Jamming Mobility in 802.11p Networks: Modeling, Evaluation, and Detection

Sharaf Malebary*, Wenyuan Xu†, and Chin-Tser Huang‡
Department of Computer Science & Engineering
University of South Carolina, Columbia, South Carolina 29208
*malebary@email.sc.edu
†{wyxu, ‡huangct}@cse.sc.edu

***Abstract*—The development of wireless Vehicle Ad-Hoc Network (VANET) aimed to enhance road's safety and provide comfortable driving environment by delivering early warning and infotainment messages. Intentional jamming attack targets at undermining such a goal by disrupting wireless communications. Detecting jamming attacks is important towards enhancing road safety. However, it is challenging because VANET operates in outdoor environment (highly changeable road conditions and atmospheric phenomena), and encompasses volatile topology and high mobility of vehicles (traveling speed and directions). To overcome the challenges, in this work, we study jamming attack mobility and behaviors in IEEE802.11p networks. In particular, we focus on analyzing jamming impact, jamming behaviors, and mobility patterns. Thus, in order to achieve reliable detection, first we identify the impact of vehicles density on network performance. Then, we study jamming effectiveness when adopting different mobility patterns (stationary, random, or targeting) and behaviors (constant, random, and reactive). Finally we propose a two phase detection algorithm and evaluate it in a simulation environment. Our approach shows promising results to detect different types of jammers accurately in IEEE802.11p networks.**

***Index Terms*—Road vehicles, Vehicle safety, Wireless Access in Vehicular, Intelligent vehicles, Jamming, Network security, Detection algorithms.**

I. Introduction

Car accidents are the leading death cause among people ages 4-34 years. Statistical analysis (US-DOT in 2009) have showed that road accidents cause more than 33000 deaths and 5,800,000 crashes per year in addition to over $78 billion cost of urban congestion. The new era is moving toward making cars more intelligent to save resources (financially), enhance drivers safety, and comfort. Therefore, cars manufacturers and governments have been cooperating and investing into proposing new solutions. In the early 2000s, VANET was seen as one-to-one application of Mobile Ad-hoc Network (MANET). Since then, VANET have been developed into research field until officially introduced earlier in 2005. The unique property of VANET (the collaboration between cars and network technology) has attracted cars manufacturers, governments, and companies to research it. For instance, Volkswagen enabled their cars to talk to each others, while Google have successfully made a fully automated cars to drive, control, and park. As a result of these efforts, VANET was standardized by IEEE group.

Since, drivers safety is the main goal behind proposing VANET (based on inserting Wireless Access in Vehicle Environment -*WAVE*), securing VANET from attacks that works against radio frequency communications is crucial. Many authors have researched different parts of VANET, Abdelgader et al. studied [15] the physical layer of the IEEE802.11p. Also, jamming and interference vulnerabilities were studied by Tengstrand et al. and provided signal interference approximation analysis for system performance predictions and the impact in terms of bit, packet error probabilities, and delay [4]. Yet, the new technology is vulnerable to most attacks that effectual in wireless based communications.

In this work, we investigate the impact of launching jamming attack by disrupting the normal operation of wireless communication causing failure to receive sensitive information (accident, weather, or road conditions alerts) by drivers. Failure to receive and maintain proper communications among car nodes can lead to crashes (e.g. Google automated car colliding with a truck in California 2016). Hence, jamming attack is an important problem that need to be addressed and researched.

Though many works existed to detect jammers in different types of wireless networks (Sensor, WiFi, satellite, etc), it is infeasible to implement those approaches in vehicle networks due to the roads and nodes characteristics (high mobility, random availability, irregular surrounding noise, etc). Furthermore, due to nodes mobility and communication standards (UDP-traffic only), links between nodes are constantly changing and packets delivery can't be verified or guaranteed by senders (no ACKs packets). Thus, in this work we investigates jamming attacks and propose a solution to the problem. The reminder of the paper is organized as follows. VANET background is Section 2. Jamming models and effectiveness is introduced in section 3. We discuss road conditions and analyze jamming impact in section 4. In section 5 we propose the detection algorithm. Experiments and results are given in section 6. Finally, the paper is concluded in section 7.

