A New Hybrid Jammer and its Impact on DSRC Safety Application Reliability

Sherif Hussein
Department of Computer Science
University of Idaho
Moscow, ID 83843–1010
Email: huss3426@vandals.uidaho.edu

Mohamed S. Mohamed
Department of Computer Science
University of Idaho
Moscow, ID 83843–1010
Email: moha3425@vandals.uidaho.edu

Axel Krings
Department of Computer Science
University of Idaho
Moscow, ID 83843–1010
Email: krings@uidaho.edu

***Abstract*—Intelligent Transportation Systems (ITS) use Vehicular Ad Hoc Network (VANET) for safety applications aiming to reduce traffic accidents. The applications, which use Dedicated Short Range Communications (DSRC) with the IEEE 802.11p Medium Access Control (MAC) protocol are exposed to the full range of security problems associated with wireless technology, including wireless jamming.**

This research introduces a new hybrid jammer, which combines the properties of so-called constant and deceptive jammers in addition to characteristics resembling random jammers. It is shown that this simple to implement jammer can 1) manipulate transmitting nodes in a way that causes safety applications to fail, and 2) make innocent nodes appear as misbehaving. All this can be done without destroying messages. The hybrid jammer's impact on the reliability of DSRC Safety Applications is analyzed and results from lab experiments with commercial DSRC equipment, as well as findings during field experiments that motivated the research, are presented. Finally, a detection algorithm is proposed as a mitigation strategy for the new jammer.

1. Introduction and Motivation

Connected vehicle safety applications aim to help avoid accidents and increase situation awareness using Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications to exchange data associated with driver advisories, warnings, as well as vehicle and infrastructure control. The safety applications use DSRC [1] to provide wireless communications between vehicles and/or the fixed infrastructure. This however requires that a vehicle is equipped with an On Board Unit (OBU) and the infrastructure, e.g., at a traffic intersection, with a so-called Road Side Unit (RSU). Together, the DSRC devices form a VANET, which is somewhat similar to a mobile ad hoc network, however, connection between nodes may be very brief.

As DSRC is wireless, the safety applications may be subjected to the full spectrum of security vulnerabilities associated with such technologies. Furthermore, since they operate in a critical infrastructure, where failure of the safety applications could result in injury and loss of life, reliability is crucial. Any failure, may it be the result of benign reasons or malicious act, could result in the public's loss of confidence in the underlying technologies.

This research focusses on malicious act, and specifically wireless jamming. We consider stationary or mobile jammers and their potential impact on DSRC safety application reliability. Of special concern are scenarios where jamming is used to render safety applications useless. Such situations may arise when jamming is combined with creating a physical hazard. For example, imagine a person launching an object into traffic while jamming the region around the hazard. A driver seeing the hazard would react, e.g., by braking hard. But jamming DSRC messages indicating the braking event would result in failure to warn drivers without visual contact, potentially leading to rear-end collisions.

2. Background and Related Work

DSRC communication utilizes 75 MHz of bandwidth at 5.9 GHz (5.850-5.925 GHz) [2] [3]. There are seven 10 MHz channels, consisting of one Control Channel (CCH), i.e., channel 178 (denoted by CH178), and six Service Channels (SCH) with even numbers, i.e., CH172, 174, 176, 180, 182, and 184. The remaining 5 MHz are reserved for future use. The most important channel for DSRC safety applications is Safety Channel CH172, which is dedicated to these applications.

2.1. DSRC Safety Applications

A range of DSRC safety applications has been described in [4]. The applications rely on beacon messages that exchange vehicle status information. The beacon is called a Basic Safety Message (BSM) and it is periodically sent by each vehicle's OBU every 100ms. Each BSM contains vehicle-specific information like speed, heading, acceleration, and brake status, its Global Positioning System (GPS) location and elevation, as well as a field (*Dsecond*) with time information. Since the BSMs over CH172 are essential for all safety applications, we will consider jamming of this channel.

The safety applications described in [4] are focussing on crash scenarios and their prevention. The applications are 1) Emergency Electronic Brake Lights (EEBL), 2) Forward

Collision Warning (FCW), 3) Blind Spot Warning and Lane Change Warning (BSW+LCW), 4) Do Not Pass Warning (DNPW), 5) Intersection Movement Assist (IMA), and 6) Control Loss Warning (CLW). We have selected the EEBL safety application. Assume a single lane highway with two vehicles separated by a short distance, i.e., a Remote Vehicle (RV) followed by a Host Vehicle (HV) whose OBU is executing the EEBL application. Assume the RV brakes hard, e.g., due to a perceived hazard. This "braking hard" event is broadcast in its next BSM to all vehicles in its transmission range. The EEBL application in the HV, which receives the BSMs of vehicles in its vicinity, will be able to alert its driver of the event upon receiving the BSM indicating the braking event. This is of special value in situations with limited visibility, e.g., fog or when line of sight between HV and RV is blocked, e.g., by other vehicles.

