Reduction Jammer Detection and Recovery Algorithms for DSRC Safety Application in VANET

Ayoob Aziz [1], Ghaith Khalil [2] * and Zozan Ayoub [3]

[1]Information & Telecommunication Public Company (ITPC), Iraqi Ministry of Communications, Nineveh, Iraq; ayoobayoob@yahoo.com

[2]Faculty of Engineering and Information Technology, University of Melbourne, VIC, Australia; ghkhalil1976@gmail.com

[3]Computer Engineering Department, College of Engineering, University of Mosul, Iraq; zozanazeez1@yahoo.com

*****Correspondence: ghkhalil1976@gmail.com

Abstract: Intelligent Transportation Systems (ITS) encompasses technologies, services, and applications facilitating communication between vehicles (V2V) and between vehicles and fixed infrastructure (V2I and I2V). This mutual interaction constitutes a Vehicular Ad-Hoc Network (VANET) which supports a plethora of applications targeting critical transportation aspects, such as safety, mobility, and environmental considerations. Dedicated Short Range Communications (DSRC), operating on the 5.9 GHz band, is pivotal for such exchanges. We introduced an innovative algorithm designed to identify jamming attacks and transition the Safety Application to a secure fail-safe mode. This algorithm leverages a dual-metric strategy, incorporating both distance and PDR measurements. Field tests confirm that our algorithm adeptly recognizes the activities of deceptive jammers, ensuring a prompt shift of the safety application into its fail-safe state. This paper delves into these countermeasures, evaluating their efficiency via mathematical modeling, simulations, and on-ground testing. Findings acknowledge that these strategies bolster the reliability of safety applications in jamming scenarios. Furthermore, the approaches propounded align with ongoing standardization endeavors by relevant authorities, ensuring communication mediums remain unhindered.

Keywords: Vehicular Networks; Jammer recovery; DSRC; VANET

1. Introduction

The National Highway Traffic Safety Administration (NHTSA) reported 6.1 million crashes in 2014, resulting in 32,675 deaths and 2.3 million injuries in the U.S[1] . Both government entities and car manufacturers have taken steps to decrease these numbers, implementing stringent regulations and leveraging the latest technologies to boost safety.

Intelligent Transportation Systems (ITS) offer a range of beneficial applications, with Safety Applications standing out as crucial for preventing collisions and enhancing driver awareness. The U.S. Department of Transportation (USDOT) estimates that Vehicle-to-Vehicle (V2V) systems using Dedicated Short Range Communications (DSRC) can mitigate up to 82% of accidents involving alert drivers in the U.S, potentially saving countless lives and significant economic costs [2]. These Safety Applications hinge on the consistent exchange of Basic Safety Messages (BSM) between vehicles and infrastructure. Effective communication requires a robust technological foundation to ensure the system's secure, consistent, and reliable operation. This article delves into the reliability of Safety Applications within ITS, given the critical nature of such infrastructure. However, the wireless communication central to this tech comes with its own set of potential vulnerabilities. Any lapse can lead to severe repercussions, including injury or loss of life. This study, in particular, examines how to counter wireless jamming in Vehicle Ad-hoc Networks (VANETs), as such interference can incapacitate Safety Applications.

Indeed, jamming can distort safety applications, possibly causing them to make incorrect decisions, heightening risks. Any breaches, whether unintentional or malicious, risk eroding public confidence in DSRC-driven VANET technologies. Traditional security approaches like digital certificates, tamper-resistant hardware, and network

security protocols fall short[3]. Hence, it's essential to integrate mechanisms that enhance reliability amidst faults directly into the system instead of merely attaching them as afterthoughts.
VANETs hold the promise to introduce a variety of applications that could significantly decrease traffic mishaps, enhance transportation fluidity, and optimize fuel consumption. Yet, several obstacles need to be overcome before these applications become a reality. This section delves into challenges closely linked to our research, especially those concerning VANET security and reliability. Ensuring the security of VANET communications and applications is pivotal. The absence of robust security, deployment of unsuitable methods, or the detrimental impacts of targeted attacks can lead to severe repercussions. Such vulnerabilities might encourage self-centered behavior or, in extreme cases, deliberate disruptions aimed at causing accidents[4]

This study contributes to the body of knowledge by presenting a jamming detection algorithm designed to transition DSRC Safety Applications to a secure fail-safe mode. The work will focus on understanding the influence of "deceptive jammers" on the reception of Basic Safety Messages (BSM). The algorithm employs two metrics: vehicle distance and Packet Delivery Ratio (PDR). When real-time information is inaccessible due to BSM jamming, it resorts to predictions for these metrics. Field tests revealed a notable disruption of BSMs by deceptive jammers. Importantly, the algorithm proves effective in guiding DSRC Safety Applications to a fail-safe state upon detecting jamming[5].

We also introduce a recovery strategy that ramps up BSM rates and tweaks transmission power and data rates but only when jamming is identified. This strategy explores the balance between channel efficiency and dependability, considering excessive retransmissions that can overwhelm the network. The data confirms this recovery approach aids safety applications in swiftly reverting from fail-safe to functional mode against multiple jammer types. In scenarios demanding utmost safety, this can be pivotal for preventing accidents and preserving live[6].
The motivation of this study was established to improve the safety measures in Intelligent Transportation Systems (ITS) by enhancing and reduce the jammer detection and recovery algorithms for Dedicated Short-Range Communications (DSRC) in Vehicular Ad-Hoc Network (VANET). In the next section two we will examined the most recent related work which is similar to our work in the literature before we explain the classification of jamming attacks in section 3.

2. Related Work

To overcome the impact of jamming, an approach of message and channel redundancy has been demonstrated in [7] for the case of constant, random and intelligent jamming. This approach implies using alternative messages, namely the À la Carte (ACM) and Probe Vehicle Data (PVD) to deliver safety related data using redundant channels. These messages were defined in SAE J2735 [8] and they facilitate Basic Safety Message (BSM) functional redundancy, i.e., communicating the BSM-relevant data on any service channel. In addition, these messages can be used along with the BSMs in a dual and triple redundancy scheme.

The redundant channels were carefully selected to ensure wide separation in the frequency spectrum. While this approach was shown to be effective, using redundancy imposes extra overhead/usage of the dedicated limited bandwidth, which is intended to be used by multiple DSRC applications. Furthermore, [9] has not dealt with the challenges such as MAC layer efficiency, the channel congestion as fail-safe operation of the security Applications.

A solution for VANET based on coefficient of correlation that is activity accordant for Between periods of error and therefore the correct of reception times, Hamieh projected [8]. The method solely depend upon reactive electronic jamming attacked and the transmitter transmits solely once sensing legitimate space activity that The approach is barely uses the Error chance like a metric, that isn't enough to incorporate electronic jamming [10] and the Jamming electronic in platoons is addressed on[11], The method alone rely on reactive ECM attacked and the transmitter transmits alone once sensing legitimate area activity that The approach is barely uses the Error likelihood sort of a metric, that may not enough to include ECM [12]. which gift an answer to notice electronic jamming by depend upon the packed delivery magnitude relation PDR and its rate of fixing . However, supported packed delivery magnitude relation PDR alone is not enough with the amendment of PDR it is often a resolve factors than alternative electronic jamming like poor link quality as a result of the massive of distance between the sender and also the receiver.

The À la Carte (ACM) and Probe Vehicle Data (PVD) systems are designed to transmit safety-related data using multiple backup channels. These message frameworks, as outlined in SAE J2735[13] , enable BSM functional redundancy, meaning they can relay BSM-pertinent information across any designated service channel. Moreover, these messages can function in conjunction with BSMs, providing dual or even triple layers of redundancy. The backup channels were meticulously chosen to guarantee a broad frequency spectrum separation.

Although this method proved effective, the inclusion of redundancy does bring its own challenges, especially concerning the potential strain on the restricted bandwidth reserved for various DSRC applications. In addition, studies [14] didn't address certain issues, such as MAC layer efficiency, potential channel congestion, and the ensured fail-safe operation of the Safety Applications.

[15] had argued that the detection ways rely upon the metrics such like (RSSI) Received Signal Strength Indicator that relative position packed delivery quantitative relation PDR may be reveal of presence the jam as way as their messages have been received. this metric could it not be accessible and there for jam electronic measures |ECM} detection methods that dependence on receiving this metric could as merely fail and to counter for this effective therefore in our propose answer it uses a path prediction to seem future locations prediction by exploitation the messages received before build coming into a jamming space.

In , [16] that continuous and periodic electronic jamming and reaction detective which might cowl to sure zone that would result in temporary and vanishes as cars traverse through the infested zone region. Once the electronic jamming affects reach to sure thresholds thus, the communication isn't any longer chance. This might imply that jamming electronic measures ECM detection applications won't happen any longer once within the sure jamming thresholds that exceeded. But crucial to own economical electronic jamming detection, like electronic jamming state thus, this may make it attainable to modify the security Application to maneuver to a fail-safe state. As an alternative, a lot of refined state model could also be permitting in several states, rely upon the severity or attainable result of electronic jamming, as considering the criticality for the security Applications. The answer for VANET relies on the Correlation of constant that activity dependence among several amounts of the error and proper reception in period times, that projected in[17].

This methodology considers the reactive ECM that the transmitter transmits when sensing legitimate o activity. The approach uses solely the Error likelihood as a metrics, that's not enough to conclude ECM [18]. jamming within the units is proposed in [19], which an easy formula model for in period detection in VANET rely on supposed beacons is given. As well as this approach is for specific cases of platoons of cars solely. The authors in [20] present an answer to notice the ECM depend upon the packed delivery quantitative relation PDR and the rates of fixing that it bases on PDR alone isn't enough as modification in packed PDR that may be resolve of things in others than jamming, and the poor link quality thanks to giant distance between receiver and sender [21]. [13] argued that detection electronic jamming ways base on metrics such like (RSSI) Received Signal Strength Indicator are relative positions furthermore as PDR, might reveal of the presence electronic jamming as way as their messages that being received. So, once the PDR drops to 1/3 this metric might not be longer be obtainable and there the electronic jamming detection ways base on receiving this metric it's going to be merely fail. On the other hand, solutions for Broadcast Base Safety Message BSM Through VANET Based on Transmit Packet Coding (TPC) was introduced in[22] and IDS or intrusion detection system classifier for VANET introduced in[23] and [24] with a brief explanation and did not covered Jamming attack thoroughly.

3. Classification of jamming Attacks

Interference attacks on Ad Hoc networks can be categorized in various ways. Based on the widely accepted classifications by researchers [25], they can be detailed as:

Constant Jamming: This attack sees the intruder ceaselessly emitting random radio signals over the communication channel, neglecting the MAC protocol. Consequently, valid users mistakenly perceive the channel as occupied when it's available.

Deceptive Jamming: This type of interference, unlike persistent ECM attacks, involves attackers not merely sending random bit sequences but transmitting semi-coherent information packets. The header of these packets appears valid, but the data they carry is essentially worthless. Such deceptive maneuvers often make channels appear perpetually engaged to genuine users, severely hampering authentic communication.

Random Jamming: This strategy is less power-consuming than the two mentioned before. Attackers using random jamming alternate between periods of active interference (attack mode) and non-interference (sleep mode). The energy used up in the attack corresponds to the ratio of these two modes. This method gives a clear perspective on how random jamming attacks function and their energy dynamics.

Reactive Jamming: Here, the attacker springs into action, jamming only when they identify an ongoing communication within the network. They prioritize jamming the receiver rather than the transmitter, ensuring minimal resource expenditure. In vehicular networks, this usually takes the form of nodes emitting potent disruptive signals, drowning out legitimate communications. This results in receivers either failing to capture signals or experiencing drastic reductions in reception quality, categorizing this as a predominant form of direct interference attack.

4. Jamming Detection and Description Scenario

4.1. Predication Location

Figure 1 supports the assumption that each vehicle equipped with an On-Board Unit (OBU) occupies one lane under normal operating conditions without electronic jamming. At time t, the Host Vehicle (HV) receives a Basic Safety Message (BSM) from the Remote Vehicle (RV) containing information such as vehicle ID, location, type, heading,

speed, and acceleration. The HV generates the same set of information about its own status. Using this information, the HV can calculate the current distance (Distance (t)) between the two vehicles and the Packet Delivery Ratio (PDR) at time t (PDR (t)), as shown in Figure 1a. As time passes, the vehicles move, and new BSMs from the RV provide updated information on its actual movement. The HV can use this information to predict the future distance between the two vehicles and the corresponding PDR values at time t+Δt, as shown in Figure 1b. As time passes, the two vehicles will move to different locations, as depicted in Figure 4.1c. Consequently, new Basic Safety Messages (BSMs) will be transmitted from the Reference Vehicle (RV) to indicate the actual movement. By comparing the estimated values with the actual values derived from these BSMs, any inconsistencies can be identified, indicating abnormal behavior.

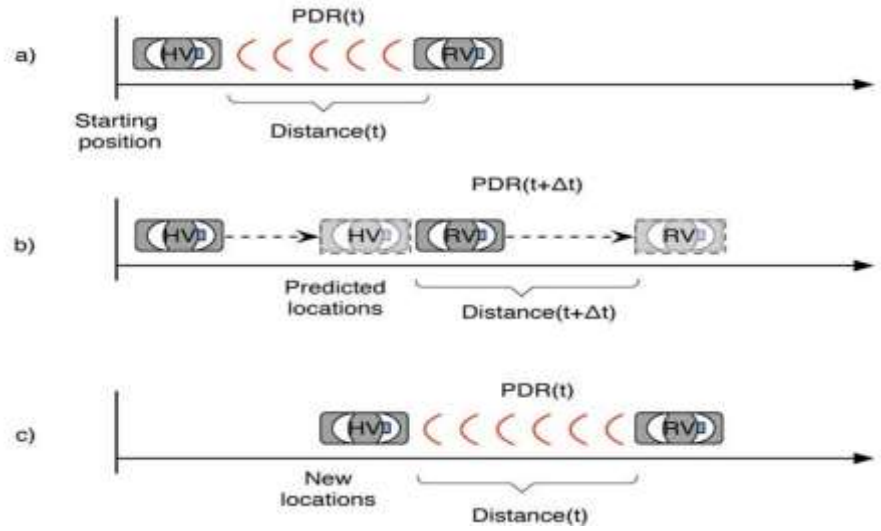


Figure1. Jamming Detection Scenario

PDR Evaluation

The Packet Delivery Ratio (PDR) is analyzed as a secondary metric for consistency checks. In order to simplify the process, a line-of-sight link budget is utilized for estimating the link quality. The main factor that causes losses in the signal is the free space path loss.

