Abstract—A method for real-time detection of Denial-of-Service (DoS) attacks in IEEE 802.11p vehicular ad-hoc networks (VANETs) is proposed. The study is focused on the ”jamming” of periodic position messages (beacons) exchanged by vehicles in a platoon. Probabilities of attack detection and false alarm are estimated for two different attacker models.

Index Terms—IEEE 802.11p, VANET, DoS attack, jamming, platooning.

I. INTRODUCTION

IEEE 802.11p is an international standard for short-range inter-vehicle communication in the 5.9 GHz frequency band. Vehicular ad-hoc networks (VANETs) comprised of the IEEE 802.11p-enabled vehicles aim at increasing road safety, efficiency and driving comfort and are currently a subject of an intensive research [3]. Platooning is an example of such an application based on vehicle-to-vehicle communication.

In a platoon the leading vehicle (normally a truck) is driven by the human, while the following vehicles either automatically maintain the velocity of the leading one, but their direction is still controlled by the driver (e.g. Connect & Drive project [4] and Grand Cooperative Driving Challenge – GCDC [5]), or follow the leading one in a fully automatic manner (e.g. Safe Road Trains for the Environment project – SARTRE [6]).

Since the IEEE 802.11p medium access control (MAC) protocol specifies random access, during its normal operation the beacons can be lost either due to the wireless channel impairments or due to collisions (i.e. overlapping transmissions of beacons from several vehicles). The probability of collisions can be reduced by the proper choice of the MAC protocol parameters [10]. However, the beacons can also be intentionally corrupted by the malicious node in case of a jamming Denial of Service (DoS) attack [11], [12]. In the latter case the safety of the platoon can be jeopardized especially seriously since the vehicles will not be able to update the information about each other within the delay requirements imposed by the automotive control systems. Therefore, the real-time detection of jammers in IEEE 802.11p VANETs is an important practical problem, which motivates our study.

Real-time detection of DoS attacks in IEEE 802.11 networks have been studied in [13], where the proposed detector observes the events happening in the wireless channel and probabilistically computes how ”explainable” occurring of each particular collision is. The method in [13] targets the basic mode of IEEE 802.11 with an arbitrary unicast traffic, which is retransmitted according to the binary exponential backoff algorithm. The method to detect the jammers in VANETs with unicast traffic, which is based on linear regression, is proposed in [14]. However, very limited performance evaluation results are reported in [14], e.g. no results on the detection time are given.

In comparison to the above studies, we consider the beacons, which are transmitted regularly in IEEE 802.11p broadcast mode without retransmissions, making it possible to propose an alternative jamming detector. To the best of our knowledge no literature has considered the problem of jamming DoS attacks detection in VANET platoons so far.

The cooperation between the vehicles in the platoon is achieved by the frequent exchange of periodic broadcast messages carrying information on vehicle position and velocity, which we refer to as beacons, in the dedicated channel [9].

The cooperation between the vehicles in the platoon is achieved by the frequent exchange of periodic broadcast messages carrying information on vehicle position and velocity, which we refer to as beacons, in the dedicated channel [9].
The following assumptions on the system operation are adopted in our study:

1) The platoon is comprised of $N$ vehicles, which are all in each others communication range. We assume a practically feasible case with the following reference values of the parameters: IEEE 802.11p communication range – 400-500 meters, inter-vehicle distances in the platoon – 5 meters, truck length – 15 meters, this assumption holds for platoons with $N \leq 25$. The current value of $N$ is known to the vehicles since joining and leaving of the platoon involves some negotiation protocol [6].

2) The time between the generation of two subsequent beacons, which is chosen by a vehicle, is fixed and denoted as $T$ and referred to as beaconing period. According to [7] the possible range for $T$ is 0.1–1 second and varies accordingly to the current rapidity of its kinematic information change. Therefore, the assumption roughly holds for the platoon keeping constant velocity on a highway.

3) Each generated beacon is broadcasted into the channel according to the IEEE 802.11p MAC rules. The random backoff counter value is chosen uniformly from the interval $[0, W - 1]$, where $W$ is the minimal Contention Window (CW). The counter is decremented by one after each slot of length $\sigma$ when no activity is sensed in the channel. In case transmission is detected, the vehicle has to ensure that the channel becomes idle for the Arbitrary InterFrame Space (AIFS) before further decreasing the backoff counter. The transmission is performed, when the counter turns to zero. The beacons are neither acknowledged by the recipients nor retransmitted. The beacon transmission time is $\tau = T_h + L/R$, where $T_h$ is the header transmission time, $L$ is the beacon payload size and $R$ is the channel rate.

