Trustworthy Broadcasting in IEEE 802.11p/WAVE Vehicular Networks: Delay Analysis
Alexey Vinel, Claudia Campolo, Jonathan Petit, and Yevgeni Koucheryavy

Abstract—Safety and non-safety applications envisioned for Vehicular Ad hoc NETworks (VANETs) heavily rely on broadcasting for the exchange of data and status messages. New threats to road safety and efficiency raise if security requirements for broadcasting are not properly met. The decision whether or not a driver can trust information about a reported hazard should take into account the tradeoff between the decision delay, false warning probability and likelihood of missing the hazard. Although broadcasting in VANETs has been analytically studied at least for the simplified assumptions, related works do not jointly consider the reliability of the medium access control (MAC) protocol and the trust issues.

In this letter, a new analytical model is designed for evaluating the latency required to guarantee trustworthiness in VANETs. This model explicitly accounts the operation of 802.11p/WAVE MAC protocol and computes mean decision delay as a function of number of vehicles, ratio of intruders as well as contention window sizes.

Index Terms—WAVE, broadcast, trust, intruders, analytical model.

I. INTRODUCTION

THE IEEE 802.11p/WAVE (Wireless Access in Vehicular Environments) standard has recently issued a set of physical (PHY) and medium access control (MAC) layer specifications to enable communications in Vehicular Ad hoc Networks (VANETs) [1]. In WAVE, vehicles use a multi-channel concept for the delivery of safety-related and information applications. Each vehicle periodically switch on a common control channel (CCH) to monitor control and warning messages, and tune onto one of available service channels (SCHs) to exchange non-safety-related data. According to WAVE coordination scheme [2], the channel time is divided into synchronization intervals with a fixed length of 100 ms, consisting of 50 ms-alternating CCH and SCH intervals. At the beginning of each interval, a 4 ms-long guard time is set to account for radio switching delay.

During the CCH interval vehicles broadcast WAVE Short Messages (WSMs) in response to certain traffic events, emergency messages, and to periodically update their kinematics information, beacons.

Since drivers of vehicles in a VANET are expected to (re)act on messages received from other road users, it is clearly necessary for these messages to be transmitted in a secure fashion. Unfortunately, conventional security mechanisms (like public key infrastructure – PKI) do not avoid authenticated users to jeopardize the VANET, e.g., by injecting false warnings with the purpose of causing accidents or manipulating traffic flow information to get faster to their destination [3]. To provide trust and avoid such attacks, a solution is to evaluate the plausibility of information received by a consensus mechanism. Thus, to avoid reaction to false information, a vehicle needs to wait for receiving a given number (let us say $X$) of WSMs from its neighbors advertising the same information before warning the driver. Recent studies have analyzed the problem of trust provisioning in VANET, e.g. [4], [5], but without considering the impact of the MAC layer on the security.

Figure 1 shows four vehicles that send WSMs on the CCH. In the first attempt, vehicles 1 and 2 succeed while vehicles 3 and 4 experience a collision. In the next CCH interval, the four vehicles send successfully a new WSM. So, if a vehicle has to wait for four messages before notifying the driver ($X = 4$), then its decision is delayed by one synchronization interval. The above example shows that the unreliability of unacknowledged broadcast packets and the MAC layer contention could affect the decision delay and hence the safety-related application performance.

In this letter we propose an analytical model to define the average delay before reaching a consensus. To our knowledge, this work is the first to study the impact of the channel contention on the trust mechanism. The decision method follows the reliable majority wins approach proposed in [4], according to which information about the hazard is considered to be trustworthy if it is received from the half of the nodes able to detect it. Such a decision algorithm can work under the very common assumption that most vehicles are honest. For such a case majority wins strategy provides zero false warning and missing the hazard probabilities, but the average decision delay is the maximal among decision-making strategies which are based on a fewer number of received messages.