2.2. Channel Access Rules

DSRC communication uses the IEEE 802.11p MAC protocol, which uses Enhanced Distributed Channel Access (EDCA), an improvement of the Distributed Coordination Function (DCF) used in IEEE 802.11 [5]. EDCA uses four different categories of Access Classes (AC) associated with each level of priorities: 1) AC0 for Background traffic (BK), 2) AC1 for Best Effort traffic (BE), 3) AC2 for Video traffic (VI) and 4) AC3 for Voice traffic (VO). EDCA is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to access channels. g When a node has a packet to transmit it senses the media, and if it is idle for an Arbitration Interframe Space (AIFS), the node delays transmission by a random backoff time. Specifically, a node selects a random backoff time from a Contention Window (CW) defined as $[0, CW+1]$, which is initialized to CW_{min}. If the transmission attempt fails, the interval size is doubled, until it reaches to CW_{max}. The backoff value will only be decreased when the channel is sensed to be idle. The node will send its packet immediately when the backoff value reaches to zero. Figure 1 depicts the timing related to channel access for different inter-frame spacings.

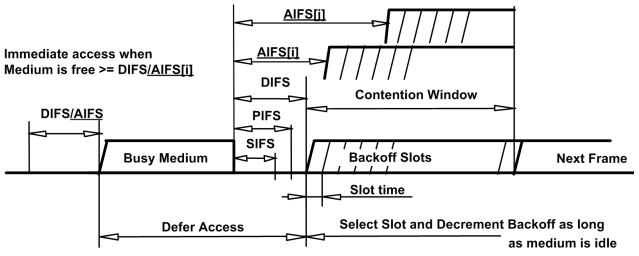

Figure 1. EDCA channel access prioritization [6]

2.3. Elementary Jamming Models

Jamming is the act of emitting radio signals to interfere with communication between nodes in a wireless network [7]. One goal of the jammer may be to decrease the Signal to Noise Ratio (SNR), thus making reception unreliable or impossible, or perhaps to destroy network packets. However, jamming can also be viewed from a data point of view as a Denial of Service (DoS), where the injection of what appears to look like valid data denies other nodes access to the media. Different jammer types have been discussed in the literature [7], [8]. Specifically, a *constant jammer* emits a constant stream of data, not necessarily following packet format or channel access timing rules, thereby not allowing other nodes to access the media. A *deceptive jammer* is somewhat similar, but unlike a constant jammer, it emits a stream of seemingly valid packets, however not following channel access rules. A *random jammer* switches between random jamming and sleeping durations. A *reactive jammer* listens to ongoing communication packets and jams briefly once a packet is detected, thereby corrupting/destroying the packet. Finally, an *intelligent jammer* is a protocol-aware jammer who can target specific packets or packet types. Beside the obvious difference in jamming behavior, the key issues for different jammers is detectability and power consumption, as described in [7], [8].

2.4. Selfish and malicious MAC misbehavior

The MAC protocol described in Subsection 2.2 assumes that every node that wants to access the media plays by the rules. A node is considered to be misbehaving if it does not follow the protocol rules, e.g., to gain an unfair advantage in transmitting its packets, or to deny other legitimate nodes transmitting packets. This misbehavior can lead to DoS attacks. MAC layer misbehavior can be classified into two general categories [9], 1) selfish misbehavior [10], [11] and 2) malicious misbehavior [7], [12].

A selfish node deliberately violates its backoff timer to obtain a larger portion of the shared channel. The selfish node thereby increases its data transmission rate at the cost of other nodes.

A malicious node could prevent other nodes from communicating by either constantly generating strong signals to disrupt a normal node's signal, or by transmitting fake packets to occupy the media. The so-called Sybil attack is also a malicious misbehavior [13], [14], where a malicious node impersonates several other nodes in order to disrupt the network. Compared to selfish behavior, malicious misbehavior is more difficult to detect and can result in more serious problems, greatly degrading the performance for normal users [9].

