Protecting Platoons from Stealthy Jamming Attack

Yaodan Hu, Haoqi Shan, Raj Gautam Dutta and Yier Jin
Department of Electrical and Computer Engineering, University of Florida
Emails: {*cindy.hu, haoqi.shan, r.dutta*}*@ufl.edu, yier.jin@ece.ufl.edu*

***Abstract*—Connected vehicles of a platoon broadcast basic safety messages (BSMs) over the control channel of dedicated short-range communication (DSRC). Nevertheless, the fixed frequency of the control channel makes the communication protocol vulnerable to jamming attacks and consequently hindering the stability of the platoon. In this paper, we investigate the impact of *stealthy* jamming attack on platoon stability. A *stealthy* jamming attack is one that only jams platoon vehicles with a specific probability, decided based on the risk of being detected. We show via simulation that the maximum distance error induced by the attack is up to eight times more than without attacks. Due to the *stealthy* nature of the attack, traditional threshold-based detection methods that monitor PLR and MAC-based methods that require high attack probability cannot effectively detect such attacks. To detect the *stealthy* jamming attack, we propose a mechanism that utilizes the received power and the transmission delay of the signal causing interference as features in Quadratic Discriminant Analysis (QDA), to distinguish the jamming attack from normal interference. We use software-defined radios (SDRs) and the Plexe simulator to demonstrate the feasibility of our *stealthy* attack and detection mechanism.**

I. Introduction

Increasing population and economic activity have gradually raised the need for road freight transportation across the world. Recently, advancements were made in the areas of information and communication technologies that led to the development of cooperative methods such as *platooning* to enhance the safety, traffic throughput, fuel efficiency of transportation networks, and reduced carbon emissions. To cooperate, vehicles in a platoon exchange the beacon/basic safety message (BSM), which includes vehicle positions, speeds, and accelerations, etc., through wireless technologies such as dedicated short-range communication (DSRC) to control the operation of vehicles. BSMs are periodically broadcasted by a vehicle to its neighbors over the control channel of DSRC (range $\sim 1000m$), approximately ten times per second. However, the limited packet length, short lifespan, and fixed broadcast control channel make BSMs susceptible to jamming at physical and MAC layers [1]. Consequently, such an attack can affect the performance of safety-critical systems in disseminating timely warnings and could also affect security verification. Further analysis of the impact of such attacks on vehicular networks was done in [2], [3]. However, the impact of *stealthy* jamming on vehicle platoon and the efficacy of current methods in detecting such an attack have not been adequately explored.

Traditional jamming models such as constant, deceptive, random, and reactive have been examined in the past [4]. These models are energy inefficient and easy to detect. To overcome their shortcomings, more advanced jamming strategies such as *stealthy* jamming have been proposed. Current *stealthy* jamming attacks focus on lowering the signal strength [5], reducing the attack probability [6], or attacking specific types of message such as the ACK packets [7]. However, lowering the signal strength or attack probability will decrease the attack success rate. Moreover, some types of messages such as ACK messages, are not available during the broadcast mode. As such, existing *stealthy* jamming approaches may not lead to a successful attack. Consequently, in this paper, we combine characteristics of prior stealthy attacks (targeting a specific type of messages with low attack probability) to develop an *advanced stealthy* jamming attack that has a higher probability of success. More specifically, in our attack, an adversary jams only when detecting transmissions from platoon vehicles. To reduce the risk of being detected, the attack probability is designed in such a way that the average packet loss ratio (PLR) of the vehicle network remains within the normal range. By doing so, the average attack probability is kept low, which is considered to have limited impacts on the system performance [8], but the impact on the victims, i.e., the platoon vehicles, are maximized. We show the feasibility of the proposed *stealthy* jamming attack with software-defined radios (SDRs) and investigate its impact on the vehicle platoon's performance with Plexe [9].

