On the Design of Jamming-Aware Safety Applications in VANETs

Hani Alturkostani, Anup Chitrakar,
Robert Rinker and Axel Krings
Department of Computer Science
University of Idaho
Moscow, Idaho 83843-1010
altu2655,chit8942@vandals.uidaho.edu,
rinker,krings@uidaho.edu

ABSTRACT

Connected vehicles communicate either with each other or with the fixed infrastructure using Dedicated Short Range Communication (DSRC). The communication is used by DSRC safety applications, such as forward collision warning, which are intended to reduce accidents. Since these safety applications operate in a critical infrastructure, reliability of the applications is essential. This research considers jamming as the source of a malicious act that could significantly affect reliability. Previous research has discussed jamming detection and prevention in the context of wireless networks in general, but little focus has been on Vehicular Ad Hoc Networks (VANET), which have unique characteristics. Other research discussed jamming detection in VANET, however it is not aligned with current DSRC standards. We propose a new jamming-aware algorithm for DSRC safety application design for VANET that increases reliability using jamming detection and consequent fail-safe behavior, without any alteration of existing protocols and standards. The impact of deceptive jamming on data rates and the impact of the jammer's data rate were studied using actual field measurements. Finally, we show the operation of the jamming-aware algorithm using field data.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General Security and Protection

General Terms

Security, Algorithms, Reliability

Keywords

Jamming, VANET, Jammer Detection, DSRC

1. INTRODUCTION

Intelligent Transportation Systems (ITS) use wireless communications between vehicles, i.e., vehicle-to-vehicle (V2V), and between vehicles and the infrastructure, i.e., vehicle-to-infrastructure (V2I). One of the main objectives of these technologies is to increase safety. In [1] the United States Department of Transportation (USDoT) predicts that V2V communication-based safety applications can prevent up to 82% of all crashes in the US, saving thousands of lives and billions of dollars. Additionally, they also allow for more effective traffic management, which in turn can result in significant reduction of fuel consumption.

The technology behind ITS is based on Dedicated Short Range Communication (DSRC), with a bandwidth of 75MHz at 5.9GHz (5.850-5.925GHz), as licensed by the Federal Communication Commission (FCC). Just like any wireless communications, DSRC inherits the entire spectrum of vulnerabilities, e.g., signal manipulation, degradation or disruption. Given that ITS is part of a critical infrastructure, and the fact that any failure may result in loss of life, it is important to consider security and safety implications that might result from malicious act. A secondary consequence would be the loss of public trust in the technologies.

The focus of this work is on jamming in Vehicular Ad Hoc Networks (VANET), which can disrupt safety applications to the point of rendering these technologies useless. In fact, safety applications may be manipulated by jamming in a way that may lead to wrong decisions or hazards.

1.1 DSRC-based Safety Application

Different types of safety applications have been identified in [2]. These applications use the *Basic Safety Message* (BSM), generated periodically every 100ms by each vehicle, to exchange information about the status of the vehicle, such as speed, GPS location, elevation, heading, acceleration and brake status [3].

Two DSRC safety applications related to rear-end collisions are shown in Figure 1. The first is the *Forward Collision Warning* (FCW) application, which warns the driver of a host vehicle (HV) in case of an imminent rear-end collision with a remote vehicle (RV), driving ahead in the same lane and direction. FCW is useful in scenarios when approaching a vehicle that is decelerating or stopped. The *Emergency*

Electronic Brake Lights (EEBL) application is a milder version of the FCW, which allows the driver of the HV to decelerate once receiving information from a RV that it is braking hard. This is most useful when the HV driver's line-of-sight is obstructed, e.g., by a large vehicle.

Other DSRC safety applications involve lane changes. Two lane change scenarios are depicted in Figure 2. The *Do Not Pass Warning* (DNPW) warns the driver of the HV during a passing maneuver attempt that another vehicle is traveling in the opposite direction. The *Blind Spot Warning + Lane Change Warning* (BSW+LCW) safety application warns the driver of the HV attempting to change into a lane which happens to be occupied by another vehicle traveling in the same direction, but is in its blind-spot.

All these DSRC safety applications rely on the BSM messages from the RV. Should the HV not receive any or sufficiently frequent BSM messages, the application may not be reliable. Such failed communication may be the result of jamming.

