Sporadic Ultra-Time-Critical Messaging in V2X

Yulin Shao, Soung Chang Liew, and Jiaxin Liang

***Abstract*—Life-critical warning message, abbreviated as *warning* message, is a special event-driven message that carries emergency warning information in Vehicle-to-Everything (V2X). Two important characteristics that distinguish warning messages from ordinary vehicular messages are *sporadicity* and *ultra-time-criticality*. This paper puts forth a medium-access control (MAC) protocol for warning messages. To circumvent potential inefficiency arisen from sporadicity, we propose an override network architecture whereby warning messages are delivered on the network of the ordinary vehicular messages. Specifically, a vehicle with a warning message first sends an interrupt signal to pre-empt the transmission of ordinary messages, so that the warning message can use the wireless spectrum originally allocated to ordinary messages. In this way, no exclusive spectrum resources need to be pre-allocated to the sporadic warning messages. To meet the ultra-time-criticality requirement, we use advanced MAC techniques (e.g., coded ALOHA) to ensure highly reliable delivery of warning messages within an ultra-short time in the order of 10 ms. The overall MAC protocol operates by means of *interrupt-and-access*. We investigate the use of spread spectrum sequences as interrupt signals. Simulation results show that the missed detection rate (MDR) of the interrupt signals can be very small given sufficient sequence length, e.g., when SIR is -32 dB, a 0.43 ms sequence (64512 symbols, 150 MHz) can guarantee an MDR of 10^{-4}. For channel access, simulation results indicate that coded ALOHA can potentially satisfy the ultra-time-criticality requirements of warning messages. In the stringent scenario where 30 emergency nodes broadcast warning messages simultaneously, the message loss rate can be kept lower than 10^{-4} with delay less than 10 ms.**

I. Introduction

With the explosive growth of vehicles on road, safety has become a major concern for future intelligent transportation systems (ITS) [1]. Statistical data show that the number of crashes in the United States is nearly 6 million each year [2]. Vehicle-to-Everything, abbreviated as V2X, is a promising means to cut the road toll [3]. Through V2X, all the entities on the road (e.g., vehicles, road side units and pedestrians) are connected, hence, they can exchange safety messages and cooperate to prevent road accidents or cut down fatality and injury rates when they do occur.

Safety messages in V2X can be classified into two categories [3]: i) *heartbeat* messages. Each on-road node periodically broadcasts heartbeat messages to declare its existence, current state and environment information. Receiving nodes can then evaluate whether there are hazards from information disseminated by transmitters and data gathered from the environment. ii) *event-driven* messages. Safety in V2X is not limited to passive evaluation of the received heartbeats. An on-road node encountering unexpected events could actively broadcast event-driven messages so that the surrounding nodes can respond quickly. Typical events that may induce event-driven messaging include lane change, roadwork, ambulance approach, to name a few.

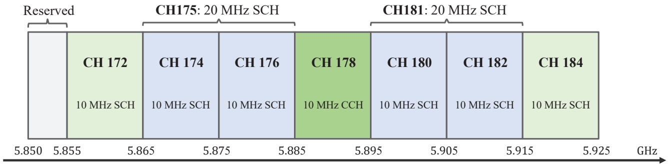

Fig. 1. The 75 MHz "5.9 GHz band". Channel 178 is a control channel dedicated for safety-message transmission. The other six channels are service channels, in which channel 172 and 184 are reserved for future advanced applications. Service channels can be used to transmit both safety and non-safety messages.

Among event-driven messages, life-critical warning messages (hereinafter, referred to as *warning* messages) deserves particular attention. Warning messages are triggered by extreme traffic emergencies that are likely to cause casualties, e.g., hard braking on the highway, imminent crash, swerving vehicles at opposite lane, etc. Two important characteristics that distinguish warning messages from ordinary vehicular messages are that (i) they are rare and sporadic. Statistics indicate that there are on average 1.04 fatal crashes every 100 million miles a vehicle travels [2]. On the other hand, (ii) when warning messages appear, they must be delivered within an ultra-short useful lifespan – extremely short time-to-live (TTL), or else their function to prevent accidents and fatalities cannot be fulfilled. According to the automotive white paper from 5G-PPP [1], the maximum tolerable end-to-end delay of these safety-of-life messages is 10 ms, and the maximum tolerable message loss rate (MLR) within 10 ms is 10^{-4}. We refer to these characteristics as *sporadicity* and *ultra-time-criticality*.

Warning messages are short but multiple warning messages may arrive in a batch. Typically, a warning message contains the following data [4]: node ID (4 bytes), message generation time (4 bytes, modulo one minute, with resolution 1 μs), message type (2 bytes, e.g., braking, acceleration, steering) and message attributes (14 bytes, e.g., for braking message type, the attributes could contain brake force, current vehicle speed and wheel state) for an aggregate of 24 bytes. Warning messages may arrive in a batch because a single accident can easily trigger multiple emergency responses from multiple nearby nodes. As a result, these emergency nodes (typically less than 30) can broadcast multiple warning messages simultaneously.

*This work was supported by the General Research Funds (Project No. 14226616) established under the University Grant Committee of the Hong Kong Special Administrative Region, China. Y. Shao, S. C. Liew and J. Liang are with the Department of Information Engineering, The Chinese University of Hong Kong. Email: {sy016, soung, lj015}@ie.cuhk.edu.hk.

In V2X, safety messages are disseminated by simple means of one-hop broadcast. Multiple access control (MAC) designs are especially crucial if the stringent delay and reliability requirements are to be met. As shown in Fig. 1, the Federal Communications Commission (FCC) in the United States allocates 75 MHz "5.9 GHz band" for V2X communication [4], [5], based on which many MAC protocols have been proposed and developed to support safety-message broadcasting [4]–[8]. However, existing schemes are designed primarily for heartbeat messages and conventional event-driven messages. When it comes to sporadic ultra-time-critical messaging, none of them can meet the stringent delay and reliability requirements.

