On Exploiting Concurrent Transmissions Through Discernible Interference Cancellation

Junmei Yao, Wei Lou, *Member, IEEE*, Lu Wang, and Kaishun Wu, *Senior Member, IEEE*

***Abstract*—This paper represents the design, feasibility evaluation, and performance validation of ICMR, a novel cross layer protocol that can maximize concurrent transmissions and avoid data frame interference in wireless networks, achieving a higher throughput comparing with the 802.11 standard and other state-of-the-art protocols. Observations on the 802.11 standard reveal that nodes around both the transmitter and receiver of the ongoing link waste concurrent transmission opportunities, degrading the network throughput dramatically. A state-of-the-art protocol IRMA is proposed to improve the network throughput through exploiting concurrent transmissions at the transmitter side. In this paper, a new ICMR protocol focuses on the receiver side to further improve the network throughput, through exploiting discernible interference cancellation, a physical layer mechanism that can successfully detect data frames when collided by control frames. We analyze the concurrent transmission opportunities of one link from the transmitter's transmission opportunities and the receiver's reception opportunities, then formulate the opportunities and give theoretical analysis to indicate that ICMR will have a higher opportunity over other protocols. Feasibility of the discernible interference cancellation mechanism is demonstrated through experiment results based on USRP2, and the throughput improvement of ICMR comparing with the other protocols is confirmed through simulations based on ns-2.**

***Index Terms*—Concurrent transmissions, wireless networks, cross layer design, discernible interference cancellation.**

I. Introduction

With the wide deployment of wireless nodes and rapid growth of data traffic, wireless networks face the persistent challenge of improving the network performance to meet the customer's requirements. Interference is a critical issue that will degrade the system performance in wireless networks. Currently, most networks adopt 802.11 standard [1] and use CSMA (carrier sense multiple access) to avoid interferences. However, it is commonly known that this mechanism has a low performance as it uses the medium's situation at the transmitter side to decide whether there is an interference at the receiver side, which induces a serious hidden terminal problem. To combat this problem, the 802.11 standard proposes a virtual CSMA mechanism, which uses the exchange of RTS (Request To Send) and CTS (Clear To Send) control frames to coordinate between transmitters and receivers. The RTS and CTS frames contain a NAV field which represents the duration that the channel will be occupied to complete the data transmission. After receiving RTS or CTS, the neighboring nodes will keep silence during the NAV time to avoid interference. However, although the RTS/CTS control frames can coordinate between nodes more effectively than the physical carrier sense, they still have a low system performance.

In a wireless network, a transmission is successful if and only if the received Signal to Interference plus Noise Ratio (SINR) is above a threshold [2]. Thus, the *basic requirement* that two transmission links $T \rightarrow R$ and $T' \rightarrow R'$ can proceed concurrently is that, there is no mutual interference affecting their data frame receptions at receivers (i.e., the SINRs at both R and R' are above a given threshold). The *basic requirement* can also be expressed using the interference range d_{IR}: As only nodes within the d_{IR} of a transmission link's receiver will interfere with the link, the two links $T \rightarrow R$ and $T' \rightarrow R'$ can proceed concurrently if both transmitters T and T' are outside the d_{IR} of the other link. However, the 802.11 standard does not conform to this *basic requirement* and will degrade the network performance from two aspects.

The first is called *the CA-CF problem* (the excessive Collision Avoidance problem induced by Control Frames). The 802.11 standard uses the RTS/CTS/ACK control frames to help nodes get proper information. Nodes that receive the control frames will decide that they are within the interference range of a transmission link and should keep silence to avoid interference. However, this mechanism should also avoid collisions introduced by CTS/ACK frames, leading to the CA-CF problem which occurs in two scenarios: (1) The collisions with the CTS/ACK frames

Manuscript received June 1, 2017; revised January 25, 2018 and April 17, 2018; accepted July 4, 2018. Date of publication July 9, 2018; date of current version October 15, 2018. This work was supported in part by the China NSFC under Grants 61702343, 61472259, and 61502313; in part by China Postdoctoral Funding (2017M610548); in part by the Guangdong Natural Science Foundation under Grant 2017A030312008; in part by Hong Kong RGC under Grant PolyU-521312; in part by Hong Kong PolyU under Grants 4-BCB6, M-N020, and G-YBXY); in part by Shenzhen Science and Technology Funding under Grants JCYJ20170302140946299 and JCYJ20170412110753954, in part by Guangdong Talent Project (2014TQ01X238, 2015TX01X111), in part by GDUPS (2015), and in part by Tencent "Rhinoceros Birds" - Scientific Research Foundation for Young Teachers of Shenzhen University. The review of this paper was coordinated by Dr. Z. Fadlullah. *(Corresponding author: Wei Lou.)*

J. Yao is with the College of Computer Science and Software Engineering, Shenzhen University 518060, Shenzhen China, and the Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong (e-mail: yaojunmei@szu.edu.cn).

W. Lou is with the Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong (e-mail: csweilou@comp.polyu.edu.hk).

L. Wang and K. Wu are with the College of Computer Science and Software Engineering, Shenzhen University, 518060 Shenzhen, China (e-mail: wanglu@szu.edu.cn; wu@szu.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2018.2853716

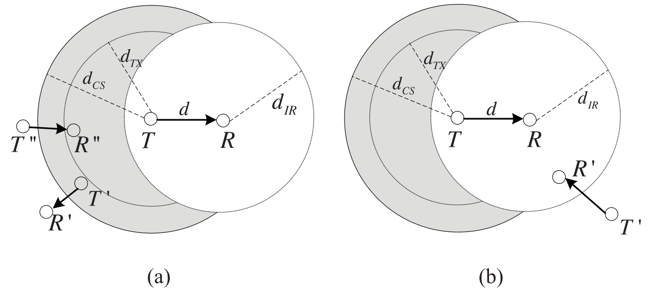


Fig. 1. Two scenarios of *the CA-CF problem*. (a) Nodes in the grey area are prohibited to transmit data or control frames. (b) Nodes in the white area are prohibited to receive data frames.

