Real-Time Jamming DoS Detection in Safety-Critical V2V C-ITS Using Data Mining

Nikita Lyamin, Denis Kleyko, Quentin Delooz, and Alexey Vinel

***Abstract*— A data-mining-based method for real-time detection of radio jamming denial-of-service attacks in the IEEE 802.11p vehicle-to-vehicle (V2V) communications is proposed. The method aims at understanding the reasons for losses of periodic cooperative awareness messages (CAMs) exchanged by vehicles in a platoon. Detection relies on a knowledge of the IEEE 802.11p protocol rules as well as on the historical observation of events in the V2V channel. In comparison with the state-of-the-art method, the proposed method allows operating under the realistic assumption of random jitter accompanying every CAM transmission. The method is evaluated for two jamming models: random and ON–OFF.**

***Index Terms*— C-ITS, VANET, jamming, denial-of-service attack, security, platooning, data mining.**

I. Introduction

COOPERATIVE ITS (C-ITS) is a promising extension of Intelligent Transport Systems (ITS) when together with recent electronic advancements, the connectivity between road users is introduced. Overall, C-ITS aims at improving road safety and vehicle fleet management, decreasing congestion, and reducing energy use. Vehicle-to-Vehicle (V2V) communications in Vehicular Ad-hoc Networks (VANETs) are expected to be a major enabler of such a connectivity in C-ITS [1].

Different novel C-ITS applications can be enabled by V2V communications [2]. Our focus is on *platooning*, where a caravan of vehicles automatically follows a human-driven leading one, which is one of the applications that is assumed to be an early adopter of VANETs [3].

The automatic control of a platoon relies, particularly, on the information in cooperative awareness messages (CAMs) transmitted on a dedicated DSRC/ITS-G5 wireless communication channel via the IEEE 802.11p protocol. Therefore, platooning is a C-ITS application where unreliability of V2V communications could seriously deteriorate the system-level performance and even cause a critical impact on road safety.

Packet losses in VANETs may be caused not only by legitimate IEEE 802.11p CSMA/CA collisions or ITS-G5/DSRC channel impairments, but also by malicious interference originating from a radio transmitter located in the vicinity of communicating vehicles.

Manuscript received November 28, 2018; revised January 17, 2019; accepted January 17, 2019. Date of publication January 24, 2019; date of current version March 8, 2019. The research leading to the results reported in this work has received funding from the Knowledge Foundation and from the ELLIIT Strategic Research Network. This support is gratefully acknowledged. The associate editor coordinating the review of this paper and approving it for publication was M. Khabbaz. *(Corresponding author: Alexey Vinel.)*

N. Lyamin and A. Vinel are with the School of Information Technology, Halmstad University, 30118 Halmstad, Sweden (e-mail: alexey.vinel@hh.se).

D. Kleyko is with the Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology, 97187 Lulea, Sweden.

Q. Delooz is with the Center of Automotive Research on Integrated Safety Systems and Measurement Area, Technische Hochschule Ingolstadt, 85049 Ingolstadt, Germany, and also with the School of Information Technology, Halmstad University, 30118 Halmstad, Sweden.

Digital Object Identifier 10.1109/LCOMM.2019.2894767

Experiments in [4] demonstrated that Denial-of-Service (DoS) attacks via jamming of CAMs are easy to implement and may have an adverse effect on platooning performance. Specifically, a jammer with the reaction time in the order of tens microseconds can be created with an open access wireless research platform. Such a reactive jammer can substantially increase the packet loss ratio at V2V links of platooning vehicles up to the level of a complete blackout.

The simulation study in [5] demonstrated that the platoon system is highly sensitive to jamming attacks and its performance can be compromised by a reactive jammer. In particular, it was shown that the presence of a reactive jammer may lead to string instability phenomena. Patounas *et al.* [6] performed a simulation experiment to test the effectiveness of radio jamming countermeasures, i.e. beamforming. The results demonstrated that in a static configuration of nodes like platooning, beamforming may reduce the harmful influence of radio jamming on platooning performance. However, no jamming detection technique was proposed in the study to identify the presence of a jammer and the power of the jammer was limited. This makes the effectiveness of beamforming questionable under a stronger jamming signal.

Thus, a need exists for reliable methods to detect radio jamming DoS intrusion into platooning C-ITS. Moreover, considering that platooning vehicles are moving with only an inter-vehicle gap of a few meters, the jamming DoS detection methods should be able to detect an attack in *real-time* within a fraction of second.