To fill this gap, this paper puts forth a medium-access control (MAC) protocol tailored for the delivery of life-critical warning messages without exclusive allocation of wireless spectrum to them. Two underpinnings of our MAC protocol are as follows: i) To address sporadicity efficiently, we build our MAC protocol upon an override network architecture whereby wireless spectrum originally allocated to regular vehicular network is used to deliver warning messages only when they appear. Specifically, no wireless spectrum is dedicated exclusively to warning messages since they rarely occur. A vehicle with warning messages will first send an interrupt message to pre-empt the transmission of regular vehicular messages so that the warning message can follow after that. ii) To address ultra-time-criticality, we use advanced MAC techniques (e.g., coded ALOHA) to ensure delivery of warning messages within the stringent delay and reliability targets. In particular, in a life-threatening situation, multiple vehicles may have life-critical messages to send. A MAC protocol that does not incur excessive hand-shaking overhead to coordinate the transmissions of these vehicles is critical if the stringent delay target is to be met.

In short, the overall MAC protocol operates by means of interrupt-and-access. For wireless interrupt, we devise an interrupt mechanism for V2X in which the interrupt signals are spread spectrum sequences. Simulation results show that the missed detection rate (MDR) of the interrupt signals can be very small provided that the interrupt sequences are long enough, e.g., when SINR is -30 dB, a 0.43 ms sequence (64512 symbols, 150 MHz) can guarantee an MDR of 10^{-4}. For channel access, simulation results indicate that coded ALOHA can potentially satisfy the ultra-time-criticality requirements of warning messages. In the stringent scenario where 30 emergency nodes are broadcasting simultaneously, the message loss rate (MLR) can be kept lower than 10^{-4} with delay less than 10 ms.

II. State-of-The-Art V2X MAC Protocols

Existing MAC protocols for V2X communication operate in either a distributed or a centralized manner[1]. Centralized MAC designs, e.g., LTE-based MAC [6], have certain limitations: i) Infrastructure could be a single point of failure. These MAC protocols may not function when infrastructure failure occurs or when vehicles are out of the coverage of the infrastructure (e.g., in blind zone, tunnels, and underground parking lots). ii) The coordination-based framework, e.g., schedule-before-transmit, does not fit delay-sensitive applications, owing to the extra delay and overhead consumed. Distributed self-organizing MAC designs are in general more suitable for ultra-delay-sensitive warning messages [1].

A. IEEE 802.11p

Dedicated short-range communication (DSRC) [4] refers to the sets of standards on the 5.9 GHz band[2]. The MAC protocol in DSRC, i.e., IEEE 802.11p [9], is an amendment from IEEE 802.11a with enhanced distributed channel access (EDCA) Quality-of-Service (QoS) extension. In 802.11p, both heartbeat and event-driven messages share the 10 MHz control channel (CCH) by means of carrier sensing multiple access (C-SMA). In particular, different types of messages are assigned with different priorities: high-priority messages have smaller interframe spacing and backoff waiting time so that they have priority over low-priority messages in channel access.

There are three main reasons why 802.11p is not suitable for sporadic ultra-time-critical messaging, even if we assign the highest priority to warning messages.

i) Delay concern – In 802.11p, messages with different priorities share the same control channel. When high-priority warning messages are generated, a low-priority message may be in the midst of occupying the channel. As a result, the warning messages must wait until the channel is idle. Furthermore, even if the channel is idle, multiple warning messages with the same high priority may compete for the channel simultaneously, leading to a high collision rate that may significantly increases the delay.

ii) Lack of acknowledgment (ACK) – Warning messages are broadcasted for all vehicles in the vicinity of the warning-message generating vehicle. However, requiring an ACK from each one-hop neighbor of the broadcaster (potentially hundreds of nodes) can be highly costly. As a result, 802.11p does away with ACK for broadcast messages. This means that nodes cannot detect collisions and there is no retransmission. In other words, collisions mean packet loss, and this makes 802.11p highly unreliable. A simple calculation shows that, if we set the contention window to 7 (7 is already the maximum contention window for the access category with the highest priority [9]), the collision rate is as high as 50.95% when there are 10 warning-message transmitters, and this number increases to 92.11% when there are 30 transmitters.

iii) Hidden node problem – To tackle the hidden node problem, RTS/CTS handshaking is implemented in conjunction with CSMA in IEEE 802.11a. However, in 802.11p, the hidden node problem is left unsolved, because for broadcast messages, the frequent RTS/CTS handshakes consumes two much resource. As a result, a warning broadcast message

[1] Some hybrid MAC designs, e.g., LTE-ProSe [7], support both distributed and centralized modes.

[2] The sets of standards in Europe are referred to as C-ITS [5]. DSRC and C-ITS share similar PHY and MAC layers.

may collide with another warning broadcast message two hops away, leading to packet loss.

B. TDMA-based MAC

Vehicular MAC protocols may also be based on time division multiple access (TDMA). Two representative examples are ADHOC MAC [10] and its multi-channel evolution VeMAC [8].

As with IEEE 802.11p, VeMAC use the control channel (CH 178) in the 5.9 GHz band for both heartbeat and event-driven messages. This 10 MHz channel is assumed to be time-slotted, and every M slots are grouped together as a frame. When operated with VeMAC, each node occupies at least one slot in every frame for the broadcast of its heartbeat message. If a node has an event-driven message to broadcast, it will need to acquire one more slot. In particular, the slots a node occupies must be different from the slots occupied by any of its neighbors within two hops (this guarantees that there is no hidden node problem). How nodes within two hops coordinate with each other and occupy different slots is an essence of VeMAC.

To enable sporadic ultra-time-critical messaging in the context of VeMAC, all nodes can reserve one slot every 10 ms to cater for the rare occasion when they have warning messages to broadcast. However, simple calculation indicates that this is not viable. Assuming the slot duration is 50 μs, and therefore, there are 200 slots available in 10 ms, if there are 200 nodes within two hops (in practice could be up to 1000), then all the slots are reserved by these nodes for warning messaging alone. Even if we assumed sparse nodes, reserving resources for warning messaging is quite inefficient, because warning messages are rare and sporadic.