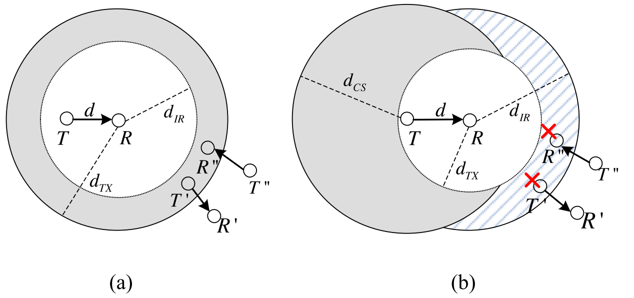


Fig. 2. Two scenarios of *the varied-IR problem*. (a) Nodes in the grey area are prohibited to transmit data or control frames. (b) Nodes in the slash area are permitted to transmit data or control frames.

should be avoided at the transmitter side of the link, as the transmitter needs to detect the CTS/ACK frames correctly to get the coordination information. The 802.11 standard uses the physical carrier sense and the NAV field in RTS to avoid the collision at the transmitter side. As demonstrated in Fig. 1(a), nodes in the grey area cannot transmit data packets or CTS/ACK control frames, due to avoiding collisions with CTS/ACK at node T. (2) The data frame being collided by control frames should be avoided at the receiver side of the ongoing link. The 802.11 standard uses the NAV field in CTS to avoid the collision at the receiver side. As shown in Fig. 1(b), nodes in the grey area are prohibited to initiate packet receptions, so as to avoid their CTS/ACK transmissions to interfere with R's data reception.

The second is called *the varied-IR problem* (the varied Interference Range problem). Based on the 802.11 standard, nodes received CTS will determine that they are within the interference range d_{IR} of the ongoing link and should keep silence. This mechanism simply fixes d_{IR} to be the transmission range d_{TX} of CTS, although d_{IR} is variable and determined by the distance of the ongoing link [3]–[5], leading to the varied-IR problem that occurs in two scenarios: (1) It may cause excessive restriction of effective transmissions when $d_{IR} < d_{TX}$ (such as the transmission of $T' \rightarrow R'$ or $T'' \rightarrow R''$ in Fig. 2(a)). (2) It may bring false permissions of ineffective transmissions which lead to collisions when $d_{IR} > d_{TX}$ (such as the transmission of $T' \rightarrow R'$ or $T'' \rightarrow R''$ in Fig. 2(b), where the sign "×" indicates a false permission of a node's data frame transmission or reception).

The two problems will degrade the network throughput through making nodes around both the transmitter and receiver of an ongoing link either waste concurrent transmission opportunities or bring more collisions. Recently, many research works have studied the 802.11 standard and design new protocols to improve the network throughput, and these designs basically focus on dealing with one or both problems, such as IRMA [6]. IRMA can solve the varied-IR problem through a differentiated NAV update scheme, based on which only nodes which are within d_{IR} of the ongoing link will update the NAV state to keep silence. For the CA-CF problem, IRMA proposes a signature detection method to detect control frames correctly under collisions, thus can permit control frames' collisions at the transmitter side. However, as IRMA should avoid the data frame being collided by control frames at the receiver side, some effective concurrent transmissions that meet the *basic requirement* cannot be exploited.

This paper presents Interference Cancellation Multiple Reception (ICMR), a novel cross-layer protocol, to further exploit the concurrent transmission opportunities and improve the network throughput. ICMR permits the reception of a data frame to be collided by control frames, and detects the collided data frame through a novel Discernible Interference Cancellation (DIC) mechanism in the physical layer. In this mechanism, nodes use signatures (certain known sequences) to convey the control information. When detecting a collided data frame, nodes first estimate the arrival and positions of control frames in the received signal, then discern signatures carried in the control frames, reconstruct the received control signal through proper channel estimations, and finally detach the control signal to recover the original data signal. We will also analyze the concurrent transmission opportunities of a link from the transmitter's transmission opportunities and the receiver's reception opportunities, then formulate the opportunities that can be exploited in the 802.11-based wireless networks from solving both the CA-CF problem and the varied-IR problem, and finally give theoretical analysis to illustrate how ICMR can exploit concurrent transmission opportunities comparing with IRMA and the 802.11 standard.

The key contributions of the paper over existing works to increase concurrent transmissions are summarized as follows:

- We design ICMR to exploit all the effective concurrent transmission opportunities which meet the *basic requirement* in wireless networks through permitting the data frame being collided by control frames.
- We design a DIC mechanism in the physical layer to detect the data frame correctly when it is collided by control frames.
- We analyze the concurrent transmission opportunities of a link from the transmitter's transmission opportunities and the receiver's reception opportunities, then formulate the two kinds of opportunities theoretically to show that ICMR can have a higher opportunity comparing with IRMA and 802.11 standard.
- We verify the discernible interference cancellation mechanism through hardware experiments. The results demonstrate the feasibility of this mechanism as the data frame

can be detected correctly with a high probability when collided by control frames.

- We demonstrate ICMR's significant throughput improvement through simulation results, which demonstrate that ICMR can outperform IRMA and the 802.11 standard under different network topologies.

The rest of this paper is organized as follows. Section II gives an overview of ICMR. Section III describes the design of the discernible interference cancellation mechanism in detail. Section IV first formulates the concurrent transmission opportunities, and then gives theoretical analysis of the opportunities. Section V uses hardware experiment results to verify the feasibility of discernable interference cancellation. Section VI uses simulation results to demonstrate the performance improvement of ICMR. Section VII gives the related work. Section VIII concludes this paper and puts forward future works.

II. Overview of ICMR

In this section, we will first describe IRMA as a preliminary work, then propose ICMR that can further exploit concurrent transmission opportunities comparing with IRMA.

A. IRMA Protocol

Based on the RTS/CTS mechanism in the 802.11 standard, IRMA [5] disables the physical carrier sense and lets one node only rely on its NAV state to decide whether it can initiate a data transmission or reception. This protocol can increase concurrent transmissions by partially solving both the CA-CF problem and the varied-IR problem.

IRMA can partially solve the CA-CF problem through permitting control frame collisions at the transmitter side. The control information is conveyed through signatures (known sequences) and can be obtained correctly under collisions, as signatures in the control frames can be detected successfully at this situation. Thus, nodes in the grey area of Fig. 1(a) can exploit transmission opportunities. However, it cannot exploit concurrent transmission opportunities in Fig. 1(b).

IRMA [5] can also solve the varied-IR problem through the combination of the signature detection method and the new designed CTS frame. As nodes can detect the control frames under low SINR environments through the signature detection method, the transmission range of CTS is much lager than d_{TX}, making CTS always detected correctly within the interference range d_{IR} of the ongoing link, no matter $d_{IR} \leq d_{TX}$ or $d_{IR} > d_{TX}$. Meanwhile, IRMA makes the new CTS frame contain d_{IR} of the ongoing transmission link. Based on the received CTS, one node can determine whether it is in the interference range or not successfully. Thus, nodes in the grey area of Fig. 2(a) can exploit transmission opportunities, while nodes in the slash area of Fig. 2(b) can properly keep silence to avoid interfering with the ongoing link.

IRMA designs new control frames (RTS/CTS/ACK) to make them be detected correctly under low SINR environments through the signature detection method.

