. In addition, the lower curve in Fig. 4 shows the standard deviation of the observed travel times. The standard deviation of travel times

Figure 4. Average travel times for different penetration rates: Error bars indicate the 0.1 and 0.9 quantiles
can be understood as a measure of travel time reliability and shows similar dependence on the penetration rate; with one in four vehicles being able to communicate, the standard deviation's value measures only 96 s, compared with more than 200 s when communication is turned off.

To determine the average increase of time delay in each scenario, we calculated an optimal travel time. To do so, we started a vehicle at each second of the simulated day on an empty road and recorded the corresponding travel time. Taking into account the share of trucks and trucks' increased travel time due to their reduced maximum velocity, one obtains an optimal average travel time of 425 s. The temporal traffic dynamics is shown in Fig. 5 (For better readability, the plot shows only data from vehicles of type car, and a moving average over ten subsequent data points is applied.)

The application of vehicle communication significantly reduces the duration and the severity of breakdown observed in the time from 6:30 am to 9:30 am. This result is confirmed by the analysis of the stationary detector data.

The variables $T_s$ and $T_t$ were introduced to define an area of relevance for traffic information. Only vehicles within this spatio-temporal area change their driving behaviour in response to received messages. To check the sensitivity of our results on the variables $T_s$ and $T_t$, we modified the original values of $T_s=3$ km and $T_t=30$ s and analysed travel times in the interval from 6 am to 9 am, where most fluctuations occur [see Fig. 3(a)]. As shown in figure 6, the qualitative behaviour of travel times is conserved when changing $T_s$ and $T_t$ for $\pm 1/3$ of the original value, serves as reference and is labelled “standard.”
To assess the success if some vehicles or drivers do not (or cannot) follow the recommended change of driving behavior, we repeated the simulations and made half of the communicating vehicles ignore any recommendation on the driving behavior. However, these vehicles did correctly broadcast messages, as described earlier. We compared the average travel times from these simulations to the previous simulation runs and found very good agreement between the values for a given penetration rate (e.g., 40%) and the results obtained for half the given penetration rate (e.g., 20%) when all communicating vehicles do follow the recommendation. Hence, the success of our strategy depends crucially on the drivers’ willingness (or capability) to follow the recommendation, whereas the benefit from better connectivity in the latter case was found to be negligible.

Whereas, certificate omission based on neighbor changes is implemented. Depending on traffic model (city or highway traffic), traffic density, and beacon intervals, the number of beacons with certificates is significantly reduced. With small beacon intervals, which are often recommended for faster reaction times of applications, more than 80% of certificates can be omitted, resulting in large bandwidth saving. At the same time, analysis of simulation results shows that the number of beacons that are not instantly verifiable due to unknown certificates is in the order of 1%.

IV. CONCLUSION

In the paper presented we employed vehicle-to-vehicle communication to ease congestion and maintain a smooth traffic flow. The proposed method, which is primarily based on periodic beacon messages and, uses only velocity and position to estimate traffic, does not need much of technical implementation.

Simulations are performed to evaluate the success of the proposed strategy by using bidirectionally coupled simulator. In contrast to other cases where in case of a jam the traffic is diverted to an alternate route, our approach becomes effective before a jam occurs. Comparison of Fig. 3(b) and 7 depicts the success of the approach. The original traffic breakdown [see Fig. 3(b)] can be no longer observed (see Fig. 7).

For the securing beacons issue also our results are quite inspiring and indicate that the fraction of security that is lost by their suggested schemes is much smaller than the performance and bandwidth benefits. The profits in resources can be used to increase rate of beaconing and build much cheaper on-board units, which will increase reliability of safety applications and the rate of deployment of Safety systems while still presents systems that are quite hard to attack.

REFERENCE