Instead of exclusive reservation of slots, a node could attempt to acquire a slot only upon the generation of a warning message. However, slot acquisition under VeMAC takes one or more frames (a frame usually lasts for 100 ms [8]), because the transmitter must wait for all its one-hop neighbors' ACKs to make sure the new slot is free for it to use. Worse still, when there are K nodes with warning messages, the interaction process for them to acquire K different new slots can take an inordinate amount of time.

III. An Override Architecture

Let us consider a typical V2X scenario where K_{all} on-road nodes are communicating with each other on the 5.9 GHz band in an ad-hoc manner. Each node is equipped with two sets of half-duplex transceivers TRX$_1$ and TRX$_2$. TRX$_1$ is aligned to the 10 MHz control channel (CH 178), on which nodes exchange heartbeat or conventional event-driven messages to get an overall perception of the environment. TRX$_2$ is aligned to the 40 MHz service channels (CH 175 and 181), on which nodes exchange non-safety messages, e.g., infotainment messages.

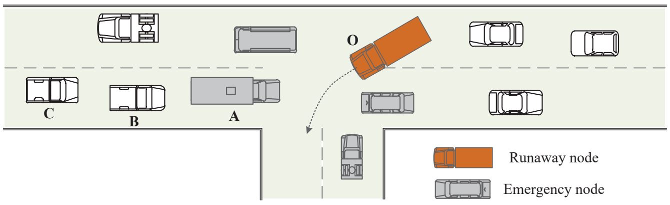

Fig. 2. The runaway vehicle O violates the traffic light. This accident triggers the urgent reactions of K nodes ($K = 4$ in this figure), and each of them generates a warning message to warn its nearby nodes.

As illustrated in Fig. 2, an accident suddenly happens: a runaway vehicle O violates the traffic light and runs to an opposite lane. This accident triggers the urgent reactions of K nearby nodes, and each of them generates a life-critical warning message to warn its nearby nodes. For example, node A brakes hard, triggering a warning message informing its neighbors (e.g., nodes B and C) of its emergency braking caused by the runaway node O, so that they could react in time to avoid further crashes.

These life-critical warning messages have stringent delay and reliability requirements. In this sense, we may need to assign them sufficient time-frequency spectrum resources, so that the stringent QoS requirements can be met. On the other hand, warning messages are highly sporadic, hence, assigning them exclusive resources is highly inefficient, because these resources are wasted most of the time in the absence of life-critical events. This motivates us to build the warning-message MAC protocol upon an override network architecture, where life-critical warning messages share the 40 MHz service channels with non-safety messages. In non-emergency situations, non-safety messages are the primary users on the service channels. When emergency arises, high-priority warning messages will override non-safety messages and seize the service channels[3].

Our override architecture operates by means of interrupt-and-access: nodes with incoming warning messages send interrupt signals to nodes transmitting non-safety messages to pre-empt them so that the nodes with warning messages can transmit warning messages on the service channels. Sections IV and V provide the details of wireless interrupt and channel access, respectively.

IV. Wireless Interrupt

Interrupt is a technique widely used in computer systems for multitasking with different priorities. Specifically, an incoming high-priority task triggers an interrupt signal to the central processor, so that the processor can suspend the currently ongoing low-priority task and process the high-priority task immediately. Interrupt is rarely used in conventional wireless communication systems. It is, however, useful for our application scenario.

[3] In practice, warning messages can override the whole 40 MHz bandwidth or part of the bandwidth of the service channels, e.g., override only the 20 MHz channel 181, so that non-safety messages would not be totally deprived of services.

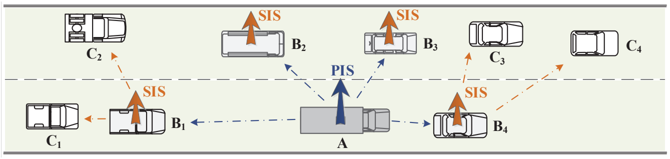

Fig. 3. Interrupt in V2X. The emergency node A broadcasts the PIS to its one-hop neighbors, and detecting a PIS will trigger the broadcasting of SIS. All node A's neighbors within two hops will keep silent after they receive a PIS or SIS.

A. Interrupt in V2X

In the vehicular network, if an emergency node intends to broadcast a warning message successfully on the service channels, a prerequisite is that all its one-hop and two-hop neighbors are silent on these channels. The objective of wireless interrupt in V2X is to silent these neighbors (i.e., neighbors within two hops) in case they are halfway transmitting on the service channels.

To this end, two interrupt signals, a primary interrupt signal (PIS) and a secondary interrupt signal (SIS), are defined. For our MAC protocol, interrupts proceed as follows:

i) A node with warning message first broadcasts a PIS.

ii) Any node detecting the PIS then broadcasts a SIS.

iii) Any node detecting a PIS or a SIS keeps silent on the service channels for 10 ms, including nodes that are halfway transmitting on a service channel when the PIS or SIS is detected[4].

An example is given in Fig. 3, where the emergency node A sends a PIS to pre-empt other nodes from using the service channels. The one-hop neighbors of A are $\boldsymbol{B} = \{B_1, B_2, B_3, B_4\}$, and, the two-hop neighbors of A are $\boldsymbol{C} = \{C_1, C_2, C_3, C_4\}$. First, node A broadcasts the PIS. The instant A's one-hop neighbors $\boldsymbol{B}$ detect the PIS, they keep silent on the service channels. Further, the detection of PIS triggers each of them to broadcast an SIS, so that A's two-hop neighbors $\boldsymbol{C}$ can detect the SIS and keep silent on the service channels as well. Once they have received a PIS or a SIS, node A's one-hop and two-hop neighbors will be silent on the service channels in the next 10 ms, and node A can broadcast the warning message safely.

Note that multiple overlapped PISs and SISs may be broadcasted simultaneously (e.g., when there are multiple warning-message transmitters). A node may detect the multiple PIS and SIS separately, and respond to each of the interrupt signal following rule (iii).

B. Interrupt signal design

We now present our designs for the PIS and SIS. Potentially, there are two alternatives: in-band interrupt and out-of-band interrupt. We could interrupt in-band[5] by exploiting special features of non-safety signal on the service channels. For instance, assuming the non-safety messages are carried by OFDM signals, we could transmit the interrupt signal on the guard-band subcarriers.