This letter enhances the model-based detector presented in [7] by relaxing one of its key assumptions. Namely, [7] assumes a fixed CAM generation period and is not designed to operate under the random deviations inherent in practical DSRC/ITS-G5 implementations [3].

The letter is organized as follows. Section II describes the scenario of interest and the assumptions adopted. The proposed detector is presented in Section III. Performance of detectors is evaluated in Section IV. Section V concludes the letter.

II. Scenario & System Model

A. Reference Scenario

We consider the following reference jamming DoS attack scenario: the platoon moves along a highway while the malicious vehicle, that implements jamming DoS attacks, drives in the proximity, for instance, on a neighboring lane (See Figure 1).

B. Assumptions

We assume a platoon of N vehicles. Following the assumptions in [3] and [7], we consider that all vehicles in the platoon are within each other's communication range.

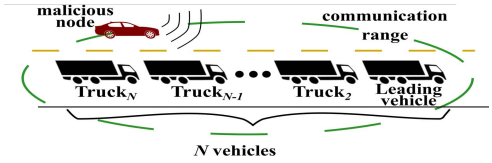


Fig. 1. Reference scenario.

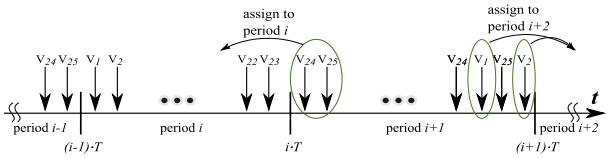


Fig. 2. Detection sets.

To enable functioning of the platooning automatic control system, we assume each vehicle is generating and transmitting CAM messages. This process involves the following steps:

- EN 302 637-2 CAM [8] is generated. Each vehicle generates f messages per second (with a corresponding generation period $T = \frac{1}{f}$).
- CAM experiences a random transmission *jitter* with distribution $\sim U[0, \delta]$ ms before the packet is placed in the Medium Access Control (MAC) queue for the actual transmission. In our previous work [7] no jitter was assumed. Although, in theory this assumption of a perfect CAM periodicity pattern makes sense, there are sources of jitter in real systems.
- CAM packet is transmitted on a *dedicated* ITS-G5 channel in accordance with the IEEE 802.11p MAC which introduces further CSMA/CA backoff delays.
- The communication channel is assumed to be error-prone with independent CAM losses and fixed packet error rate (PER).

Following [7], we focus on the two following jamming models:

- *"Random jamming"*. Each transmitted CAM is jammed randomly and independently with probability p.
- *"ON-OFF jamming"*. In the OFF state no packets are jammed, while in the ON state K subsequent CAMs are destroyed. Then the attacker switches to the OFF state. The OFFON transitions occur at the moments CAMs transmission start with probability p_0. We set $p_0 = p/K$ to have the same expected number of jammed CAMs in both random and ON-OFF attack scenarios.

To enable functioning of the jamming DoS detector, we assume the leading vehicle in the platoon is equipped with ITS-G5 communication device and able to *sniff* the communication exchange between platoon members and implement the detection algorithm. Also, we consider that the platoon leader is continuously aware of the current platoon configuration (number of vehicles N, adopted CAM generation period T) [3].

The detectors were evaluated using platoon communication exchange traces. The traces were obtained via the simulations of the system described above. Table I presents the parameters of simulations. Training sequences were not exposed to jamming.

TABLE I

SUMMARY OF DATA PARAMETERS (UNLESS STATED OTHERWISE)

Parameter	Values	Parameter	Values
Trace duration	150 s	CAM frequency	$f = 30$ Hz
Training sequence	first 75%	ON-OFF jamming par.	$K = 2$
Testing sequence	last 25%	Jitter par.	$\delta = 10$ ms
Detection period	$T = \frac{1}{f}$ ms	Detection delay	$1.5T$ ms
Error rate, PER	0.1	# of traces per setup	10

III. DETECTION METHODS

A. Model-Based Detector

The operation of the model-based detector [7] is divided into training and detection phases.[1] During the training phase the method collects statistics of $N+1$ subsequent successfully received CAM transmissions. After this, the detector classifies them into *groups* following the rule: only CAM messages that could potentially collide from a CSMA/CA standpoint are placed into the same group. A detection mode operates on the independent *detection periods* (the duration of which is fixed and is equals to CAM generation period T). During the detection phase the alarm is raised when there is a group formed in the training phase where exactly one CAM is not received.[2] For brevity, we omit the technical details of the model-based detector operation. These can be found in [7].

B. Hybrid Detector

In terms of data mining, the jamming DoS scenario in this letter can be treated as a problem of *anomaly detection in a discrete sequence* [9].