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

FSPLdB represents the free space path loss in decibels, while d represents the distance between the receiver and transmitter in meters, f represents the frequency of the channel in hertz, and c represents the speed of light [20]. The received power can be expressed as the difference between the gains and losses.

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

The received power is denoted by P_RX in dBm, while PTX represents the transmitter output power in dBm, GTX represents the transmitter antenna gain in dBi, and GRX represents the receiving antenna gain in dBi [20]. To calculate the ratio of signal-to-noise, we can use the following equation:

SNR = (P_RX - PTX + GTX + GRX) - N

So, the calculate ratio of signal-to-noise can be represent by

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

The signal-to-noise ratio (SNR) for signal r in dB is denoted as SNR_db, while P_noise represents the power of the noise in dB. DSRC uses Phase Shift Keying (PSK), which enables the calculation of energy per bit and the Bit Error Rate (BER) at both 3 Mbps and 6 Mbps. The equation for this is shown below:

BER = 0.5 * erfc(sqrt(0.5 * (Eb/N0)))

Where Eb/N0 represents the energy per bit to noise power spectral density ratio.

$$\frac{E_b}{N_0} = SNR \times \frac{B}{R}$$

(4)

The energy per bit to the noise power spectral density ratio is represented as Eb/N0, where B is the channel capacity bandwidth in Hz, and R represents the data rate in bits per second [20]. The Bit Error Rate (BER) can be calculated as follows:

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

(5)

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

Where N is length of the packed in bits and the PDR follows directly from the Pp.

Model designed to detect jamming attacks on VANETs.

To describe the operation of a jamming attack detection model, shown in Figure 2, in a VANET from the perspective of the Host Vehicle (HV). The algorithm model is triggered at time t if no BSM messages have been received during

a time interval of Δt. When a BSM message is received within this interval, the status of the Remote Vehicle (RV) is updated with details such as the RV's location, speed, heading, and distance from the HV. The Packet Delivery Ratio (PDR) is also calculated based on the predicted packet rate of BSM, which is assumed to be 100ms. The PDR indicates the fraction of BSMs received during the designated time interval. If the flag value is not 1, the algorithm model has received its first BSM packet from the RV, and it will predict future distance (t+Δt) and PDR (t+Δt). The current time t is replaced, and the flag status is set to 1, indicating the RV's existence. The algorithm model continues to wait for additional BSM messages. The algorithm utilizes a flag, initially set to flag=0, to determine its current state. When a new BSM message is received, the flag information is updated, and the expected status becomes available. Once the flag is set to 1, the algorithm compares the current distance between the HV and RV with the distance calculated from the prediction status. If these distances are inconsistent, it may indicate that the GPS is malfunctioning or that the information was injected, and the system enters a fail-safe application mode. In Figure 2, the consistency check is calculated by taking the absolute value of the difference between Distance(t) and Distance(t+Δt), where Distance(t) is the distance measured by GPS coordinates at time t and Distance(t+Δt) is the predicted distance. To account for GPS accuracy deviations, a tolerance factor α is introduced. Additionally, the algorithm performs a PDR check, which calculates the PDR for a window with an estimated PDR, and predicts the PDR based on the predicted link quality or previously measured behavior. If the calculated PDR is inconsistent with the expected PDR, it could indicate jamming, and the system enters fail-safe application mode. The notation used for the calculated versus expected PDR is similar to that used for distances above, i.e., |PDR(t)-PDR(t+Δt)|, where PDR(t) is the calculated PDR at time t=t+Δt, and PDR(t+Δt) is the expected PDR. A tolerance of β is introduced to account for deviations in PDR values. If both consistency checks pass and the algorithm models assume normal operation, the flag value is updated to 2, and the system continues to receive new BSMs. If a new BSM is received, the algorithm performs two checks to determine if the expected distance is out of range. If the RV is out of range, the algorithm starts over. Otherwise, jamming is suspected, and the system enters fail-safe application mode.

The algorithm designed to detect jamming attacks in VANETs operates based on the perspective of the Host Vehicle (HV) and utilizes a series of checks and predictions to identify potential jamming scenarios. Here's a step-by-step breakdown of the algorithm's key operations:

1- Triggering the Algorithm.

The algorithm is triggered at time t if no Basic Safety Message (BSM) messages have been received during a time interval Δt

2- Updating Remote Vehicle (RV) Status.

When a BSM message is received within the interval Δt, the status of the Remote Vehicle (RV) is updated with details such as location, speed, heading, and distance from the HV.

3- Calculating Packet Delivery Ratio (PDR):

The Packet Delivery Ratio (PDR) is calculated based on the predicted packet rate of BSM, assumed to be 100ms. This indicates the fraction of BSMs received during the designated time interval.

4- Flag and Prediction Status:

The algorithm uses a flag, initially set to $f\ lag = 0$ is the algorithm receives its first BSM packet from the RV, predicts future distance (t+Δt) and PDR(t+Δt) update the current time t, and sets $f\ lag = 10$ indicating the RVs existence.

5- Consistency Checks:

The algorithm compares the current distance between the HV and RV with the distance calculate from the prediction statues. inconsistencies may indicate GPS malfunction or injected information,leading to a fail-safe application mode.

Consistency checks for distance: $Distance\ (t) - Distance\ (t + \Delta t\ ) \leq \alpha$

Consistency checks for distance: PDR $PDR - PDR(t) - PDR(t + \Delta t) \leq$ ß

6-Normal Operation:

It both consistency checks pass, the flag value is update to $f\ lag = 2$, indicating normal operation, and the system continues to receive new BSMs.

7-Out-of-Range Checks:

If new BSM is received, the algorithm performs checks to determine if the expected distance is out of range. If the RV is out of range, the algorithm restarts. otherwise, jamming is suspected, and the system enter fail-safe application mode.

In summary, the algorithm monitors BSM message, update the statues of remote vehicles predicts future parameters, and performs consistency checks to identify potential jamming attacks. If inconsistencies are detected, the system enters a fail-safe mode to mitigate the impact of the suspected attack.

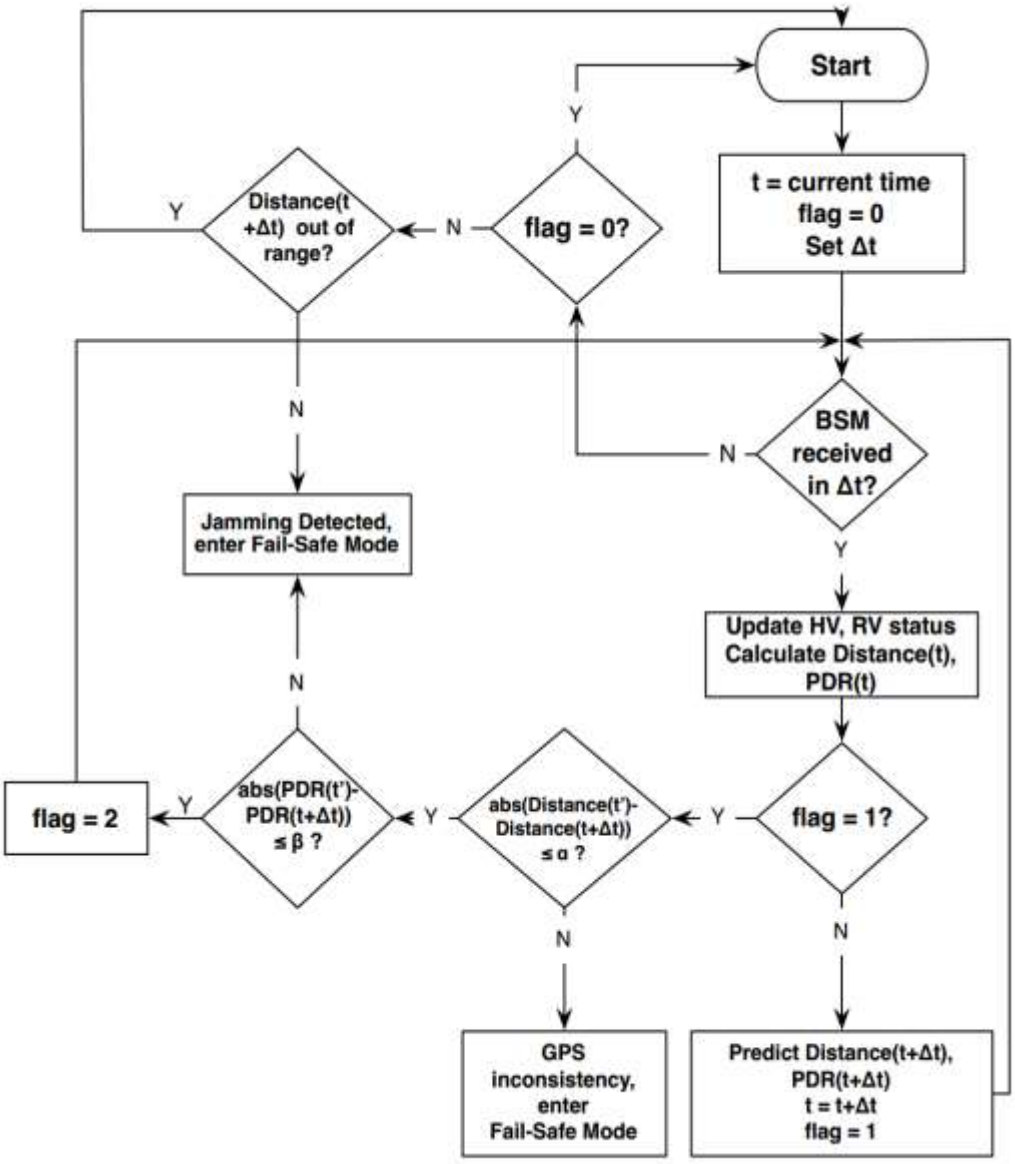


Figure 2. model designed to detect jamming attacks.

Jamming Attack Recovery Algorithm for Dedicated Short-Range Communications (DSRC) Safety Applications in Vehicular Ad-Hoc Networks (VANET).

6.1. Reliability and Redundancy

Figure 3 showcases several vital Safety Applications, which we'll delve into below:

Forward Collision Warning (FCW) – Pictured in Figure 3a, the FCW alerts the driver of the Host Vehicle (HV) about a potential rear-end collision with a Rear Vehicle (RV) ahead, moving in the same lane and direction. This system proves especially valuable when the HV is closing in on a vehicle that's either decelerating or has come to a halt.

Emergency Electronic Brake Lights (EEBL) – As illustrated in Figure 3b, the EEBL is somewhat of a toned-down version of FCW. Upon receiving data that an RV ahead is braking sharply, it prompts the HV driver to slow down. The significance of this feature is amplified when an obstruction (like a big truck) limits the HV driver's view.

Do Not Pass Warning (DNPW) – Depicted in Figure 3 c, DNPW sounds an alert to the HV driver during an overtaking maneuver if there's an incoming vehicle from the opposite direction.

Blind Spot Warning + Lane Change Warning (BSW+LCW) – Demonstrated in Figure 3d, this Safety Application cautions the HV driver wanting to switch lanes if another vehicle—moving in the same direction—is present in their blind spot.

It's imperative to note that the success and reliability of these DSRC Safety Applications are heavily dependent on the Basic Safety Messages (BSM) from the RV. If the HV doesn't receive these messages or they aren't frequent enough, the effectiveness of the application may be compromised.

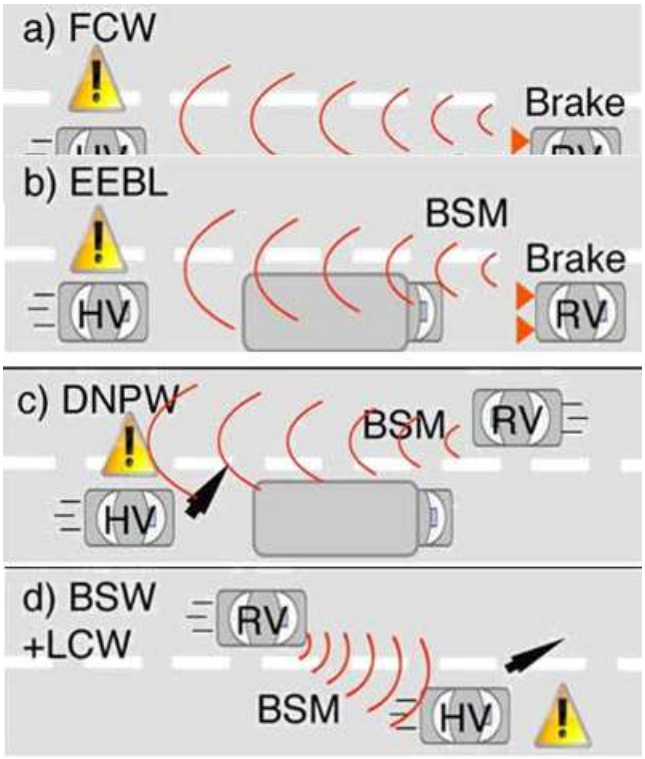


Figure 3. Safety Application Scenarios

Remember that each On-Board Unit (OBU) sends out a Basic Safety Message (BSM) every 100 ms using the safety channel (CH172). This results in a broadcast frequency of 10 BSM/s as referenced in sources [9] and [8]]. Building on this, we're looking into the idea of redundancy by amplifying this message frequency. We're keen to understand its effect on the reliability of Safety Applications and the subsequent overhead. Take, for example, the forward

collision warning system illustrated in Figure 3.a. In this scenario, the rear vehicle (RV) brakes abruptly, possibly to avoid a hurdle. Such abrupt braking will trigger a brake system status notification in the BSM of the RV. From the perspective of the Host Vehicle (HV), this means it should receive at least one BSM reflecting this status update early enough to factor in the driver's reaction time. Consequently, the reliability of the Safety Application can be described as the likelihood of the HV getting a minimum of one BSM notification in time to allow the driver to react, specifically by time t_react.