This paper considers out-of-band interrupt. Specifically, we transmit interrupt signals on the 5.8 GHz ISM band. PIS and SIS are designed as spread-spectrum sequences on this 150 MHz band, so that they can be detected in the presence of interference.

1) Interference on the 5.8 GHz band: The 5.8 GHz ISM band (5.725-5.875 GHz) is a free radio band centered on 5.8 GHz, the channel characteristics of which is similar to that of 5.9 GHz vehicular band. The primary traffic on the 5.8 GHz band is Wi-Fi signal, and Wi-Fi are commonly deployed indoors.

To evaluate the interference of indoor Wi-Fi signal to our outdoor interrupt signal, we conducted an experiment over our campus to capture 5.8 GHz Wi-Fi signal using USRP X310 (with BasicTX daughter board). The experimental data indicates that in the outdoor environment, i) most of the time, the 5.8 GHz band was calm and quiet, and nothing can be detected; ii) when Wi-Fi signal was detected on the 5.8 GHz band, the signal power was much lower than the indoor power.

In one experiment, an access point (AP, Linksys EA6900) was deployed indoors. The AP used Wi-Fi channel 153 (5.765 GHz) with 20 MHz channel bandwidth. We measured the received Wi-Fi signal intensities from the AP at two locations. The first location was indoor (5 meters from the AP, LOS), and the second location was outdoor (straight distance 20 meters from the AP, NLOS).

The Power Spectral Densities (PSDs) of the received signals captured indoors and outdoors are plotted in Fig. 4. As can be seen, there is a 32-dB gap between them. In particular, for the outdoor signal, the signal-to-noise ratio (SNR) is about 11.3 dB over the 150 MHz ISM band.

2) Interrupt signal design: This subsection presents the design of PIS and SIS on the 5.8 GHz ISM band. We only explain the generation and detection of PIS in the following, SIS is generated and detected similarly.

The PIS consists of Q N-point Zadoff-Chu (ZC) sequences embedded in a Q-point maximum-length sequence (m-sequence), for a total of QN samples. Denote the m-sequence by $\boldsymbol{c_p}$. Let $\boldsymbol{z}$ be a ZC sequence given by [11]

$$z[n] = \begin{cases} \exp\frac{-j\pi M n(n+1)}{N} & \text{for } N \text{ odd,} \\ \exp\frac{-j\pi M n^2}{N} & \text{for } N \text{ even,} \end{cases}, \tag{1}$$

where $n = 0, 1, 2, ..., N-1$, and M is a positive integer coprime to N. For our application, we set $M = 1$ (the reason for choosing $M = 1$ will be explained later).

[4] For any neighbor within two hops of an emergency node, interrupt is successful as long as at least one interrupt signal is detected, whether it is PIS or SIS.

[5] Another alternative to realize in-band interrupt is full duplex communication. However, full duplex communication requires dedicated full duplex transceivers, i.e., tailor-made RF chips with self-interference cancellation. Interrupt via full-duplex techniques is overkill, because unlike the receiver of a full-duplex link, the receiver of an interrupt does not need to receive a data stream in the reverse direction; it only needs to be able to detect the presence of an interrupt signal.

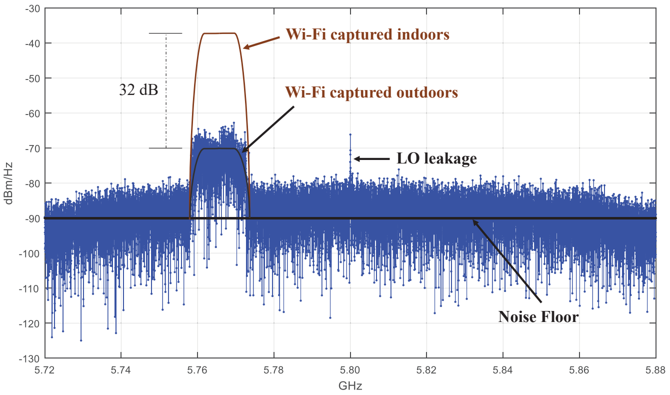

Fig. 4. The PSDs of the 5.8 GHz Wi-Fi signal captured indoors and outdoors, where the AP transmits 20 MHz Wi-Fi signal on channel 153 (5.765 GHz). The SNR of the outdoor received signal is 20 dB over the 20 MHz channel 153, and is 11.3 dB over the 150 MHz ISM band.

Then, the QN-point PIS $\boldsymbol{I_p}$ is generated by

$$\boldsymbol{I_p} = \boldsymbol{c_p} \otimes \boldsymbol{z}, \tag{2}$$

where $\otimes$ is the Kronecker product, and each element in $\boldsymbol{I_p}$ is given by $I_p[i] = c[\lfloor i/N \rfloor] z_p[i \bmod N]$, $i = 0, 1, 2, ..., QN-1$. In (2), the ZC sequence acts like a spread spectrum sequence with rate 150 MHz, thereby spreading the power of the m-sequence over the 150 MHz band.

The receiver computes two cross-correlations to detect the PIS. Given the received sequence $\boldsymbol{r}$ (i.e., the 150 MHz samples after ADC), the receiver first cross-correlates $\boldsymbol{r}$ and $\boldsymbol{z}$ as follows:

$$y[i] = \sum_{j=0}^{N-1} z^*[j] r[i+j]. \tag{3}$$

Note that the target interrupt signal is embedded in $\boldsymbol{r}$. Thus, in the presence of an interrupt signal, the operation in (3) produces Q peaks if we look at the absolute values of the resulting sequence $\boldsymbol{y}$, thanks to the correlation property of ZC sequences. Then, we make use of the m-sequence $\boldsymbol{c_p}$ modulated on the ZC sequence, and accumulate the power of all Q peaks, yielding

$$u[i] = \sum_{j=0}^{Q-1} c_p[j] y[i+Nj]. \tag{4}$$

Finally, a sharp peak emerges from the absolute values of sequence $\boldsymbol{u}$. The capture of this peak results in successful detection of PIS.