1) Control Frame Design: As shown in Fig. 3, IRMA adds new fields to the 802.11 standard control frames. Each new field is in the physical layer and filled by a signature to carry specific control information.

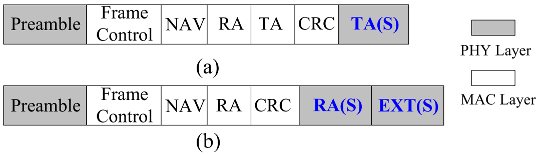


Fig. 3. The control frame formats in IRMA.

The TA(S) field (shown in Fig. 3(a)) in the tail of the RTS frame is used to assign a signature that represents the transmitter's address. For the CTS or ACK frame (shown in Fig. 3(b)), RA(S) indicates the receiver address of this frame, which will be filled directly by the TA(S) signature from the received RTS frame, EXT(S) is used to carry the combined information of both the NAV duration and interference range of the ongoing link.

IRMA uses a signature set for each field and maps the original information to a specific signature in the set. A signature set $S_{Addr} = \{s_1, \ldots, s_p\}$ is designed for TA(S)/RA(S). One node randomly selects a signature s_i $(s_i \in S_{Addr})$ as its own address. Another signature set $S_{EXT} = \{S_{m\times n}, s_{ACK}\}$ is used for EXT(S), where s_{ACK} is used to differentiate the CTS and ACK frames, $S_{m\times n}$ is a matrix and each element s_{ij} $(s_{ij} \in S_{m\times n}$, where $i = 1, 2, ..., m, j = 1, 2, ..., n)$ is used to represent a NAV time (carried by i) and an interference range (carried by j). Thus, through the RA(S) and EXT(S) fields, the CTS or ACK frame can convey three key control information (the receiver address, the NAV duration and the interference range) that can be detected under interferences.

We should point out that the number of NAV indicators, which is determined by the maximum packet transmission duration $t_{\max}$, can remain constant when the 802.11 standard updates to support higher data rate and longer packet length, due to the little change of $t_{\max}$ (e.g., $t_{\max} = 5.46$ ms for 802.11a [1], and $t_{\max} = 5.848$ ms for 802.11n and 802.11ac [7]). Therefore, this design is suitable to all the 802.11 standards.

2) Signature Detection Method: The process of the signature detection in IRMA is to first discern signatures from the received signal, then recover the original control information.

IRMA exploits the cross correlation technology to discern the signatures, while this technology has already been used in preamble synchronization and some other recent works, such as [8], [9]. In IRMA, the cross correlation will be conducted between the "cut samples" (the sample sequence with fixed position and length) of the incoming signal and all the elements in the signature set S_{Addr}. A signature is determined to be in the coming signal if its correlation result is maximum and over a given correlation threshold.

B. ICMR Protocol

In this paper, we propose ICMR to further exploit the concurrent transmission opportunities in wireless networks. ICMR enhances IRMA, which also utilizes the exchange of RTS and CTS to determine data transmissions and receptions. It can fully

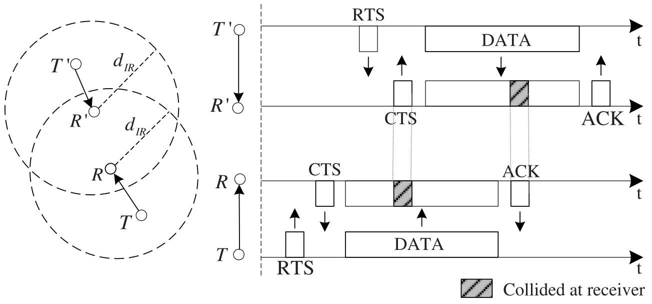


Fig. 4. An example of the ICMR protocol.

solve the CA-CF problem as the collided control frames can be detected successfully through the same signature detection method as that in IRMA, and the collided data frames can be detected successfully through a DIC mechanism. Based on DIC, concurrent transmissions in the scenario of Fig. 1(b) can be exploited successfully. Here we just give an overview of ICMR, and remain the details of DIC in Section III.

To explain how ICMR is designed to exploit concurrent transmissions, we illustrate this protocol in a simple scenario demonstrated in Fig. 4. There are two links $T \rightarrow R$ and $T' \rightarrow R'$ in the network. The transmitters T and T' are outside the interference range of the other link, while the receivers R and R' are within the interference range of the other one. ICMR permits their concurrent transmissions. Comparing with the 802.11 and IRMA protocols, the process of ICMR is illustrated as follows:

- At the beginning, the channel access scheme of ICMR permits T' data transmission as its NAV state is zero, making T send a RTS frame to initiate the transmission. It can then transmit the data frame after receiving the corresponding CTS from R correctly. R' should update its NAV state based on the received CTS as it is in the interference range d_{IR} of R, while T' need not as it is outside d_{IR} of R. These operations are the same as those in IRMA.
- During the data transmission from T to R, T' has the transmission opportunity as its NAV state is zero, it can send a RTS frame after a backoff time to initiate the transmission. After receiving the RTS frame, R' can decide that its data frame reception will not be interfered by the other link's data frame transmission as it can detect the RTS frame correctly. It has the reception opportunity and will respond a CTS frame to initiate the data reception. Note that the CTS feedback from R' will have interference on R's data reception, this interfered data frame can be detected correctly by using DIC.
- After receiving the data frame successfully, R will reply an ACK to T to complete the transmission. The ACK frame will also have interference on R''s data reception. The interfered data frame can also be detected using DIC. Therefore, the two concurrent transmissions can be completed successfully.

Note that ICMR has the same channel access scheme and NAV state update mechanism as those in IRMA. One node just needs to update its NAV state when it is outside the interference range of the ongoing link, and it can transmit a data frame only when its NAV state is zero. Thus, nodes that adopt ICMR or IRMA have the same transmission opportunities. Meanwhile, nodes in ICMR have different reception opportunities from IRMA. Based on ICMR, one node can respond a CTS feedback when it receives a RTS frame correctly, no matter its NAV state is zero or not, the data frame interfered by control frames will be detected correctly by DIC.

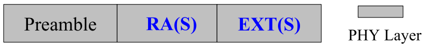


Fig. 5. The new CTS/ACK frame formats.

According to the ICMR design, its performance would not be affected significantly by the node mobility. ICMR's performance is related to nodes' channel access decision, which is determined by the received control frames of the ongoing links. Since the data transmission duration is only up to 5.8 ms while nodes' average moving speed is about 1 m/s, nodes can be considered static when making each channel access decision.