2.4.1. Selfish misbehavior detection techniques. A considerable amount of research has focussed on detection of selfish behavior. In [10] the authors present a modification to the IEEE 802.11 protocol to detect selfish misbehaving nodes by following these main steps: First, the receiver decides on the backoff value to be used by a sender and at the end of each transmission the receiver checks if the sender deviated from the protocol for that particular transmission. Second, if the receiver identified a deviation in transmission from the sender, it penalizes the sender, based on a particular

(penalty scheme). Third, if the receiver detects the deviation of a sender over multiple transmissions, it identifies the sender as misbehaving. They also propose an extension to this technique by adding multiple hosts to monitor the traffic in order to prevent receivers from misbehaving.

Another detection algorithm for selfish or greedy behavior in the MAC layer of IEEE 802.11 public networks was proposed in DOMINO [15]. DOMINO, can be implemented on any access point (AP) in the network. It periodically collects traffic traces of active nodes during short intervals of time called monitoring periods. Next the collected traces are analyzed using a series of tests in order to detect misbehaving nodes. DOMINO relies mainly on a large amount of historical data to perform its detection algorithm.

Schemes to detect and defend against MAC-layer selfish misbehavior in IEEE 802.11 multi-hop ad hoc networks was proposed in [9]. Their algorithm is based mainly on channel occupation durations or channel occupation ratio r. Based on these two parameters a selfish node can be detected as it will occupy the channel more than normal nodes.

A passive method for detecting selfish misbehaving nodes in VANET was presented in [16]. Their algorithm combined and enhanced linear regression and watchdog concepts. Both of these concepts had been used separately in Mobile Ad Hoc Network (MANET).

We will show that the new hybrid jammer has the potential to make innocent nodes appear selfish misbehaving for detection algorithms such as those shown above.

2.4.2. Malicious misbehavior detection techniques. Detection mechanisms for malicious misbehavior attacks have been shown in [12] and [17]. In [12] malicious misbehaving attacks are considered intelligent jamming attacks in an IEEE 802.11 network. Their technique monitored successful transmissions and collisions of nodes and analyzed how collision could be explained. Differentiation between abnormal and normal operation was based on observing the change in the distribution of packet collisions. In [17] VANET DoS attack detection was based on so-called "Packets entropy", by monitoring traffic traces during short monitoring windows. Based on the fact that selfish nodes emits more data packets, and given that when the probability of emission of packets changes, the entropy will also change, the distinction can be made between a normal network and a network under attack by calculating packets entropy in each case.

3. A New Hybrid Jammer for VANET

We now describe a new hybrid jammer that combines properties of constant, deceptive and random jammers. The jammer emits continuous random bits like a constant jammer but it may appear as regular packets, without following the CSMA protocol, like deceptive jammer. In addition the jammer will be dormant for most parts and only jam for specific durations, e.g., half a second to a few seconds. This makes it appear like a random jammer, but it will be shown in Subsection 3.3 that the time and duration of jamming is not random at all, but carefully selected. During jamming all other nodes believe that legitimate transmissions are taking place. As a result nodes cannot transmit any packets and queue, i.e., buffer, them instead until jamming stops and the media becomes available again. No packets will be lost as long as the queues of the nodes do not overflow. Due to this overall behavior, no messages of legitimate nodes are destroyed and the jamming cannot be detected as a malicious attack by mechanisms using packet error rates or delivery ratios. A formal definition of the new hybrid jammer will be given in conjunction with the EEBL safety application's BSM timing and queuing model, and their impact on the application reliability is analyzed.

3.1. EEBL Timing Model and Reliability

The EEBL safety application introduced in Subsection 2.1 is shown in Figure 2. Recall that the RV's "hard braking" event in response to an observed hazard needs to be communicated to the HV's safety application. Starting with the moment the RV brakes hard at t_{brake}, its BSMs will indicate this event in the BSM's *BrakeSystemStatus* field. For the EEBL application to be effective, the HV in the detection area has to receive a BSM with the event indication before t_{react}. In the figure BSM_x is the last BSM that can be received before this cutoff time is reached. An event indication received after t_{react} would result in an EEBL alert not giving the driver enough time to react.