Existing methods to detect jamming can be broadly classified into (i) threshold-based and (ii) MAC-based. The threshold-based methods consider network performance metrics such as PLR, correlation coefficient, etc. to detect jamming by comparing the metric in normal and jammed scenarios [10], [11]. In contrast, MAC-based methods rely on detecting misbehavior of messages at each control channel interval [1]. However, threshold-based methods that monitor PLR, cannot effectively detect the $stealthy$ jamming attack as the adversary keeps the PLR within the normal range. The MAC-based method of [1] requires a high attack probability to detect the attack. As the $stealthy$ attack has low average attack probability, it cannot be detected accurately by such a method. To address this issue, we look into the physical characteristics of a jamming attack that differentiates it from normal interference. We explore the relationship between the signal power and the transmission delay of the received signals causing interference and train a Quadratic Discrimination Analysis (QDA) classifier with the two features. The classifier does not rely on statistic measurements such as PLR or the attack probability and can distinguish normal interference from

978-1-7281-8952-9/20/$31.00 ©2020 IEEE

jamming. To show the feasibility of our detection method, we conduct jamming attacks with SDRs to verify the observation we made. Moreover, we compare our method against existing approaches in simulation and show that our method detects *advanced stealthy* jamming attack with higher accuracy.

The rest of the paper is organized as follows: We provide the platoon model in Section II, and stealthy jamming attack model and its analysis in Section III. Our detection algorithm is discussed in Section IV. SDR experiment and simulation study results are presented in Section V and Section VI respectively. Final conclusions are drawn in Section VII.

II. Platoon Model

We consider a highway scenario where there are $N - M$ benign vehicles, a malicious vehicle, and a platoon of size M. The benign vehicles drive at a desired speed, while the malicious vehicle drives close to the platoon with the intention of conducting jamming attacks. All vehicles are assumed to be equipped with DSRC radios and can broadcast BSM approximately ten times per second on the control channel by following the CSMA/CA model of IEEE 802.11p MAC protocol. We assume N vehicles in total are in the transmission range of the malicious vehicle and each vehicle either transmits or receives a beacon at a time, which is the same setting as the current DSRC protocol. The network topology of the platoon is considered to be predecessor-leader following and the vehicles are assumed to be uniformly distributed. Considering the fact that the DSRC communication range is $\sim 1000m$, which is typically larger than the length of a platoon, we do not consider the hidden node problem in this paper.

III. Stealthy Jamming Attack

A. Attack Strategy

We consider a scenario in which the adversary intends to decrease the performance of the platoon with jamming attacks, which are easy and cheap to implement. Due to the critical information such as location, speed and acceleration contained in BSM, compromising BSM will result in the degradation of the performance of the platoon and even collisions between vehicles. Thus the adversary targets BSM exchanged among platoon vehicles and conducts jamming attacks on the control channel, on which BSM is transmitted. Since the power control problem in jamming attacks is beyond the scope of this paper, we simply assume that the power of the jamming signal is the same with other benign vehicles. To maximize the success rate of the attack and avoid unnecessary fading of the jamming signal, the adversary vehicle drives close to the leader of the platoon. To be $stealthy$, i.e., to avoid detection and hide in the network as long as possible, the attacker intends to avoid noticeable changes in the overall Packet Loss Ratio (PLR) by jamming only when platoon vehicles are transmitting messages. Since the distance between the adversary to platoon vehicles are smaller than that between the adversary to other vehicles, the signals from platoon vehicles received at the adversary are stronger than the signals from other vehicles. Based on this fact, the attacker can distinguish platoon vehicles from other vehicles by measuring the signal strength of the received signal. If the signal is determined to be from a platoon vehicle, then the attacker can carry out the jamming attack with a certain probability. The attack probability is decided by considering its impact on platoon and the risk of detection.

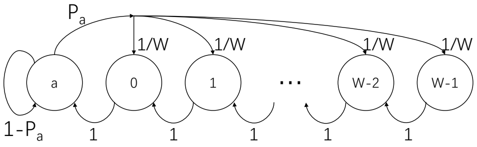


Fig. 1: MC depicting the communication process. The state i ($0 \leq i < W$) represents the backoff countdown number and the state ‘a’ represents the waiting state.