There are two types of event in the considered system: Natural collisions (legitimate CSMA/CA collisions) and anomalous collisions (jammed CAMs). The proposed method is hybrid in nature. Following a data mining approach, it uses historical data of platoon communications. Additionally, *a priori* knowledge about a platoon is employed in the method.

The detector monitors the transmissions of CAMs from different vehicles as well as the collisions. An outline of the jamming detector is presented in the form of a flowchart in Fig. 4.

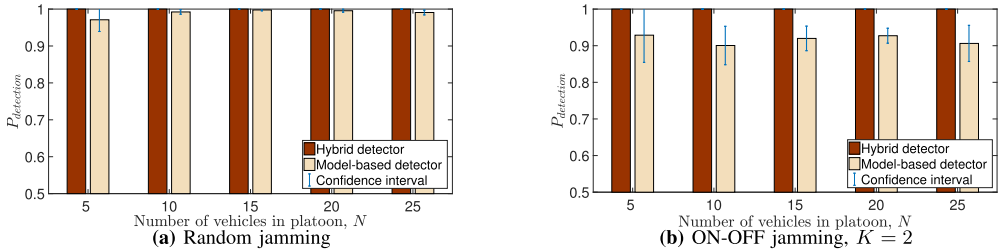
1) Training Phase: Our initial target is to group received CAMs, which are closely located on the time axis, into *detection sets* so that each set contains N received CAMs (one from each vehicle). Our heuristic approach tries to do so.

First, we find N subsequently successfully received CAMs from different vehicles and assign the identifiers V to these CAMs (or respective vehicles) via their enumeration in the ascending order from 1 to N. An interval of duration T which starts from the transmission time of the first CAM in this sequence will be referred to as the *detection period*. We use this initially identified period to further slot the entire time axis into detection periods.

Second, for each detection period i, we create *detection sets* $\mathcal{R}_i$ of pairs {CAM identifier, CAM transmission time}. Our objective is to try making sets where each set has exactly N different CAM identifiers. To do so, we process each CAM received and apply the following heuristic rule to determine

[1] In the original manuscript [7] the training phase was referred to as the *installation phase*, while the detection phase had a notion of *normal operation.*

[2] If an attacker destroys more than one CAM from the same group, the detector will treat such jamming as natural CSMA/CA collision.



(a) Random jamming **(b)** ON-OFF jamming, $K = 2$

Fig. 3. Probabilities of attack detection for the model-based and hybrid detectors against the number of vehicles in a platoon in the absence of jitter ($\delta = 0$) and noise-free channel for $p = 0.4$. Plots depict mean values and 95% confidence intervals.

if it should be assigned to the previous, current or next detection set. In each detection period we store the last highest CAM id H received so far. When a collision is observed, H is incremented by one. Then, currently processed CAM is assigned to $\mathcal{R}_{i-1}$ if its id is larger than $H + \frac{N}{2}$, and to $\mathcal{R}_{i+1}$ if its id is less than $H - \frac{N}{2}$. Otherwise it is assigned to $\mathcal{R}_i$. A depiction of this process is shown in Fig. 2. CAM transmission time is measured from the start of the detection period to which it belongs.

Our next target is to "make a guess" which CAMs could have been involved into each collision. For each detection period i and respective detection set $\mathcal{R}_i$ we consider time intervals of the observed CAM transmissions. For every vehicle V we average the data from different detection periods and compute the mean μ_V and the standard deviation σ_V of these intervals. As a result we get intervals of highly probable transmission of each vehicle V: $\tau_V = [\mu_V - \sigma_V, \mu_V + \sigma_V]$.

2) Detection Phase: During the detection phase, the detector keeps operating on the detection periods of length T and uses intervals of most probable transmissions τ_V for all the vehicles from 1 to N obtained in the training phase. Moreover, for each detection period i the detector builds a detection set $\mathcal{R}_i$, which is constructed by the middle of detection period $i + 1$ as explained above.

We analyze each observed collision. At every detection period i for each collision c with starting time t_c counted on the period i we try to "make a guess" as to CAMs from which vehicles could create it and make a set $\mathbf{M}_c$ (initially, $\mathbf{M}_c$ is empty) consisting of their corresponding ids. To this end, we consider all the CAMs with ids V, which are *not* in the detection set $\mathcal{R}_i$ and if t_c falls into interval τ_V, then V is added into set $\mathbf{M}_c$. Also, the set $\mathbf{C}_c$ with an only element - collision identifier c - is created. Thus, for each collision c (occurred at time t_C) $\mathbf{M}_c$ stores all the ids V of vehicles from which CAMs were not received on $\mathcal{R}_i$ which could collide/be jammed at time t_c (for this V should be able to transmit its CAM at time t_c, i.e. τ_V should have intersect with t_c). $\mathbf{C}_c$ simply stores id of the collision under consideration.