To harmonize with the conventional definition of reliability – that is, R(t) representing the chance that a system operates as intended throughout a set timeframe [0, t], as mentioned in source[8] – we can define our specific application reliability, R(t)app, as the likelihood of receiving a minimum of one BSM by time t_react. If we label the BSM as BSMi, then it's imperative to receive one of the BSMi, where i ranges from 1 to x, with BSMx being the final BSM before t_react. Hence, the application would only falter if not even one BSM is received by t_react. The metric for unreliability, Q(t)app, can be represented as 1 − R(t)app. This metric essentially gives the probability of not receiving any BSMi within the range of i = 1 to x.

At a regular interval of 100 milliseconds, every On-Board Unit (OBU) transmits a Basic Safety Message (BSM) on the safety channel (CH172), resulting in a message frequency of 10 BSMs per second[26] and [9]. To assess the impact of redundancy on the dependability and overhead of Safety Applications, we increase the BSM message rate. Let us consider the forward collision warning application where the Recreational Vehicle (RV) abruptly applies the brakes to evade an obstacle, resulting in a brake system status alert in the RV's BSM. To inform the driver sufficiently in advance, allowing adequate reaction time, the Host Vehicle (HV) needs to receive at least one BSM containing this status. As a result, the reliability of the Safety Application pertains to the probability of the HV receiving at least one BSM message before the reaction time threshold, i.e., at time t_react.
Following the standard definition of reliability, where R(t) is the probability of the system performing in accordance with the specifications throughout the time interval [0, t] [27], we define our application reliability R(t)app as the probability of receiving at least one BSM message before at time t_react. Assuming the i^th BSM as BSM_i, at least one of the BSM_i, i = 1... X, must be received, where BSM_x refers to the last BSM before at time t_react. Consequently, the application fails only if no BSM message is received before t_react. The unreliability 〖Q(t)〗_(app =1- 〖R(t)〗_app) i.e., the probability of not receiving any BSM_i, i = 1... X, can be expressed as:

$$Q(t)_{app} = \prod_{i=1}^{x} Qi^{(ti)} \qquad (7)$$

Where $Q_i$is the probability that BSM_i was not received at t_i. It should be noted that $Q_{i(t_i)}$is the packet error probability of BSM_i. If N redundant channels are used, then

$Q_N(t)_{app} = \prod_{j=1}^{N} Q_{ci}(t)$ Where $Q_{ci(t)=} \prod_{i=1}^{x} Q_{i(t_i)}$ represents the unreliability for each channel, as Equation .3, introduced in [28], can be used to calculate the Safety Application's unreliability and channel redundancy for a single channel. Increasing the BSM rate has the potential to improve the system's reliability, but the impact depends on the intensity of jamming, as illustrated in Figure 4. If the left region experiences jamming, the jamming detection will activate the Safety Application's fail-safe mode. The right region remains unaffected by jamming. However, the central region is crucial, as increasing the BSM rate can mitigate moderate jamming. This

strategy is not only applicable to the safety channel (CH172) but can also be extended to other channels, such as CH178 using ACM in a dual redundant approach or incorporating CH184 using PVD for a triple redundant scheme.

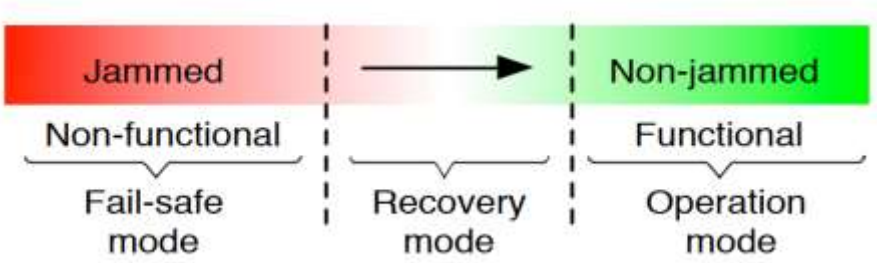


Figure 4. Jamming impact regions.

Effectiveness of various BSM Rates.

The MAC layer can face additional strain with an increase in BSMs due to higher BSM rates, which may lead to a decrease in PDR as a result of collisions. Determining the upper limit of BSM rates is dependent on several critical factors, including the number of vehicles in the vicinity, data rate, and message size. To gain insight into this upper limit, Figure. 5 illustrates the maximum available BSM rates for different data rates and two sample BSM sizes, 300 and 180 Bytes, using a PHY Preamble of 32µs, DIFS of 64µs, and PLCP header of 8µs. For instance, when sending a 300 Bytes message at a data rate of 6Mbps.

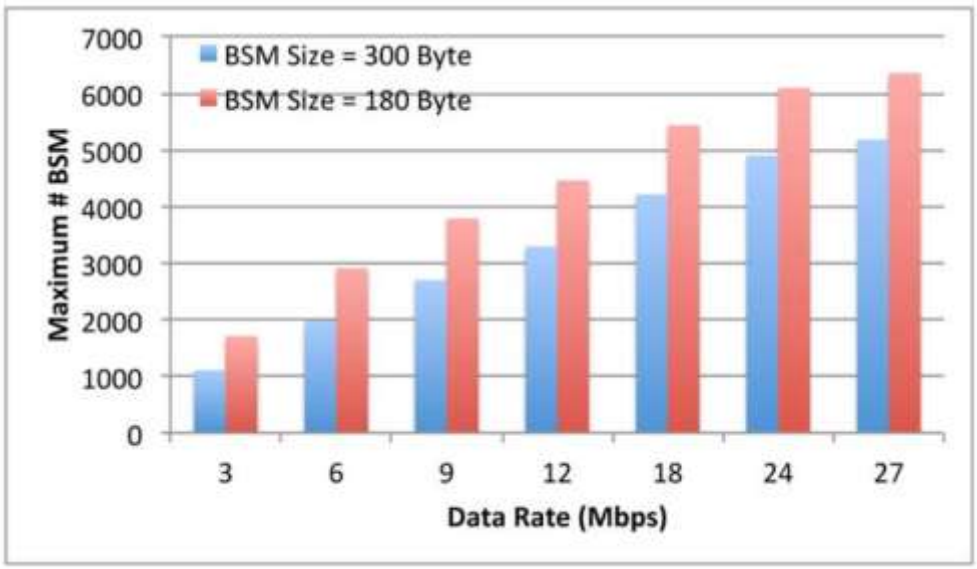


Figure 5. Upper bound on BSM rates for different data rates

transmmision Delay $= \frac{\text{Message Size}}{\text{Data Rate}} = \frac{8\times300}{6000000} - 400\text{Ms}$ And now by adding all delays 32µs + 64µs + 8µs + 400µs, these sums up to a total delay of 504µs per message. As BSM data rates higher than 6Mbps have been shown to be too unreliable in the presence of jamming, the data rates that should be used by DSRC Safety Applications are

3Mbps and 6Mbps [65]. For a 6Mbps data rate, the maximum number of messages the media can handle is 1984 BSM/s for 300 Bytes message size.

This can be calculated considering. The Maximum Throughput $= \frac{\text{Massage Size}}{\text{Totall Delay}} = \frac{2400 \text{ bits}}{504 \text{ Ms}} = 4{,}671{,}904 \text{ bits /}$ Sec.

Thus, when sending a BSM of size 300 Bytes (2400 bits), the total messages that can be handled by the media is $\frac{\text{Maximum Throughput}}{\text{Packet Siz}} = 1984\text{BSM /S}$. Likewise, at 6 Mbps and for a message.

Assuming a message size of 180 bytes, the media can handle a maximum of 2906 BSMs per second. With each vehicle sending 10 BSMs per second, one can estimate the upper limit of vehicles that the media can handle. However, it is important to note that these calculations do not take into account the potential collisions that may occur when multiple vehicles attempt to send BSMs simultaneously. Collisions can lead to packet corruption, bandwidth consumption, and a decrease in PDR, particularly as the number of vehicles increases. It is worth noting that VANET uses the DCF and CSMA/CA protocols of the IEEE 802.11 standard. Despite these considerations, the maximum number of messages shown in Figure. 4 was calculated without accounting for collisions, and it is important to consider the impact of redundant BSMs on the medium in a more realistic scenario.

Collisions in VANETs can occur through direct collisions or hidden terminals. Direct collisions happen when the sender and receiver are within each other's transmission range, and they send messages simultaneously due to similar back-off times. In contrast, hidden terminal collisions occur when three or more nodes are positioned such that the outer nodes are not within each other's transmission range, but they are within the range of the middle node. This leads to more collisions since the outer nodes cannot sense each other's presence, resulting in simultaneous communication with the middle node. To prevent these collisions, wired and wireless networks use several mechanisms, including physical carrier sensing and virtual sensing. Physical carrier sensing involves the sender monitoring the medium and deferring transmission if the medium is busy. Only when the medium is idle, the sender transmits the data frame after a random back-off time to avoid direct collisions with other nodes competing for the medium.

Physical carrier sensing involves monitoring the medium and waiting for an idle period before transmitting data to avoid direct collisions. Virtual sensing, on the other hand, sets a Network Access Vector (NAV) based on Request-to-Send and Clear-to-Send (RTS/CTS) frames. Before transmitting data, a source node sends an RTS and waits for a CTS reply from the destination, and hidden nodes outside the source range can still hear the CTS reply and set their NAV accordingly to reduce collisions in hidden terminal situations. However, virtual sensing is not suitable for safety applications in VANETs, where minimal delay is crucial for broadcasting BSMs to high-speed vehicles. Therefore, hidden terminal situations have a more severe impact on safety applications in VANETs. The impact of transmission collisions on Packet Delivery Ratio (PDR) is studied using the IEEE 802.11p MAC protocol in [29], which measures performance for both hidden and direct collision cases. The average number of vehicles in the transmission range is denoted by N_tr.

$$N_{tr} = 1 + 2\beta R \quad (8)$$

Which β represents the density of vehicle [vehicles/km] and R is transmission range. The queue utilization ρ can be expressed as

$$\rho = \lambda E[S]$$

(9)

Where λ is the packet generation rate [packets/sec] and E[S] is the average of the servant time.
Now let as τ be a probability of that a transmit vehicle in the slot random considering which a packet in a queue,

$$\tau = \frac{1}{\bar{W}+1} \quad (10)$$

Where $\bar{w}$ is the average number of back-off slots. The probability of direct collision P_{dc} is calculated as follows,

$$P_{dc} = (1 - (1 - \rho)(1 - \rho\tau)^{N_{tr}} - 1)$$

(11)

Note that P_b represents the probability that a channel is sensed busy when a new packet arrives,

$$P_b = (N_{tr} - 1)\lambda T(\frac{1-P_{dc}}{2}) \quad (12)$$

Where T is the complete transmission time of a packet including DIFS period.
Finally, the PDR_{dc} for direct collision case is,

$$PDR = 1 - P_{dc} \quad (13)$$

As for the hidden terminal case, let P_{hc} represents the probability of a hidden terminal collision,

$$P_{hc} = 1 - (1 - P_{dc})P(S_1)\,P(S_2) \quad (14)$$

Where, S1 denotes the event where none of the hidden terminals transmit, considering the number of hidden terminals is N_{ph} this probability can be expressed as,

$$P(S_1) = 1 - N_{ph}\lambda T\,(1 - \frac{P_{dc}}{2}) \quad (15)$$

and S_2 denotes the case where a vehicle starts its transmission,

$$(S_2) = e^{-}\lambda N_{ph}(t_{data} - t_{DIFS}) \quad (16)$$

Where, t_{data} is the transmission time for a packet, and t_{DIFS} is the duration of DIFS period.
Finally, the PDR_{hc} for hidden terminal case is expressed as,

$$PDR = 1 - P_{hc} \quad (17)$$

To compute the PDR in direct collision and hidden terminal scenarios, we employ Equations 13 and 17, respectively, using the collision parameters outlined in Table 1. The model used in this study, as presented in, examines Safety Applications for vehicles traveling on a multi-lane highway, where the inter-lane distances are negligible compared to the overall network length.

Table. 1 MAC model parameters

Average number of back-off slots, W	I6
Transmission range, R	6oo m
DIFS time	64 micro s
Data rate	6 Mbps
BSM rates	IO, 2o and 3o BSM/s
BSS size	i8o Bytes
Vehicle density	z-zoo vehicles/km

The impact of direct collisions on the PDR with varying vehicle densities is illustrated in Figure. 6 With an increase in vehicle density from 2 to 200 vehicles/km, the PDR declines for all three tested BSM rates. However, the impact of direct collisions on the PDR is insignificant for the 10 BSM/s message rate, even at a vehicle density of 200 vehicles/km, with a PDR of 92%. On increasing the BSM rate to 20 BSM/s, the PDR decreases to 72%, and further increasing the rate to 30 BSM/s results in a PDR of only 4%. Such a low PDR would make the Safety Application ineffective at high vehicle densities. The high BSM rates can only be used at lower vehicle densities, e.g., sending 20 BSM/s at vehicle densities below 115 vehicles/km, or 30 BSM/s for 78 vehicles/km.