For the SIS, the same ZC sequence is used, but in place of $\boldsymbol{c_p}$, another Q-point m-sequence $\boldsymbol{c_s}$ is used.

Remark: ZC sequences have a nice correlation property: the periodic autocorrelation function of a ZC sequence is zero everywhere except at a single maximum per period [11]. However, when we modulate m-sequence onto ZC sequence, this nice correlation property no longer holds. To be specific, let us consider the first two ZC sequences in PIS.

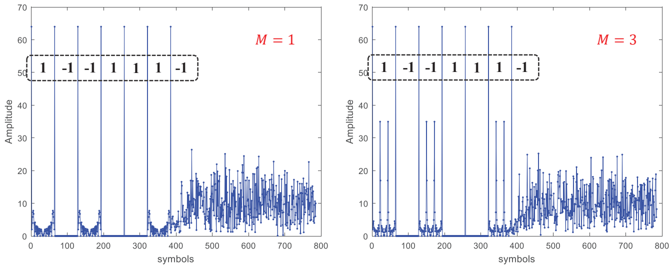

Fig. 5. The amplitude of the cross-correlation results, i.e., $|\boldsymbol{y}|$. We set $N = 64$, $Q = 7$, $M = 1$ or 3. The orthogonality no longer holds when the adjacent two ZC sequences in PIS are modulated by opposite values.

i) If these two ZC sequences are modulated by same values 1 or -1, then $|y[l]| = 0$ for $l = 1, 2, 3, ..., N-1$, because a ZC sequence is orthogonal to its cyclic shift.

ii) If these two ZC sequences are modulated by opposite values 1 and -1, we show in Appendix A that

$$|y[l]| = 2 \times \left| \frac{\sin(\pi M l^2/N)}{\sin(\pi M l/N)} \right|, \tag{5}$$

where $l = 1, 2, 3, ..., N-1$.

As can be seen, when the two adjacent ZC sequences in PIS are modulated by opposite values, the resulting cross-correlated signal is in general nonzero at $l = 1, 2, 3, ..., N-1$. The cross-correlated signals for $M=1$ and $M=3$ are shown in Fig. 5. Among all possible M, we found that setting $M=1$ minimizes the maximal interference $\max_l |y[l]|$ as well as the overall interference $\sum_l |y[l]|$ (to conserve space, we omit the detailed simulations and analyses here). Thus, we set $M=1$ for ZC sequence.

C. Performance evaluation

There are three components in the received sequence $\boldsymbol{r}$: the target interrupt signal, the Wi-Fi signal on the 5.8 GHz band as interference, and noise. If we fix the noise power, then the successful detection of interrupt signal depends on the amount of interference, or more precisely, the signal-to-interference ratio (SIR).

To evaluate the detection performance of our scheme under various SIR, we simulated the following single interrupter case: an interrupt node A broadcasts a PIS, and this PIS triggers three SISs by one-hop neighbors of A. For node A's one-hop neighbors, detection of the PIS peak means a successful interrupt; for node A's two-hop neighbors, detection of at least one SIS peak means a successful interrupt.

Performance metrics in our simulation are missed detection rate (MDR) and false alarm rate (FAR). We set a threshold $\gamma_{\text{th}}(Q, N)$ commensurate with the PIS (SIS) length (longer sequence corresponds to higher thresholds). Any entry in sequence $|\boldsymbol{u}|$ above γ_{th} is considered as a peak. Moreover, the real data we collected outdoors only contains one Wi-Fi signal (SNR 11.3 dB). For the simulation, we deliberately added additional Wi-Fi signal so that we can vary the SIR.

The MDR versus SIR (dB) are shown in Fig. 6, where we fix the received power of PIS and SIS to be equal to the noise

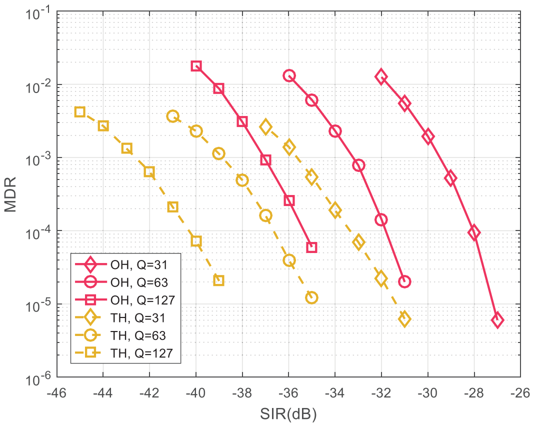

Fig. 6. The MDR versus SIR. The solid curves mark the MDRs of the interrupter's one-hop(OH) neighbors, and the dashed curves mark the MDRs of the interrupter's two-hop (TH) neighbors. For PIS (SIS), the received power is fixed to -8.24 dBm, and we set $N = 1024$, $Q = 31$, 63 or 127.

power[6] (that is, -90 dBm/Hz × 150 MHz $= -8.24$ dBm), and set different interference power P_I to obtain the target SIR (e.g., for SIR $= -28$ dB, we set $P_I = 19.76$ dBm).

We have two observations from Fig. 6: i) The MDR of the interrupter A's two-hop neighbors outperforms that of A's one-hop neighbors, given the same PIS (SIS) length. This is intuitive because each of A's two-hop neighbors has three chances to capture the SIS, while A's one-hop neighbors only have one chance to capture the PIS[7]. ii) If we set 0.0001 as the required MDR, then setting $Q = 31$ can meet the requirement when SIR ≥ -28 dB; setting $Q = 63$ can meet the requirement when SIR ≥ -32 dB. Moreover, when $Q = 63$, the number of symbols in PIS (SIS) is $NQ = 64512$, and the overall time consumed by interrupt is about 0.43 ms (we ignore the processing time).

We now evaluate the FAR versus interference power with the same simulation set-up as for Fig. 6. In this simulation, there is no interrupt signal, and the received sequence contains only interference and noise. The noise power is fixed to -8.24 dBm as in Fig. 6, and the interference powers are set as in Fig. 6 (e.g., for SIR $= -28$ dB, we set $P_I = 19.76$ dBm; for SIR $= -40$ dB, we set $P_I = 31.76$ dBm). FAR is defined as the probability that we detect a false alarm within a sample sequence of PIS (SIS) length (i.e., QN samples). Thus, given a FAR, we can calculate the number of false alarms per hour by FAR $\times 3600 \times 150$ MHz$/QN$.