II. Background

Although VANET is based on IEEE 802.11 standards for Wireless local area networks (WLANs), its unique characteristics led to introducing IEEE802.11p amendment to insert Wireless Access in Vehicle Environment (WAVE). The amendment introduces some alterations to cope with the

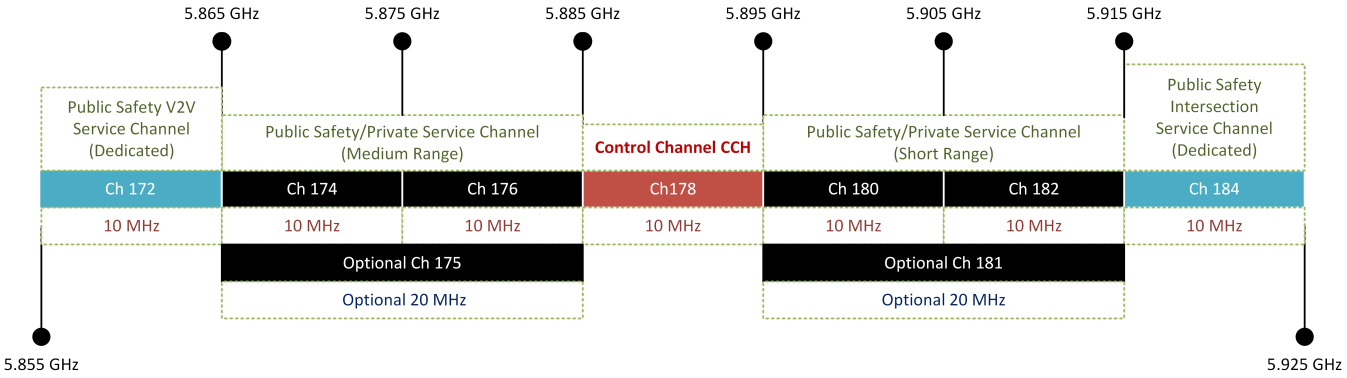

Fig. 1: U.S. DSRC Band Channel Allocation

high mobility of nodes and sustain more noise in outdoor environment. Due to limited space, details were omitted from this section and reader can refer to [7]–[12] to learn about VANET standards and features.

A. Standard & Spectrum

In October 1999, the U.S. Federal Communication Commission (FCC) released an official announcement of allocating 75MHz spectrum in 5.9GHz range for Intelligent Transportation System (ITS) uses. The announcement dictates the FCC decision to use 5.850-5.925GHz band for a variety of Dedicated Short Range Communication (DSRC) uses to create more robust environment with higher noise resistance compared to the current 2.4GHz. DSRC/WAVE consists of a set of IEEE1609 standards for wireless access in vehicular environment. The IEEE1609 family illustrates the architecture (1609.0), communications model, protocols, security mechanisms (1609.2), network services (1609.3), multichannel operation (1609.4) and their operation in ISO/OSI model Figure2. They define the main architectural components of two types of nodes (On Board & Road Side -Units), WAVE interface, and describe the functionality of WAVE based applications (approved in 2010).

B. Channels

The DSRC band (licensed yet free to use) spectrum is divided into seven 10Mhz channels (6 service, 1 control) and support 6, 9, 12, 18, 21 and 27Mbps data rate (3Mbps preamble). Central channel (178), Control Channel (CCH), is used exclusively to broadcast critical messages and manages data. IEEE defined nodes operation on CCH (5.890GHz) to generate maximum antenna power of 28.8dBm. The two main purposes of CCH are announcing: (i)WAVE Short Messages (WSMs) that provide safety related information, and (ii)WAVE Service Advertisements (WSAs) of available services on Service Channels (SCHs). In this work, we focus on CCH where safety related messages are broadcasted thus, it is an attractive and fruitful channel for adversaries to attack.

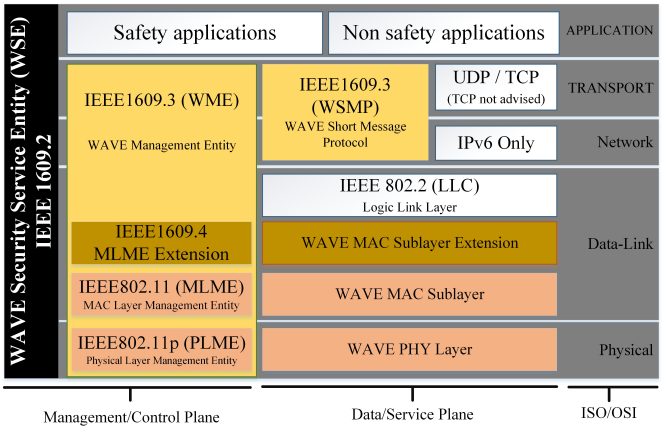

Fig. 2: WAVE Communication Protocol Stack standards

C. Wireless Nodes

Two types of wireless nodes are introduced in VANET that allow bidirectional communications among them Figure3.