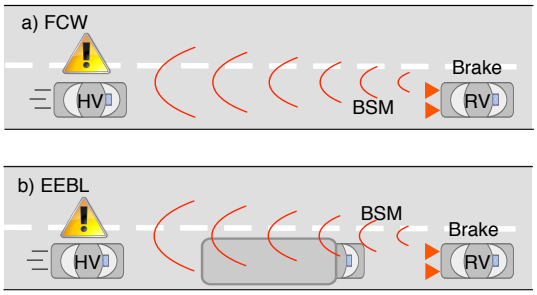

Figure 1: Rear-end collision scenarios

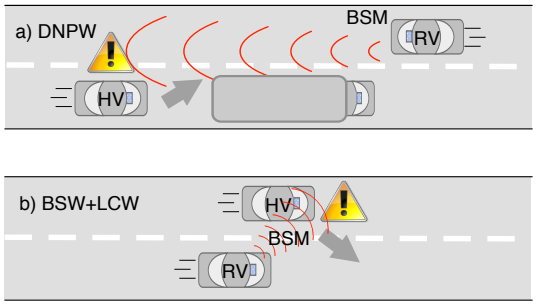

Figure 2: Lane-change scenarios

1.2 Wireless Jamming

Wireless jamming is a common attack in wireless communication, which can be launched using off-the-shelf equipment to interfere or block legitimate transmission by emitting radio signals that interfere with the communication. As a consequence, nodes are blocked and are no longer able to communicate with each other inside the jammed zone. Jamming can take several forms, commonly targeting the physical layer or creating a denial of service. The wireless medium is shared by nature, and the signals transmitted in this medium are susceptible to noise.

Several types of jammers have been defined, based on their behavior [4, 5]:

Constant Jammer: This type of jammer simply emits radio signals continuously (e.g. random noise), which interferes with the signal, i.e., it decreases the signal-to-noise ratio. The constant jammer has the most damaging impact, capable of causing large blind spots, since it can block communication entirely. However, it is relatively easy to detect, and is considered energy inefficient.

Random Jammer: This kind of jammer also operates at the physical layer, however unlike the constant jammer, it alternates between random periods of jamming and sleeping. This jammer type is more difficult to detect and consumes less energy.

Reactive Jammer: This jammer listens to the channel continuously and starts emitting noise once activity is sensed. It it difficult to detect as it only operates during legitimate transmissions.

Deceptive Jammer: A deceptive jammer causes a Denial of Service (DoS) by not following MAC layer access rules. It continuously sends out bogus packets that appear to be legitimate, thus causing the channel to appear indefinitely busy for legitimate nodes. As opposed to a constant jammer, the deceptive jammer does not send noise, e.g., white noise or random bits, but validly formed packets. This research focuses on the impact of deceptive jammers on the communication of DSRC safety applications.

Intelligent Jammer: This is a protocol aware jammer that has the ability to analyze ongoing traffic. Thus, it can target only specific packets or packet types. Once a desired packet is sensed, the intelligent jammer can inject enough noise to corrupt these packets. This is the most sophisticated jammer and it is extremely difficult to detect.

Some of the common metrics to identify jamming are as follows: *Packet Delivery Ratio* (PDR) is measured at the receiver and is the ratio of the number of packets sent to the number of packets correctly received during a time window. *Carrier Sensing Time* is measured at the transmitting node and measures the total waiting time before the medium becomes idle. *Signal Strength* is a measure of signal power at the receiver side. Signal power levels are affected by abnormal interference, e.g., jamming. *Signal-to-Noise Ratio* (SNR) is the ratio of signal and noise power levels. The Signal-to-Jamming Ratio (SJR) is defined analogously. Typically the SNR or SJR can be used to determine the packet error probability, which in turn can be used to determine the PDR.

1.3 Reliability of Safety Applications

The ITS is a critical infrastructure, and any benign or malicious fault could have far-reaching consequences. Thus, reliability, security and survivability are of paramount importance. Failure of DSRC safety applications can have catastrophic consequences, e.g., injury or loss of life. At the core of DSRC safety applications is the reliability of BSMs, as they are the most important messages. Any attack or disruption of BSMs could cause failure of the safety applications.

Whereas standards such as [6] address security mechanisms

like authentication and encryption, they do not address willful disruption of communications due to jamming. Deterring jamming completely is most likely improbable. However, minimizing its impact is achievable. This can be done by having detection mechanisms, which lead to situational-awareness in the presence of the jammer. Once jamming is confidently detected, the dependency on safety applications becomes unwise. Accordingly, our approach suggests jamming detection and consequent transition of the safety applications to a fail-safe mode. This could be achieved by notifying drivers that the applications are temporarily unavailable.

2. RELATED WORK

There are many papers that discuss the topic of jamming detection in wireless networks, including wireless sensor networks (WSN), mobile ad hoc networks (MANET) and 802.11, however little research discusses detection schemes designed specifically for VANETs, which impose different requirements as will be explained in Subsection 2.2. Besides their application domain, e.g., WSN, MANET or VANET, research efforts can be partitioned into jamming prevention and jamming detection. A general overview of jamming attacks in wireless networks based on jamming prevention and jamming detection is given in [5].