To design such an attack, i.e. to determine the probability of the attack, we first analyze the vehicle communication protocol to find out the normal behavior of the network. In IEEE 802.11 MAC protocol, “carrier sense multiple access/collision avoidance” (CSMA/CA) is used as the basic medium access method [12]. Following the methods used in [13], we construct a discrete-time Markov Chain (MC) as depicted in Fig. 1 to describe the behavior of each vehicle’s transmission. Before sending a beacon, a station, i.e. a DSRC equipped vehicle in our case, senses the channel before transmitting. It performs a random backoff process in which the vehicle waits for a random countdown number (between zero to a predefined window size) of idle slots before transmitting. The node ‘i’ ($i \in 0, \ldots, W-1$) to represent the backoff countdown number, and W is the contention window size. During the backoff process, the countdown number decreases by 1 at each idle time slot, and the node will transit to the next state. If the channel turns busy, the node freezes. Therefore, the average transition time of the chain, which is called a *virtual slot* duration T_{vs}, can be calculated as $T_{vs} = P_{busy} \cdot T_p + (1 - P_{busy}) \cdot T_s$, where, P_{busy}, T_p and T_s represent the probability that the channel is busy, the duration of a packet transmission, and the duration of a time slot respectively. The state ‘a’ of the MC represents the waiting state. When a vehicle senses the channel to be idle and has a packet to transmit, it will transmit out of state ‘a’. We assume that the packet arrival follows a Poisson distribution of rate R and $P_a = 1 - e^{-RT_{vs}}$, indicates the probability of packet arriving during a *virtual slot* duration.

By solving the MC in Fig. 1 and considering the normalization condition, the stationary probabilities $P(a)$ of state ‘a’ and $P(i)$ of states $i \in 0, \ldots, W-1$ respectively, are as follows:

$$P(a) = \frac{1}{P_a} P(0) \tag{1}$$

$$P(i) = \frac{W-i}{W} P(0), \quad i \in 1, \ldots, W-1 \tag{2}$$

$$P(0) = \frac{1}{1/P_a + (W+1)/2} \tag{3}$$

Since the state ‘0’ represents the state in which a node transmits a packet, its stationary probability is the probability of transmission in a virtual slot $\tau = P(0)$. When the channel is busy, there is at least a node transmitting. Assume the total number of nodes (representing platoon vehicles and other benign vehicles) is N. Then, $P_{busy} = 1 - (1-\tau)^N$. The probability of transmission collision in a virtual slot is the probability that at least two nodes transmit together, which can be calculated as $P_c = 1 - (1-\tau)^N - N\tau(1-\tau)^{N-1}$. Therefore, the Packet Loss Ratio (PLR) sensed at the receiver's side, which is defined as the ratio of the number of lost packets to the number of total packets, can be calculated as:

$$PLR = \frac{P_c}{P_{busy}} = \frac{1-(1-\tau)^N - N\tau(1-\tau)^{N-1}}{1-(1-\tau)^N} \tag{4}$$

Next, we discuss how the attacker should build her attack. Assume that the attacker conducts jamming attack with probability q. Then, the collision probability is

$$P_c' = 1 - (1-\tau)^N - (N-qM)\tau(1-\tau)^{N-1} \tag{5}$$

where M is the platoon size and the PLR in presence of the attack is:

$$PLR' = \frac{P_c'}{p_{busy}} = \frac{1-(1-\tau)^N - (N-qM)\tau(1-\tau)^{N-1}}{1-(1-\tau)^N} \tag{6}$$

To keep the attack $stealthy$ and prevent it from being detected by existing detection methods [10], the attacker intends to limit noticeable changes in PLR. We use KL-Divergence to quantify the change in PLR:

$$D_{KL}(PLR||PLR') = PLRln\frac{PLR}{PLR'} + (1-PLR)ln\frac{1-PLR}{1-PLR'} \tag{7}$$

The attacker's objective is to impede the information transmission among platoon vehicles, i.e., maximize the attack probability q, while limiting the risk of being detected, i.e., $D_{KL}(PLR||PLR')$. Therefore, we can find the desired attack probability q by solving the following optimization problem:

$$\begin{aligned} &\max_{0\leq q\leq 1} \quad q, \\ &\text{s.t.} \\ &\qquad D_{KL}(PLR||PLR') \leq TH \end{aligned} \tag{8}$$

where, TH is the threshold to limit the probability of being detected.

$D_{KL}(PLR||PLR')$ reaches its minimum when $q = 0$ and keeps increasing as q increases to 1. The optimum value of q is reached when $D_{KL}(PLR||PLR') = TH$.