1) Control Frame Design: We make some changes to the IRMA control frames to complete the ICMR control frame design. The RTS frame of this protocol has the same format as that of IRMA (shown in Fig. 3(a)), while the CTS/ACK frame only remains the fields in the physical layer.

According to the basic idea of DIC, when receiving a collided signal containing the CTS/ACK control signal and data signal, one node should first detect the control signal so as to detach them and recover the original data signal. As the fields in the MAC layer cannot be detected correctly under interferences, we remove all the fields in the MAC layer in the new ICMR CTS/ACK frame design.

The new CTS/ACK control frame has three fields, as shown in Fig. 5, including the preamble, RA(S) and EXT(S), which are the same as those in the physical layer of the IRMA CTS/ACK control frame (shown in Fig. 3(b)), and the detailed signature design for both RA(S) and EXT(S) fields are the same as that in the IRMA protocol.

III. Discernible Interference Cancellation (DIC) Design

ICMR uses the Discernible Interference Cancellation (DIC) mechanism to detect data frames when they are interfered by CTS or ACK control frames. In this section, we first introduce the process of DIC as an overview, then give the detailed process of data signal recovery, including the preamble synchronization, signature discernment, control signal reconstruction and detachment, and a refined control channel estimation mechanism.

A. Overview of DIC

Before describing the process of DIC, we first formulate the signal at the transmitter and receiver sides.

To transmit a wireless signal, the transmitter first transforms the bit sequence of the signal to a series of complex samples through a modulation process. The received samples will differ from the transmitted ones due to amplitude attenuation, frequency offset, phase offset, and so on.

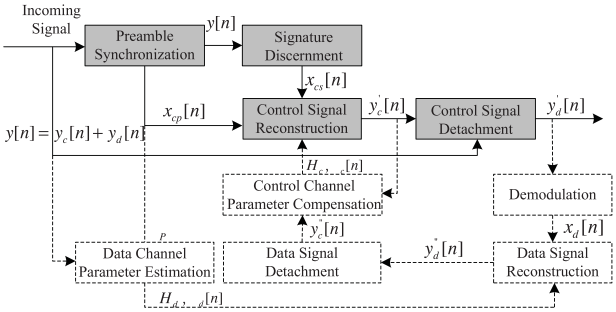


Fig. 6. The process of DIC.

We let $x_c[n]$ be the nth transmitted control sample, and let $y_c[n]$ be the corresponding sample at the receiver side, both $x_c[n]$ and $y_c[n]$ are complex numbers. Then we have

$$y_c[n] = H_c x_c[n] e^{j(2\pi n \delta_{f_c} T + \theta_{c0})}, \tag{1}$$

where H_c refers to the control signal's amplitude attenuation, δ_{f_c} and θ_{c0} refer to the frequency offset and phase offset respectively, and T is the sample period.

Similarly, if $x_d[n]$ is the nth transmitted data sample, the received data signal $y_d[n]$ can be denoted as:

$$y_d[n] = H_d x_d[n] e^{j(2\pi n \delta_{f_d} T + \theta_{d0})}, \tag{2}$$

where H_d is the the amplitude attenuation between the data signal's transmitter and receiver, δ_{f_d} and θ_{d0} refer to the frequency offset and phase offset, respectively.

When a node receives a collided signal containing a data signal and a CTS/ACK control signal, the collided signal $y[n]$ is represented as:

$$y[n] = y_c[n] + y_d[n] + w[n], \tag{3}$$

where $w[n]$ is the random noise.

The process of DIC is described as follows (Fig. 6): The node continuously conducts the preamble synchronization to determine the arrival and position of the control frame. From this module it also gets the transmitted control samples $x_{cp}[n]$ in the preamble field. It then estimates the positions of the control frame's new fields shown in Fig. 5, and conducts the signature discernment at each position to obtain the transmitted control samples $x_{cs}[n]$ in each field. Combining $x_{cp}[n]$ and $x_{cs}[n]$, the node gets all the transmitted control signal $x_c[n]$. It can reconstruct the received control signal based on Eq. (1), where the channel parameters H_c, δ_{f_c} and θ_{c0} should be estimated properly. The output $y_c'[n]$ may be a little different from the original received control signal $y_c[n]$ because of the error introduced in channel parameter estimations. The node can finally recover the data signal $y_d'[n]$ through detaching the control signal $y_c'[n]$ from the received signal $y[n]$. $y_d'[n]$ is transformed into bits after demodulation and will be finally passed to the MAC layer to complete the protocol disposal. The white blocks are used to refine the control channel estimation, which will be discussed in Section 3.5.

Note that DIC does not consider the scenario when a data frame is collided by a RTS control frame, as this scenario is not permitted based on the ICMR design.

B. Preamble Synchronization and Signature Discernment

After receiving a data frame collided by CTS or ACK frames, a node should first use the preamble synchronization module to determine the positions of control frames, and use the signature discernment module to determine the signatures in each field of the control frames. Note that the preamble can be treated as a specific signature s_P, and both the preamble and the signature in the RA(S) or EXT(S) can be discerned through exploiting the cross correlation.

Suppose the received collided signal $y[n]$ contains a data frame and a control frame, as described in Eq. (1), Eq. (2) and Eq. (3), we have:

$$y[n] = H_c x_c[n] e^{j(2\pi n \delta_{f_c} T + \theta_{c0})} + H_d x_d[n] e^{j(2\pi n \delta_{f_d} T + \theta_{d0})} + w[n].$$

Suppose a signature $s_i[k]$ ($1 \leq k \leq L$) is in $x_c[n]$, and its position is Δ in $y[n]$. Here, L denotes the number of samples each signature has. When doing cross correlation between $y[n]$ and s_i at position Δ, we get:

$$\begin{aligned} R(\Delta) &= \sum_{k=1}^{L} \overline{s_i[k]} y[k+\Delta] \\ &= \sum_{k=1}^{L} \overline{s_i[k]} \left(H_c s_i[k] e^{j(2\pi [k] \delta_{f_c} T + \theta_{c0})} \right) \\ &+ \sum_{k=1}^{L} \overline{s_i[k]} \left(H_d x_d[k+\Delta] e^{j(2\pi [k+\Delta] \delta_{f_d} T + \theta_{d0})} + w[k+\Delta] \right). \end{aligned}$$

As x_d and w are independent of s_i, we get:

$$R(\Delta) \approx \sum_{k=1}^{L} \overline{s_i[k]} (H_c s_i[k] e^{j(2\pi [k] \delta_{f_c} T + \theta_{c0})}). \tag{4}$$

Then we have:

$$\mid R(\Delta) \mid \approx H_c \sum_{k=1}^{L} |s_i[k]|^2. \tag{5}$$

Eq. (5) indicates that, $|R(\Delta)|$ will have a peak value if the signature s_i is in the received signal at the position Δ. Otherwise, $|R(\Delta)|$ would have a very low value as the incoming signal is independent of this signature.