4) The communication channel is assumed to be error-prone with independent losses of beacons and fixed packet error rate ($PER$). As it follows from the practical measurements reported in [17], when the platoon length does not exceed 400 meters, $PER$ is lower than 1%, given the line-of-sight condition between the antennas of vehicles holds (this can be achieved by placing them, e.g. at the outdoor rear-view mirrors). Apart from the noise, collisions with beacons from any of the $N - 1$ remaining vehicles are also possible.

Two attacker models are assumed [13]:

- "Random jamming". Each packet transmitted in the channel is corrupted independently with probability $p$.
- "ON-OFF jamming". In the OFF state no packets are jammed, while in the ON state $K$ subsequent beacons are destroyed with probability one. Then the attacker switches to the OFF state. The OFF–ON transitions occur at the moments of beacon transmission start with probability $p$.

III. SIMPLE JAMMING DETECTION METHOD

A. Preliminaries

Let us assume that there is a node (detector), which continuously listens to the channel, where the exchange of beacons between the vehicles in the platoon occurs. Practically the detector can be envisioned as a sniffer mounted on the leading vehicle.

The operation of the proposed jamming detector comprises two phases: installation phase and normal operation.

B. Installation phase

The objective of the installation phase is to divide all the vehicles in the platoon into groups in a way that the beacons from different groups never collide with each other. For this reason the detector tries to obtain some estimates for the beacons generation moments of all the vehicles in the platoon. The actual transmissions may occur at a later moments due to the random backoff delays.

The detector listens to the channel until it has received the sequence of $N + 1$ successfully transmitted beacons in a row. The sequence of time intervals between these transmissions is denoted as $(t_1, t_2, \ldots, t_N)$, where $t_i$ is the duration between the end of transmission of the $i$-th beacon and start of the transmission of the $(i + 1)$-th one, see Fig. 2.
Proposition 1. Beacons from nodes $i$ and $i+1$ never collide if both the following conditions hold:

$$\tau + \text{AIFS} > (W - 1)\sigma,$$  \hspace{1cm} (1)

$$t_i > \text{AIFS} + (W - 1)\sigma.$$  \hspace{1cm} (2)

Proof: Let $x$ be the moment of time when the transmission of node $i$ has finished. From (1) it follows that independently of its backoff counter choice, node $i$ could not start its transmission later than $x + \text{AIFS}$. Analogously from (2) it follows that node $i+1$ could not start its transmission earlier than $x + \text{AIFS}$. \hspace{1cm} \blacksquare

In the following we assume that system parameters are chosen in a way that (1) is satisfied (see Section IV) and we adopt the notation $S = \text{AIFS} + (W - 1)\sigma$.

Proposition 2. Let $t_m = \max_{1 \leq i \leq N} t_i$, then nodes $m$ and $m+1$ never collide if $\frac{T}{N} > \tau + S$.

Proof: The minimal possible value of $t_m$ is achieved when the transmissions of all the $N$ vehicles are uniformly spread in time within the beaconing period $T$, i.e. the difference between their transmission times is $T/N$. Taking this into account, it is easy to see that inequality (2) for $t_m$ holds. \hspace{1cm} \blacksquare

Applying Proposition 2 the detector operation is divided into independent detection periods of duration $T$. We define that the first detection period begins $\sigma(W - 1)$ prior to the transmission start of the $m$-th beacon, see Fig. 3.

Let $\bar{t} = (t_{m+1}, t_{m+2}, \ldots, t_N, t_1, t_2, \ldots, t_m)$. For easiness of notation let us renumber the components of this vector as $\bar{t} = (t_1^*, t_2^*, \ldots, t_N^*)$, where $t_j^*$ is the duration between the end of transmission of the $j$-th beacon and start of the transmission of the $(j+1)$-th one.

Applying Proposition 1 it is possible to divide all the vehicles into groups in a way that beacons from different groups never collide. For this reason vector $\bar{t}$ should be analyzed:

- If for some vehicle $j$: $t_{j-1}^* > S$ and $t_j^* > S$, then the beacon of this vehicle never collide with other beacons.
- Analogously if there is a group of $K > 1$ vehicles $j_1, j_2, \ldots, j_K$ such as $t_k^* \leq S$ holds for for all $k : 1 \leq k \leq (K-1)$, but $t_{K-1}^* > S$ and $t_K^* > S$, then the beacons of these $K$ vehicles can collide with each other, but not with the ones of the other $N-K$ vehicles.

Therefore, the outcome of the installation phase is the sets $\Omega_t$ of vehicle identifiers such as beacons from different sets never collide with each other, which is obtained by analyzing the transmission in the first detection period. By the end of the first detection period the detector switches to normal operation.