2.1 General Wireless Networks

Prevention:

Some typical mechanisms for jamming prevention are Frequency Hopping, Channel Surfing, Spread Spectrum, and Spatial Retreats [7, 8]. Frequency Hopping, Channel Surfing, and Spread Spectrum operate at the physical layer and are not effective in VANETs, because the channels are preassigned and fixed in their spectrum, according to standard [9]. Any modifications would imply deviating from the standards. Spatial retreat helps mitigate jamming by moving nodes outside the affected area. However, in VANET this is generally not applicable as the geometry of the roads are fixed. Diverting traffic to use other roads is at a much higher level of granularity.

Other research uses directional antennas [10], or coding such as Low Density Parity Check (LDPC) [11], or redundant encoding [12]. Directional antennas take advantage of sectored or smart antennas, which produces more focused beams between transmitter and receiver. This will increase the antenna gain and potentially overpower jamming signals. However, in VANETs antennas are omni-directional [2], uniformly emitting power in all directions to broadcast to surrounding vehicles.

Detection:

Jamming detection methods vary according to the different types of jammers, e.g., constant, deceptive, reactive, random and intelligent. Some of these methods depend on metrics such as Signal Strength, Carrier Sensing Time or Packet Delivery Ratio, which may be measured or averaged from the network over time. Jamming is detected once a significant deviation from normal behavior is sensed. A single metric is not enough to confidently differentiate jamming situations from other normal situations, where deviations in performance could be due to network conditions such as congestion or failure at the sender side [4]. Thus, to increase the jamming detection probability, [4] proposed schemes that combine metrics, namely by combining signal strength with packet delivery ratio, or combining location information with the packet delivery ratio. These two methods were used in consistency checks, and effectively increased the probability for detecting the presence of a jammer. Whereas this work addresses general wireless networks, the overall idea also applies to VANETS. We will leverage this general strategy in our jamming-aware algorithm by also using multiple metrics.

In [13] an approach was presented where individual nodes maintained lists of observed communication behavior. These lists were consequently exchanged with neighboring nodes in order to determine abnormal behavior, e.g., jamming. However, such an approach is not suitable in the fast-changing topology of VANET. In fact, any detection mechanism intended for VANET needs to 1) adapt quickly to topology changes, and 2) detect jamming in a timely manner. These two requirements eliminate detection methods that require multi-hop data exchanges among nodes.

2.2 Related VANET Research

The impact of jamming on DSRC has been investigated at different levels. Since our interest is in DSRC safety applications, we focus our attention at the safety application level. Specifically, we focus on solutions that conform to the existing standards, rather than consider mechanisms that go beyond these standards. Diverse solutions are proposed in the literature. In [14] the impact of constant, random, and intelligent jamming on DSRC safety applications is shown for homogeneous channel behavior, where signal-to-jamming ratios were the basis for packet error probabilities. Different redundancy schemes are introduced in an attempt to increase resilience against jamming. This is extended in [15] to consider the impact of jamming on different data, and the effect of channel power in [16]. While these approaches appear to be effective, the redundancy consumes additional bandwidth, thereby limiting use by other DSRC applications. Furthermore, the research did not not deal with challenges such as MAC layer efficiency, processor utilization, channel congestion and fail-safe operation of the safety applications.

In [17], the authors demonstrate that constant, periodic and reactive jamming could cover certain areas in which its effect is temporary and vanishes as vehicles traverse through the plagued region. Once jamming levels reach certain thresholds, communication is no longer possible. This implies that jamming-unaware applications will not work anymore once certain jamming thresholds are exceeded. It is therefore crucial to have efficient jamming detection, e.g., a jamming state. This makes it possible to switch the safety application to a fail-safe state. Alternatively, a more refined state model may be used, allowing different states, based on the severity or possible impact of jamming, e.g., considering the criticality of the safety applications.

A solution for VANET based on Correlation Coefficient, by measuring dependance among periods of error and correct reception times, is proposed in [18]. The method only considers reactive jamming, i.e., the jammer transmits only after sensing legitimate activity. The approach uses only the

Error Probability as a metric, which is not sufficient to conclude jamming [4].

Jamming in platoons is addressed in [19], where a simple algorithm for real-time detection in VANET based on so-called beacons is given. However, this approach is for the specific case of platoons of vehicles only.

The authors in [20] propose a solution to detect jamming based on the PDR and its rate of change. However, depending on PDR alone is not sufficient as the change in PDR can be a result of factors other than jamming, e.g., poor link quality due to large distance between sender and receiver [4].

In [21] it is argued that detection methods that depend on metrics such as Received Signal Strength Indicator (RSSI), relative position, or PDR, could reveal the presence of jamming as long as there are messages being received. Thus, when the PDR drops to 0% these metrics may no longer be available. Hence, jamming detection strategies that depend on receiving these metrics may simply fail.

To counter this effect, our proposed solution uses path prediction to infer future locations using messages received prior to entering a jammed zone. Thus it can estimate future distances and PDR based on normal, prior, behavior as will be explained next.