The FAR versus interference power under different thresholds are shown in Fig. 7. As can be seen, higher threshold yields better FAR performance. If we set $Q = 63$, $N = 1024$, the number of false alarms per hour is less than 1 when $P_I = 21.76$ dBm (corresponding to SIR $= -30$ dB in Fig. 6).

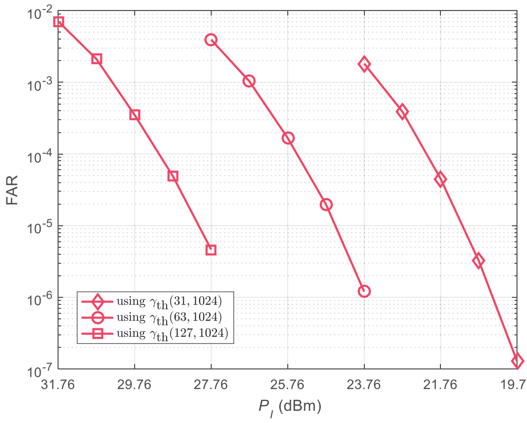

Fig. 7. The FAR versus interference power under different thresholds. Higher threshold yield better FAR performance.

Remark: If we use a long NQ-point ZC sequence instead of our design in this paper (i.e., Q cascaded N-point ZC sequences), the detection performance will be the same (we omit the simulation results here to conserve space). However, long ZC sequences greatly increases the computational complexity. Specifically, i) for our design, the two-step cross-correlation takes $N + Q$ multiplication and $N + Q - 2$ addition; ii) for a long NQ-point ZC sequence, one NQ-point cross-correlation is needed, and it takes NQ multiplication and $NQ-1$ addition.

V. Channel Access

After interruption, the service channels are set aside for ultra-time-critical messaging, and the only concern left is the channel access of multiple emergency nodes. Overall, this MAC problem can be outlined as follows: i) there are K (out of K_{all}) active nodes, where $K \in [0, 30]$ and $K_{\text{all}} \in [0, 1000]$. ii) node activations are random. iii) all the active nodes intend to transmit a message (24 Bytes) within $T_a = 10 - T_I$ ms, where T_I is the time consumed by interrupts. iv) the available bandwidth is 40 MHz. In practice, we may override only 20 MHz so that the primary traffic of the service channels would not be clipped suddenly, and can still transmit on the other 20 MHz channels.

Schedule-based MAC protocols, e.g., TDMA, FDMA, CDMA, OFDMA, requires pre-allocating orthogonal resources for the overall K_{all} nodes. Let us take CDMA for instance. When operated with CDMA, all the nodes within two hops are pre-assigned different spread spectrum codes, e.g., PN codes, so that the spread spectrum signals from distinct nodes will not interfere with each other. For one thing, a background coordinator must run all the time to guarantee all the nodes within two hops use different PN codes; for another, since there is no prior information on the potential transmitters, a receiving node must despread the received signal using all the potential PN codes (up to a few thousands). This poses great challenges to the processing capacity of the receiver. In this context, random MAC protocols are preferable in our framework.

[6] In practice, a transmitter can evaluate the nearby Wi-Fi signal intensity before transmission, and adjust its transmitted power accordingly.

[7] A caveat here is that if a one-hop neighbor B_1 did not detect the PIS, it is possible for it to detect SIS sent by another one-hop neighbor B_2 who detected the PIS, if B_1 and B_2 are within transmission range of each other. Thus, the MDR of a one-hop neighbor presented here is conservative.

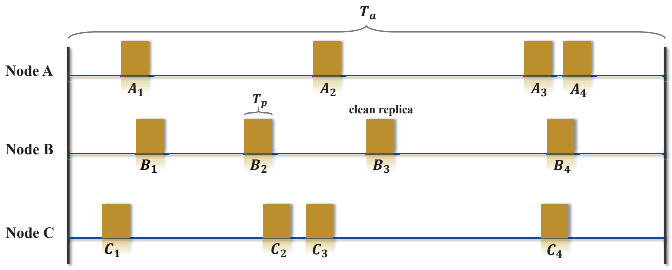

Fig. 8. Multi-replica ALOHA. Each of the K emergency nodes transmit d replicas within T_a ms. In this figure, $K = 3$ and $d = 4$.

A. Multi-replica ALOHA

A simple random-access protocol is ALOHA. However, ALOHA requires ACK to inform the transmitter whether the previous transmission is successful or not. As stated in the introduction, ACK is not viable for the broadcast scenario, because each broadcast requires feedback from all one-hop neighbors, and incurs excessive overhead when the network is dense, compromising the ability to meet the critical time constraint.

One alternative is multi-replica ALOHA. The basic idea is that, since transmitters cannot determine whether their transmissions are successful or not given the lack of ACK, they can replicate their warning packet d times and randomly broadcasts these d replicas within T_a ms. If one or more replicas from a node are broadcasted without any collision, then the delivery of the warning message is considered successful. An example is given in Fig. 8, in which three transmitters A, B and C broadcast their four replicas, respectively. It turns out that only replica B_3 are clean. Thus, only node B successfully broadcast its warning message while nodes A and C fail.

To analyze the performance, we first derive a probability P_0: for any two nodes A and B, P_0 is defined as the probability that one of A's replicas, say A_1, does not collide with B's all d replicas. Calculating P_0 is essentially a problem of $d+1$ dimensional integral, yielding

$$P_0 = \frac{[T_a - (d+1)T_p]^{d+1}}{(T_a - dT_p)^d (T_a - T_p)}. \tag{6}$$

P_0 is the probability that A_1 is clean with respect to B's messages. By our independence assumption, P_0 is also the probability that A_1 is clean with respect to any other node's messages and that P_0^{K-1} is the probability that A_1 is clean with respect to all other node's messages.