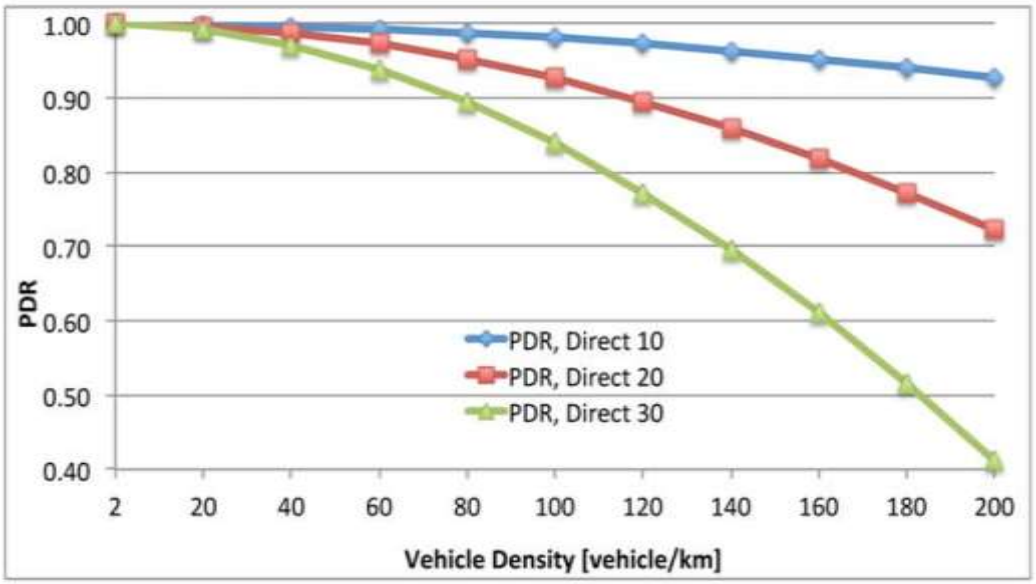


Figure 6. Impact of direct collisions on PDR (BSM size=180 Byte, data rate=6Mbps, BSM rate= 10, 20, 30 BSM/s)

In this analysis, we examine the effect of hidden terminal collisions on PDR at different vehicle densities, as depicted in Figure 7. The results show that when transmitting at a rate of 10 BSM/s, a PDR of over 90% can only be achieved at a density of 20 vehicles/km. When using higher BSM rates, significant degradation in PDR is observed, which raises concerns about the suitability of the 802.11p MAC layer in dense environments.

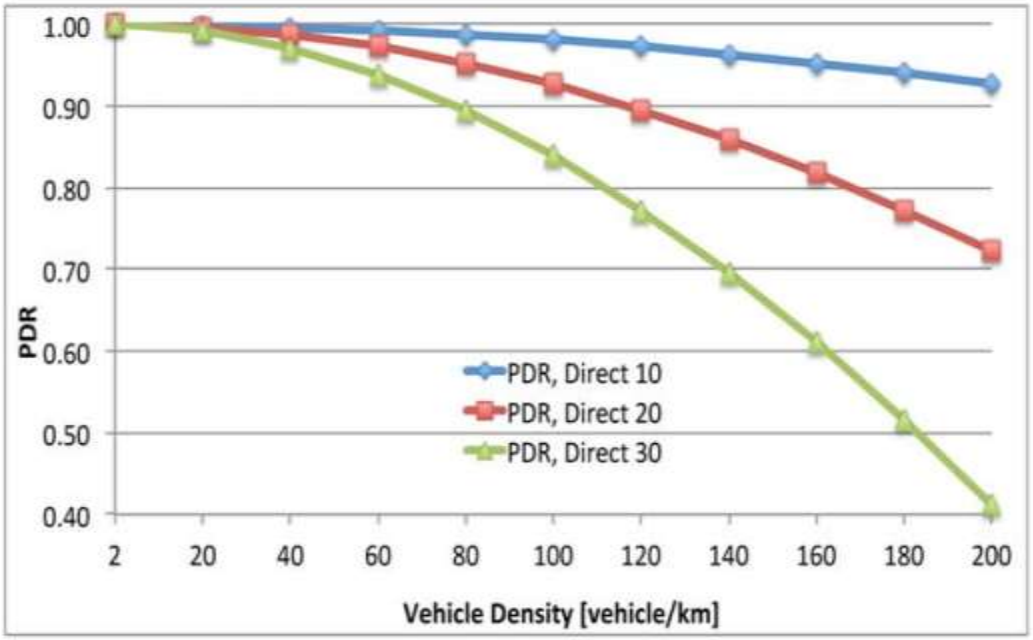


Figure 7. Impact of collisions resulting from hidden terminals (BSM size=180 Byte, data rate=6Mbps, BSM rate=10, 20,30 BSM/s).

Jammer Fail-Safe Mode and Recovery Algorithm

In this section, we present a strategy for mitigating jamming attacks in DSRC Safety Applications. The approach involves jamming detection as a means of transitioning the applications to fail-safe mode, and a recovery algorithm to transition back to functional mode. Jamming detection is based on the jamming attack detection model described in figure 2, which uses vehicle location and PDR estimations. If jamming is detected, the Safety Application transitions to fail-safe mode and the driver is notified that the application is no longer dependable. The recovery algorithm, as shown in Figure 8, is initiated when jamming is detected and the Safety Application transitions to fail-safe mode. The algorithm first calculates Max.Rate, which is the maximum number of BSMs a vehicle can send based on the last observed number of vehicles before entering the jammed area. The algorithm then compares the current BSM rate, BSM.Rate, with Max.Rate. If BSM.Rate is less than Max.Rate, the algorithm increases the BSM rate while ensuring that the upper bound of channel capacity is not exceeded. The algorithm then waits for Δt duration to receive BSMs. If no BSMs are received during this time, the algorithm further increases the BSM.Rate, if possible. If a BSM is received through Δt, its content is examined to see if it is a high priority BSM indicating a hazard. For high priority BSMs, a warning is passed to the driver. For other BSMs, no warning is issued.

For each successful BSM reception, the confidence level is increased. Once a threshold of confidence is reached, the BSM.Rate is reset, and the algorithm issues a mode switch from fail-safe to normal operational mode. However, if the threshold is not met, the recovery mode waits for another Δt to receive more messages at the same increased rate, and the process is repeated. We note that the increase in BSM rates only occurs during execution of the recovery algorithm, and the standard 10 BSM/s rate is used otherwise.

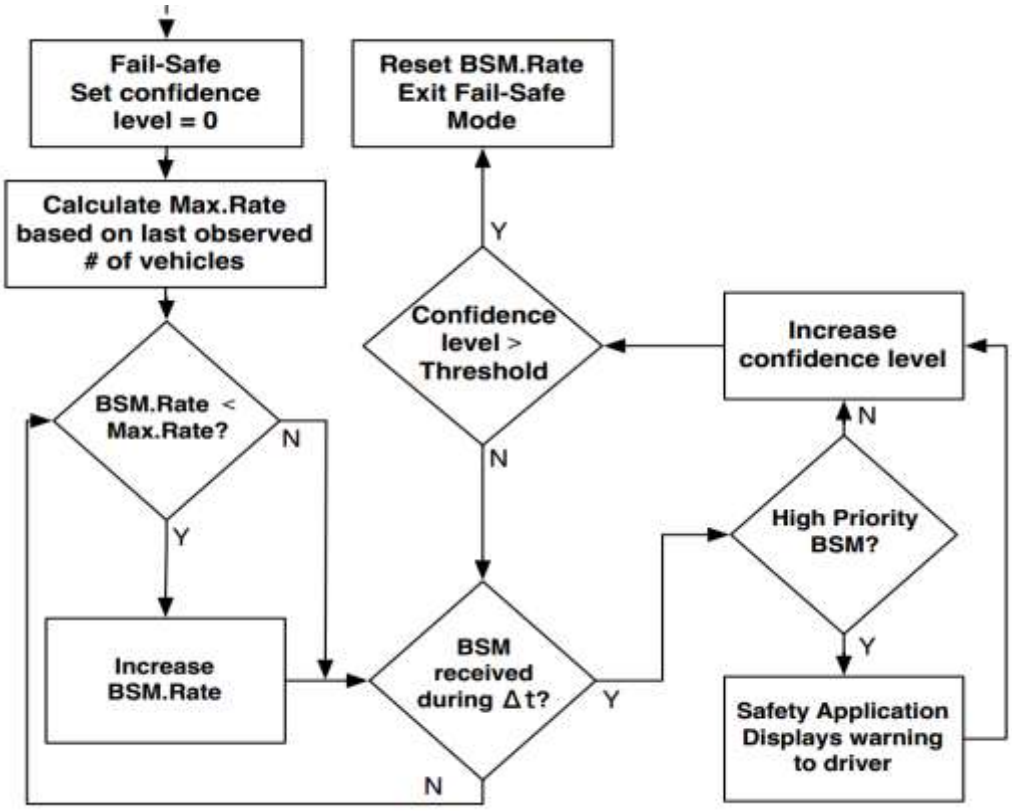


Figure .7 The jammer recovery model Algorithm

Performances Evaluation

The study assessed the influence of jamming on VANETs by conducting a field experiment involving both high and regular vehicles equipped with on-board units (OBU) that employed the LocoMate basic OBU Arada framework[30]. To simulate interference, deceptive OBUs were created by modifying them to generate a constant stream of false packets that would disrupt other OBUs from accessing the network, using the DCF distributed coordination function of the IEEE 802.11p protocol. These deceptive OBUs were capable of jamming at varying data rates. Table 2 displays the parameters employed in the field trial.

Table 8. Field test parameters

Vehicle speed	16.6 m/s
OBU	Arada Systems LocoMate Classic
Length test range	1.53 km
Test range	Straight of 2-lane road
Rate of BSM	10 BSM/s (the BSM for every 100ms)
Jammer position	700 m from starting point
Effective bandwidth	8.3 MHz
Channel	Safety Channel 172
Rate of Data	6and 3 Mbps
Power Transmitter	19 dBm
Data rates jammer	3, 6,, 12 Mbps
Jammer power	18 dBm

8.1. Indigenous PDR

The experiment aimed to assess the impact of jamming on the Packet Delivery Ratio (PDR) of communication between high and regular vehicles. A jamming detection algorithm was utilized to forecast potential outcomes. The experiment was conducted in an unobstructed area to ensure accurate outcomes. The PDR was measured under normal (non-jamming) communication conditions as the distance between Basic Safety Messages (BSMs) received by the high and regular vehicles was increased.

The findings of the PDR measurements are displayed in figures 9 and 10, demonstrating that the experimental results align with the predicted evaluations.

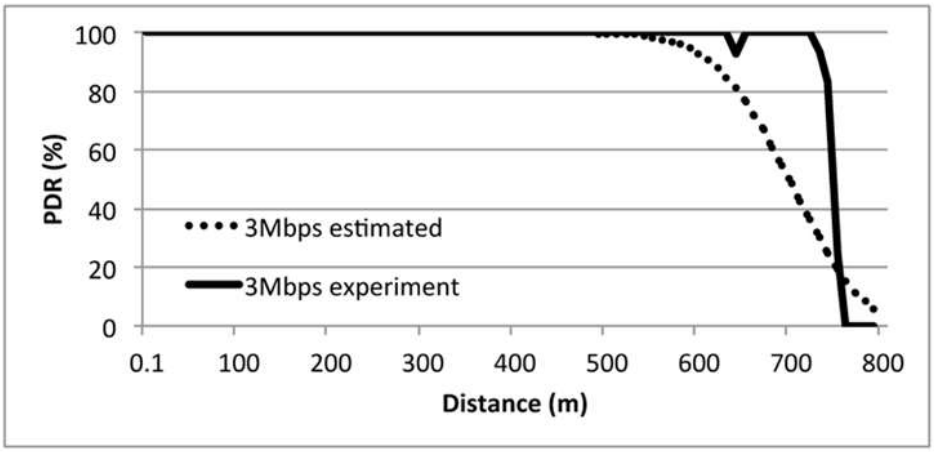


Figure 9. Estimated PDR for 3 Mbps

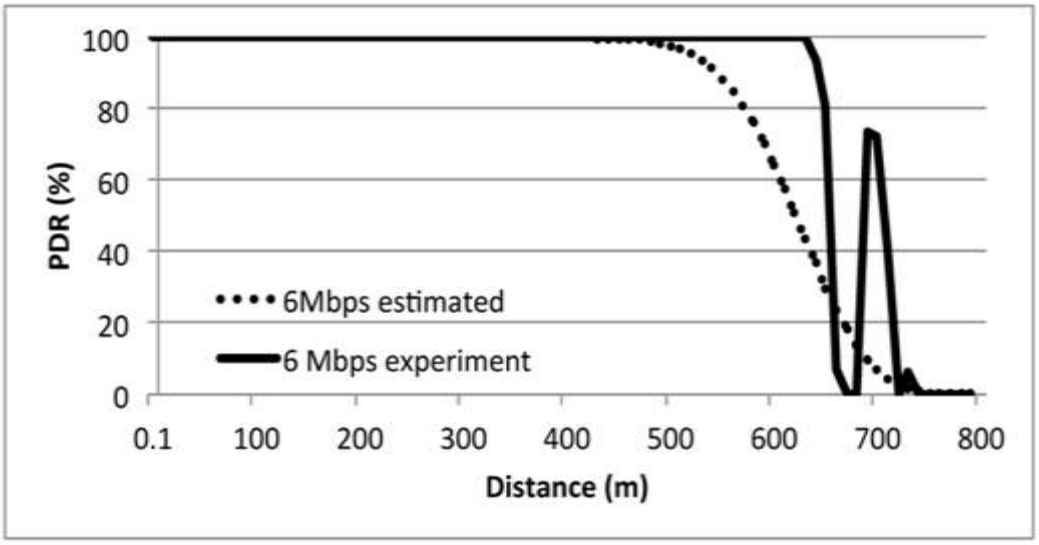


Figure 10. Estimated PDR for 6 Mbps

The Effect Jamming for PDR

To evaluate the impact of jamming on PDR, a test was conducted with two vehicles (RV followed by HV) driving straight on a two-lane road with a stationary jammer present on the road. During the test, BSM messages were logged by the OBU in the HV for data rates of 3 and 6 Mbps, while being subjected to deceptive jamming at rates of 3, 6, and 12 Mbps. It should be noted that a data rate of 12 Mbps was deemed inappropriate for BSM communication in the presence of jamming in previous studies[31][32]. Figure 11 illustrates the PDR for 3 Mbps BSM communications under different jamming rates in a standard test scenario. As the HV and RV approached the jammer stationed at 600m, the HV could not receive BSMs at a distance of about 375-425m. The impact of the jammer diminished at around 750-800m. The transmission rate of the jammer had only a modest effect on the PDR. It is not recommended to draw conclusions from small variations in these experiments due to the nature of this type of jammer.