3. DESIGN CONCEPTS

Jamming detection, which will be the basis of the proposed jamming-aware algorithm, is based on the concept of consistency checks of relevant metrics [4]. By combining several metrics, the efficiency of detecting jamming increases. The detection algorithm leverages the use of two metrics, i.e., distance and PDR, which can be derived from information available in BSMs. The distance metric reveals important information regarding the expected link quality. In the case of jamming, when no BSMs are received, the distance is no longer available. Thus, the jamming-aware algorithm uses path prediction. In our algorithm, PDR is used to represent link quality.

The new jamming-aware algorithm is based on the concept of consistency check [4]. Consistency checks using several metrics provide higher detection probability than detection schemes that depend only on one metric. The diversity of the selected metrics helps differentiate between jamming and deteriorating communication due to benign effects such as signal fading. Our consistency checks use PDR and the distance between RV and HV, based on GPS coordinates embedded within the BSMs. We extend the principle of consistency check by incorporating path prediction based on prior received GPS coordinates. Prediction is important when vehicles travel inside a jammed zone, as they will no longer be able to communicate via BSMs. In this case the HV will no longer receive location data from the RV.

3.1 Location Prediction

Prediction is explained in Figure 3, where we assume both vehicles equipped with On-Board Units (OBUs) are traveling in a single lane. In normal operational conditions, when no jamming is present, the HV receives a BSM from the RV

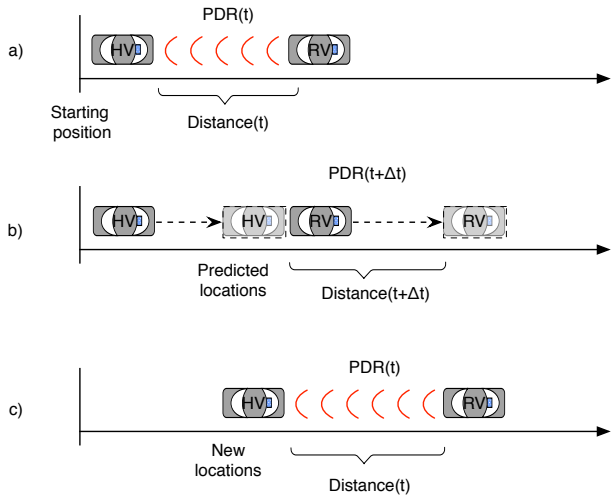

Figure 3: Jamming-aware scenario

at time t, which contains information such as vehicle ID, type, location, speed, heading, and acceleration. Each received message reflects the status of the RV at the time the message was generated. The HV also generates a similar set of information regarding its current status. Thus, the HV will be able to calculate the current distance, $Distance(t)$. In addition, each received BSM will contribute to the calculation of the $PDR(t)$. This is shown in Figure 3a.

The HV will be able to estimate the future distance between both vehicles and the expected PDR, i.e., $Distance(t + \Delta t)$ and $PDR(t + \Delta t)$, shown in Figure 3b. As time progresses, the two vehicles will relocate, as shown in Figure 3c, and new BSMs will be sent from the RV inferring actual movement. The estimated values can be compared against the actual values, and any discrepancies reveal abnormality. The actual path prediction is described in Annex C-8 of SAE J2735 Standard [3].

3.2 PDR Estimation

PDR estimation is the second metric for consistency checks. For simplicity, a line-of-sight link budget can be used to estimate the link quality. The major losses result from free space path loss, which can be quantified as

$$FSPL_{dB} = 10 \log_{10} \left(\frac{4\pi df}{c} \right)^2 \quad (1)$$

where $FSPL_{dB}$ is the free space path loss in dB, d is the distance between the transmitter and receiver in meters, f is the channel frequency in Hz, and c is the speed of light [22].

The received power can be expressed as the difference between gains and losses

$$P_{RX} = P_{TX} + G_{TX} + G_{RX} - FSPL_{dB} \quad (2)$$

where P_{RX} is received power in dBm, P_{TX} is the transmitter output power in dBm, G_{TX} is the transmitter antenna gain in dBi, and G_{RX} is the receiver antenna gain in dBi [22].

The signal-to-noise ratio is then calculated by

$$SNR_{dB} = 10log_{10}\frac{P_{signal}}{P_{noise}} = P_{RX} - P_{noise} \quad (3)$$

where SNR is the signal-to-noise ratio in dB, and P_{noise} is the noise power in dB.

Considering that DSRC uses Phase Shift Keying (PSK), we obtain the energy per bit and the Bit Error Rate (BER) for both 3 Mbps and 6 Mbps as

$$\frac{E_b}{N_0} = SNR \times \frac{B}{R} \quad (4)$$

where E_b/N_0 is the energy per bit to noise power spectral density ratio, B is the channel bandwidth in Hz, and R is the data rate in $bits/s$ [22]. The BER is now computed by

$$BER = \frac{1}{2}erfc\left(\sqrt{\frac{E_b}{N_0}}\right) \quad (5)$$

where *erfc* is the complementary error function.