$|R(\Delta)|$ is the sum of energy of this segment of signal, and it reaches a peak value if the signature s_i appears in the received signal. If not, $|R(\Delta)|$ would be close to zero as the received signal is independent of this signature.

Please note that through doing cross correlation between $y[n]$ and the preamble s_P, we can obtain the position of s_P as Δ_P, which also represents the position of the control signal in the received collided signal. The obtained position information will be further used in the control signal detachment module in Section 3.5.

The cross correlation process conducted in the signature discernment module will certainly increase the system computational complexity, which is in the order of the sizes of the two signature sets, S_{Addr} and S_{EXT}. However, we consider this complexity is relatively small comparing with that in the preamble synchronization process, which needs a node to correlate the preamble s_P with the incoming samples at all the positions. Since preamble synchronization is a standard module in 802.11, the computational complexity increased by signature discernment is affordable to current systems.

C. Control Signal Reconstruction and Detachment

After passing the received collided signal through the preamble synchronization and signature discernment modules, the node can only obtain the control signal at the transmitter side (denoted by $x_c[n]$), it should then reconstruct the control signal at the receiver side (denoted by $y_c[n]$), thus detach it to recover the original data signal. To reconstruct $y_c[n]$, we should accurately estimate three key parameters, H_c, δ_{f_c} and θ_{c0}.

1) Amplitude Estimation: We estimate the parameter H_c in a simple way: The incoming of a new control signal makes a sharp change to the strength of the received signal. We can utilize this strength variation to obtain the amplitude A_c of the control signal, then the parameter H_c can be calculated as:

$$H_c = \frac{A_c}{\frac{1}{L}\sum_{k=1}^{L}|x_c[k]|}.$$

2) Frequency and Phase Offsets Estimation: Different from Zigzag [8] or DAC [10] that use clean samples to estimate the frequency and phase offsets of the following collided samples, ICMR cannot use clean samples to estimate these parameters of the control frame as the control samples may be fully collided by data samples. In this paper, we propose a *Blind Estimation Algorithm* to estimate the phase offset of control samples by further exploiting cross correlation, which is described as follows.

As the effect of wireless channels can be approximated by amplitude attenuation and phase shift [2], the frequency offset δ_{f_c} will finally affect the overall phase offset of the received signal (that is, $\theta_c[n] = 2\pi n\delta_{f_c}T + \theta_{c0}$). Hence, we make $\theta_c[n]$ as one parameter to estimate.

Suppose the received collided signal $y[n]$ contains a data signal and a control signal, and a signature $s_i[k]$ $(1 \le k \le L)$ in the received signal is at position Δ. The correlation result between $y[n]$ and s_i at Δ is described in Eq. (4), which can be simplified as:

$$R(\Delta) \approx \sum_{k=1}^{L} \overline{s_i[k]}(H_c s_i[k] e^{j\theta_c[k]}).$$

where $\theta_c[k] = 2\pi k\delta_{f_c}T + \theta_{c0}$.

As δ_{f_c} can be compensated based on history information, this value can be very small. That means, within the L samples of the signature s_i that we do cross correlation, the overall phase offset of each sample $\theta_c[k]$ can be approximately equal to a constant value Θ. Here we denote Θ as the central phase offset of this signature, then the correlation result can be simplified as:

$$R(\Delta) \approx e^{j\Theta} H_c \sum_{k=1}^{L} |s_i[k]|^2.$$

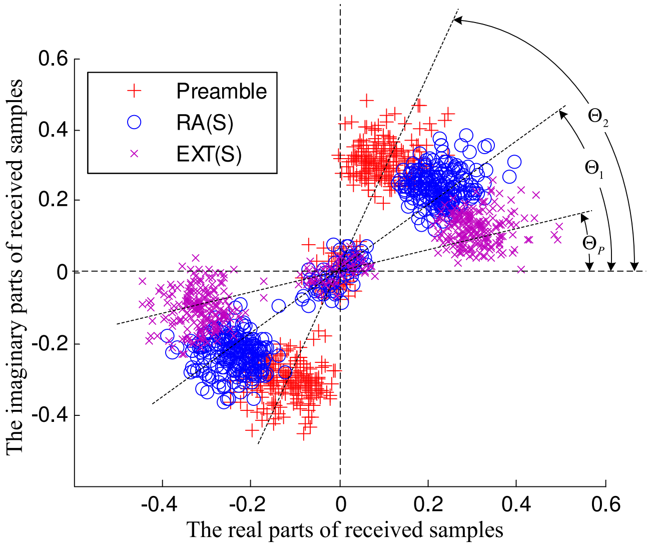


Fig. 7. An example of the central phase offset in a received control frame.

The central phase offset of this signature can be calculated as:

$$\Theta = arctan\left(\frac{Imag(R(\Delta))}{Real(R(\Delta))}\right). \tag{6}$$

According to the format of the CTS/ACK frame (Fig. 5), there are one preamble and two signatures in a CTS or ACK frame. We let the sample length L of the control frame's three fields be L_P, L_1 and L_2, and let the calculated central phase offsets in the corresponding fields be Θ_P, Θ_1 and Θ_2. Note that the preamble can be treated as a specific signature and its central phase offset Θ_P can also be calculated by Eq. (6). Fig. 7 shows an example of the three values in a control frame. It uses three different marks to represent the constellation positions of the received samples in the three fields, respectively.

Upon calculating Θ_P, Θ_1 and Θ_2, the receiver just gets a rough estimation about the phase offset of each field, it will then recover the phase offset of each sample in the control frame, so that each received control sample can be reconstructed and detached from the collided samples. Suppose the jitter of δ_{f_c} is small, that means, the change of phase at each sample is approximately uniform. Then we recover the phase offset of each sample in the preamble as:

$$\theta_P(k) = \Theta_P - \frac{\Theta_1 - \Theta_P}{2} + \frac{\Theta_1 - \Theta_P}{L_P}\cdot k,\ k \in [1, L_P], \tag{7}$$

and the phase offset of each sample in the following two fields as:

$$\theta_1(k) = \Theta_1 - \frac{\Theta_1 - \Theta_P}{2} + \frac{\Theta_2 - \Theta_P}{L_p + L_1}\cdot k,\ k \in [1, L_1], \tag{8}$$

$$\theta_2(k) = \Theta_2 - \frac{\Theta_2 - \Theta_1}{2} + \frac{\Theta_2 - \Theta_1}{L_2}\cdot k,\ k \in [1, L_2]. \tag{9}$$

The Blind Estimation Algorithm is listed as Algorithm 1, based on which we can estimate the phase of each received control sample even when there is no clean control signal in the received signal.