C. Normal operation of the detector

Normal operation is organized in detection periods of length $T$. The detector listens to the channel and records the identifiers of the vehicles for which beacons have been successfully received. The decision is made by the end of each detection period as follows:

- "Alarm": if there is at least one group among $\Omega_t$, where exactly one beacon has not been received.
- "No alarm": otherwise.

The underlying idea of such an approach is simple: in case of a beacon loss there should exist at least two nodes involved in the collision within the same group.

IV. PERFORMANCE EVALUATION

A. Preliminaries

We study an IEEE 802.11p system with $N=25$ vehicles and $T=0.1$ s with the following parameter values (see [2], best effort MAC access category): $\text{AIFS} = 110$ $\mu$s, $W=16$, $L=400$ bytes, $R=3$ Mbit/s, $\sigma=13$ $\mu$s, $T_h=52$ $\mu$s.

It is easy to check that for the above parameters, the condition (1) holds. Simulations demonstrate that the installation phase time, i.e. the time from the moment when the detector is turned on until the end of the first detection period, does not exceed 150 ms for the error-free channel and 200 ms for $PER = 0.01$, see Fig. 4.

![Fig. 4. Cumulative distribution function (CDF) of installation phase time](image)

Under the given set of assumptions and based on the rules of detector operation, the probability of false alarm, i.e. the probability that the alarm is triggered although no beacons have been jammed in the detection period, is zero for error-free channel and does not exceed 2% for $PER = 0.01$ (0.1 $\leq p \leq 0.5$).

In the following subsections we study the probability of attack detection $P_{\text{detection}}$, i.e. the probability that the alarm is triggered, given that at least one successfully transmitted beacon is jammed in the detection period.

B. Random jamming case

For the random jamming case, the relation between the probability of attack detection and the jamming probability is depicted in Fig. 5. We average the detection probability for different initial mutual offsets of beacon generation moments. For any $p$ value the averaged $P_{\text{detection}}$ exceeds 0.996 for error-free case and 0.993 for $PER = 0.01$. Taking into account that one detection period is $T = 0.1$ s, in most cases the attack is detected with probability close to one within a few hundred milliseconds.

The minimal value of $P_{\text{detection}}$ is observed when two beacons in average are jammed during the detection period, i.e. when $pN \approx 2$, since the probability that these two beacons belong to the same group and, therefore, the attack is not detected, is high.

The operation of the system for the error-free case can be analytically modeled using the following approximate approach.

...
Let us assume that the detection period is divided into $M$ slots, such that $M = \frac{T}{\tau + \text{ATFS} + W \sigma}$. If $i$ vehicles choose the same slot for the transmission (each with probability $1/M$), then they form one group. Due to time diversity provided by the backoff mechanism, transmissions of the group take $i$ slots.

For such a model, the probability that a particular group of $i$ beacons is formed ($2 \leq i \leq N$), can be computed recursively as:

$$P_i = \left(\frac{N - (i - 2)}{2}\right) \frac{1}{M} P_{i-1} \left(1 - \frac{1}{M} P_{i-1}\right)^{N-i}, \quad (3)$$

where $P_1 = 1/M$.

Assuming for simplification that there are no collisions in the detection period and, therefore, potentially any beacon can be jammed, we calculate the probability that at least 2 beacons (out of the group with $n$) are corrupted by the jammer as:

$$Q(n, p) = \sum_{j=2}^{n} \binom{n}{j} p^j (1 - p)^{N-j}. \quad (4)$$

Finally, taking into account the detector operation rules, which cannot detect the cases when more than one beacon is jammed in a group, we obtain:

$$P_{\text{detection}} \approx 1 - \sum_{n=2}^{N} P_n Q(n, p). \quad (5)$$

Fig. 5. Attack detection probability for random jamming

C. ON-OFF jamming case

For the ON-OFF jamming case ($K = 2$), the relation between the probability of attack detection and the jamming probability is depicted in Fig. 6.

In contrary to the random jamming, $P_{\text{detection}}$ in this case is an increasing function of the jamming probability. Small $p$ values correspond to the case when exactly two subsequent (and therefore highly probable – belonging to one group), beacons are jammed, which is not detected. With the increase of $p$, more pairs of beacons are likely to be jammed, i.e. it is more probable, that a group of exactly one beacon is involved and, consequently, the attack is detected. Further increase of the $K$ value also increases $P_{\text{detection}}$.

V. CONCLUSION AND FUTURE WORK

We have proposed a simple algorithm for real-time detection of jamming attacks against beaconing in 802.11p vehicular networks. For the reference platooning scenario under the simplified assumptions our algorithm provides in average the probability of detection not lower than 0.9 and no false alarm for any jamming probability.

Our ongoing work is focused on relaxing the assumptions of the presented model (especially about the fixed beaconing period) and correspondingly enhancing the detector for realistic scenarios.

REFERENCES