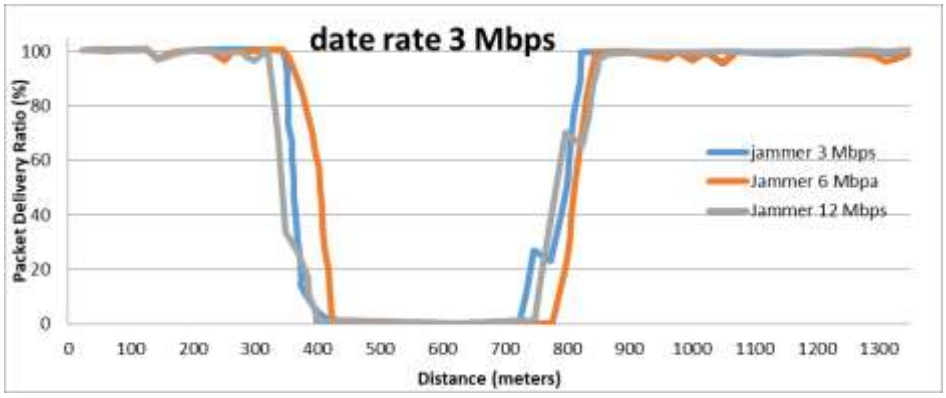


Figure 11. PDR at 3 Mbps with deceptive jamming

The assessment of the impact of jamming on the PDR was carried out by testing two vehicles (RV followed by HV) driving on a straight two-lane road, while a deceptive jammer was located in a stopped car on the side of the road. During the tests, BSM messages were logged by the OBU in the HV for data rates of 3, 6 Mbps while being subjected to deceptive jamming with rates of 3, 6, and 12 Mbps. It should be noted that a data rate of 12 Mbps is considered unsuitable for BSM communication in the presence of jamming. Figure 11 shows the PDR for 3 Mbps BSM communication at different jamming rates for a typical test scenario. As the HV and RV approached the jammer stationed at 600m, the HV was unable to receive BSMs from about 375-425m. The effect of the jammer dropped off at around 750-800m, and the transmission rate of the jammer had only a modest effect on the PDR. However, it should be noted that a sample size of these small variations is needed for further experimentation. The results for the normal test with a data rate of 6 Mbps are shown in Figure 12. Again, the PDR was only modestly influenced by the rate of the deceptive jammer. Interestingly, a peculiar situation was observed during the 3 Mbps jamming test. After the HV was caught in the jamming zone, it was able to receive messages from the RV again at around 475m. This was because a small truck passed the test cars and positioned itself temporarily between the vehicles and the jammer, thereby reducing the effect of the deceptive jammer.

To sum up, the field test results indicated that the transmission rate of the deceptive jammer had a minor impact on the transmissions. However, further tests are necessary to determine how the transmission of different data rates is affected. Although the overall effect of jamming was significant, no clear pattern in the impact of the jamming on different data rates of the vehicles and the jammer was observed. This is in contrast to continuous jamming, which significantly reduces the PDR for higher data rates.

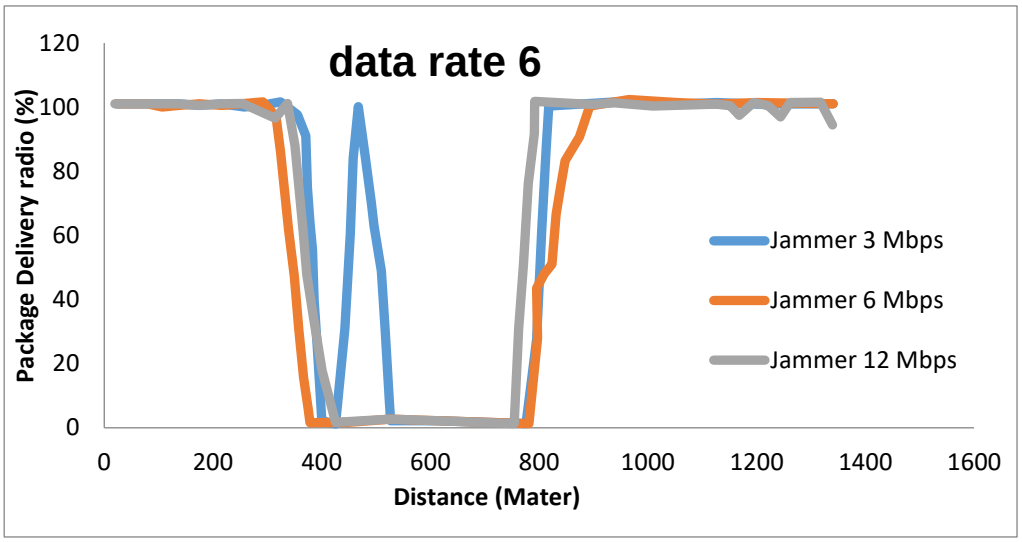
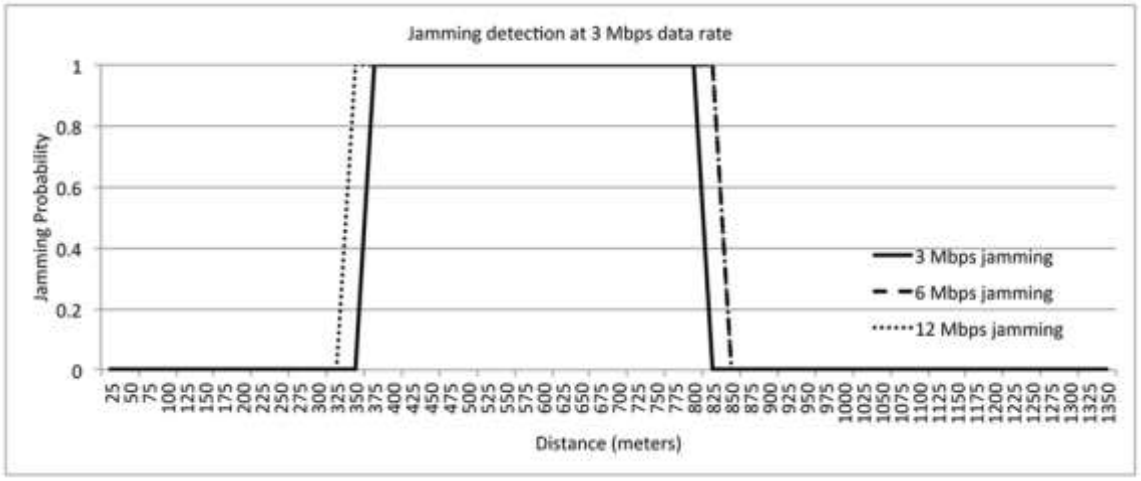


Figure 12. PDR at 6 Mbps on jamming deceptive.



8.3

Jamming Detection Evaluation of Algorithm

The outcomes of the jamming detection algorithm assessment for the 3, 6, and 12 Mbps region test data are shown in Figure 12. The algorithm was successful in detecting jamming as soon as the PDR drop was identified by the consistency test, which was based on distance and PDR. The algorithm did not detect any inconsistencies in distances and GPS, indicating that only one of the two detections mechanisms used in the region test was sufficient. Moreover, PDR inconsistencies were detected.

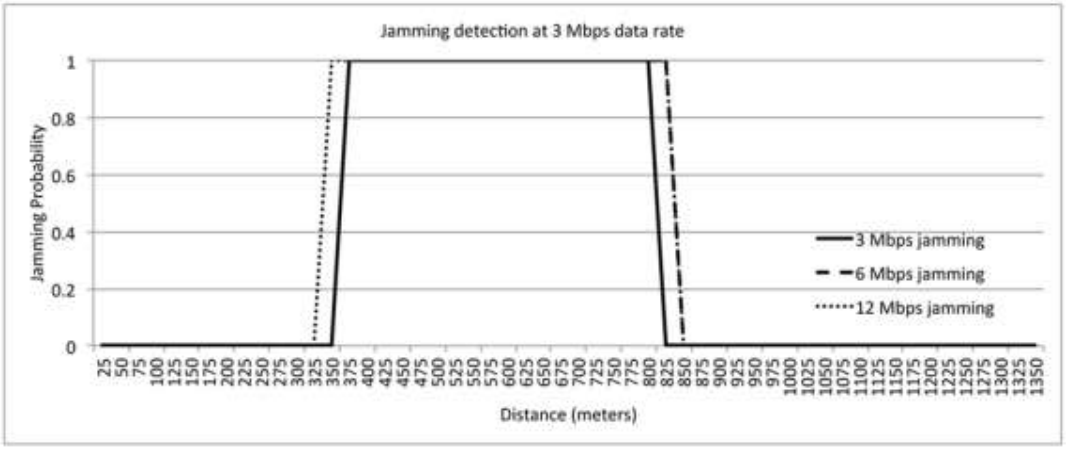


Figure 13. of Jamming Attack Evaluation Algorithm in Data rate

Discussion and Results

Here, we will evaluate the effectiveness of the recovery algorithm in mitigating the impact of jamming, by testing it against two types of jammers: constant and deceptive jammers.

9.1. Constant Jammer

Consider the scenario illustrated in Figure 14, where an RV is followed by an HV on a single-lane road. Suppose that the RV suddenly brakes due to a hazard, resulting in the dissemination of BSMs carrying braking information to surrounding vehicles. Assuming that the vehicles' speed is 35 mph (15.6 m/s), and the safety distance between them is 3 seconds, the reaction time is 1 second (typical reaction times are around 0.95 seconds). Thus, the HV will have only 2 seconds to receive BSMs about the braking event before it needs to react. We will assume a constant jammer as the source of a malicious attack in this scenario, positioned behind the HV,, we define the unreliability Q(t) of the Safety Application as the inability of the HV to successfully receive at least one BSM before $t_{react} = 1\ s$, The inability of the HV to receive BSMs from the RV is directly attributed to the jammer's signals overpowering the legitimate communication signals. We will now analyze how BSM rates, power levels, and data rates affect the unreliability Q(t) of the Safety Application. It is important to note that we assume all BSM communication occurs in the safety channel (CH172).

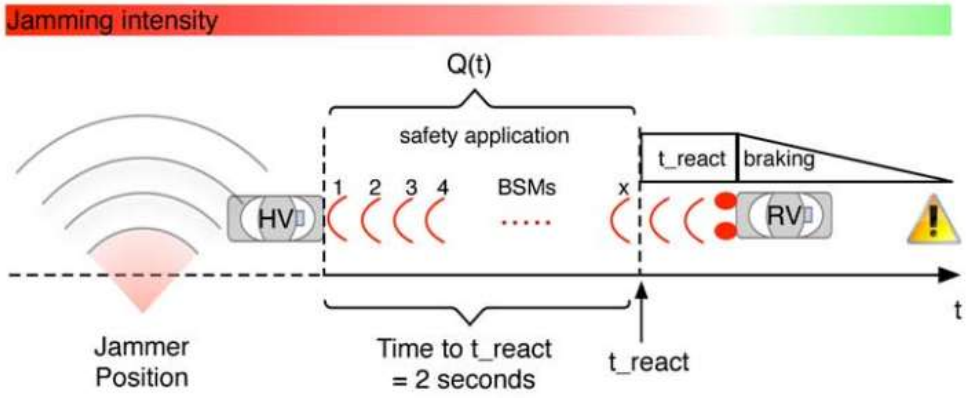


Figure 14. The effect of BSM rates on the reliability of the safety application

The Impact of BSM Rats

In order to investigate the effect of BSM rates on the reliability of the safety application, we examined three different BSM rates: 10, 20, and 40 BSM/s, as illustrated in Figure 14. During this experiment, the transmission power was set to P_t=21 dBm, the jammer power was set to P_j=15 dBm, and the data rate was set to R = 6 Mbps. The figure demonstrates how jamming affects Q(t) for different BSM rates. As shown, Q(t) almost reaches 1, indicating complete failure, for the entire time frame leading up to 0.4s before t_react. High BSM rates demonstrate me improvement, but unreliability only decreases when there is almost no time left to react. BSM rates of 10 and 20 BSM/s resulted in unacceptable unreliability of more than 0.2 and 0.45, respectively. At t_react (0 in the figure), only a message rate of 40 BSM/s met the safety application's unreliability requirements with $Q(t_{react}) = 0.04$, implying a safety application reliability of 0.96. However, generally, this is too close to the threshold for reacting. On the other hand, in the context of saving lives using safety applications, this could still be helpful. The above analysis only considers BSM rates and does not take into account the impact of other adjustments, such as transmission power and data rates, which will be discussed next.

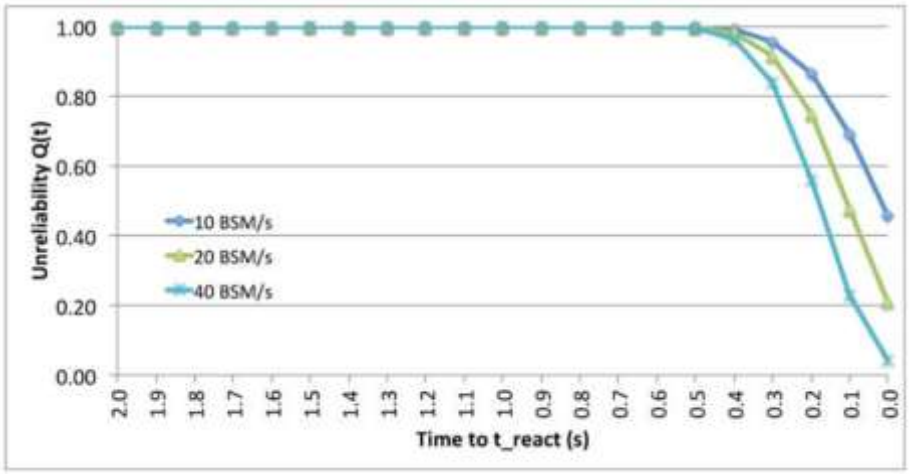


Figure 15. The impact of BSM Rates on Q (t)

The effect of Transmission Power.