Algorithm 1: Blind Estimation Algorithm.

```
Input: $y$, $s$; $\Delta_p$, $\Delta_{sRA}$ and $\Delta_{sEXT}$; $L_p$, $L_1$ and $L_2$.
Output: $\theta_p(k)$, $\theta_1(k)$, $\theta_2(k)$.
Calculate $R(\Delta_p)$, $R(\Delta_{sRA})$ and $R(\Delta_{sEXT})$ using Eq. (4);
Calculate $\Theta_p$, $\Theta_1$ and $\Theta_2$ using Eq. (6);
for $k = 1 : L_p$ do
    Calculate $\theta_p(k)$ using Eq. (7);
for $k = 1 : L_1$ do
    Calculate $\theta_1(k)$ using Eq. (8);
for $k = 1 : L_2$ do
    Calculate $\theta_2(k)$ using Eq. (9);
```

After the preamble synchronization and the signature discernment module, one node has the transmitted control signal to be $x_c[n]$ at position Δ_P; combining with the estimated control channel parameters H_c and $\theta[n]$, the node can reconstruct the received control samples as $y'_c[n]$. It will then detach $y'_c[n]$ from the received signal at the position Δ_P, and get the data samples $y'_d[n]$, which will be finally transformed into bits after the normal demodulation process. Please note that one node may conduct the processes of the control signal reconstruction and detachment for multiple times within a data frame reception, as the data frame may be collided by several CTS or ACK frames. The module will be processed once the preamble synchronization module indicates that a control frame arrives.

D. Refined Channel Estimation

We let Θ calculated by Eq. (6) as the central phase offset of the received signature. However, this value is just an estimated value and may deviate from the real central phase offset. The deviation of Θ will affect the calculated phase offset of each control sample, and finally affect the recovered data samples $y'_d[n]$, introducing more errors to the demodulated bits of the data frame. Meanwhile, the amplitude distortion H_c may also have some deviation when estimated using the method in Section III-C1.

To mitigate the deviation of control channel parameters, we refine the channel estimation through a simple feedback algorithm in the process of control signal reconstruction and detachment, as shown in the white blocks of Fig. 6. The data signal always has clean samples as the data frame is longer than the control frame, these clean data samples can be utilized to refine the control channel estimation. After recovering the original data samples $y'_d[n]$, one node will obtain the bits of the data packet $x_d[n]$ after passing $y'_d[n]$ through the normal demodulation process. As the data samples are clean when $n < \Delta_P$, the node can calculate the amplitude distortion H_d and phase offset $\theta_d[n]$ during this period, according to which it then reconstructs the collided data samples as $y''_d[n]$, and gets a new estimation of the control samples as $y''_c[n] = y[n] - y''_d[n]$. The new channel parameters H'_c and $\theta'_c[n]$ in the control samples $y''_d[n]$ can be calculated and will be used to compensate the values estimated in the control signal reconstruction module.

IV. Theoretical Analysis

In this section, we will first formulate the concurrent transmission opportunities, then give the opportunity comparison among ICMR, IRMA and the 802.11 standard.

A. Formulation

Determining whether a link $T' \rightarrow R'$ can have concurrent transmission opportunities with an ongoing link $T \rightarrow R$ in a wireless network is equivalent to determining both the two conditions: (1) whether T' can be permitted to send a data frame and (2) whether R' can be permitted to receive a data frame. To make the analysis clear, we introduce two concepts, *transmission opportunity*, which is the opportunity that a node can send a RTS frame to initiate a data transmission, and *reception opportunity*, which is the opportunity that a node can response a CTS frame to grant a data reception.

The concurrent transmission of the link $T' \rightarrow R'$ can proceed only if the transmitter T' has the transmission opportunity and the receiver R' has the reception opportunity. In the following parts, we will give detailed analysis about the two opportunities in the 802.11-based wireless networks. All the opportunity analysis will start from solving the CF-CA problem and the varied-IR problem. In the analysis, we use $D(A, B)$ to denote the distance between nodes A and B.

1) Transmission Opportunity: According to the *basic requirement* of concurrent transmissions, one node has the transmission opportunity if its data transmission have no interference on the ongoing link's data reception. We will discuss this opportunity from solving both the CF-CA problem and the varied-IR problem in the current 802.11 standard.

a) Solving the CA-CF problem: According to *the CA-CF problem* shown in Fig. 1(a), when a node T', which is a neighbor of the transmitter T of the link $T \rightarrow R$, intends to initiate a transmission, it should not interfere with T's reception of the CTS/ACK control frames, so that T can get the proper control information. The 802.11 standard uses the physical carrier sense to avoid this collision, therefore, nodes within the carrier sense range d_{CS} of T will be prohibited to transmit a packet. We call this as the *Tx transmitter-side data-excessive-restriction*, which is formulated as:

$$D(T', T) < d_{CS}. \tag{10}$$

b) Solving the varied-IR problem According to the varied-IR problem, the 802.11 standard uses the NAV field in the CTS frame to reserve the medium around the receiver side, thus fixing the interference range d_{IR} of the receiver to be the transmission range d_{TX} of CTS. That means, T' is prohibited to transmit a packet if $D(T', R) < d_{TX}$. This problem occurs in two scenarios:

1) As shown in Fig. 2(a), T' is prohibited to initiate a transmission although it will not interfere with R's data reception if:

$$d_{IR} < D(T', R) < d_{TX}. \tag{11}$$

Ineq. (11) is referred as the *Tx receiver-side data-excessive-restriction* in the 802.11 standard.

2) As shown in Fig. 2(b), T' is permitted to initiate a transmission although it will definitely interfere with R's data reception if:

$$d_{TX} < D(T', R) < d_{IR}. \tag{12}$$

Ineq. (12) is referred as the *Tx receiver-side data-false-permission* in the 802.11 standard. In this condition, nodes will bring some "threat" to the ongoing link because of improperly using this transmission opportunity. The threat can be regarded as a negative opportunity.

As a conclusion, considering both problems, with an ongoing link $T \rightarrow R$, a node T' may exploit the transmission opportunity if the condition of Ineq. (10) or Ineq. (11) is satisfied, and may suppress the threat if the condition of Ineq. (12) is satisfied.