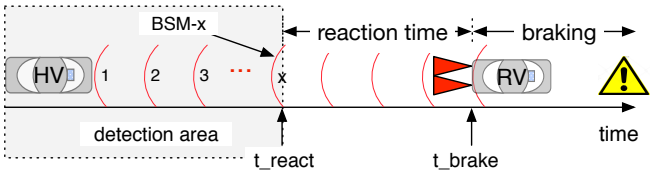

Figure 2. EEBL BSM Timing Model

The EEBL application reliability is directly linked to the probability of the HV receiving BSM messages before it is too late to react. Assume that the distance d between the HV and RV is equivalent to t_d seconds. Given that BSMs are spaced 0.1s in time, this distance accounts for $b = t_d/0.1$ safety messages. However, one can only consider those BSM that are received at or before t_{react}. Different values for reaction time have been used, e.g., in [18] a driver's minimum reaction time used was 0.7 seconds, whereas [21], [22] assumed it to be 1s. Let t_r denote the reaction time. Then reaction time accounts for $r = t_r/0.1$ BSMs. In line with the standard definition of reliability, i.e., $R(t)$ is the probability that the system is working to specifications during the entire time interval $[0, t]$ [20], we can define the EEBL application reliability as the probability of receiving at least one BSM message at or before t_{react}, i.e., one of BSM_i, for $i = 1, .., x$, where $x = b - r$. The safety application fails only if no BSM message is received at or before t_{react}. If one assumes that the reliability of one BSM is independent of that of another BSM, and using

unreliability $Q(t) = 1 - R(t)$, the probability of all x messages being lost is

$$Q(t) = \prod_{i=1}^{x} Q_i(t_i) \quad (1)$$

where $Q_i(t_i)$ is the probability that BSM$_i$ was not received and t_i is the time it should have been received. In [22] Q_i was computed based on packet error rates and packet delivery ratio. Equation 1 assumes that packet failure is independent. We will manipulate this independence of faults assumption via the jammer.

3.2. Transmission Queue Behavior

After an OBU generates a BSM it is placed in the transmission queue, which is a First-in First-out (FIFO) queue [23], [24]. Once the node has access to the media, e.g., using CSMA/CA, the BSM is taken from the queue for transmission. Should the node not be able to send the BSM before the subsequent BSM arrives, i.e., within 100ms, the new BSM is also queued. This could go on until the capacity of the transmission queue overflows, in which case packets are dropped.

With respect to timeliness, the longer a BSM is queued, the more outdated its information becomes. In [19] queuing and timing issues were discussed in the context to buffering and scheduling. They investigated two queuing mechanisms for use in the MAC layer. The first, Newest Packet Drop (NPD), also known as tail-drop queuing, implies that when a packet arrives at a full queue the newest packet is dropped. The second, Oldest Packet Drop (OPD), also known as head-drop queuing, drops the oldest packet when a new one arrives at a full queue. They further investigated FIFO and Last-in First-out (LIFO) scheduling of NPD and OPD.

In the absence of misbehavior jamming, given the relatively slow rate of 10 BSM/s, BSMs are unlikely to queue if traffic density is not overloading the media. However, during field tests related to the study of the impact of deceptive jamming on V2V communications, we observed excessive queuing. In the field test three OBU-equipped vehicles, V1, V2, and V3 passed a stationary deceptive jammer at a speed of about 35mph. The logging at V3 of BSMs sent from V1 and V2 just before the media was completely jammed is shown in Figure 3. In regions not jammed single BSMs from V1 and V2 were received with the expected spacing. Once the vehicles were affected by the jammer, gaps in reception were observed, as expected. However, bursts of BSM were logged, which followed small gaps of reception. After careful analysis of the timing and content of packets we could confirm that the bursts were due to OBU message queueing as the media was jammed with media access afterwards. This queuing and subsequent burst behavior will be exploited by the hybrid jammer.

3.3. Hybrid Jammer Definition

We now formally describe the behavior of the new hybrid jammer. Let Δt_{jam} denote the duration of jamming

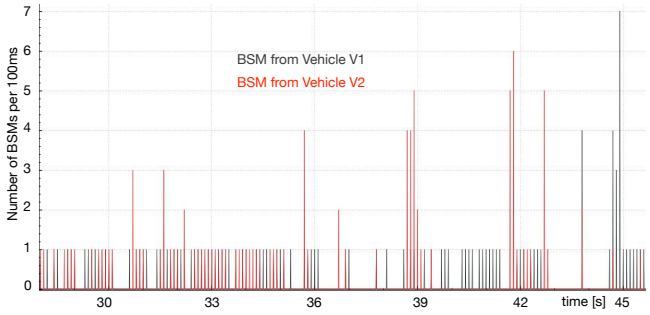

Figure 3. BSMs from vehicles 1 and 2 received by vehicle 3

and let t^s_{jam} and t^e_{jam} denote the time jamming starts and ends respectively. A jamming period Δt_{jam} is thus $\Delta t_{jam} = t^e_{jam} - t^s_{jam}$. Now assume that the queue size of the OBUs is q. Jamming for Δt_{jam} will theoretically result in each OBU in the jamming area queuing $m = \Delta t_{jam}/0.1$ BSMs, where 0.1s is the BSM spacing, i.e., 100ms. Several issues arise.