To examine the impact of transmission power levels on Q(t), we tested three power levels: 21 dBm, 23 dBm, and 25 dBm. For this experiment, we kept the BSM rate fixed at 40 BSM/s, the jammer power P_j was set to 15 dBm, and the data rate was set to R = 6 Mbps. In Figure 16, the impact of different transmission power levels on Q(t) is presented. The experiment was conducted by examining three power levels, namely 21 dBm, 23 dBm, and 25 dBm, while keeping the BSM rate fixed at 10 BSM/s, the jammer power at 15 dBm, and the data rate at 6 Mbps. The results show that, for a transmission power of 21 dBm, the unreliability remains high until around 0.4s prior to t_{react} , making it insufficient for the safety application. However, when the transmission power is increased to 23 dBm, Q(t) starts dropping earlier, around 0.9s prior tot_{react} , and reaches an acceptable unreliability level around 0.4s before t_{react} . Further increasing the transmission power to 25 dBm results in even earlier drop in Q(t), starting around 1.4s prior tot_{react} , and reaching acceptable Q(t) about 0.9s before t_{react} . The improvement in reliability is attributed to the increase in Signal-to-Jamming Ratio (SJR) as the transmission signals become stronger. This increase allows the safety application to receive at least one BSM before t_{react} , contributing to more time for drivers to react. It is worth noting that the chosen transmission power levels are in line with the FCC amendment [33], which states that transmission power levels for public safety operations in CH172 should not exceed 33 dBm EIRP.

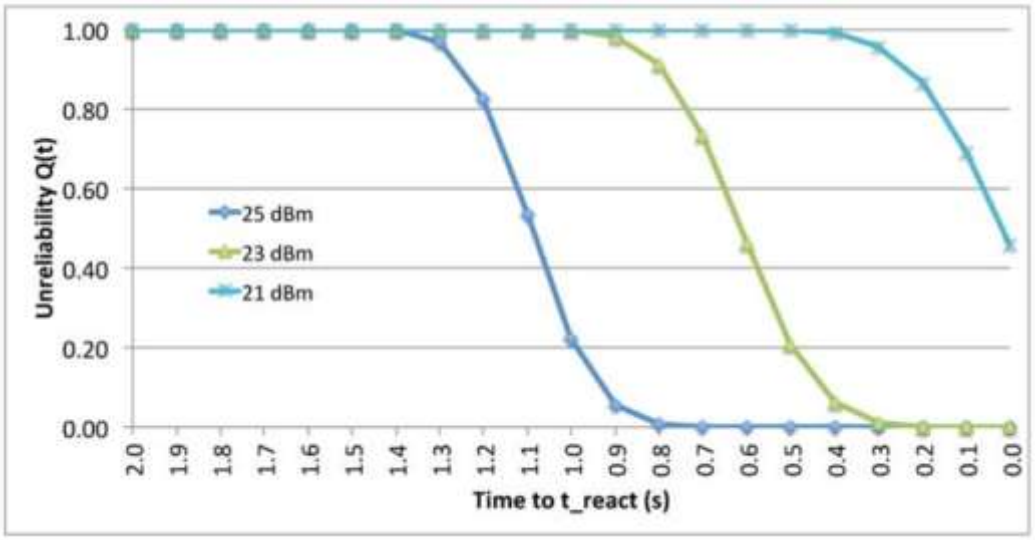


Figure 16. The impact of Transmission Power on Q(t)

The effect of Data Rate.

To investigate the effect of data rates on Q(t), two data rates were examined, namely 3 Mbps and 6 Mbps. During the experiment, the power of the jammer, P, was set to 15 dBm, the transmission power was set to P = 21 dBm, and the BSM rate was fixed at the standard 10 BSM/s. Due to their unreliability in the face of constant jamming[34], higher data rates were not considered. Figure.16 illustrates how jamming affects the reliability of the safety application for the two data rates. When using 6 Mbps, Q(t) begins to decline only 0.4s prior to t_{react} and never reaches an acceptable level of unreliability. However, when the lower data rate of 3 Mbps was used, Q(t) starts to decline before 1.1s and meets the application's unreliability requirements before 0.6s fromt_{react}, providing the driver with additional time to react. The benefit of employing lower data rates stems from the fact that 3 Mbps data rate employs Binary Phase Shift Keying (BPSK) with a coding rate of 1/2, while 6 Mbps uses Quadrature Phase Shift Keying (QPSK) with a coding rate of 1/2, as specified by the ASTM E2213 standard. Higher modulation modes are generally more susceptible to transmission errors.

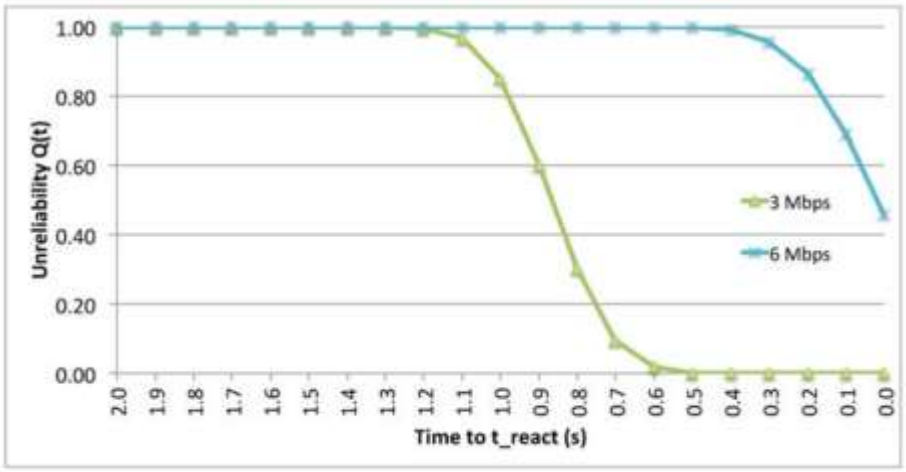


Figure 17. The impact of Data Rate on Q(t)

Deceptive Jammer.

In Subsection 9, we examine the recovery concepts for the case of a deceptive jammer. Specifically, we investigate how the BSM rates, transmission power levels, and data rates impact the recovery time. While in the case of a constant jammer, we measured the impact of each parameter on the Safety Application using the unreliabilityQ_t, in the case of a deceptive jammer, we conducted actual field experiments to obtain the results. Therefore, we could no longer calculate the individual $Q_t$which represents the probability that $BSM_i$was not received t_i. Instead, we used the recovery time, defined as the time required for the HV to resume steady reception after passing the jammer, to measure the impact of BSM rates, transmission power, and data rates. It is important to note that we considered the communication fully recovered only when a steady reception was resumed, even though intermittent reception of BSMs may occur after passing the jammer. The field experiments were conducted on a straight 2-lane road with an average speed of 35 mph (15.6 m/s), with an RV followed by an HV passing a stationary deceptive jammer on the roadside. The moderate speed allowed us to better understand the impact of the tested parameters in the presence of the jammer while not exceeding the speed limit of the test road. Additionally, a third vehicle was included to collect extra data and investigate its impact on the two communicating vehicles when leaving the jammed zone. We focused on the HV's reception of the alert messages during the experiments, as our main concern was the vehicle receiving the messages. Figure.18 shows the position of the test vehicles, with the RV being the first vehicle exposed to the jammer's impact in Figure 18a. The impact of the jammer on the RV is different when the vehicles have passed, as shown in Figure 18b, where the last two vehicles provide a shielding effect on the RV. The figures presenting the results of the field test depict the impact of the jammer on the RV in two scenarios, i.e., moving towards or leaving from the jammer position. Table. 3 provides details on the specific parameters utilized in the field tests. However, it is important to acknowledge the challenges involved in conducting these experiments. Conducting field experiments presents several challenges, such as ensuring safety during the tests, controlling testing conditions, and obtaining reliable and accurate data. To address these challenges, the test road was carefully selected, safety measures were implemented, and various data collection methods were employed, such as GPS and video recordings. Furthermore, due to the unpredictable nature of road and traffic conditions, multiple tests were conducted to obtain statistically significant results. The collected data were then analyzed to draw conclusions regarding the impact of BSM rates, transmission power levels, and data rates on recovery time.

Table 3. Field test parameters

OBU Model	Arada Systems LocoMate Classic
Vehicle speed	20 m/s
Range test	Two lines for the road
Test range length	1000 m
Jammer position	500 m from starting point
BSM generation	10,20 and 40 BSM/s
Channel	Safety Channel 172
Effective bandwidth	8.3 MHz
Transmitter power	21,23 and 25 dBm
Data rate Transmission	3 and 6 Mbps
Data rate Jammer power	6 Mbps and 18 dBm

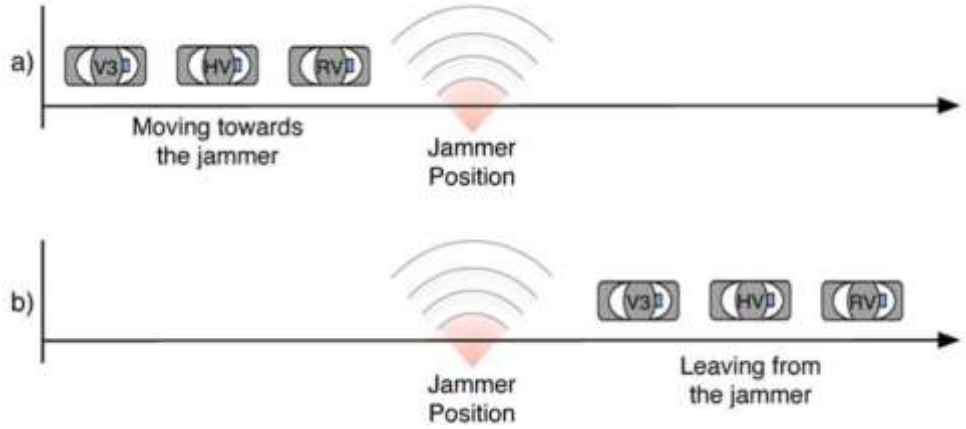


Figure 18. The position of the test vehicles prior to and after encountering the jammer.

The Impact of BSM Rates.

To examine how different BSM rates affect recovery time, we conducted field tests using rates of 10, 20, and 40 BSM/s. Results for each rate are displayed in Figures.20, and 21, respectively. The number of BSMs received by the HV was measured over the entire test area (Figure 24) from start to finish, with the time at which the HV passes the jammer indicated by a dashed line. Although passing times varied slightly across trials due to slight speed variations, recovery times were consistent within each test. Figure 19 shows results for a typical experiment using the standard 10 BSM/s rate. When the HV passed the jammer at t = 31s, no BSMs were received because the jamming impact was at its peak and the HV was nearly parallel to the jammer. Steady reception of BSMs resumed only after 12 seconds following the passage of the jammer, with only intermittent reception prior to that time.

Figure.20 illustrates the impact of sending at 20 BSM/s on the recovery time. During this experiment, the RV increased its sending rate to 20 BSM/s, and the HV passed the jammer at t = 31s. As shown in the figure, the HV resumed steady reception at t = 41s, resulting in a recovery time of 9s for this trial.

In the last trial, 40 BSM/s was used, and the HV passed the jammer at t = 29s, as depicted in Figure 21. The HV started receiving BSMs continuously from the RV at t = 39s, leading to a recovery time of 9s.