IV. Detection of Stealthy Jamming Attack

As our *stealthy* attack does not cause significant changes to PLR, traditional methods relying on PLR will fail to detect it. Consequently, we look into the fundamental physical difference between the attack and normal packet collisions. We observe that the nature of the *stealthy* adversary is a reactive jammer that senses the channel before attacks. Thus, transmission delays such as the radio switching delay are introduced into the jammed signals. Here, the transmission delay of a signal means the difference in time of two interfering signals arriving at the receiver. On the other hand, the time cost for transmission mainly depends on the distance between the sender and receiver, which also determines the signal power received at the receiver. Thus, we leverage the received power and the transmission delay of the signal causing interference to distinguish our jamming attack from normal packet collisions.

We begin by investigating the relationship between the received power of the signal causing interference and the maximum possible transmission delay of it. We consider all the possible scenarios of interference with different relative positions of a receiver and senders in Fig. 2. R is the receiver node, T_1 is the first node starting transmission, and T_2 is the sender node causing interference. $d(i,j)$ indicates the distance between node i and j, c is the speed of light, D_t, D_r are the antenna gain of the sender node and the receiver node respectively, f is the signal frequency, and P_t is the transmission power. The maximum possible transmission delay of T_2 is calculated by assuming that sender T_2 starts transmitting at the same time it receives signals from T_1. Subsequently, we use the free space path loss model to find the received power of the signal. The received power of the signal causing interference, i.e., the signal power of T_2 received at R, is $P_r = D_tD_r(\frac{1}{4\pi d(T_2,R)f})^2P_t$. In the first situation, the maximum possible received power of interfering signal is achieved when R located at the same place of T_1, thus $P_e = D_tD_r\left(\frac{c}{4\pi d(T_1,T_2)f}\right)^2 P_t$. Since $d(T_2,R) \geq d(T_1,T_2)$, the signal power of T_2 received at R P_r should be no larger than P_e. Similarly, we get $P_r \leq P_e$ for the second and third situations. Thus, a large transmission delay indicates that the interfering node is far away and also the interfering signal power should be low. However, the signal from an attacker has a relatively longer transmission delay, while the received power of the signal causing interference is large compared to normal interference with the same transmission delay. Therefore, we can leverage these two observations to distinguish a jamming attack from normal interference.

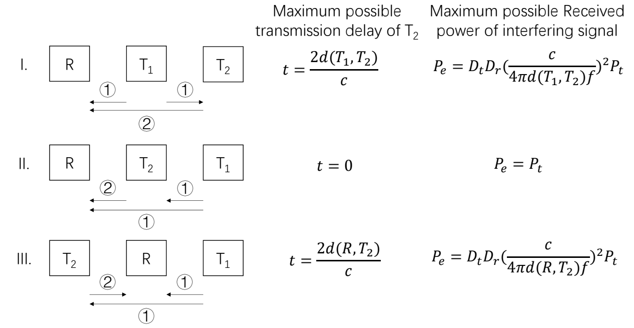

Maximum possible transmission delay of T$_2$
Maximum possible Received power of interfering signal
I.
R
T$_1$
T$_2$
①
①
②
$t = \frac{2d(T_1,T_2)}{c}$
$P_e = D_tD_r(\frac{c}{4\pi d(T_1,T_2)f})^2P_t$
II.
R
T$_2$
T$_1$
②
①
①
$t = 0$
$P_e = P_t$
III.
T$_2$
R
T$_1$
②
①
①
$t = \frac{2d(R,T_2)}{c}$
$P_e = D_tD_r(\frac{c}{4\pi d(R,T_2)f})^2P_t$

Fig. 2: Possible interference scenarios

Based on these observations and because the power of the signal causing interference is quadratic in the transmission delay of it according to the free path loss model, we use Quadratic Discrimination Analysis (QDA) [14] to classify the signals. Quadratic Discriminant Analysis (QDA) is a Bayesian-based machine learning method. It assumes the data points are normally distributed and labels of data points are