- *Road-Side Units (RSUs).* Stationary towers-like infrastructures deployed on the side of roads. The purpose of deploying RSUs is to provide road coverage to disseminate, exchange, and forward data between nodes. Although RSUs are expected to serve as the main component to spread safety messages within their range, no clear definition exists regarding their placements. Hence, RSU placement remains an open problem for research to investigate and find optimum placement. Regardlessly, in this work we prove that our solution works despite the number or location of deployed RSUs.
- *On-Board Units(OBUs).* Vehicles equipped with wireless capabilities to enable drivers/vehicles to exchange data on roads. These data can be safety related or application based service data.

The combination of the aforementioned wireless nodes RSUs and OBUs allows mainly two types of communications in VANET: Vehicle To Vehicle (V2V) and Vehicle To RSU (V2R) Figure3.

III. Jamming Models and Effectiveness

In this section we introduce intentional radio interference that may be launched to disrupt Inter-Vehicle Communications (IVC). We first classify jammers based on two independent features: *mobility* and *behavior*. Attackers can adopt different combination of jamming behavior and mobility.

A. Jamming Models

Since one of the most distinguished feature of VANET is mobility, we model jammers in VANET based on their mobility and jamming behavior.

1) Mobility: We assume that a jammer does not have unlimited transmission power and only affect the communication nearby. Considering that VANET consists of both stationary (RSUs) and mobile (OBUs) nodes, a jammer may target at an RSU, an OBU, or randomly roam around. To model these jamming patterns, we consider the following mobility patterns of a jammer. Note that in this paper, we focus on highway roads, and we assume that jammers are interested in remaining undetected.

- *Stationary*. A none moving jammer is considered stationary. Such a jammer can be sitting in a parked car or at road side. This type of jamming can only affect the same area effectively where jammer is located. A stationary jammer has full control over the attack location. Yet jammers will have limited time to stay stationary due to the in-feasibility of remaining stationary in a highway scenario.
- *Targeting mobility*. This type of mobile jamming intends to target at a specific node (vehicle). Targeting-mobile jammers stay in close range to one car to ensure the jamming effect throughout the attack period. Depending on the adopted jamming model, this type of mobility makes detecting jamming hard especially when combined with reactive jamming behavior.
- *Random mobility*. Jammers of this category would be driving in their cars or motorcycles that keep them mobile without targeting at a chosen target. They can exhibit a random and high mobility and the only constrains are road boundary and speed limit. Thus, this type of mobility makes it challenging to detect.

2) Behavior: In addition to mobility patterns, attacker may also adopt different jamming attack behaviors.

- *Constant*. A constant jammer sends out random radio signals all the time without following any MAC protocols. The objective of this type of behavior is to prevent legitimate nodes from accessing communication channels or corrupt near packets by creating high interference causing higher bit-error-rate (BER) at the receiver and leading to a high packet drop rate.
- *Random*. Launching jamming attack that blocks and interferes with communication consumes a large amount of energy. To reduce the energy consumption, a jammer can alternate between sleep mode for t_S and jam for t_J seconds. This allows jammers to have more control over energy consumption by altering (t_S & t_J) as needed.
- *Reactive*. Instead of targeting packets at the sender and prevent them from being transmitted without considering the channel condition, sophisticated active jammers target at the receivers. They constantly listen to the targeted channel, and once the jammer sense packets being transmitted, they immediately start jamming to corrupt packets at the receiver nodes upon arrival. This particular jamming behavior is challenging to detect due the hidden nature of jamming (jamming signals overlap with the packet transmission).

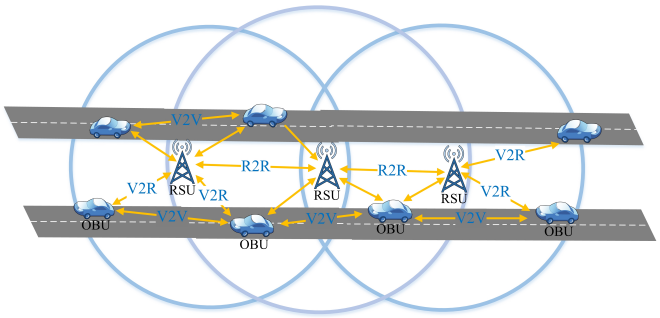

Fig. 3: VANET communication and architecture

The combination of the aforementioned behaviors and mobility can produce nine types of jammers. Instead of examining all nine, we focus on reactive jammers with all three types of mobility patterns. This is because reactive jammers are harder to detect. We believe that any methods that can detect reactive jammers can identify constant and random jammers. Already in [1], authors have studied random and constant jammers in VANET and proposed detection algorithm, their method rely on the successful reception of at least one beacon, and are not effective against reactive jammers since it is hard to distinguish reactive behavior from congestion scenario. Thus, without lose of generality, we study and validate stationary reactive jammers, targeting mobility jammers, and random mobility jammers.