2) Reception Opportunity: According to *the basic requirement* of concurrent transmissions, one node has the reception opportunity if its data reception will have no mutual interference with the data reception of the ongoing link. We will also discuss this opportunity in the 802.11 standard from solving both the CF-CA problem and the varied-IR problem.

a) Solving the CA-CF problem: According to *the CA-CF problem* shown in Fig. 1(a), when a node R' around the link $T \rightarrow R$ receives a RTS frame and determines whether to response a CTS frame to initiate a data reception, its CTS/ACK transmission should not interfere with T's CTS/ACK reception. The 802.11 standard avoids this collision through the NAV field in RTS. R' cannot be permitted to receive a data frame if it has updated its NAV state according to the received RTS frame from T. The constraint that R' will be prohibited to receive a packet is:

$$D(R', T) < d_{TX}. \tag{13}$$

Ineq. (13) is referred as the *Rx transmitter-side control-excessive-restriction* in the 802.11 standard.

Meanwhile, according to *the CA-CF problem* shown in Fig. 1(b), the node R''s CTS/ACK transmission should also not interfere with the receiver R's data reception, that means, R' is prohibited to receive a packet if it is within the interference range d_{IR} of R. We formulate it as:

$$D(R', R) < d_{IR}. \tag{14}$$

Ineq. (14) is referred as the *Rx receiver-side data-excessive-restriction.*

b) Solving the varied-IR problem: To avoid collisions under the condition of Ineq. (14), the 802.11 standard reserves the medium for an ongoing link through the NAV field in CTS. R' cannot be permitted to receive a data frame if it has updated its NAV state according to the received CTS frame from R. However, this mechanism itself also has the varied-IR problem as d_{TX} of CTS is fixed but d_{IR} of the ongoing link $T \rightarrow R$ is variable. This problem occurs in two scenarios:

1) As shown in Fig. 2(a), R' is prohibited to initiate a data frame reception although its CTS/ACK frame transmission has no interference on $T \rightarrow R$'s data reception if:

$$d_{IR} < D(R', R) < d_{TX}. \tag{15}$$

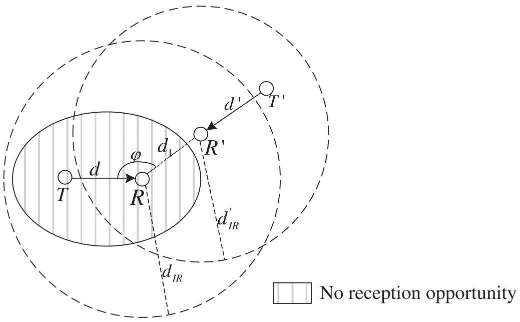


Fig. 8. An illustration of the limitations of reception opportunity.

Ineq. (15) is referred as the *Rx receiver-side control-excessive-restriction* in the 802.11 standard.

2) As shown in Fig. 2(b), R' is permitted to initiate a data frame reception although its CTS/ACK frame transmission will interfere with $T \rightarrow R$'s data reception if:

$$d_{TX} < D(R', R) < d_{IR}. \tag{16}$$

Ineq. (16) is referred as the *Rx receiver-side control-false-permission* in the 802.11 standard.

Similar to Ineq. (15) and Ineq. (16), we can see that when d_{IR} varies, Ineq. (14) also has two conditions:

$$D(R', R) < d_{IR} < d_{TX} \tag{17}$$

or

$$D(R', R) < d_{TX} < d_{IR}. \tag{18}$$

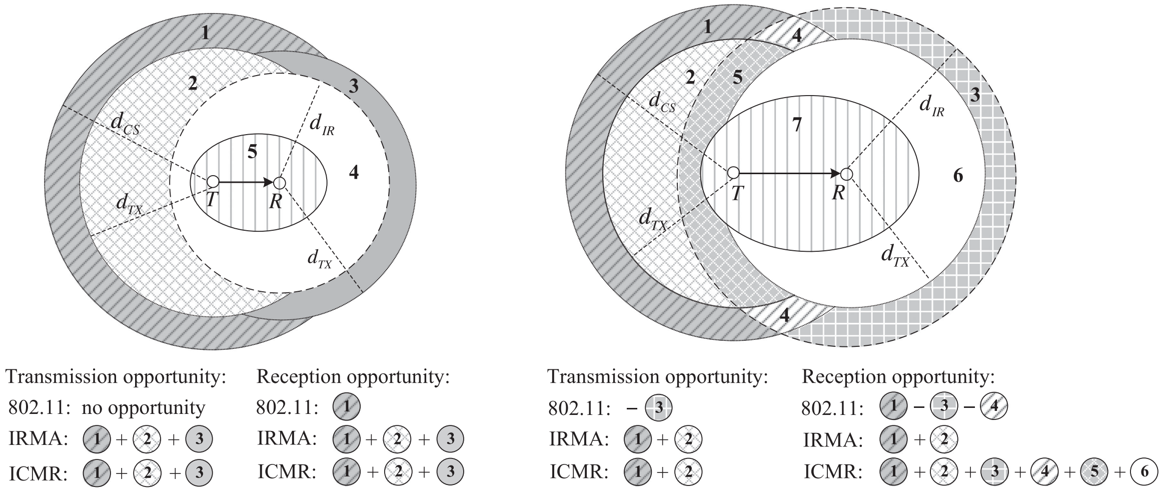
For the analysis simplification, we refer Ineq. (17) and Ineq. (18) as the *Rx receiver-side data-excessive-restriction 1* and *Rx receiver-side data-excessive-restriction 2*.

As a conclusion, considering both problems, with an ongoing link $T \rightarrow R$, a node R' may exploit the reception opportunity if the condition of Ineq. (13), Ineq. (15), Ineq. (17) or Ineq. (18) is satisfied, and may suppress the threat if the condition of Ineq. (16) is satisfied.

c) Limitations of reception opportunity: The concurrent transmissions of one link with the ongoing link is permitted if and only if its transmitter has the transmission opportunity and its receiver has the reception opportunity. With this limitation, one node that satisfies Ineq. (17) and Ineq. (18) may still have no reception opportunity if any of its transmitters has no transmission opportunity (its transmitters cannot be out of the interference range of the ongoing link). Here we will quantify how many reception opportunities that satisfy Ineq. (17) and Ineq. (18) cannot be exploited.