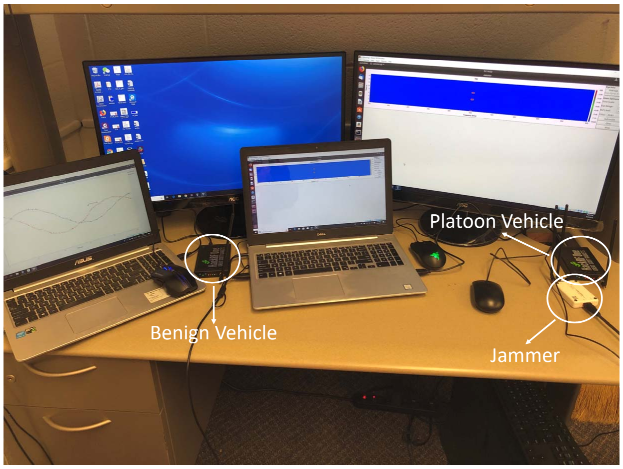


Fig. 3: Experiment setup.

decided by finding the class that maximizes the following discrimination function: $-\frac{1}{2}log|\Sigma_k|-\frac{1}{2}(x-\mu_k)^T\Sigma_k^{-1}(x-\mu_k)+log\pi_k$, where, Σ_k, μ_k and π_k are the covariance matrix, mean, and prior distribution of class k respectively. QDA learns a quadratic boundary between data points belonging to different classes. Therefore, QDA has better performance when the label of the data point is quadratic in the measurements.

In the training phase, data for both attack and attack-free situations are collected by each vehicle to train a local model. Then in the prediction phase, each time an interference occurs, the vehicles record the received power and the transmission delay of the signal causing interference, and uses their trained local model to predict whether the interference is caused by a normal packet collision or a jamming attack. If it is determined to be a jamming attack, an alarm is raised. This method can perform real-time detection of jamming attacks.

V. Attack and Defense Hardware Validation

In this section, we demonstrate the feasibility of our detection method in GNU Radio [15] with the help of a setup consisting of HackRF One and USRP.

A. Experimental setup

The experimental setup to demonstrate the validity of our *stealthy* jamming attack and detection method is shown in Fig. 3. We use two HackRF One to represent DSRC units of a benign and a platoon vehicle and a USRP B205mini-i as the jammer. Each of these units is connected to a computer. To show the transmission of signals clearly, we set our duration of the time slot to 1 second. The HackRF One waits for a random number (chosen from 0 to 7) of idle time slots before transmission. The signal is a cosine wave with a frequency of 500 MHz and it transmits for 1 second. In our experiment, transmitted signals are not encoded or decoded. The jammer keeps probing the channel 10 times per second (i.e., per time slot) and records the power of the received signal. A threshold of the signal amplitude is set for the jammer to detect the presence of the target vehicle transmission. Once it detects a transmission from the platoon vehicle, the jammer starts transmitting for a second.

B. Feasibility of Our Detection Method

The key idea of our detection method is that the jammer incurs physical limitations such as radio switching delay, which introduces a delay in its transmission. As interference detection is not the focus of this paper, we use a simple interference detection method based on the amplitude (the signal power is proportional to the square of the amplitude) and show the transmission delay of the jammed signal. When two signals interfere with each other, the amplitude of the received signal will deviate from the original signal. We notice that the fluctuation of the signal without interference is less than 0.1 while the fluctuation of the signal with interference is quite large. Based on this, we detect signal interference by monitoring the fluctuation of the signal amplitude. The amplitude values larger than 0.1 marks the start of transmission. After detecting the start of a transmission, we monitor the change in amplitude until the amplitude is lower than 0.1, which is regarded as the end of a transmission. Once we detect a change in amplitude greater than 0.1125, which is the maximum fluctuation of signal amplitude observed in the attack-free situation, we mark it as the start of interference. The interference detection result is shown in Fig. 4. The zoomed-in section of the figure shows that the interference occurs a delay of 0.1s after the start of signal transmission, which is caused by the radio status switch.

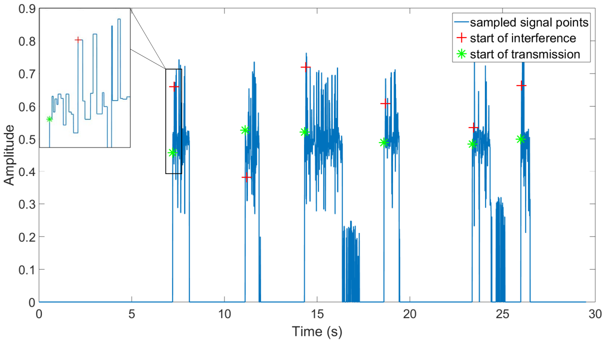


Fig. 4: Interference detection result.