Finally, the packet error rate is

$$P_p = 1 - (1 - BER)^N \quad (6)$$

where N is the packet length in bits. The PDR follows directly from the P_p.

4. JAMMING-AWARE ALGORITHM

The jamming-aware algorithm shown in Figure 4 is executed on all vehicles, but is described here from the viewpoint of the HV. The algorithm contains a flag, initialized to $flag = 0$, that helps determine its state. Starting at time t equal to the current time, if no BSM message is received during a time interval Δt, the algorithm updates $t = t + \Delta t$ and starts over. In case a BSM message is received during Δt, it updates the status of the RV. This status consists of information contained in the received BSM, most importantly the RV's location (latitude, longitude and elevation), speed and heading. Given this location information, the distance between the two vehicles is calculated. Furthermore the PDR is determined. This is possible since the expected BSM packet rate is known to be 100ms. Thus the PDR is equal to the fraction of BSMs received during a predetermined window. If the value of the flag is not equal to 1, i.e, the flag is 0, the algorithm has received its first BSM from RV and proceeds to predict the future $Distance(t+\Delta t)$, and $PDR(t + \Delta t)$. It will then update the current time t and change the flag to $flag = 1$, which represents an acknowledgement of the existence of the RV. Then the algorithm proceeds to wait for another BSM.

When a new BSM is received, the new status information as well as the predicted status are available. Since now the flag is 1, the algorithm proceeds to compare the current distance between the RV and HV with the distance calculated from the prediction. If these distances are inconsistent, e.g., the GPS is malfunctioning or malicious data was injected, the system enters a fail-safe mode. Otherwise the algorithm proceeds to the PDR check, comparing the PDR calculated for the window with the predicted PDR. The prediction of the PDR could be based on the expected link quality from Subsection 3.2, or based on previously measured behavior, as will be explained in Section 5. If the calculated PDR is inconsistent with the predicted PDR, jamming is assumed and the system will enter a fail-safe mode. Such inconsistency indicates a significant change in PDR that cannot be the result of normal signal fading. Should both consistency checks pass, the algorithm assumes normal operation, it will set the flag value to 2, and resumes receiving BSMs.

If no new BSM is received after successfully receiving at least one BSM, the algorithm checks to see if the predicted distance is out of range. In this case the RV is out of HV's range and the algorithm starts over. Otherwise we conclude that jamming has occurred and fail-safe mode will be entered.

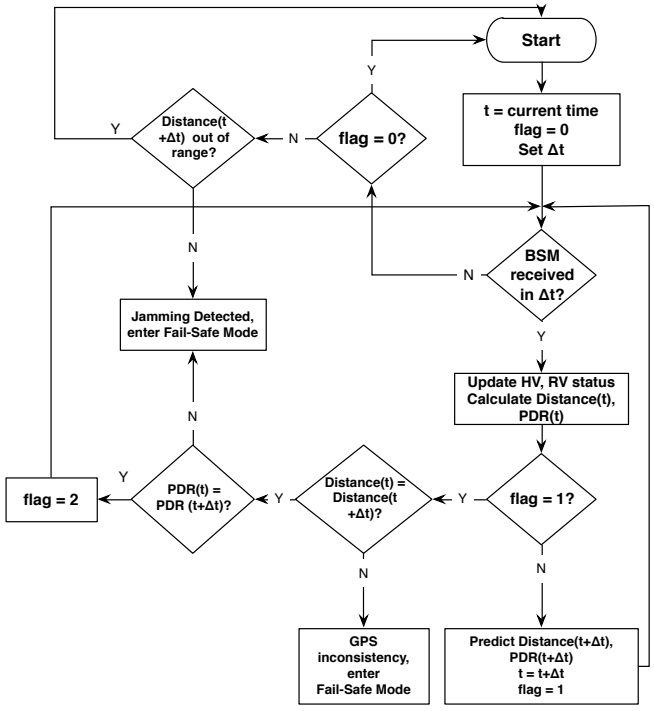

Figure 4: Jamming-aware algorithm

5. PERFORMANCE EVALUATION

The impact of jamming on vehicle communications and the performance of the jamming-aware algorithm were evaluated in a field test. For this purpose an HV and RV were equipped with OBUs, specifically LocoMate Classic OBUs from Arada Systems [23]. An additional LocoMate Classic OBU was configured to be a deceptive jammer capable of operating at different data rates by reprogramming the OBU. Specifically, the jamming OBU sent out a constant stream of bogus packets, violating the distributed coordination function (DCF) of the IEEE 802.11p protocol, which blocked other OBUs from accessing the media. The exact parameters for the field test below are shown in Table 1.