First, with respect to timeliness of BSM messages, jamming for a duration of Δt_{jam} will result in a reception delay d_i for each BSM$_i$ queued, i.e., after jamming stops at t^e_{jam} the minimum message delay of a queued BSM$_i$ is

$$d_i \geq \Delta t_{jam} + \sum_{1}^{i} t_{min}, \quad 1 \leq i \leq m \quad (2)$$

where t_{min} is the lower bound on the BSM transmission time from a specific OBU.

Second, a jamming period of Δt_{jam} will not result in the lost of BSMs if i) the period is short enough to not overflow an OBU's transmission queue, i.e., if $m \leq q$, and if ii) subsequent queue flushing of affected OBUs does not cause congestion.

An attacker can take advantage of both issues by selectively choosing Δt_{jam} to 1) intentionally causing BSM delays suiting its attack objectives, e.g., causing the EEBL to fail, and 2) ensuring the jamming duration does not cause queues to overflow. The consequences are multifold.

First, the attacker can minimize being detected by carefully selecting the smallest BSM delay that renders a DSRC safety application useless. For example, if one blocks reception of x BSMs for the HV in the scenario depicted in Figure 2, the driver of the HV will not have ample time to react to the hazard. A jamming period of $\Delta t_{jam} = x0.1s$ would theoretically achieve this.

Second, the jammer makes other vehicles appear to be misbehaving. Since jamming causes each affected OBU to queue BSMs that are subsequently send in bursts after t^e_{jam}, the OBUs appear to be selfishly misbehaving by the algorithms described in Subsection 2.4. Specifically, each OBU's burst will be interpreted as getting disproportional access to the media, since the BSM rate of each node is expected to be 10 BSMs per second.

Third, jamming detection mechanisms relying on Packet Delivery Ratio (PDR), e.g., [25], will be ineffective as the jammer does not cause packets to be dropped.

From the EEBL safety application point of view, in the end what matters is that the application fails if no BSMs indicating an event are received in time to alert the driver before it is too late to react. Even assuming BSM delivery omissions were independent, which they are not, this would be an instance in which the unreliability in Equation 1 would evaluate to one, $Q(t) = 1$ or $R(t) = 1 - Q(t) = 0$. This constitutes failure of the EEBL application.

3.3.1. Stationary Attack Model. The stationary version of the jammer is demonstrated in the scenario depicted in Figure 4a). Assume a hazard is introduced and the jammer, positioned on the roadside next to the RV, jams for Δt_{jam} in coordination with the creation of the hazard. This causes the OBU of the RV to queue BSMs, as it cannot access the media during the jamming time. Once jamming stops, as indicated in Figure 4b), the RV sends all queued BSMs in a burst, followed by regularly spaced BSMs. The EEBL in the HV, which did not receive BSMs during Δt_{jam}, will receive its first BSM from the burst when it is already too late to react, i.e., after time t_{react}.

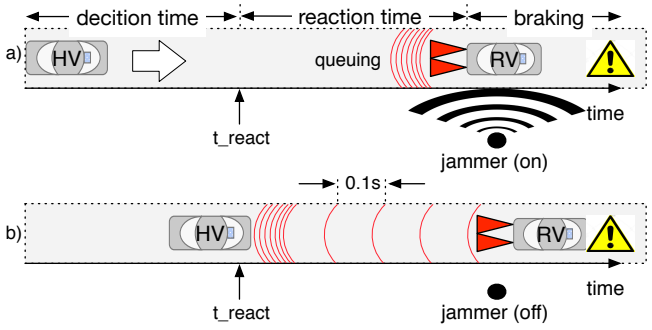

Figure 4. Stationary jammer

3.3.2. Mobile Attack Model. The scenario in Figure 5 shows how two collaborating attack vehicles H and J can cause the safety application to fail. Assume, as shown in part a) of the figure, that vehicle H causes a hazard, e.g., by launching an obstacle into oncoming traffic. The driver of the RV, who sees the hazard, will take some time to react. Now consider the scenario just before RV's driver reacts, as shown in Figure 5b). The collaborating vehicle J, which has a mobile jammer, follows vehicle H at a distance that positions it close to the RV just before the driver of the RV is expected to react to the hazard. Specifically, vehicle J keeps a distance from H short of 0.7s, the minimum reaction time. After H induced the hazard vehicle J jams for Δt_{jam}, which can be determined based on the speed of HV and its distance to RV. An example is $\Delta t_{jam} = d_{RV,HV}/v_{HV} - 0.7s$, the time separation between the RV and HV minus the reaction time. Just as in the case of the stationary jammer, once jamming blocks the reception of BSMs in HV's detection area, the burst of delayed BSMs from the RV arrives too late to warn the driver of HV about the braking event.