VI. Platoon Simulation

We use the Plexe simulator to simulate the attack and the detection method on a platoon of eight vehicles.

A. Simulation Setup

We modify the Plexe [9] simulator to show the impact of our *stealthy* attack on a platoon of eight vehicles and to evaluate the performance of our QDA based detection method. Unlike prior works [3], [16] that simulate jamming by discarding packets at the time of attacks, we build an attacker module in which the MAC protocol is modified to schedule transmission with certain probability immediately after packets from a targeted platoon vehicle are detected. By doing so, we ensure that our simulated attack closely resembles the jamming attack in a real-world scenario. We use the sinusoidal scenario implemented in Plexe to analyze the impact of our *stealthy* jamming attack on the platoon. In Plexe, the leader vehicle's acceleration and deceleration generate a sinusoidal velocity profile. The selection of communication characteristics is based on the DSRC standard. We consider a platoon of size $M = 8$ and our attacker is on the left lane of the platoon, besides the platoon leader. The desired inter-vehicular distance is set as 5m and the target speed is 100km/h. Our attack strategy changes with the total number of vehicles (vehicles in the platoon and other benign vehicles) on the road. As such, we run multiple simulations by considering 32, 48, 64, 80, and 96 total vehicles (8 of them are platoon vehicles) on the road. For a typical two-lane highway, it is safe to assume up to 100 vehicles on the road that are 20m apart. We use Cooperative Adaptive Cruise Control (CACC) [17] as the control algorithm in our platoon simulation. Each simulation lasts 120s.

B. Evaluation of Stealthy Jamming Attack

We first present the numerical results of our attack strategy and then examine the impact of the attack on the platoon. The parameters used in the optimization problem of equation (8) are given in Table I. By solving equation (8), we obtain the optimal attack probability (q) as given in Table I. Note that this can be done offline. Therefore, there is no computational overhead for the attacker when he conducts the attack. The only thing the attacker needs to do is to generate a random number and decide whether to jam based on the attack strategy. As presented in Table I, when there are more vehicles on the road, the number of normal interference increases. Therefore, the attacker can increase the probability of attack and the inter-vehicle distance error of the platoon without significantly increasing the PLR.

Parameter	T_p	T_s	R	TH	M	W
Value	500μs	13 μs	10	0.01	8	8

Number of Vehicles in total N	32	48	64	80	96
q	0.0584	0.0984	0.1459	0.2014	0.2672

TABLE I: Attack parameters and Jamming strategy. T_p is the transmission duration of a packet, T_s is the length of a time slot, R is the packet arrival rate, TH is the threshold of the change of PLR, M is the platoon size, W is the window size, and q is optimal attack probability

Next, we evaluate the impact of the attack strategy presented in Table I on the platoon. The impact is quantified in terms of the error between the desired inter-vehicular distance of the platoon and the actual inter-vehicular distance measured during the simulation. We relate the attacker's capability to the maximum distance error it can introduce. In a platoon, a large distance among vehicles decreases the fuel efficiency whereas a small distance increases the risk of collision. We consider errors occurring in both these scenarios. We also compare the results of the attack scenario with the attack-free scenario. To understand how much the platoon has deviated from the normal situation, we consider the ratio of errors in attack and attack-free scenarios. The presented ratio is the maximum ratio of errors occurring when the distance is smaller or larger than the desired distance. We run each scenario five times and present the results of the worst scenarios in Table II. The error between the desired distance and the actual distance increases as the number of vehicles increases for both attack and attack-free situations. Furthermore, we observe that for 96 total vehicles, the maximum distance error induced by the attack can be up to eight times more than without attack. The attacker can decrease the distance between vehicles by 1.476m or increase it by 2.224m, which is 29.5% less and 44.5% more than the desired distance. When there are 32 vehicles in total, the impact will be smaller because there is less normal interference. To keep the attack *stealthy* in such scenarios, the adversary has to decrease the attack probability. However, even in this situation, the attacker can induce distance error up to five times more than the attack-free scenario.