Finally, the probability that node A can broadcast its warning message successfully, denoted by $P_{1,\text{succ}}$, is equal to the probability that one or more replicas from node A are clean. That is,

$$P_{1,\text{succ}} \approx 1 - (1 - P_0^{K-1})^d, \tag{7}$$

where the approximation comes from the assumption that all d replicas from node A are independent (strictly speaking, they are not, since they cannot collide with each other; but the independence assumption is a conservative assumption). This approximation is valid when $dT_p \ll T_a$.

TABLE I

Types	Description	Value
OFDM PHY	available bandwidth	20 MHz
	subcarrier spacing	156.25 KHz
	available data subcarriers	96
	modulation	QPSK
	channel code rate	1/2
	CP duration	1.6 μs
	OFDM symbol duration	8 μs
	preamble duration	8 μs
warning message	potential transmitters	$K \in [0, 30]$
	warning message size	24 Bytes
	warning packet duration	24 μs
	Overall TTL of *warning* messages	10 ms
	Time consumed by interruption	$T_I = 0.5$ ms
	Time left for channel access	$T_a = 9.5$ ms

Furthermore, $P_{1,\text{succ}}$ is equal to the "message success rate" R_{ave}, defined as the number of successful nodes over the number of all emergency nodes.

B. Coded ALOHA

At the transmitter, as with the multi-replica approach, each emergency node repeats its broadcast for d times to increase the success rate. At the receiver, successive interference cancellation (SIC) [12] is used to boost performance.

Consider the example in Fig. 8 again. Only B_3 can be decoded with the previous multi-replica reception mechanism. With coded ALOHA, the receiver stores all the signal received during the T_a ms, and make use of SIC to recursively cancel the interference caused by the decoded nodes. First, the clean replica B_3 can be used to cancel other replicas of node B, i.e., B_1, B_2, and B_4. As a result, the interference from node B to other nodes is removed. Moreover, this interference cancellation process creates a new clean replica C_2, and all node C's replicas can be removed accordingly. Finally, only replicas from node A is left, and they are all clean and decodable.

This scheme, multi-replica ALOHA with SIC (or for simplicity, coded ALOHA), is similar to coded slotted ALOHA [12], [13], except that the concept of slotted time is missing. Practically, enabling a time-slotted system causes two problems in our application: i) The slot must be short, e.g., as short as 50 μs. However, small slot duration poses difficult challenge and overhead on slot alignment/synchronization among nodes. ii) This slotted system must be maintained all the time since we cannot predict the arrival of emergencies. Both (i) and (ii) may induce significant inefficiency.

C. Performance evaluation

To evaluate the above two potential MAC schemes, we consider a specific OFDM-based PHY layer. The parameters are given in Table. I [4], where we assume warning messages override half of the service channels, i.e., 20 MHz, so that the non-safety messages would not be totally deprived of services.

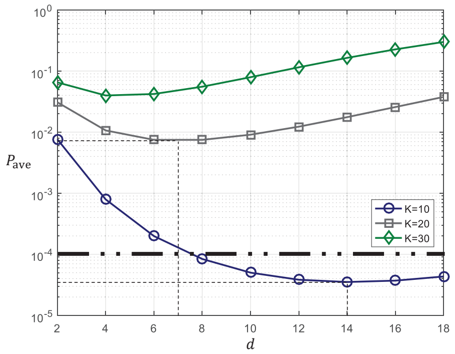

Fig. 9. The message loss rate P_{ave} of multi-replica ALOHA, where each of the K emergency nodes broadcasts d replicas of their warning packets. Each replica is 24 μs, and the overall time available for channel access is $T_a = 9.5$ ms.

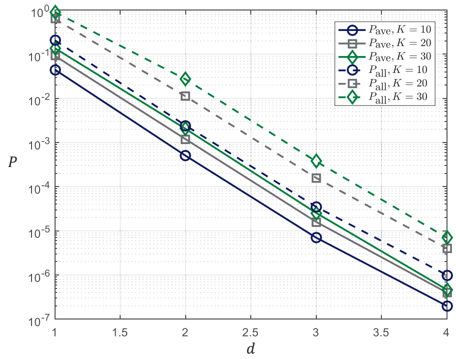

Fig. 10. The message loss rate and global loss rate of coded ALOHA under different d, where the interference cancellation at the PHY layer is assumed to be perfect. The solid curves are the message loss rates, and the dashed curves are the global loss rate.

As can be seen from Table. I, a typical 24 Byte warning message occupies two OFDM symbols, leading to a 24 μs warning packet at the PHY layer (each OFDM symbol is 8 μs and the preamble is 8 μs). The time we left for interruption is $T_I = 0.5$ ms, hence, the available time for channel access is $T_a = 9.5$ ms.

For multi-replica ALOHA, the numerical results of "message loss rate" $P_{\text{ave}} = 1 - R_{\text{ave}}$, is shown in Fig. 9. As can be seen, for different number of emergency nodes K, the optimal performance (i.e., the minimum P_{ave}) can be obtained by different duplication factor d. For example, when $K = 10$, the optimal $d = 14$, and when $K = 20$, the optimal $d = 7$. Given $P_{\text{ave}} = 10^{-4}$ as the target performance, then multi-replica ALOHA can meet the requirement only when $K \leq 10$ and $d \geq 8$

For coded ALOHA, the simulation results are plotted in Fig. 10, where we assume perfect interference cancellation at the PHY layer. The solid curves depict the message loss rate P_{ave}. As can be seen, when $d \geq 3$, the 10^{-4} requirement is satisfied for all $K \leq 30$. Another stricter performance indicator is "global success rate" R_{all}, where a global transmission is deemed successful only if all the K nodes can successfully broadcast their warning messages. The dashed curves in Fig. 10 depict the "global loss rate" $P_{\text{all}} = 1 - R_{\text{all}}$. As can be seen, even for this stricter performance metric, coded ALOHA can guarantee the reliability requirement. When $d \geq 4$, P_{all} for $K \leq 30$ are less than 10^{-4}.