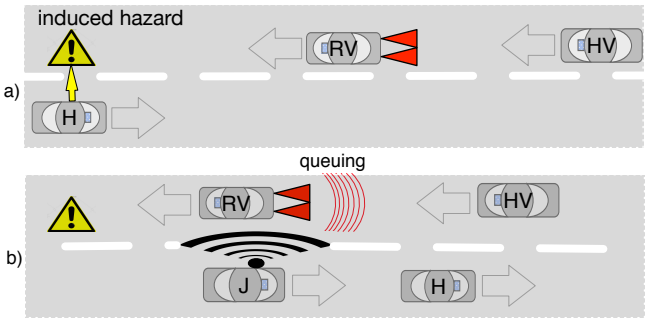

Figure 5. Mobile jammer

3.4. Jamming Impact on Queuing

As indicated in the discussion of Figure 3 in Subsection 3.2 queuing of BSMs due to jamming was observed in real tests using commercially available OBUs. To validate the hybrid jammer's effect on queuing and to investigate if queuing is deterministic, we conducted experiments using three Locomate Classic OBUs from Arada Systems [26]. One OBU was programmed to act as the hybrid jammer, the second served as the RV and the third as the HV. The experiments were conducted in a controlled environment with no objects interfering with communications. The test parameters used are shown in Table 1.

TABLE 1. HYBRID JAMMER PARAMETERS

OBU Model	Arada Systems LocoMate Classic
Number of OBUs	3 (2 OBUs for two vehicles and 1 for the stationary jammer)
BSM generation	10 packets/s
Channel	Safety Channel 172
Transmitter power	21 dBm
Data rate	6Mbps
Jammer power and data rate	18 dBm, 6Mbps

The impact of jamming with $\Delta t_{jam} = 1$, 2, 3 and 4s of a typical experiment can be seen in Figure 6, where the number of BSMs that the HV received from the RV per 100ms is shown. After each jamming period a burst of BSMs, consistent with the number of BSMs expected to have been queued based on Δt_{jam}, can be observed. However, after careful examination the experiment also revealed that jamming in practice is not as precise as in theory, and we observed several factors that introduced variability.

First of all, the time from starting the jammer until it effectively jammed the media was nondeterministic, as it was not possible to start jamming precisely at the time intended. We attribute the observed differences to process initialization delays and runtime overhead of the Arada LocoMate Classic's operating system, which is Linux based, and the overhead associated with the jammer program. This

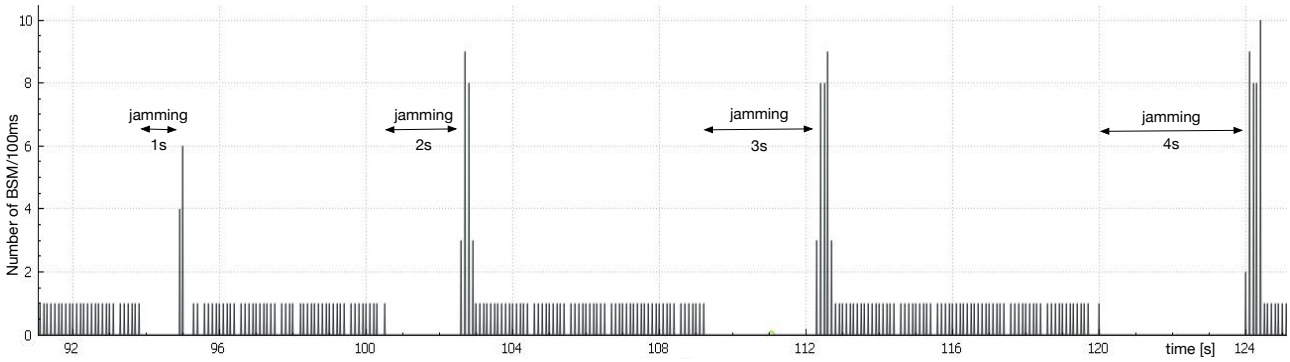

Figure 6. Queuing effect for jamming periods of 1, 2, 3, and 4s

delay can be observed in the scenario with $\Delta t_{jam} = 1$, which actually resulted in an effective jamming period slightly longer than 1s.