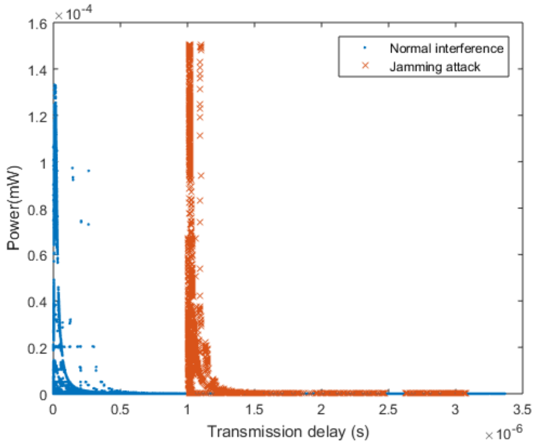


Fig. 5: Relationship between transmission delay and signal power causing interference during normal interference and Jamming.

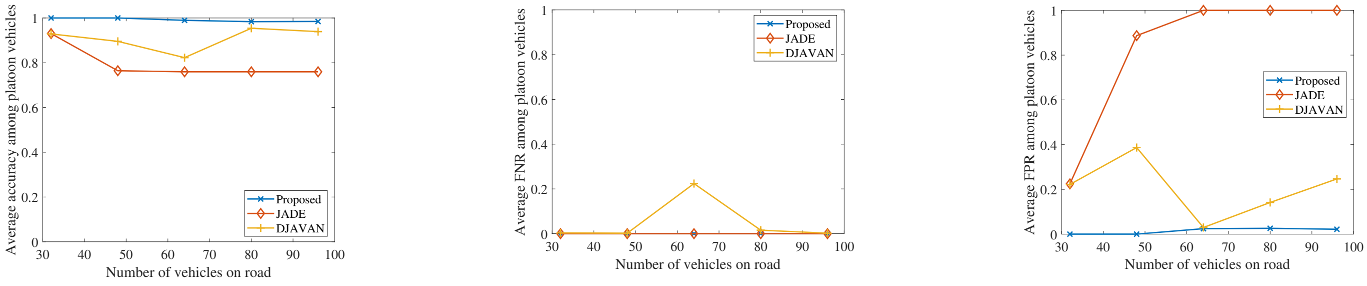
C. Evaluation of Detection Method

In this section, we evaluate the effectiveness of our proposed detection method. To show the feasibility of our detection method, we empirically show the difference in interference caused by normal packet collision and jamming in Fig. 5. We observe that the data points for interference caused by jamming shifts to the right of the data points for interference caused by normal packet collisions (which is consistent with our analysis). Then, we present the performance of our detection method and compare it with JADE [8] and DJAVAN [10]. To test the performance of our method, JADE and DJAVAN under attack and attack-free situations, we start the attack at 60s and start the detection after 40s. The data collected before 40s was used as the baseline to set the threshold for JADE and DJAVAN. A time step of 0.5s is set up for JADE and DJAVAN to measure the PLR.

The results are summarized in Fig. 6. We use Accuracy, False Positive Rate (FPR) and False Negative Rate (FNR) as the metric to evaluate the performance and investigate the average performance of the detectors in platoon vehicles. The proposed method achieves the highest average accuracy $(0.9835 \sim 1)$ compared with JADE (< 0.9304) and DJAVAN $(0.8228 \sim 0.9541)$. The average FNR of the proposed method

Platoon size	Number of vehicles on road	Attack		Attack free		Ratio
		Error when closer	Error when further	Error when closer	Error when further	
8	32	-0.599	0.239	-0.115	0.0972	5.21
8	48	-0.369	0.481	-0.115	0.0972	4.95
8	64	-0.791	0.743	-0.123	0.1444	6.43
8	80	-0.974	1.156	-0.239	0.202	5.72
8	96	-1.476	2.224	-0.295	0.2659	8.37

TABLE II: Results of the impact of attack on platoon. The error between the desired inter-vehicular distance in the platoon and the actual inter-vehicular distance measured during simulation increases as the number of vehicles on road increases.