5.1 Normal PDR

The estimates of the PDR of communication between the RV and HV in the absence of jamming is used by the jamming-aware algorithm to predict future behavior. To see how realistic such estimates are, a field test was conducted in open

OBU	Arada Systems LocoMate Classic
Vehicle speed	10 *m/s*
Test range	straight 2-lane road
Test range length	1.35 km
Jammer position	600m from starting point
BSM rate	10 BSM/s (a BSM every 100ms)
Channel	Safety Channel 172
Bandwidth	8.3 MHz
Transmitter power	18 dBm
Data rate	3 and 6 Mbps
Jammer power	18 dBm
Jammer data rates	3, 6, and 12 Mbps

Table 1: Field test parameters

space. Specifically, to obtain the PDR during normal (non-jamming) operation, communication was logged over the entire OBU communication range, where BSMs were collected at the HV as the RV increased its distance. The results of the measured PDR (the field test) and the calculated PDR (see Subsection 3.2) are shown in Figure 5 and Figure 6. One can observe in the figures that the experiment is in line with the calculated estimates.

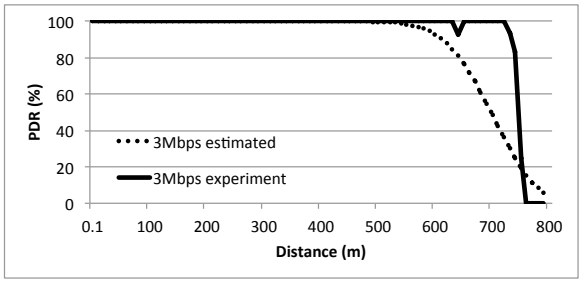

Figure 5: Estimated and actual PDR for 3Mbps

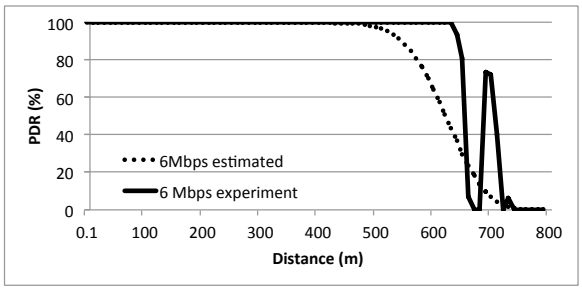

Figure 6: Estimated and actual PDR for 6Mbps

5.2 The Impact of Jamming on PDR

The experiment to measure the impact of jamming on the PDR consisted of two cars (RV followed by the HV) driving on a straight 2-lane road, passing a deceptive jammer located in a parked vehicle on the roadside. During the tests BSMs were logged by the OBU in the HV for data rates of 3 and 6 Mbps as they were subjected to deceptive jamming with rates of 3, 6, and 12 Mbps. It should be noted that data rates of 12 Mbps were shown to be unsuitable for BSM communication in the presence of jamming in [14, 15, 16]. Figure 7 shows the PDR for 3 Mbps BSM communication for different jamming rates for a typical test scenario. As the HV and RV approached the jammer stationed at 600m, the HV could not receive BSMs around 375-425m. The impact of the jammer dropped off at around 750-800m. The transmission rate of the jammer had only modest impact on the PDR. However, for this kind of jammer we could not establish a pattern for these small differences during several experiments.

The result from a typical experiment with a data rate of 6 Mbps is shown in Figure 8. Again the PDR is only modestly affected by the rate of the deceptive jammer. An interesting situation can be seen for the experiment with the 3 Mbps deceptive jammer. Here, after the HV was jammed, it could briefly receive messages from the RV again around 475m. The reason for this was that a small truck passed the test vehicles and positioned itself briefly between the vehicles and the jammer, thus reducing the impact of deceptive jamming.

In summary, the field test revealed that the data rates of the deceptive jammer only modestly affected transmissions. The same could be observed over different tests about how transmissions of different data rates were affected. Whereas the overall impact of jamming was very high, we could not establish a clear pattern in the differences of the impact for different data rates of the jammer and vehicles. This is in contrast to constant jamming, where the impact of jamming drastically decreases PDRs for higher data rates [14].

5.3 Jamming-aware Algorithm Evaluation

The results from the evaluation of the jamming-aware algorithm for the 3Mbps field test data of the previous subsection are shown in Figure 9. The algorithm successfully detected jamming once the PDR drop was detected by the consistency check based on distance and PDR. No inconsistency of distances were observed by the algorithm. Thus, in this specific field experiment only one of the two detection mechanisms was sufficient, as no GPS inconsistencies were injected. However, the PDR inconsistency was detected.

6. CONCLUSIONS

This paper addressed jamming detection as a method to guide DSRC safety applications to a fail-safe mode. A new jamming-aware detection algorithm was introduced that uses two different types of metrics, i.e., distance between vehicles and PDR. Furthermore, the algorithm uses predictions for distances and PDR when real information is not available due to jamming of the BSMs. The jamming model used was the deceptive jammer, and the impact of this jammer type on BSM reception was studied.