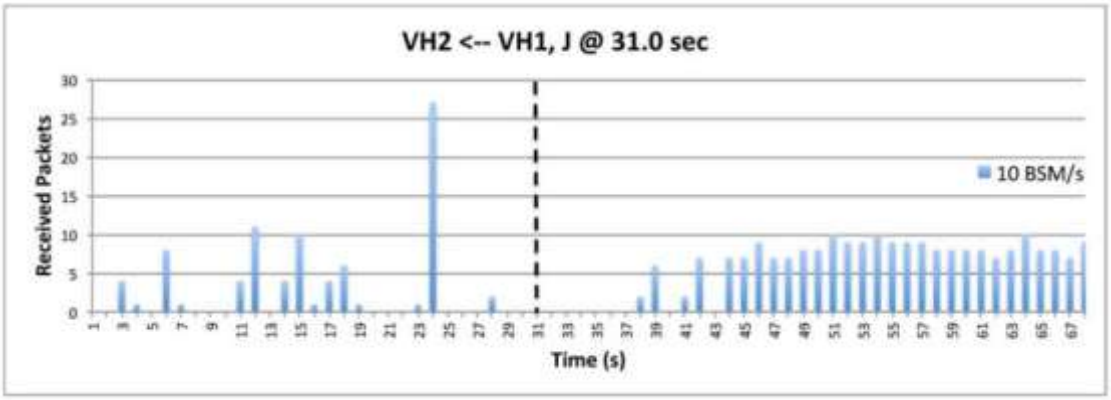


Figure19. Reception using 10 BSM/s

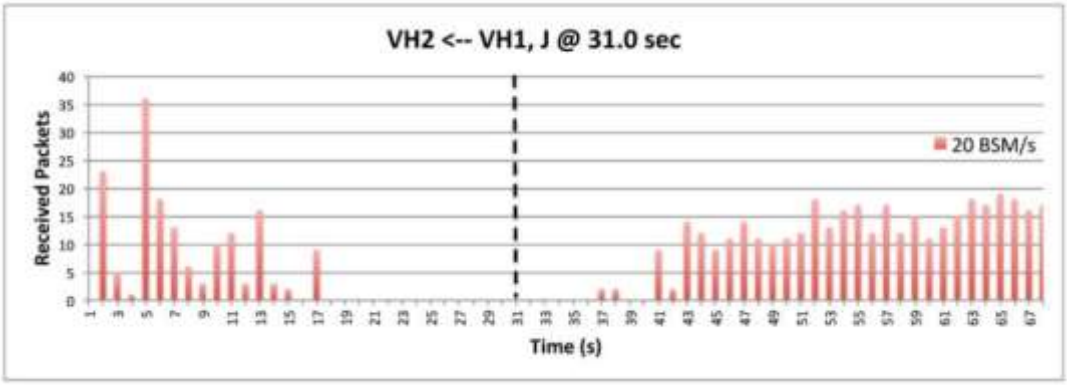


Figure 20. Reception using 20 BSM/s

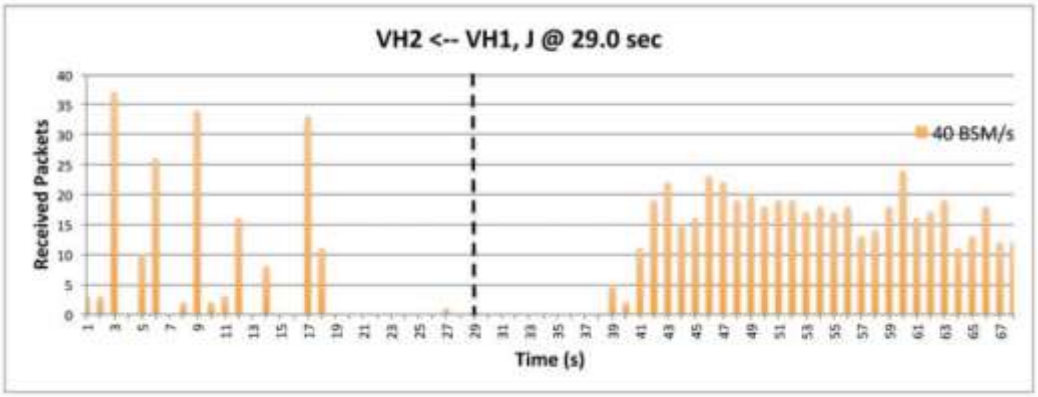


Figure 21. Reception using 40 BSM/s

The Impact of Transmission Power.

To investigate the impact of transmission power on the recovery time in the presence of a deceptive jammer, three different power levels have been investigated, i.e., 21, 23 and 25 dBm. The impact of these

Studying the impact of different power levels on recovery time in typical test runs is presented in Figures 22, 23, and 23. Figure 22 illustrates a scenario where transmissions were made at a power level of 21 dBm and the corresponding recovery time. At point t = 31s, the HV passed the jammer and communication was completely disrupted due to the deceptive jammer. However, at point t = 41s, a steady reception of BSMs was observed, resulting in a recovery time of 9s. Figure 23 depicts the case of transmission power level of 23 dBm, where the HV passed the jammer at point t = 28s, and steady reception was only resumed after 7s from the point of passing the jammer. Figure 24 considers a transmission power level of 25 dBm. The HV passed the jammer at t = 28s and regained steady reception at t = 34s, resulting in a recovery time of 6s.

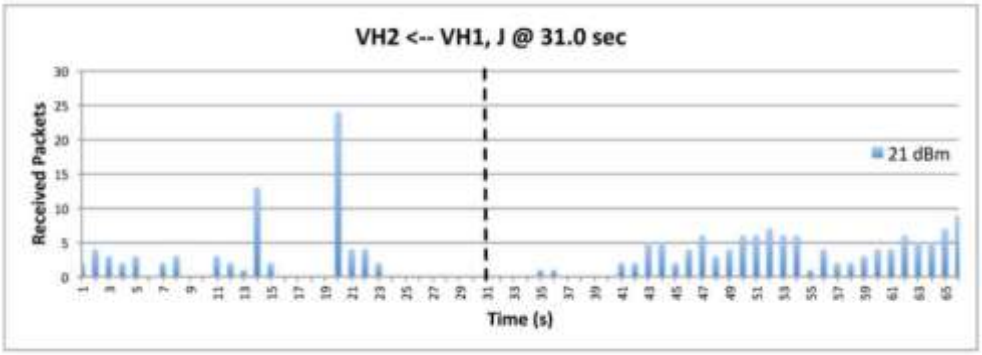


Figure 22. Reception using 21 dBm transmissions Power.

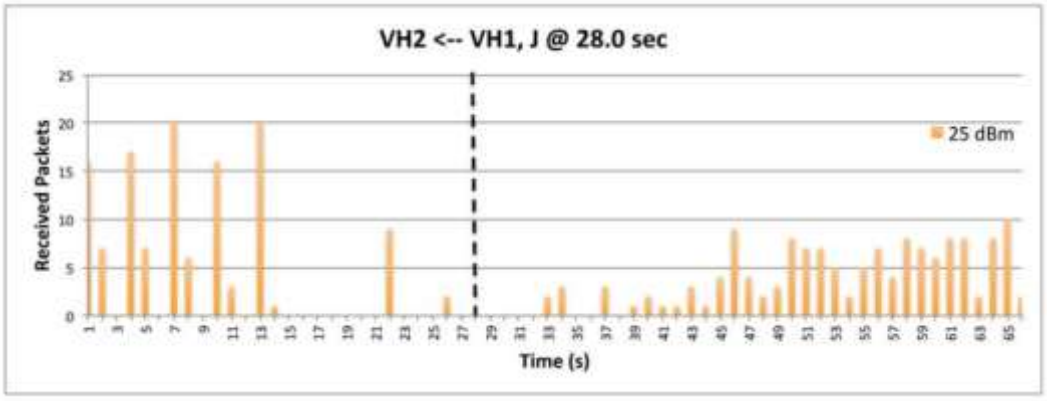


Figure 23. Reception using 23 dBm transmissions Power

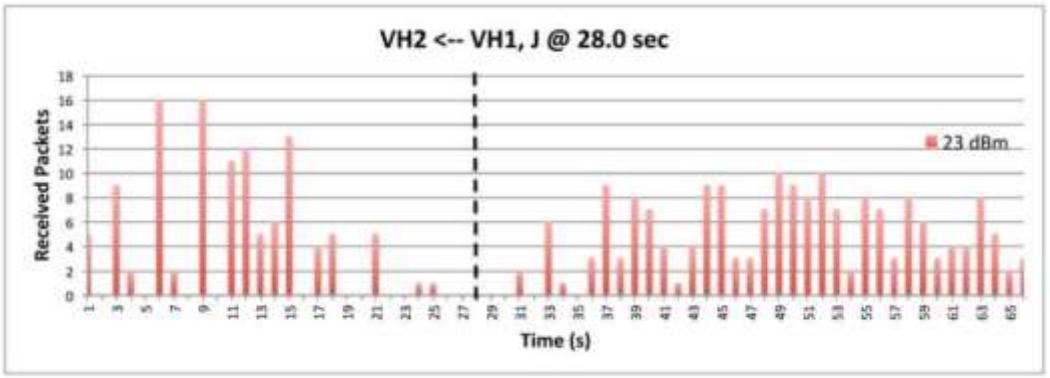


Figure 24. Reception using 25 dBm Transmissions Power

The Impact of Data.

To study the effect of data rates on the recovery time, two different rates, namely 3 Mbps and 6 Mbps, were tested, and the results are presented in Figures 24 and 25, respectively. Figure 25 shows an example of the recovery time using a data rate of 3 Mbps, where the HV passed the deceptive jammer at t = 30s and resumed reception of BSMs from the RV at 42s, resulting in a recovery time of 11s. In contrast, Figure 26 depicts the recovery time using a data rate of 6 Mbps, where the HV passed the jammer at t = 31s, and a constant reception of BSMs was regained at t = 44s, accounting for a recovery time of 12s.

However, an abnormal behavior was observed during the field experiments, as spikes in the number of received BSMs were detected. This behavior suggests that the number of received BSMs exceeded the number of transmitted ones. For instance, in Figure 26 at t = 24s, the number of received BSMs was more than 25, while only 10 BSMs were transmitted. This unusual behavior is due to the deceptive jammer preventing the OBU from accessing the media, which causes packets generated by the application layer to accumulate in the OBU's queue for deferred sending. When the OBU eventually gains access to the media, the queued packets are transmitted simultaneously, resulting in the observed spikes. This effect is particularly noticeable at the beginning of the test period when the communication was partially affected by the jammer.

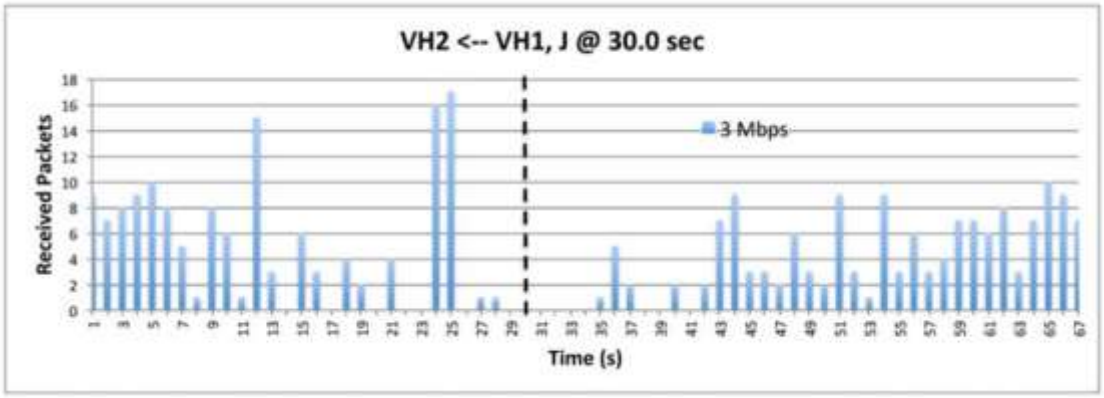


Figure 26. Reception using 3 Mbps data rate

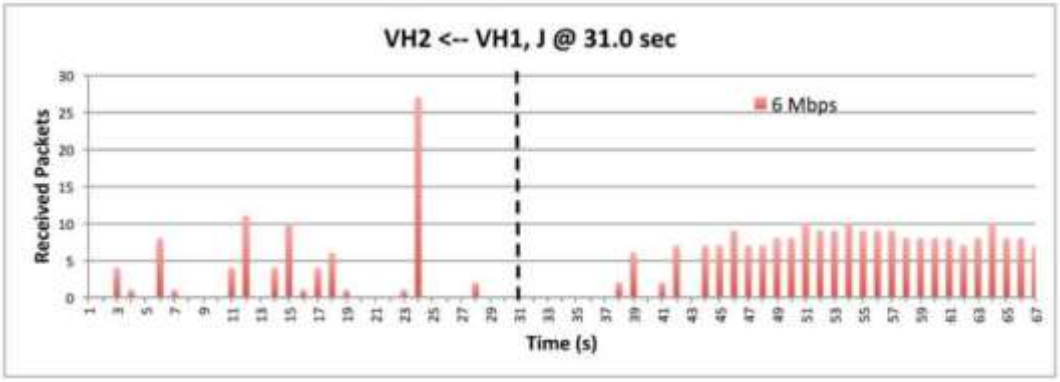


Figure 27. Reception using 6 Mbps data rate

Upon analyzing the data collected from the field experiments, we noticed abnormal spikes in the number of received BSMs, which exceeded the number of transmitted BSMs. This behavior can be observed in Figure 26, where at t = 24s, the number of received BSMs was more than 25, while the number of transmitted ones was only 10. This abnormal behavior is due to the fact that the deceptive jammer is preventing the OBU from accessing the media. As a result, the OBU queues the packets generated by the application layer for deferred sending. However, since the jamming persists, packets were not sent in time and accumulated over a period. This is especially evident at the beginning of the test period when the communication was partially affected by the jammer. Once the OBU gains temporary access to the media, all queued packets are pushed at once, resulting in the observed spikes. It's worth noting that the queue has a certain capacity, which prevents it from buffering all packets during prolonged inaccessibility to the media.

Table 4: Recovery Times for Deceptive Jammer Of The Trials Presented.

Deceptive Jammer (Field Experiment}	BSM /s			Power (dBm)			Data Rate (Mbps)	
	10	20	40	21	23	25	3	6
Recovery Time (Seconds)	12.0	9.0	9.09.0	9.0	7.0	10.0	11.0	12.0
Distance (meters)	145	115	125	106	68.5	120	125	150

Table 4 presents the recovery times and distances between HV and RV for the representative cases. However, due to unavoidable differences in distances and environmental conditions, the observed results cannot be generalized. The results obtained from the presented scenarios confirm the predictions made by the mathematical models and intuition. For instance, the increase in recovery time when the power level was increased from 23 dBm to 25 dBm was due to the actual distances observed in the post-analysis of the data. Therefore, the reader should consider the "Distance" column when examining the recovery times. Despite our best efforts to maintain consistent distances between different trials, it was challenging to achieve this without a towrope between vehicles. Nonetheless, due to the unavailability of a facility that could accommodate such a test range length, we were unable to maintain consistent distances.

Also, table 4 shows the recovery times and distances for the representative cases that were examined. But, due to differences in environmental conditions and distances, these results are not conclusive and cannot be generalized. To provide a fair comparison with similar test conditions, one can simulate different BSM rates in a post-analysis based on a single field trial. Figure 27 shows the comparison of different BSM rates (10, 20, and 40 BSM/s) using the data from the field test with 40 BSM/s. This allows us to understand the impact of BSM rates while maintaining almost the exact same test conditions, such as environmental and physical factors, including distances and antenna positions. However, the conditions using this approach are not entirely identical, as the transmitter queue behavior for 40 BSM/s is unlikely to be the same for rates of 10 and 20 BSM/s. Our results indicate that sending at a rate of 10 BSM/s resulted in a 11s recovery time, while sending at higher rates of 20 and 40 BSM/s resulted in a shorter recovery time of 9s. These results are consistent with our previous observations during the field experiments, as summarized in Table 4. However, we were unable to directly observe the impact of transmission power levels for the deceptive jammer due to variations in inter-vehicle distances during the field experiment. These variations in distances resulted in different levels of SNR, which in turn impacted the reception of BSMs and affected the change in recovery times that we observed during the field test.