II. SYSTEM MODEL

The reference scenario for our study is depicted in Fig.2. There are $N$ vehicles located in a close proximity to each
other, which are capable to detect road events (e.g., congestion, accident, dangerous road conditions, etc., block A in Fig. 2) autonomously via on-board cameras and sensors. We refer to the area occupied by these vehicles as detection area. The detection process is assumed to be absolutely trustworthy. We assume that \( N_0 \) \((N_0 < N/2)\) out of \( N \) vehicles in detection area are intruders, others are legitimate nodes. Legitimate nodes always broadcast WSMs conveying the same true information about the detected event, while intruders always broadcast the same fake information (cooperation between the intruders is assumed). There are other \( N^* \) vehicles next to the detection area, forming the decision area, which make a decision about the realism of the hazard based on the received broadcasts.

Our goal is to derive the mean decision delay \( \bar{D} \) of the majority wins decision scheme - namely \( X = \lfloor N/2 \rfloor \) messages from different vehicles have to be received to inform the driver about the hazard. Note that this scheme (and the corresponding decision delay) depends on the ratio of intruders \( N_0/N \).

One-hop broadcast communication via IEEE 802.11p/WAVE from the detection area to the decision area is studied. Based on 802.11p MAC specifications, a vehicular node is allowed to transmit only if it detects the channel idle for a time duration equal to Arbitrary Inter Frame Space (AIFS) seconds. Otherwise, the node waits for the channel to become free and then, it randomly selects a backoff value taken from a given range of integer numbers, called Contention Window (W). This random value is used to set a backoff counter that is decremented at the end of each idle slot. As soon as the counter is decreased to zero, the node is allowed to access the channel.

In agreement with the WAVE documents [2], the application layer is assumed to be aware of channel switching; this implies that packets are sent to the MAC layer only during the CCH interval; specifically, each of \( N \) vehicular nodes has a WSM packet ready to be transmitted at the beginning of every CCH interval after a random backoff. Lifetime of considered WSMs is assumed to be bounded to one CCH interval; after this period non-transmitted frames are dropped. As a consequence, the MAC-layer buffer of a vehicular node keeps only one frame for CCH interval at a time.

The following simplifying assumptions hold in this letter (analogously to [6]): (1) the radio channel is ideal, so bit errors are not considered; (2) both groups of \( N \) and \( N^* \) vehicles are within reciprocal communication range of each other (no hidden terminals); (3) the carrier sense range coincides with the communication range; (4) the one-hop neighborhood of a node does not significantly change due to node mobility in the short time frame under analysis. In addition, it is supposed that no packets are lost due to expiration of the CCH interval, what happens in most of typical working conditions of 802.11p/WAVE (see Table II [6] for the corresponding parameters of \( W \) and \( N \)).

Then, the following approach is applicable for the computation of the distribution of the number of successfully transmitted packets during a CCH interval \( Q_i(x) \) \((0 \leq x \leq N)\).

Denote by \( B(r, k, w) \) the total number of ways to put \( k \) balls into \( w \) boxes under the condition, that exactly \( r \) boxes contain one ball. This function is computed recursively using the following rule [7]:

\[
B(0, 0, w) = 1, B(0, k, 0) = 0,
B(0, k, w) = w^k - \sum_{i=1}^{\min(k, w)} B(i, k, w), k > 0,
B(r, k, w) = \binom{k}{r} w^r B(0, k-r, w-r), 0 < r \leq \min(k, w).
\]

Therefore, \( Q_1(x) = B(x, N, W)/W^N \).

The distribution of the number of successfully transmitted legitimate packets in CCH given that \( x \) packets totally are successfully transmitted in CCH is \( Q_2(y|x) \), \( 0 \leq y \leq x \):

\[
Q_2(y|x) = \frac{\binom{N-N_0}{y} \cdot \binom{N_0}{x-y}}{\binom{N}{x}} Q_1(x).
\]

Then the distribution of the number of successfully transmitted legitimate packets in CCH is:

\[
Q(y) = \sum_{x=0}^{N} Q_2(y|x).
\]