The second factor that created nondeterminism was attributed to the Arada Locomate Classic OBUs way of flushing their buffer. Specifically, experiments revealed that BSM spacing during flushing was on average 12.5ms, with minimum and maximum observed spacings as 10ms and 16ms respectively, and standard deviation of 1.6. In Figure 6 this behavior was responsible for several spikes after the jamming period rather than one large spike.

Thirdly it should be noted that the figure only shows BSMs sent by the RV and received by the HV. The HV also queued messaged during jamming, which also accessed the media using CSMA/CA. However, due to the low utilization of the media this should have had minimal impact on the data in the figure.

The experiments further suggested that the Arada Locomate Classic OBUs queued up to around 40 BSMs before messages were dropped.

4. Hybrid Jammer Detection Approaches

We will now present a hybrid jamming detection algorithm that detects hybrid jamming with a maximum jamming time of t_{max}. During actual jamming of $\Delta t_{jam} \leq t_{max}$. Algorithm 1 outlines detection executing in the receive thread in each OBU. In order to detect omissions of BSMs a Vehicles Neighborhood Table (VNT) of records is defined. The i^{th} record in VNT stores 1) the last BSM received from vehicle i, 2) receiving time of this BSM, and 3) the number of missing BSMs for vehicle i. Whereas the algorithm considers any BSM, it should be noted that for all practical purposes only BSMs from vehicles ahead of the HV could be selected, as they are relevant to the EEBL application. Since a BSM is expected from each vehicle approximately every 100ms, the omission of a BSM from vehicle i can be detected, e.g., using a watchdog mechanism, as indicated in the first "if" statement of the algorithm. If the time passed since the last BSM was received exceeded the maximum jamming time of t_{max}, it is deleted from the table.

START: Receiving Thread
if *(BSM not received)* **then**
  if *(time since last BSM reception $> t_{max}$)* **then**
    Delete vehicle record from VNT;
  else
    Increment $VNT[i].MissingBSM$;
  end
else
  if *(this is the first BSM)* **then**
    Add new vehicle record to VNT;
  else
    Diff$_1 \leftarrow |Dsecond_{new}$ - $Dsecond_{saved}|$;
    Diff$_2 \leftarrow |Dsecond_{HV}$ - $Dsecond_{new}|$;
    if *(Diff*$_1$ *<<100ms)* **then**
      Call misbehaving detection technique ;
    else
      if *(MissingBSM* $\leq \alpha$*)* **then**
        $VNT[i].BSM \leftarrow NewBSM$;
        $VNT[i].MissingBSM \leftarrow 0$;
      else
        $VNT[i].BSM \leftarrow NewBSM$;
        Decrement $VNT[i].MissingBSM$;
        if *(Diff*$_2/100ms \approx$
        $VNT[i].MissingBSM$*)* **then**
          Jamming detected. Mark vehicle as victim of jamming;
        end
      end
    end
  end
end
Goto: START;

Algorithm 1: Hybrid Jamming Detection

If a BSM is received from a vehicle that is not in VNT then a new record is created. A missed BSM from a vehicle does not necessarily imply the presence of a jammer, but would most likely be due to environmental conditions or collisions. We therefore declare a threshold α to account for such benign message losses. It the number of missed BSMs surpasses α ongoing jamming is assumed.

Two values $Diff_1$ and $Diff_2$ are used to identify if misbehavior is occurring or if a node is falsely accuse of such behavior. Specifically, $Diff_1$ is the difference in time between the creation of the last received and the currently received BSM. If this time is much less than 100ms a misbehavior detection algorithm should be executed. The difference in time $Diff_2$ between the *Dsecond* field of the received BSM and the time at the HV is used to identify if a vehicles is innocently framed as behaving selfishly. The value in $Diff_2/100ms$ should be the number of missing BSMs if a burst occurred. This is used to determine that the vehicle is not misbehaving, but sending a burst queued due to jamming.

5. Conclusions

This research presented a new hybrid jammer capable of impacting DSRC safety applications. The jammer exposed queueing behavior that was exploited for an effective attack strategies. Scenarios for stationary and mobile jammers were presented together with their impact on the EEBL safety application, however we expect that the jammer will have similar implications for other DSRC safety applications. Experiments conducted with commercial DSRC equipment validated the expected impact of the jammer. A mechanism was presented that allowed detection of hybrid jamming. This algorithm can also distinguish between misbehaving nodes and nodes that are impacted by the jammer in such a way that makes them appear to be selfishly misbehaving by current misbehavior detection strategies. Current research focusses on measuring the impact of the jammer and jamming detection strategy in extended field tests, the results of which are intended to be published separately.