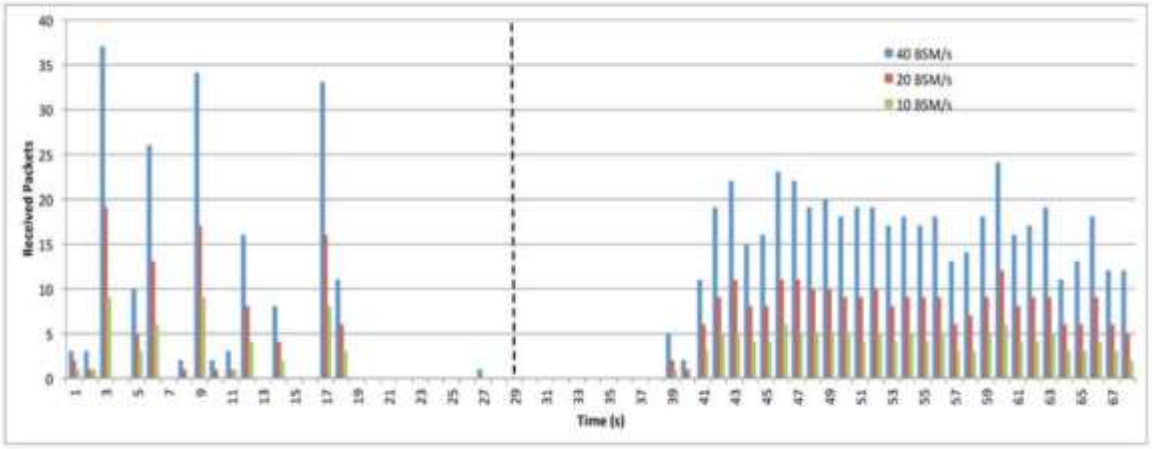


Figure 27. Comparing the impact of BSM rates

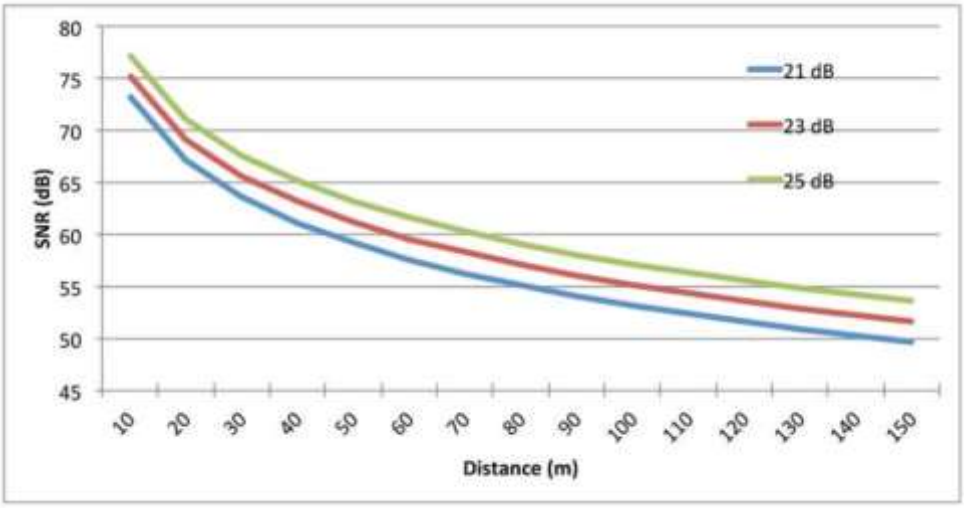


Figure 28. The impact of relative distance between vehicles on SNR

To better understand the impact of higher transmission powers, we analyzed the relationship between signal-to-noise ratio (SNR) levels and inter-vehicle distances, as shown in Figure 28. By assuming a fixed distance of 100 m between the vehicles, we were able to observe the real impact of using higher transmission power. Comparing the results for 23 dBm and 25 dBm at a distance of 100 m, we found that using a higher transmission power resulted in improved SNR levels. Higher SNR levels translate to lower bit error rates (BER) and overall higher chances of successfully receiving messages. In contrast to the field experiments with the deceptive jammer, where maintaining consistent physical conditions was challenging, we were able to control the physical conditions in this analysis. Therefore, these results provide valuable insights into the potential benefits of using higher transmission powers in similar scenarios.

Conclusion

In this study jamming discovery a strategy for measurements DSRC Security applications in VANET communication to a fail-safe mode. We have proposed a new recovery strategy based on adjusting the communication parameters, i.e., BSM rates, transmission power levels and data rates only when jamming is detected. This has shown to help increase the reliability of the Safety Applications, by transitioning them from the jammed to the non-jammed state faster. We have also studied the tradeoff between channel efficiency and reliability by investigating the impact of increased number BSMs in the safety channel. The maximum possible number of BSMs obtained for both cases, direct and indirect collisions. Direct collisions result from what is known as the hidden terminal situation. It was shown that for the case of hidden terminal case, the safety channel will struggle supporting high number of vehicles when sending at rates higher than 10 BSM/s. We furthermore studied the concepts behind the recovery algorithm, by considering the impact of BSM rates, transmission power and data rates on the reliability of the Safety Applications, for both constant and deceptive jammers. For the constant jammer, increasing the BSM rates slightly improved the reliability of the Safety Application. The results, based on mathematical analysis and data collected during field tests show that this recovery strategy can help the Safety Applications to transition from fail-safe mode to operational mode earlier. In the context of safety critical applications, this has the potential to reduce accidents and save lives.

References

[1] N. 2015.] Traffic Safety Facts: Crash Stats, U.S. Department of Transportation, National Highway Traffic Safety Administration, DOT HS 812 219, “No Title.”

[2] “J. B. Kenney, Dedicated Short-Range Communications (DSRC) Standards in the United States, Proceedings of the IEEE, vol. 99, no. 7, pp. 1162-1182, 2011.”

[3] “No TitleIEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE Std 1609.2TM, 2018.”

[4] Mahmood A. Al-Shareeda; Selvakumar Manickam, “A Systematic Literature Review on Security of Vehicular Ad-Hoc Network (VANET) Based on VEINS Framework,” *IEEE 66th Veh. Technol. Conf.*, vol. 11, pp. 46218–46228, 2023.

[5] S. Blessy, A.M.C., Brindha, “Energy-efficient fuzzy management system using tri-parametric methodology in vanet,” *IEEE*, vol. 14, 2023.

[6] G. Ayoob, A., Su, G. and Al, “Hierarchical Growing Neural Gas Network (HGNG)-Based Semi cooperative Feature Classifier for IDS in Vehicular Ad Hoc Network (VANET,” *J. Sens. Actuator Networks*, vol. 7, no. 3, p. 41, 2018.

[7] Jinsong Zhang; Kangfeng Zheng; Dongmei Zhang; Bo Yan, “AATMS: An Anti-Attack Trust Management Scheme in VANET,” *IEEE Access*, vol. 8, no. 10, 2020.

[8] M. Hadded, P. Muhlethaler, A. Laouiti, R. Zagrouba, and L. A. Saidane, “TDMA-Based MAC Protocols for Vehicular Ad Hoc Networks: A Survey, Qualitative Analysis, and Open Research Issues,” *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2461–2492, 2015.

[9] G. Lu, Vasukidevi, “A Survey on Security and Key Management in,” *IJIRST –International J. Innov. Res. Sci. Technol.*, vol. 3, no. 08, pp. 107–111, 2017.

[10] Y. Hu, A. Perrig, and D. B. Johnson, “Ariadne : A Secure On-Demand Routing Protocol for Ad Hoc Networks,” *Wirel. Networks 11*, vol. 5, pp. 21–38, 2015.

[11] F. , Xu Hao , J. Hortelano , Sakiz and S. Sen, “Ad Hoc Networks Survey paper A survey of attacks and detection mechanisms on intelligent transportation systems : VANETs and IoV,” *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017.

[12] H. M. Maier, “Florida State University Libraries Nutritional Status and the Relationship of Dietary and Serum Advanced Glycation End-Products with Inflammation , Oxidative Stress and Healing of Diabetic Foot Ulcers,” 2013.

[13] S. I. Sou and O. K. Tonguz, “Enhancing VANET connectivity through roadside units on highways,” *IEEE Trans. Veh. Technol.*, vol. 60, no. 8, pp. 3586–3602, 2017.

[14] E. F. Ahmed Elsmany, M. A. Omar, T. C. Wan, and A. A. Altahir, “EESRA: Energy efficient scalable routing algorithm for wireless sensor networks,” *IEEE Access*, vol. 7, pp. 96974–96983, 2019.

[15] J. Puñal, Ó., Pereira, C., Aguiar, A., & Gross, “Experimental characterization and modeling of RF jamming attacks on VANETs.,” *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 524–540, 2015.

[16] Y. Shi, “LTE-V: A Cellular-Assisted V2X Communication Technology,” 2019.

[17] F. B. and A. P. A. Studer, E. Shi, “TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs, in Sensor, Mesh and Ad Hoc Communications and Networks,” *Access IEEE*, pp. 1–9, 2018.

[18] H. L. and M. G. Jie Li, “A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, pp. 938–948, 2019.

[19] J. P. and Z. Mammeri, “Authentication and Consensus Overhead in Vehicular Ad Hoc Networks, in Telecommunication systems,” *IEEE 66th Veh. Technol. Conf.*, vol. 52, no. 4, pp. 2699–2712, 2015.

[20] M. G. and Z. C. Z. Cao, J. Kong, U. Lee, “Proof-of-relevance: Filtering False Data via Authentic Consensus in Vehicle Ad-hoc Networks, in IEEE INFOCOM,” *Workshops*, vol. 20815, pp. 1–6.

[21] U. Rajput, F. Abbas, H. Eun, and H. Oh, “A Hybrid Approach for Efficient Privacy Preserving Authentication in VANET,” *IEEE Access*, vol. 3536, no. c, pp. 1–1, 2017.

[22] P. Donadio, A. Cimmino, and G. Ventre, “Enhanced Intrusion Detection Systems in ad hoc networks using a Grid based agnostic middleware,” *Proc. Int. Conf. Pervasive Serv. ICPS 2008 2nd Int. Work. Agent-Oriented Softw.*, pp. 15–19, 2008.

[23] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, “VANET security surveys,” *Comput. Commun.*, vol. 44, 2014.

[24] F. Anjum, D. Subhadrabandhu, and S. Sarkar, “Signature based intrusion detection for wireless ad-hoc networks: a comparative study of various routing protocols,” *2003 IEEE 58th Veh. Technol. Conf.*, vol. 3, 2003.

[25] Y. Hu, A. Perrig, and D. B. Johnson, “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols,” *[Computer Commun. Networks*, vol. 3.

[26] T. O. Address, U. In, and H. Times, “by Maria Isabel Portal Palomo A Thesis Submitted to the Faculty of The College of Engineering and Computer Science in Partial Fulfillment of the Requirements for the Degree of Master of Science Florida Atlantic University Boca Raton , Florida,” no. May, 2013.

[27] and C. S. B. Awerbuch, A. Richa, “A Jamming-Resistant MAC Protocol for Single-Hop Wireless Networks, in Proceedings of the twenty-seventh ACM symposium on Principles of distributed computing,” *ACM/Springer Mob. Networks Appl.*, vol. 2015.

[28] Y. P. and K. H. R. C.D. Jung, C. Sur, “A Robust Conditional Privacy-Preserving Authentication Protocol in VANET, in Security and Privacy in Mobile Information and Communication Systems,” *Springer Berlin Heidelb.*, p. 35-45, 2014.

[29] A. H. and J. Ben-Othman, “IEEE International Conference on Communications, Dresden,” in *Detection of Jamming Attacks in Wireless Ad Hoc Networks Using Error Distribution*, 2015, pp. 877–889.

[30] A. K. Sampigethaya, M. Li, L. Huang and R. Poovendran, “Robust Location Privacy Scheme for VANET,” *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 569–1589.

[31] A. Mokdad, L., Ben-Othman, J., & Nguyen, “DJAVAN: Detecting jamming attacks in Vehicle Ad hoc Networks,” *Perform. Eval.*, vol. 87, pp. 47–59, 2015.

[32] M. I. A. S., “Radio Jamming Attacks Against Two Popular Mobile Networks.,” *Semin. Netw. Secur.*, vol. 11(2), pp. 135–142, 2000.

[33] Alasmary, W.; Zhuang, “Public safety application for approaching emergency vehicle alert and accident reporting in VANETs using WAVE,” *Ad Hoc Netwowking*, vol. 10, p. 90, 2012.

[34] W. Chen, R. K. Guha, T. J. Kwon, J. Lee, and Y. Hsu, “A survey and challenges in routing and data dissemination in vehicular ad hoc networks,” *Wirel. Commun. Mob. Comput.*, vol. 15, no. October 2009, pp. 787–795, 2011.

Supplementary Materials: The following supporting information can be downloaded at: www.mdpi.com/xxx/s1, Figure S1: title; Table S1: title; Video S1: title.

Author Contributions: Conceptualization, Ayoob Aziz and Zuzan Ayoub; methodology, Ayoob Aziz and Zuzan Ayoub ; software, Zuzan Ayoub and Ayoob Aziz; validation, Ghaith Khalil., Ayoub Aziz and Zuzan Ayoub; formal analysis, Ayoob Aziz and Ghaith Khalil; investigation, Ayob Aziz and Ghaith Khalil; resources, Zuzan Ayoub.; data curation, Ayoub Aziz; writing—original draft preparation, Ayoub Aziz; writing—review and editing, Ghaith Khalil; visualization, Zuzan Ayoub; supervision, Ghaith Khalil; project administration, Ghaith Khalil; funding acquisition, Ghaith Khalil All authors have read and agreed to the published version of the manuscript

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.