Let \( R(i, j, x) \) be the probability that \( i \) new legitimate nodes successfully transmit in CCH under the condition that totally \( x \) nodes (both legitimate and intruders) successfully transmit in CCH interval and \( j \) different legitimate nodes have already successfully transmitted in previous intervals:

\[
R(i, j, x) = \frac{x \cdot \binom{N-N_0-x}{j} \cdot \binom{N_0-x}{j-i}}{\binom{N-N_0}{j}}.
\]

The denominator corresponds to the number of ways to allocate randomly previously transmitted nodes (out of \( N-N_0 \) legitimate nodes). The numerator corresponds to the product: the number of ways to allocate previously transmitted \( x-i \) nodes out of \( x \) successfully transmitted in the current CCH and the number of ways to allocate the rest \( j-(x-i) \) nodes out of \( N-N_0-x \), which are not transmitting in the current CCH interval. If \( x-i > j \) or \( x < i \) then \( R(i, j, x) = 0 \).
Fig. 3. Mean decision delay $\overline{D}$ for a small $W$ and $N$.

Denote $D[i]$ the mean transmission delay (measured in the number of synchronization intervals) of $\lceil N/2 \rceil$ successfully transmitted messages from different legitimate nodes given that $i$ messages from different legitimate nodes have been already successfully transmitted in previous intervals:

$$D[j] = 1 + \sum_{y=0}^{N} Q(y) \sum_{i=0}^{\lceil N/2 \rceil-j} R(i, j, y)D[j+i] \Leftrightarrow$$

$$\Leftrightarrow D[j] = \frac{1 + \sum_{y=0}^{N} Q(y) \sum_{i=0}^{\lceil N/2 \rceil-j} R(i, j, y)D[j+i]}{1 - \sum_{y=0}^{N} Q(y)R(0, j, y)}$$

Stop condition of this recursion is $D[j \geq \lceil N/2 \rceil] = 0$ and the mean decision delay, computed in terms of number of synchronization intervals, is $\overline{D} = D[0]$.

III. MODEL VALIDATION AND NUMERICAL RESULTS

To validate the model, an event-driven custom simulation program has been developed in Matlab, that closely follows the 802.11p/WAVE protocol specifications and the model assumptions. Results are shown for a set of parameter values that we consider as the most meaningful for analysis:

- $\overline{D}$ is the mean decision delay, computed in terms of number of synchronization intervals, is $\overline{D} = D[0]$.

The lowest 802.11p data rate–3 Mbps–is chosen to privilege robustness and reliability (very critical for unacknowledged broadcasting); 300-bytes long packets to account for additional security overhead [5], and a contention window size in the range (4–128). Other system parameters are set as in [6].

Results in Fig. 3 and Fig. 4 plot the mean decision delay $\overline{D}$ (measured in the number of CCH intervals) by assuming the worst case scenario, namely, for the case when a fixed number of intruders $N_0$ equal to $N - \lceil N/2 \rceil$ is considered. We vary the number of vehicles in the detection area $N$ as well as $W$ size in the typical settings for 802.11p. From Fig. 3 it can be observed that the analytical results (lines) closely match simulation results (symbols), witnessing that the proposed approach precisely models the underlying multidimensional stochastic process. We have also validated our analytical model for different percentage of intruders $N_0/N$ and the modeled scenarios always matched with simulations. Figures 3 and 4 show the impact of $W$ and $N$ on the decision delay. As expected higher values of decision delay are experienced for low values of $W$ (and high values of $N$), because of the increasing number of collisions among nodes attempting to seize the channel at the beginning of the CCH interval.

If we consider typical VANET with one-hop communication range equal to 300 meters and safety distance of 100 meters for the speed of 120 km/h, we get that the mean decision delay should not exceed 6 seconds (60 CCH). Therefore, in the framework of the proposed model, majority wins looks to be a reasonable strategy for the small or medium number of vehicles in the detection area as well as for the large value of $W$. Otherwise, more sophisticated decision strategies should be used, which is the subject of our current research.

ACKNOWLEDGEMENTS

The authors thank the anonymous reviewers for their valuable constructive feedback.

This work has been done in the framework of COST IC0906 WiNeMO “Wireless Networking for Moving Objects (2010–2014)” project.

REFERENCES