References

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

[2] 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) Spec., ASTM E2213-03, 2010.

[3] *Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band)*, Federal Communications Commission FCC 03-324, 2004.

[4] *Vehicle Safety Communications-Applications (VSC-A) Final Report*, DOT HS 811 492 A. U.S. DoT, NHTSA. September 2011.

[5] *802.11-2007 - IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part 11: Wireless lan medium access control (MAC) and physical layer (PHY) specifications*, IEEE Std 802.11, 12 June 2007.

[6] *IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements*, IEEE Std 802.11e, 2005.

[7] Xu W, Trappe W, Zhang Y, Wood T, *The feasibility of launching and detecting jamming attacks in wireless networks* In: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2005, pp 46-57.

[8] K. Pelechrinis, et. al., *Denial of Service Attacks in Wireless Networks: The Case of Jammers*, Communications Surveys & Tutorials, IEEE, Vol.13, No.2, pp.245-257, 2^{nd} Quarter 2011.

[9] M. Li, S. Salinas, P. Li, J. Sun, and X. Huang, *MAC-Layer Selfish Misbehavior in IEEE 802.11 Ad Hoc Networks: Detection and Defense*, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 6, JUNE 2015.

[10] P. Kyasanur and N. Vaidya, *Selfish MAC layer misbehavior in wireless network*, IEEE Trans. on Mobile Computing, vol. 4, no. 5, pp. 502-516, Sep. 2005.

[11] Z. Lu, W. Wang, and C. Wang, *On order gain of backoff misbehaving nodes in CSMA/CA-based wireless networks*, in Proc. IEEE Conf. Comput. Commun., San Diego, CA, USA, Mar. 2010, pp. 1-9.

[12] L. Toledo, and X. Wang, *Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks*, IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 347-358, Sep. 2008.

[13] T. Zhou, R. R. Choudhury, and P. Ning, *P2dap-sybil attacks detection in vehicular ad hoc networks*, IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 582-594, Mar. 2011.

[14] H. Yu, P. B. Gibbons, and M. Kaminsky, *Sybillimit: A near-optimal social network defense against sybil attacks*, IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 885-898, Jun. 2010.

[15] M. Raya, J. Hubaux, and I. Aad, *Domino: A system to detect greedy behavior in ieee 802.11 hotspots*, in Proc. ACM 2nd Int. Conf. Mobile Syst., Appl. Serv., Boston, MA, USA, Jun. 2004, pp. 84-97.

[16] M. N. Mejri and J. Ben-Othman, *Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks*, Global Communications Conf. (GLOBECOM), 2014 IEEE, pp.5032 -5037

[17] M. N. Mejri and J. Ben-Othman, *Entropy as a new metric for denial of service attack detection in vehicular ad-hoc networks*, In Proceedings of the 17th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems, 2014.

[18] X. Ma, X. Yin, and K.S. Trivedi, *On the Reliability of Safety Applications in VANETs*, Invited paper, International Journal of Performability Engineering Special Issue on Dependability of Wireless Systems and Networks, 8(2), March 2012.

[19] Hendriks L., *Effects of Transmission Queue Size, Buffer and Scheduling Mechanisms on the IEEE 802.11p Beaconing Performance*, 5th Twente Student Conference on IT, June 20, Enschede, NL, 2011.

[20] W. B. Johnson, *Design and Analysis of Fault-Tolerant Digital Systems*, Addison-Wesley Publishing Company, New York, 1989.

[21] H. Alturkostani, A. Chitrakar, R. Rinker, and A. Krings, *On the Design of Jamming-Aware Safety Applications in VANETs*, Cyber and Information Security Research Conference (CISR 2015), Oak Ridge National Laboratory, Tennessee, USA, April 2015.

[22] Ahmed Serageldin, Hani Alturkostani, and Axel Krings, *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.

[23] IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation, IEEE Std 1609.4TM, 2010.

[24] *IEEE Standard for Information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*, IEEE Std 802.11p, 2010.

[25] A. Nguyen, et.al., *Solution of detecting jamming attacks in vehicle ad hoc networks*, Proc. 16th ACM international conference on Modeling, analysis & simulation of wireless and mobile systems (MSWiM 13), ACM, New York, 405-410, 2013.

[26] Arada Systems, *www.aradasystems.com*