In general, lost CAM of vehicle V could be involved into any observed collision c, which t_c intersects with vehicle's τ_v. Thus, we're looking for intersections between different $\mathbf{M}_c$ of different collisions. For all possible pairs of $\mathbf{M}_i$ and $\mathbf{M}_j$ ($i \neq j$) we check if there is a CAM id V exists which is included in both of them (i.e., we check if the intersection of sets $\mathbf{M}_i$ and $\mathbf{M}_j$ is non-empty). If found, we merge $\mathbf{M}_i$ with $\mathbf{M}_j$ and $\mathbf{C}_i$ with $\mathbf{C}_j$, respectively. The process is repeated until we no longer find any such CAM V.

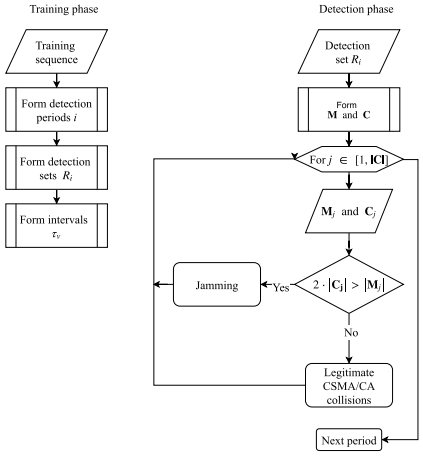


Fig. 4. Flowchart summarizing the operation of the proposed detector.

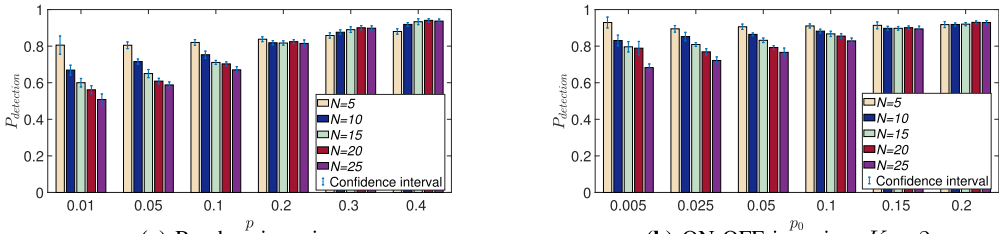
Finally, for each detection period i we construct *dependent collision set* $\mathbf{C} = \{\mathbf{C}_1, \ldots, \mathbf{C}_k\}$ and *involved vehicles set* $\mathbf{M} = \{\mathbf{M}_1, \ldots, \mathbf{M}_k\}$, which both consist of all subsets from the previous step. The jamming detection is built on the basic knowledge of the system: *In order to create a legitimate CSMA/CA collision, at least two vehicles need to transmit their CAMs simultaneously.* The decision to raise a jamming alarm is prompted if inequality $|\mathbf{M}_j| \geq 2|\mathbf{C}_j|$ does not hold for at least one pair of subsets $\mathbf{M}_j$ and $\mathbf{C}_j$.

IV. Performance Evaluation

In this section the detectors are studied from two angles. First, we conduct a comparison of their performance in the absence of jitter. Second, since the model-based detector is vulnerable to jitter, we introduce jitter in our experiments and focus on the performance of the hybrid detector only. As a simulation tool we use our own simulation framework written in MATLAB, the same as that was used in the reference model-based detector in [7].

We are interested in the following performance metrics:

- *Upper boundary on decision delay:* For the model-based detector a decision on the presence of jamming presence is taken every T. Since the operation of the hybrid detector is based on the construction of detection sets $\mathcal{R}_i$, the decision delay does not exceed $1.5T$. Thus, both detectors can detect jamming in real-time and the decision delay is bounded. For our numerical values it does not exceed 50 ms.
- *Probability of attack detection:* We employ the approach used in [7] and in the following subsections we use the probability of attack detection $P_{detection}$, i.e. the



(a) Random jamming **(b)** ON-OFF jamming, $K = 2$

Fig. 5. Probabilities of attack detection for the hybrid detector against the number of vehicles in a platoon in the presence of jitter and packet loses. Plots depict mean values and 95% confidence intervals.

probability that the alarm is triggered, given that at least one successfully transmitted beacon is jammed in the detection set (the probability of missed jamming – false negative rate is $1 - P_{detection}$, accordingly.).[3]