VI. Conclusion

This paper addressed the problem of life-critical warning messaging in V2X. Our main contributions can be summarized as follows. First, we put forth a new MAC protocol for the delivery of life-critical warning messages. The overall MAC is built upon an override architecture, and operates by means of interrupt-and-access. In this architecture, no exclusive spectrum resource is allocated to warning messages. Instead, a vehicle with warning messages first sends an interrupt signal to pre-empt the transmission of non-safety messages, so that the warning message can use the wireless spectrum originally allocated to non-safety messages. Second, for wireless interrupt, we devised an interrupt mechanism for V2X and presented an out-of-band interrupt signal design where the interrupt signals are spread spectrum sequences on the ISM band. Simulation results validate the nice detection performance of our design, e.g., for a 0.43 ms (64512 symbols, 150 MHz) sequence, the missed detection rate can be kept lower than 0.0001 when SIR ≥ -32 dB. Third, for channel access, we investigated different uncoordinated MAC techniques to meet the stringent delay and reliability requirements of warning message. Simulation results indicate that coded ALOHA can potentially keep the message loss rate lower than 10^{-4} with delay less than 10 ms, in a stringent scenario where 30 emergency nodes broadcast simultaneously.

Appendix A

In this Appendix, we derive the cross-correlation results when the two adjacent ZC sequences in PIS are modulated by distinct values.

First, from (2), the PIS is given by $\boldsymbol{I_p} = \boldsymbol{c_p} \otimes \boldsymbol{z}$, where $\boldsymbol{c_p}$ is a Q-point m-sequence and $\boldsymbol{z}$ is an N-point ZC sequence given by (1). In the following derivations, we consider even N (odd N yields the same results).

As with (3), at the receiver, we cross-correlate PIS $\boldsymbol{I_p}$ with the conjugate of ZC sequence $\boldsymbol{z}$, yielding

$$y[i] = \sum_{j=0}^{N-1} z^*[j] I_p[i+j].$$

Given sequence $\boldsymbol{y}$, we find peak in its modulus $|\boldsymbol{y}|$. Without loss of generality, we now focus on the first two ZC sequences in PIS.

If these two ZC sequences are modulated by same values, then

$$y[l] = \sum_{n=0}^{N-l-1} z^*[n] z[n+l] + \sum_{n=N-l}^{N-1} z^*[n] z[n-N+l] = 0, \quad (8)$$

where $l = 1, 2, 3, ..., N-1$. Eq. (8) follows since a ZC sequence is orthogonal to its cyclic shift.

If these two ZC sequences are modulated by distinct values, say 1 and -1, respectively. We have

$$\begin{aligned} y[l] &= \sum_{n=0}^{N-l-1} z^*[n]z[n+l] - \sum_{n=N-l}^{N-1} z^*[n]z[n-N+l] \\ &= 2\sum_{n=0}^{N-l-1} z^*[n]z[n+l] \end{aligned} \tag{9}$$

Substituting (1) into (9), yields,

$$|y[l]| = 2 \times \left| \frac{\alpha^{l^2} - \alpha^{-l^2}}{1-\alpha^{2l}} \right|, \tag{10}$$

where $\alpha = \exp\left(-j\pi M/N\right)$.

Notice that $\left|\alpha^{l^2} - \alpha^{-l^2}\right|$ and $\left|1-\alpha^{2l}\right|$ are two strings of a unit circle on the complex plane. According to the Law of cosines, we have

$$\left|\alpha^{l^2} - \alpha^{-l^2}\right| = \sqrt{1^2+1^2-2\cos(\frac{\pi M}{N}*2l^2)} = \left|2\sin(\frac{\pi M}{N}l^2)\right|,$$

$$\left|1-\alpha^{2l}\right| = \sqrt{1^2+1^2-2\cos(\frac{\pi M}{N}*2l)} = \left|2\sin(\frac{\pi M}{N}l)\right|,$$

Thus, (10) can be written as

$$|y[l]| = 2 \times \left| \frac{\sin(\pi M l^2/N)}{\sin(\pi M l/N)} \right|.$$

References

[1] 5G-PPP, "5G automotive vision," *The 5G infrastructure public private partnership, avaliable: https://5g-ppp.eu/white-papers/*, 2015.

[2] NHTSA, https://www.nhtsa.gov/research-data, the National Highway Traffic Safety Administration, accessed Sept. 2017,.

[3] R. Popescu-Zeletin, I. Radusch, and M. A. Rigani, *Vehicular-2-X communication: state-of-the-art and research in mobile vehicular ad hoc networks*. Springer Science & Business Media, 2010.

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

[5] E. G. Strom, "On medium access and physical layer standards for cooperative intelligent transport systems in Europe," *Proc. IEEE*, vol. 99, no. 7, pp. 1183–1188, 2011.

[6] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for vehicular networking: a survey," *IEEE Commun. Mag.*, vol. 51, no. 5, pp. 148–157, 2013.

[7] X. Lin, J. Andrews, A. Ghosh, and R. Ratasuk, "An overview of 3GPP device-to-device proximity services," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 40–48, 2014.

[8] H. A. Omar, W. Zhuang, and L. Li, "VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs," *IEEE Trans. Mobi. Comput.*, vol. 12, no. 9, pp. 1724–1736, 2013.

[9] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," in *IEEE VTC Spring*, 2008, pp. 2036–2040.

[10] F. Borgonovo, A. Capone, M. Cesana, and L. Fratta, "ADHOC MAC: New MAC architecture for ad hoc networks providing efficient and reliable point-to-point and broadcast services," *Wireless Networks*, vol. 10, no. 4, pp. 359–366, 2004.

[11] D. Chu, "Polyphase codes with good periodic correlation properties (corresp.)," *IEEE Trans. Inf. Theory*, vol. 18, no. 4, pp. 531–532, 1972.

[12] E. Paolini, G. Liva, and M. Chiani, "Coded slotted ALOHA: A graph-based method for uncoordinated multiple access," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6815–6832, 2015.

[13] S. Yang, Y. Chen, S. C. Liew, and L. You, "Coding for network-coded slotted ALOHA," in *IEEE Inf. Theory Workshop (ITW)*, 2015.