B. Jamming Effectiveness

In order to achieve reliable detection, one has to understand the jamming impact on the network. Xu et al. studied the feasibility of launching and detecting jamming attacks in wireless networks [13]. They evaluated jamming impact and effectiveness in their work using Berkeley motes. Although their algorithm showed promising results, it is infeasible to apply their technique in VANET due to its nature (encompass high mobility and volatile topology). Thus, we present three metrics that will be used throughout this paper to identify jamming attacks targeting at vehicle network. These metrics are closely related to the network performance and are used to identify abnormalities that any wireless network may encounter.

- Packet Delivery Ratio (*PDR*). The ratio of successful delivered packets to destination compared to number of

packets that have been sent out by sender. In vehicle network, the density of vehicles is highly changeable and dependent on road conditions and the time of day. For instance, during rush hours or holidays, roads experience more traffic (congestion) which corresponds to observing lower PDR. Also, if jammer exists, packets will suffer from intentional interference causing a significant drop in the PDR. Consequently, distinguishing between low PDR caused by congestion or jamming attack is impossible by relying on PDR as a single metric.

- Packet Send Ratio (*PSR*). The ratio of packets that are successfully sent out by a legitimate source compared to the number of packets it intends to send out in the MAC layer. In congested roads, vehicles tend to travel at much lower speed which entitles longer communication period between nodes. Consequently, channel observes more RTS/CTS (Request/Clear -to send) requests leading to higher drop in PSR. Additionally when jammer exists, the noise introduced by jammer may hold the channel status as busy, which leads to an increase in node's back-off-timer and delay to receive CTS response. Regardless whether road is congested or jammed, more packets will be buffered and discarded upon the arrival of new packets or when they timed-out causing low observed PSR. Therefore, it is inadequate to rely on PSR alone to identify congested or jammed channel especially in the presence of reactive jammer whose targeting at packets after being sent out.
- Signal Strength (*SS*). Is a powerful tool measured at receiver that defines the signal quality of radio frequency signals that carry data from source to destination. Since wireless node can sample SS during any period of time (depends on the employed protocol), many researches have been utilizing SS to detect jamming attacks in different wireless networks. In VANET, vehicles have the freedom to enter and exit communication range at random speed. As a result, observing high SS may correspond to high vehicles intensity (congestion), or jammer existence. Also, in case of a reactive jamming (stay hidden until packets being transmitted), a lower SS maybe observed when measured during the transmission period.

To summarize, we introduced three different mobility patterns and three jamming techniques that jammer may adopt when launching attacks. We analyzed jamming impact using three network metrics (*PDR, PSR, and SS*). We also discussed the deficiency to rely on these metrics (individually) to distinguish between a jamming attack or a congested road scenario.

IV. Road Conditions and Jamming Analysis

In this section we study road conditions that impact VANET performance. Since vehicles are expected to travel at high and random speed on highway roads, the presence of jammers and their effect is unsustainable. Thus, we introduce road conditions based on vehicles flow intensity to identify the conditions that leads to poor network performance.

A. Road Conditions

Road conditions are unpredictable by nature. Many factors impact traffic on road including but not limited to (vehicles density, obstacles, weather conditions, construction zones, traffic lights, and speed limit). Most of these factors tends to be the same when analyzing a specific road. Vehicle density is the only factor that inclusive rapid change over short period of time (matter of seconds or minutes). For instance, road could pack up with cars simply because it is rush-hour, work zone or due to accidents. Regardlessly, when number of vehicles increases, the network throughput will follow until reaches certain threshold and consequently, influencing the observed PDR and Packet lost rate(PLR). In this work we focus on highway roads where traffic expected to move freely at relatively high speed which increase the severity when incidents happen. In order to evaluate vehicle density impact on the network, we constructed a highway road that consists of two lanes (common in US), and place RSU at the edge of the road (to ensure maximum link-time between nodes) in a simulator platform. Each simulation case ran for period of time (the time needed by a car to enters the RSU range until exiting). We define nodes maximum transmission power of (28.8dBM) and broadcasting dissemination rate at 10 Basic Safety Messages per second (BSM/s). Each BSM was generated as UDP traffic and size of (200-500 bytes) according to [12] standards. We start running first case with 1 vehicle which correspond to vehicle traveling on idle interstate (commonly not busy) or at off-peak traffic time (e.g. after mid-night). It is worth mentioning that vehicle nodes were defined with collision avoidance behavior rules where they can freely accelerate, decelerate, and switch lanes based on road conditions. Then we incremented the number of vehicles (to simulate road traffic under different conditions) and observed the impact of various vehicles density on traveling speed, communication time, and network performance. Figure4 shows that when vehicle density reaches %52 -around 60 cars/lane- of the roads capacity [calculated by dividing road length per lane within RSU range (1000m) over the length of average size vehicle (6m)], a noticeable drop in PDR, and PSR occur due to slower traveling speed causing longer communications time and more data exchange among nodes. We also noticed a slight increase in the measured SS which justified as more noise generated due to high vehicle density. Additionally, when the drop in the PDR reaches more than %45, the measured SS tend to remain almost the same. The key observation is the relation between vehicles density, velocity, and flow intensity. Thus we classify road conditions on roads based on the nodes density as follow:

- Normal Period. Represents low density of vehicles traveling at, or close to, the posted speed limit on that road. Vehicles experience reliable communication links within RSU range until exiting. This period tend to be insignificance to the attacker interest due to the low number of cars.
- Rush-Hour Period. Vehicle are forced to travel at much lower speed when vehicle density exceeds a certain

threshold. Nodes observe lower PDR and PSR which correspond to higher lost packet rate than in normal period Figure4. Therefore, ensuring reliable delivery of safety messages is essential during this period. Failure to receive sensitive data may result drivers to fail to slow, reroute, or stop in timely manner to avoid crashes.

- Incident Period. When number of vehicles is high and close to the capacity of the road, vehicles experience what's called a traffic jam (hours of non-moving or stop-and-go traffic). This tend to be the most favorable and effective period for jammers to launch their attack and remain undetected. The significance of this period is the tight relation between vehicles density and the probability of incidents to occur.

B. Jamming Analysis

Although several studies [1]–[6], investigated jamming problem targeting 802.11p communications yet, no clear definition of jammers capabilities exist. A common assumption is that jammers move freely at random or steady speed to block wireless communications. We believe that jammers effect and mobility can be refined (e.g. in congested road, jammers mobility is restricted). It is infeasible to assume the free roaming of jammers at high speed during congestion. Therefore, we present the following refinements:

- Mobility. Generally, jammers mobility is limited to road boundaries and assigned speed limit. Depending on the road conditions (i.e. slippery, accident, traffic jam), jammers speed is bounded by traffic flow which may be significantly lower than the speed limit. In high vehicle density roads, stop and go traffic is very common. This phenomena will define jammers mobility since traveling at high speed during traffic jam is infeasible. Jammers may opt to move as road permits while launching jamming attack, or stay silent (to remain undetected) until exiting the congested road. Therefore, we can define maximum jammers speed to equals to the posted speed limit on road or the highest traveling speed of cars (depending on road conditions) whichever is higher.
- Signal Strength. The common goal of intentional jamming is to disrupt communication effectively, regardless the motive, which requires jammer to operate at relatively higher power level than legitimate nodes. In [13], authors have studied jamming signals and provided a base for detecting wireless interference based on the consistency between the observed PDR and the SS. When wireless communications get disrupted due to jamming attack, a high signal strength is observed which is inconsistent with the corresponded low PDR. Hence, since jammers doesn't comply with MAC protocol, it is reasonable to assume that jammers are expected to emit high power signals when launching their attacks.
- Jammed Zone. Defines the area which affected by jamming signal. The wider range that attacker may want to impact, the higher cost and more sophisticated equipments needed. Therefore, we assume jamming range is limited and is close or equal to the communication range of legitimate nodes. A special case where jammer is targeting a specific node, jammer adopting reactive behavior may choose to block incoming or outgoing communication of the targeted node. When jammer's targets at transmitted packets of victim node, other nodes will still receive messages from different nodes (RSUs or OBUs) since VANET uses broadcasting technique when exchanging warning messages. Alternatively, when jammers targets at dropping all incoming communication to victim node, node will fail to receive any communications. Therefore, in case jammers adopting targeting mobility pattern, we assume their interest to block victim node from receiving communications.

In summary, we consider reactive jammers adopting stationary, random, or targeting mobility pattern. Since 802.11p introduces the usage of seven different channels, we assume jammers interest targeting CCH (Ch178) where safety information are exchanged. Thus is a fruitful channel for adversaries to attack. Although our work discusses detecting jammers targeting packets at CCH, our approach can be applied to all six other service channels.

V. Detection algorithm With Consistency Check

In this section, we propose a two phase algorithm (*(i) Initialization* and *(ii) Detection*) to detect jammers based on the consistency between SS and Packet Delivery/Send Ratio (*PDSR*). Since road conditions vary from road to another, we consider vehicles density on road to serve as dynamic variable that correspond to different road conditions.