A. Performance Comparison of Two Detectors

Fig. 3 compares both detectors in terms of $P_{detection}$ against a varying number of vehicles in a platoon when there is no jitter in CAM transmissions and an assumption of a noise-free channel. From Fig. 3 one can see that the performance of the model-based detector deteriorates under an ON-OFF jamming strategy. The reason is the design of detection algorithm. As the number of vehicles N increases, the probability of groups in the detection period of the model-based detector with more than one CAM also increases. Thus, when several of jammed CAMs or a jammed CAM together with a natural legitimate collision appear in the same group, the model-based detector is unable to detect it. This can contribute to the marked decrease in true positives $P_{detection}$. The same principle applies to the increase of CAM generation frequency[4]: with a decrease in time diversity within a detection period, more large groups are formed during the training phase, which leads to a decrease in $P_{detection}$ under the same jamming probabilities p. One can conclude that the performance of the hybrid detector outperforms that of the model-based one.

B. Performance of Hybrid Detector

Fig. 5 and 6 evaluate the hybrid detector in terms of $P_{detection}$ when jitter is added to CAM transmissions and packet losses are also introduced. Overall, the hybrid detector performs better under ON-OFF jamming. The performance of the hybrid detector decreases in the presence of jitter and packet loss, though the lowest $P_{detection}$ is still higher than 0.7 (for $N = 25$, $p = 0.1$).

The results also show that the hybrid detector does not require a long training sequence to attain its best performance. In fact, even for short training sequences (5 s) $P_{detection}$ are identical to the values achieved for 100 s, for example. Moreover, the performance for short training sequences is as stable as for long training sequences since standard deviations (not shown) are comparable. These results suggest that the hybrid detector can be easily retrained if necessary, for example, when the number of vehicles in a platoon has changed.

[3]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, does not exceed 0.6% for presented experiments.

[4]In [7] the value of f is 10 Hz, while it is 30 Hz in the current study.

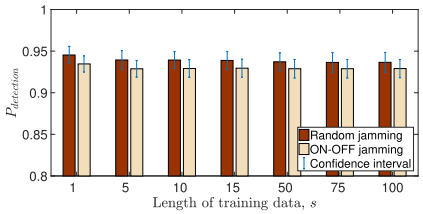


Fig. 6. Probabilities of attack detection of the hybrid detector against the length of the training sequence for random and ON-OFF jamming strategies. The plot depicts mean values and 95% confidence intervals. The number of vehicles in a platoon is fixed at $N = 25$, $p = 0.4$.

Let us note here that a platoon configuration is rather static and does not change within a time scale of minutes or even hours: new members join/leave platoon relatively infrequently. Moreover, when the platoon configuration changes, the hybrid detector could be retrained in 1–5 s.

V. Conclusion & Future Work

In our future work, we will perform a detailed study of additional performance dimensions of the proposed method. We also plan to include additional jamming models and known data mining techniques [9]. Additionally, we intend to evaluate the performance of the proposed DoS detection approach on the real measurement data and fine-tune the detection capabilities (e.g., adjustment of the operation for practical receiver, initial calibration and real-time adaptations to the observed channel quality).

References

[1] K. Sjoberg *et al.*, "Cooperative intelligent transport systems in Europe: Current deployment status and outlook," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 89–97, Jun. 2017.

[2] C. Englund *et al.*, "Future applications of VANETs," *Vehicular ad hoc Networks*. Cham, Switzerland: Springer, 2015.

[3] A. Vinel *et al.*, "Vehicle-to-vehicle communication in C-ACC/platooning scenarios," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 192–197, Aug. 2015.

[4] Ó. Puñal *et al.*, "Experimental characterization and modeling of RF jamming attacks on VANETs," *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 524–540, Feb. 2015.

[5] A. Alipour-Fanid *et al.*, "String stability analysis of cooperative adaptive cruise control under jamming attacks," in *Proc. IEEE 18th Int. Symp. High Assurance Syst. Eng.*, Jan. 2017, pp. 157–162.

[6] G. Patounas *et al.*, "Evaluating defence schemes against jamming in vehicle platoon networks," in *Proc. IEEE 18th Int. Conf. Intell. Transp. Syst.*, Sep. 2015, pp. 2153–2158.

[7] N. Lyamin *et al.*, "Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 110–113, Jan. 2014.

[8] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, document ETSI EN 302 637-2 V1.3.2, 2014.

[9] V. Chandola *et al.*, "Anomaly detection for discrete sequences: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 24, no. 5, pp. 823–839, May 2012.