(a)

(b)

(c)

Fig. 6: Comparison of the average performance of platoon vehicles among the proposed detection method, JADE and DJAVAN with respect to different numbers of vehicles on road: (a) accuracy, (b) FNR and (c) FPR

is 0 for platoon vehicles regardless of the number of vehicles on road, meaning that we can detect all attacks. Even with such low FNR, we achieve average FPRs lower than 0.0260. JADE also achieves average FNRs equal to 0, but this comes with a tradeoff with FPR, the average FPR reaches 1 when there are more than 64 vehicles, meaning that JADE regards all interference as attacks. For DJAVAN, the FNR can be as large as 0.2240, and the FPR can be as large as 0.3869. Considering the aspects mentioned above, our method not only achieves high attack detection effectiveness but is also robust to the variations in the number of vehicles on road.

VII. Conclusion

In this paper, we design an *advanced stealthy* jamming attack and study its impact on vehicle platoon. We formulate the attack strategy as an optimization problem, where the risk of being detected is quantified as the KL-Divergence between expected PLR in attack and attack-free situations. We demonstrate the attack with SDR and Plexe simulation. In our simulation, we empirically show that traditional jamming detection methods that monitor PLR cannot effectively detect the stealthy jamming attack. To mitigate this issue, we propose a novel detection method using QDA to distinguish normal interference from jamming attacks. We evaluate our method and compare it against existing approaches. The results show the effectiveness of our method in defending against the *advanced stealthy* jamming attack.

Acknowledgment

This work is partially supported by National Science Foundation (CNS-1818500) and CyberFlorida Collaborative Seed Award Program.

References

[1] A. Benslimane et al. Jamming attack model and detection method for beacons under multichannel operation in vehicular networks. *IEEE Transactions on VT*, 66:6475–6488, 2017.

[2] Oscar Puñal, Ana Aguiar, and James Gross. In vanets we trust?: characterizing rf jamming in vehicular networks. In *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications*, pages 83–92. ACM, 2012.

[3] Rens van der Heijden, Thomas Lukaseder, and Frank Kargl. Analyzing attacks on cooperative adaptive cruise control (cacc). In *2017 IEEE Vehicular Networking Conference (VNC)*, pages 45–52. IEEE, 2017.

[4] K.Pelechrinis et al. Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications surveys & tutorials*, 13(2):245–257, 2011.

[5] Bruce DeBruhl and Patrick Tague. How to jam without getting caught: Analysis and empirical study of stealthy periodic jamming. In *2013 IEEE International Conference on Sensing, Communications and Networking (SECON)*, pages 496–504. IEEE, 2013.

[6] Mingyan Li, Iordanis Koutsopoulos, and Radha Poovendran. Optimal jamming attacks and network defense policies in wireless sensor networks. In *IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications*, pages 1307–1315. IEEE, 2007.

[7] Zhiguo Zhang, Jingqi Wu, Jing Deng, and Meikang Qiu. Jamming ack attack to wireless networks and a mitigation approach. In *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*, pages 1–5. IEEE, 2008.

[8] Z. Lu et al. Modeling, evaluation and detection of jamming attacks in time-critical wireless applications. *IEEE TMC*, 13(8):1746–1759, 2014.

[9] M.Segata et al. Plexe: A platooning extension for veins. In *Vehicular Networking Conference*, pages 53–60. IEEE, 2014.

[10] L.Mokdad et al. Djavan: Detecting jamming attacks in vehicle ad hoc networks. *Performance Evaluation*, 87:47–59, 2015.

[11] A.Hamieh et al. Detection of radio interference attacks in vanet. In *GLOBECOM 2009*, pages 1–5. IEEE, 2009.

[12] John B Kenney. Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182, 2011.

[13] Y. P. Fallah et al. Analysis of information dissemination in vehicular ad-hoc networks with application to cooperative vehicle safety systems. *IEEE TVC*, 60:233 – 247, 2011.

[14] Brian D Ripley. *Pattern recognition and neural networks*. Cambridge university press, 2007.

[15] Naveen Manicka. *GNU radio testbed*. University of Delaware, 2007.

[16] Mani Amoozadeh, Hui Deng, Chen-Nee Chuah, H Michael Zhang, and Dipak Ghosal. Platoon management with cooperative adaptive cruise control enabled by vanet. *Vehicular Communications*, 2(2):110–123, 2015.

[17] J.Ploeg et al. Design and experimental evaluation of cooperative adaptive cruise control. In *ITSC*, pages 260–265. IEEE, 2011.