Field tests using vehicles equipped with Arada LocoMate OBUs revealed that disruption of BSMs by deceptive jammers was significant. However, different data rates of the deceptive jammer did not change the observed PDRs of vehicle communication. Furthermore, there were no significant differences of PDR between 3 and 6 Mbps data rates of the BSMs.

As jamming cannot be avoided, the jamming-aware algorithm used two metrics, each of which were observed and

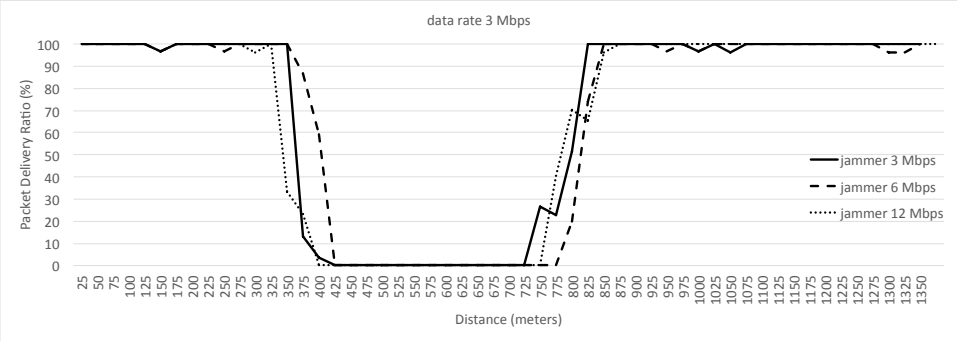

Figure 7: PDR at 3 Mbps with deceptive jamming

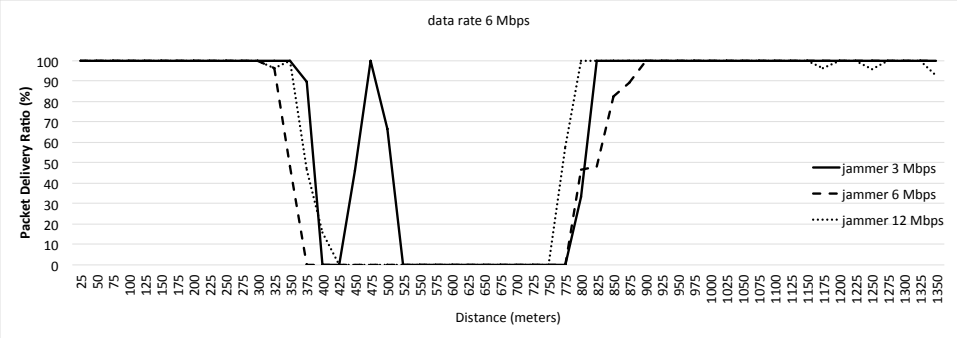

Figure 8: PDR at 6 Mbps with deceptive jamming

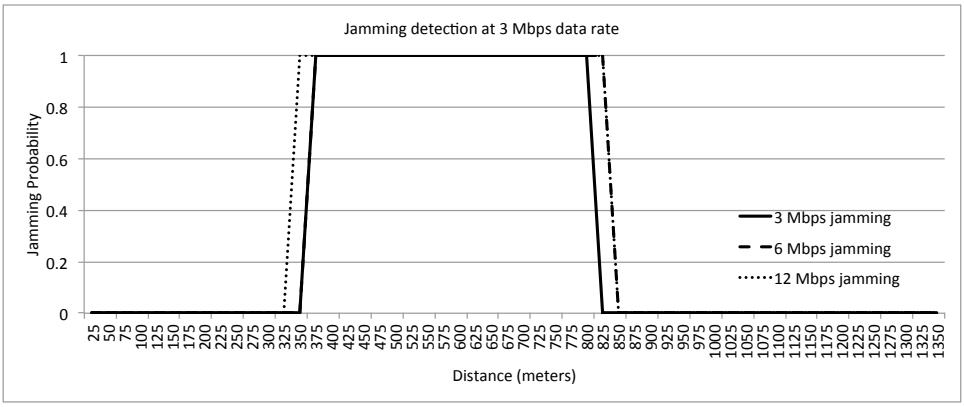

Figure 9: Evaluation of jamming-aware algorithm for 3 Mbps data rate

additionally predicted, to achieve detection of jamming. The field-test data demonstrated that the jamming-aware algorithm is capable of shifting DSRC safety applications to a fail-safe mode when jamming is detected.

7. ACKNOWLEDGEMENTS

We would like to thank Vinay Thadani and Nazeer Shaik from Arada Systems for their assistance and jammer programming. Furthermore we would like to thank Sanjeev Shrestha, Anirudh Bhandari, and Dan Pierce for their help conducting the field experiments.