A. Initialization Phase -Ip

This phase may be conducted during a guaranteed time of non-interfered network operation (easily achieved by monitoring *SS* distribution over initialization time period (T_{Ip}), or equipping RSU with *SS* meter to filter out any amplified or unwanted measurements). Also, Initialization Phase (Ip) must be conducted when vehicle density is relatively high, i.e. rush-hour, which easy to find depending on the road that RSU being deployed at. During this phase, RSU will calculate and collect (*PDSR, SS, PLR*) Packet-delivery/send-ratio, signal strength and packet lost rate in a table for T_{Ip}. Once the initialization period timer T_{Ip} expires, RSU will find upper bound (*SS*) value that would have produced a particular *PDSR* in non-jammed-rush-hour scenario [$PDSR_{\mathrm{j}}$, Max(SS_{j})]. After forming the table, RSU will assign two threshold values γ_{PDSR} and γ_{PLR}, the maximum $PDSR_{\mathrm{j}}$ and the minimum PLR_{j} respectively, calculated during (T_{Ip}). Then a simple regression will be conducted to build a relation between (*PDSR, SS*) values for all ($PDSR_{\mathrm{x}}$) that have not been observed, and are less than the set threshold (γ_{PDSR}). Finally, each RSU node will calculate and set periodic monitoring timer (T_{wind}) by calculating the needed time by a car to enter and exit that RSU range denoted [T_{Cap}= $\frac{road\ length\ within\ RSU\ range(L_{oR})}{posted\ speed\ limit\ on\ road(SL_{oR})}$]. Upon the completion of this phase, each RSU will have a table contains

an upper bound *SS* value to produce a particular *PDSR*, a periodic monitor window (T_{wind}), and two thresholds (γ_{PDSR}, γ_{PLR}) Algorithm 1. It is worth mentioning, the collected data including thresholds will vary from one RSU to another depending on the roads that been deployed on.

Algorithm 1: [Initialization phase]

Input: T_{Ip}, L_{oR}, SL_{oR}
Output: ($PDSR_j$, SS_j), ($PDSR_x$, SS_x), γ_{PDSR}, γ_{PLR}, T_{wind}, W_{PLR}

for ($j = 1, j <= T_{Ip}, j{+}{+}$) **do**
  Sum = 0
  for ($i = j\text{-}1 \rightarrow i{=}j$) **do**
    Data[i] = (PDR_i, PSR_i, SS_i, PLR_i)
    Sum = Sum++
  end
  $PDSR_j = \frac{\sum PDR_i + \sum PSR_i}{2Sum}$
  $SS_j = \{SS_i, SS_{i+1}, SS_{i+2}, ...\}$
  PLR_j = Average (PLR_i)
  Data[j] = ($PDSR_j$, SS_j, PLR_j)
end
$T_{Cap} = \frac{L_{oR}}{SL_{oR}}$, $W_{PLR} = T(PLR_j)$, $T_{wind} = \frac{T_{Cap}}{W_{PLR}}$
γ_{PDSR} = Max($PDSR_j | PDSR_j \in$ Data[j])
γ_{PLR} = Min($PLR_j | PLR_j \in$ Data[j])
foreach $PDSR_j \in$ Data[j] **do**
  Find upper bound Max(SS_i) $\in SS_j$ that would produce ($PDSR_j$)
end
foreach $PDSR_x \notin$ Data[j], and $PDSR_x < \gamma_{PDSR}$ **do**
  Conduct simple regression to build a relation between ($PDSR_x, SS_x$)
  Data[x]= ($PDSR_x$, SS_x)
end
return (γ_{PDSR}, γ_{PLR}, T_{wind}, W_{PLR}, Data[j], Data[x])

B. Detection Phase with consistency check

RSU will monitor (*PDSR, SS*) and calculate *PLR* every time window (W_{PLR}). When the observed *PDSR* and *PLR* exceed γ_{PDSR} and γ_{PLR} set during *Ip*, a consistency check is performed $C\_Check(MaxPDSR, SS)$ to check whether the low observed *PDSR* is consistent with the measured *SS*. The C_Check function, algorithm 3, takes an input (*MaxPDSR, SS*) as pair and check whether the measured *SS* is consistent with the observed *PDSR* by checking the ($PDSR_{Ip}$, SS_{Ip}) table generated during the initialization period. The boolean C_Check return decides whether the low observed *PDSR* is due jamming attack, or a typical congested road. The detector will also return "normal state" when T_{wind} runs out and no congestion or jammer is detected algorithm 2.

VI. Experiment Setup and Evaluation

In order to evaluate our work, we simulate a two-lane highway road of 1000 meter length (maximum RSU range)

Algorithm 2: [Detection phase]

Input: γ_{PDSR}, γ_{PLR}, T_{wind}, W_{PLR}
Output: *State*

Initialize: Counter = 0, *State* = NORMAL
while ($Counter < T_{wind}$) **do**
  Counter++
  foreach W_{PLR} **do**
    Calculate ($PDSR_j$, SS_j, PLR_j)
    if ($PLR_j > \gamma_{PLR}$) && ($PDSR_j < \gamma_{PDSR}$) **then**
      if C_Check(MaxPDSR$_j$, SS$_j$) == True **then**
        Counter =0
        State = (CONGESTED)
      else
        Counter =0
        State = (JAMMED)
      end
    end
    return (*State*)
    State = (NORMAL)
  end
end
return (*State*)

Algorithm 3: *Consistency_Check()*

function: boolean $C\_Check(MaxPDSR, SS)$
if (SS) consistent with (SS_j) to produce (MaxPDSR = $PDSR_j$), or with (SS_x) to produce (MaxPDSR = $PDSR_x$) **then**
  return *True*
else
  return *False*
end

with different vehicle density (1-100 OBUs) cases. We defined same simulation parameters mentioned in sectionIV. We considered free space and shadowing propagation model which is more appropriate when simulating outdoor environment. Observations are summarized as follow.

1) In **Non-Attacker** cases, we observed a significant drop in network performance when vehicles occupied more than %52 of the maximum road capacity. Thus, we assign this value (52%) as vehicle density threshold which corresponds to road condition during rush hour (congested road) to run Initialization phase -Ip. After running experiments and collecting data, we plotted our results shown in figure 4 with trend-line corresponding to threshold calculated during Ip.
2) For **Attacker** scenarios, we implemented reactive-jammer with multi-mobility capabilities (stationary, random, and targeting) and defined the mobility to follow the posted speed limit on road when possible (i.e. clear lane). Also, we defined fixed jamming power of 44dbm (such a device can be obtain for less than $200).

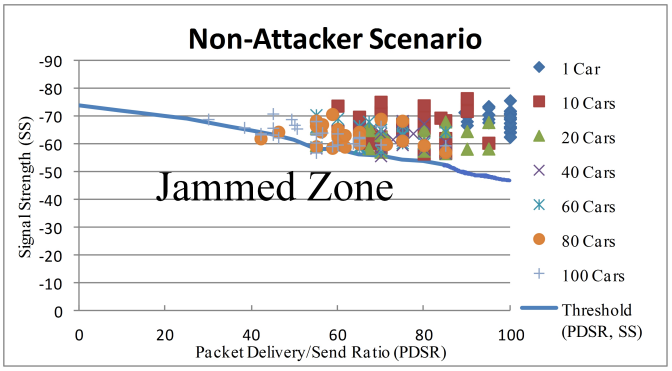

Fig. 4: Trend-line shows Initialization Phase (Ip) congestion threshold ($PDSR_{Ip}$, SS_{Ip}). Resulting (*PDSR, SS*) appear above trend-line representing minimal false detection

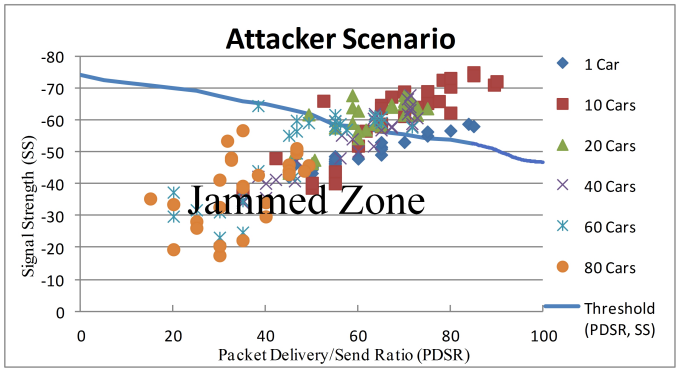

Fig. 5: Resulting (*PDSR, SS*) based on jammer's location.

3) **Results** Figure5 shows a strong tie between jammer effect depending on its location, *SS*, and correspondent packet lost rate. In **low vehicle density**, we detected jammer when its location is close enough to affect the transmission/receiving of packets. Also, in **targeting mobility** jamming case, some packets still got delivered correctly depending on the targeted node location and RSU. Additionally, when vehicle density reaches **congestion** threshold, RSU detected jammer efficiently once nodes failed to receive sufficient communications based on vehicle density on road. By looking at Figure4 & 5, one can clearly see the relation between the observed *SS* and *PDSR* in the present and absence of jammers. In summary, our algorithm proved it's effectiveness by achieving high, (>%99) true positive/negative and low (<%1) false positive/negative, detection accuracy especially when RSU nodes are initialized properly (choosing optimum time to run initialization phase).