8. REFERENCES

[1] Kenney, J. B. Dedicated short-range communications (DSRC) standards in the United States. In *Proc. of the IEEE*, vol. 99, no. 7, pp. 1162-1182, 2011.

[2] *Vehicle safety communications-applications (VSC-A) final report*, DOT HS 811 492 A. U.S. Department of Transportation, NHTSA. September 2011.

[3] *Dedicated Short Range Communications (DSRC) Message Set Dictionary. Society of Automotive Engineers*, SAE J2735, November 2009.

[4] Xu, W., Trappe, W. Zhang, Y. and Wood, T. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proc. of the 6th ACM international symposium on Mobile ad hoc networking and computing*, (MobiHoc '05). ACM, New York, NY, USA, 46-57, 2005.

[5] Pelechrinis, K., Iliofotou, M. and Krishnamurthy, S.V. Denial of service attacks in wireless networks: the case of jammers. In *Communications Surveys & Tutorials*, IEEE , vol.13, no.2, pp.245,257, Second Quarter 2011.

[6] *IEEE standard for wireless access in vehicular environments - security services for applications and management messages*, IEEE Std 1609.2TM, 2013.

[7] Xu, W., Ma, K. Trappe, W. and Zhang, Y. Jamming sensor networks: attacks and defense strategies. In *IEEE Network 20*, no. 3, 41-47, 2006.

[8] Xu, Wenyuan, et al. Channel surfing and spatial retreats: defenses against wireless denial of service. In *Proc. of the 3rd ACM workshop on Wireless security*, ACM, 2004.

[9] *Standard specification for telecommunications and information exchange between roadside and vehicle systems - 5 GHz band dedicated short range communications (DSRC) medium access control (MAC) and physical layer (PHY) specifications*, ASTM E2213-03, 2010.

[10] Noubir, G. On connectivity in ad hoc networks under jamming using directional antennas and mobility. In *Technical Report*, Dec. 2003.

[11] Noubir, G., and Lin, G. Low-power DoS attacks in data wireless LANs and countermeasures. In *ACM SIGMOBILE Mobile Computing and Communications Review 7*, no. 3: 29-30, 2003.

[12] Wood, A., Stankovic, J. A. and Zhou, G. DEEJAM: defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07*, 4th Annual IEEE Communications Society Conference on, pp. 60-69. IEEE, 2007.

[13] Aime, M.D., Calandriello, G. and Lioy, A. A wireless distributed intrusion detection system and a new attack model. In *Proc. 11th Symp. Comput. Commun.*, (ISCC 06), 2006.

[14] Serageldin A., Alturkostani, H. and Krings, A. On the reliability of DSRC safety applications: a case of jamming. In *Proc. International Conference on Connected Vehicles & Expo*, (ICCVE 2013), Dec. 2-6, 2013, Las Vegas, 2013, (6 pages).

[15] Serageldin, A. and Krings, A. The impact of redundancy on DSRC safety application reliability under different data rates. In *Proc. 6th International Conference on New Technologies, Mobility and Security*, (NTMS 2014), Dubai, March 30 - April 2, 2014.

[16] Serageldin, A. and Krings, A. The impact of dissimilarity and redundancy on the reliability of DSRC safety applications. In *Proc. 10th International Symposium on Frontiers of Information Systems and Network Applications*, (FINA 2014), Victoria, Canada, May 13-16, 2014.

[17] Puñal, O., Aguiar, A. and Gross, J. In VANETs we trust?: characterizing RF jamming in vehicular networks. In *Proc. 9th ACM international workshop on Vehicular inter-networking, systems, and applications*, pp. 83-92. ACM, 2012.

[18] Hamieh, A., Ben-othman, J. and Mokdad, L. Detection of radio interference attacks in VANET. In *Global Telecommunications Conference, 2009. GLOBECOM 2009, IEEE*, vol., no., pp.1,5, Nov. 30 2009-Dec. 4 2009.

[19] Lyamin, N., Vinel, A., Jonsson, M. and Loo, J. Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks. In *Communications Letters, IEEE*, vol.18, no.1, pp.110,113, January 2014.

[20] Nguyen, A.T., Mokdad, L., and Ben Othman, J. Solution of detecting jamming attacks in vehicle ad hoc networks. In *Proc. of the 16th ACM international conference on Modeling, analysis & simulation of wireless and mobile systems (MSWiM '13)*, ACM, New York, NY, USA, 405-410, 2013.

[21] Puñnal, O., Pereira, C., Aguiar, A. and Gross, J. Experimental characterization and modeling of RF jamming attacks on VANETs. In *IEEE Transactions on Vehicular Technology*, vol.64, no.2, pp.524-540, Feb. 2015.

[22] Sklar, B. *Digital Communications: Fundamentals and Applications*, 2nd Edition, Prentice Hall PTR, 2001.

[23] Arada Systems, www.aradasystems.com