VII. Conclusion

VANETs, which is based on inserting wireless access in vehicle environments, are becoming reality and being deployed to enhance safety and provide a variety of services. Although VANET's main goal is to enhance safety and comfort on roads, intentional jamming aims to undermine this goal by interfering with the wireless communications. Therefore, understanding the nature of jamming attacks in vehicle environment is critical to ensure the network operation. This paper has sought to focus on investigating jamming mobility and behaviors in highway roads. We have presented three different jamming behaviors and three mobility patterns that jammer can adopt when launching attacks. We then studied reactive jamming impact, adopting various mobility patterns (stationary, random, or targeting), in different road conditions. We showed jamming effect on PDSR and SS causing failure to receive safety messages. We then proposed a solution to detect jammers based on road conditions in which RSUs are deployed at. Our algorithm proved its effectiveness by achieving high detection accuracy in different vehicle density scenarios.

References

[1] N. Lyamin, A. Vinel, M. Jonson, and J. Loo, *Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks*, IEEE Communication Letters, VOL. 18, NO. 1, JANUARY 2014.

[2] R. Raw, M. Kumar, and N. Singh, *Security Challenges, Issues and Their Solutions for VANET*, Vol.5, pp95-105, IJNSA 2013.

[3] A. Hamieh, J. Othman and L. Mokdad, *Detection of Radio Interference Attacks in VANET*, IEEE, 2009.

[4] S. Tengstrand, K. Fors, P. Stenumgaard, and K. Wiklundh, *Jamming and interference vulnerability of IEEE 802.11p*, EMC Europe 2014.

[5] H. Minh, A. Benslimane and A. Rachedi, *Jamming detection on 802.11p under multi-channel operation in vehicular networks*, Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on, Abu Dhabi, 2015, pp. 764-770.

[6] Y. Qian, K. Lu, and N. Moayeri, *A Secure VANET MAC Protocol for DSRC Applications*, IEEE Globecom, 2008.

[7] U.S. Department of Transportation, IntelligentTransportation Systems (ITS) Home, http://www.its.dot.gov/index.htm

[8] U.S. Department of Transportation, IntelligentTransportation Systems (ITS), IEEE1609 Family of Standards for Wireless Access in Vehicular Environment (WAVE), http://www.standards.its.dot.gov/Factsheets/Factsheet/80

[9] U.S. Department of Transportation, IntelligentTransportation Systems (ITS), DSRC: The Future of Safer Driving, http://www.its.dot.gov/factsheets/dsrc_factsheet.htm

[10] National Highway Traffic Safety Administration, Laws & Regulations, Vehicles, http://www.nhtsa.gov

[11] Y. Li,*An Overview of the DSRC/WAVE Technology*, International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. Springer Berlin Heidelberg, 2010, pp. 544-558.

[12] SAE Standard J2735 SAE International DSRC Committee, *Dedicated Short Range Communications (DSRC) Message Set Dictionary*, SAE International, 2016.

[13] W. Xu, W. Trappe, Y. Zhang, and T. Wood, *The feasibility of Launching and Detecting Jamming Attacks in Wireless Networks*, MobiHoc, 2005.

[14] L. Humeng, Y. Xuemei, A. Li, and W. Yuan, *Distributed Beacon Frequency Control Algorithm for VANETs (DBFC)*, ISDEA 2012

[15] A. Abdelgader, and W. Lenan, *The physical Layer of the IEEE802.11p WAVE Communications Standard: The Specifications and Challenges*, Vol II, WCECS 2014.

[16] F. Nyongesa, K. Djouani, T. Olwal and Y. Hamam, *Doppler Shift Compensation Schemes in VANETs*, Mobile Information Systems (MIS), vol. 2015, Article ID 438159, 11 pages, 2015.

[17] Z. Rawashdeh, and S. Mahmud, *Communications in Vehicular Ad Hoc Networks, Mobile Ad-Hoc Networks: Applications*, ISBN: 978-953-307-416-0, InTech 2011.

[18] R. Reinders, M. Eenennaam, G. Karagiannis, and G. Heijenk, *Contention Window Analysis for Beaconing in VANETs*, 7th IEEE Int'l Wireless Communications and Mobile Computing conference, IWCMC 2011, Turkey, pp. 1481-1487.

[19] W. Alasmary, and W. Zhuang, *Mobility impact in IEEE 802.11p infrastructureless vehicular networks*, Ad Hoc Netw. (2010), doi:10.1016/j.adhoc.2010.06.006