As shown in Fig. 8, there is an ongoing transmission link $T \rightarrow R$ with the distance d. Its interference range is $d_{IR} = \rho \cdot d$, where $\rho = \sqrt[\alpha]{\beta_{SINR}}$ is a constant [5]. If a node R' within the interference range has the reception opportunity from any other node T', that means, T should be out of the interference range of R', that is:

$$D(T, R') = d^2 - 2\cos\varphi \cdot d \cdot d_1 + d_1^2 > d'_{IR},$$



(a) The scenario of $d_{IR} \le d_{TX}$

(b) The scenario of $d_{IR} > d_{TX}$

Fig. 9. Opportunity comparison among ICMR, IRMA, and 802.11 standard. (a) The scenario of $d_{IR} \leq d_{TX}$. (b) The scenario of $d_{IR} > d_{TX}$.

where $d_1 = D(R, R')$ and $d' = D(T', R')$, φ is the intersection angle of $T \to R$ and $R \to R'$, $d'_{IR} = \rho \cdot d'$. We have:

$$d_1^2 - 2\cos\varphi \cdot d \cdot d_1 + d^2 - \rho^2 d'^2 > 0,$$

that is:

$$d_1 > d \cdot \cos\varphi + \sqrt{\rho^2 d'^2 - d^2 \sin^2 \varphi}. \tag{19}$$

There is another limitation that, for any transmitter T', it should be out of the interference range of R, which means:

$$d' + d_1 > d_{IR}. \tag{20}$$

With Ineq. (19) and Ineq. (20), we get:

$$d_1 > \frac{d}{\rho^2 - 1}\left(\rho^3 - \cos\varphi - \sqrt{\cos^2\varphi - 2\rho^3\cos\varphi + \rho^4 + \rho^2 - 1}\right). \tag{21}$$

According to Ineq. (21), when φ rotates from 0 to 2π, there is an ellipse region within which nodes have no reception opportunity. We denote the right-side expression of Ineq. (21) to be $f(d, \varphi)$ and simplify Ineq. (21) to be $d_1 > f(d, \varphi)$, then the two *Rx receiver-side data-excessive-restriction* conditions in Ineq. (17) and Ineq. (18) can be updated as:

$$f(d, \varphi) < D(R', R) < d_{IR} < d_{TX} \tag{22}$$

and

$$f(d, \varphi) < D(R', R) < d_{TX} < d_{IR}. \tag{23}$$

B. Opportunity Analysis

In this part, we first analyze the transmission and reception opportunities of 802.11, IRMA and ICMR, then give an opportunity comparison among the three protocols.

To simplify the analysis, we let $C(A, r)$ represent the area of a disk whose center is A and radius is r. We let $E(d)$ represent the area of an ellipse formed by Ineq. (21). We also let $O_T(\cdot)$ and $O_R(\cdot)$ represent the transmission and reception opportunity area of each protocol, respectively. We will analyze the opportunities in the scenario that there is an ongoing link $T \to R$ in the network, and let both the overall transmission opportunity area $O_T(All)$ and reception opportunity area $O_R(All)$ in the vicinity of the link be the influence region of T and R. We will analyze both opportunities in two cases: $d_{IR} \le d_{TX}$ and $d_{IR} > d_{TX}$.

1) Transmission Opportunity. Case 1.1: $d_{IR} \le d_{TX}$. As shown in Fig. 9(a), the transmission opportunity area of each protocol in this case is listed as follows:

$$\begin{aligned} O_T(All) &= C(T, d_{CS}) \cup C(R, d_{TX}), \\ O_T(802.11) &= \phi, \\ O_T(IRMA) &= C(T, d_{CS}) \cup C(R, d_{TX}) \setminus C(R, d_{IR}), \\ O_T(ICMR) &= C(T, d_{CS}) \cup C(R, d_{TX}) \setminus C(R, d_{IR}). \end{aligned} \tag{24}$$

The 802.11 has no transmission opportunity in this case, while IRMA and ICMR can exploit the transmission opportunities formulated in Ineq. (10) and Ineq. (11), as the collided CTS or ACK can be detected successfully through the signature detection method, and channel access is determined according to the real interference range in these two protocols. Thus, nodes in the areas ① + ② + ③ in Fig. 9(a) can exploit transmission opportunities.

Case 1.2: $d_{IR} > d_{TX}$. As shown in Fig. 9(b), the transmission opportunity area of each protocol in this case is listed as follows:

$$\begin{aligned} O_T(All) &= C(T, d_{CS}) \cup C(R, d_{IR}), \\ O_T(802.11) &= -C(R, d_{IR}) \setminus C(R, d_{TX}) \setminus C(T, d_{CS}), \\ O_T(IRMA) &= C(T, d_{CS}) \setminus C(R, d_{IR}), \\ O_T(ICMR) &= C(T, d_{CS}) \setminus C(R, d_{IR}). \end{aligned} \tag{25}$$

From Fig. 9(b), we can see that for the 802.11 standard, nodes in the area ③ satisfy Ineq. (12), so their transmissions will bring some "threat" to the ongoing link $T \to R$. We regard the threat as the negative opportunity since the nodes' transmission opportunity in this area will be negatively affected. We use the label "−" to denote it. On the contrary, nodes that adopt IRMA or ICMR in this area can detect the CTS frame through the signature detection method, and keep silence to suppress the threat successfully. Meanwhile, IRMA and ICMR can also exploit transmission opportunities formulated in Ineq. (10), which corresponds to the areas ① + ② in Fig. 9(b).

2) Reception Opportunity. Case 2.1: $d_{IR} \leq d_{TX}$. As shown in Fig. 9(a), the reception opportunity area of each protocol in this case is listed as follows:

$$\begin{aligned} O_R(All) &= C(T, d_{CS}) \cup C(R, d_{TX}), \\ O_R(802.11) &= C(T, d_{CS}) \setminus C(T, d_{TX}) \setminus C(R, d_{TX}), \\ O_R(IRMA) &= C(T, d_{CS}) \cup C(R, d_{TX}) \setminus C(R, d_{IR}), \\ O_R(ICMR) &= C(T, d_{CS}) \cup C(R, d_{TX}) \setminus E(d). \end{aligned} \tag{26}$$

For the 802.11 standard, one node that is within the carrier sense range but outside the transmission range of T may have the reception opportunity if its NAV state is zero and the received signal's SINR is over the threshold β_{SINR}, which corresponds to the area ① in Fig. 9(a). IRMA can exploit the reception opportunity formulated in Ineq. (13) and Ineq. (15), which corresponds to the areas ① + ② + ③ in Fig. 9(a), while ICMR can further exploit the reception opportunities formulated in Ineq. (22), which corresponds to the area ④ in Fig. 9(a).

Case 2.2: $d_{IR} > d_{TX}$. As shown in Fig. 9(b), the reception opportunity area of each protocol in this case is listed as follows:

$$\begin{aligned} O_R(All) &= C(T, d_{CS}) \cup C(R, d_{IR}), \\ O_R(802.11) &= C(T, d_{CS}) \setminus C(T, d_{TX}) \setminus C(R, d_{TX}) \\ &\quad - C(R, d_{IR}) \setminus C(R, d_{TX}) \setminus C(T, d_{CS}), \\ O_R(IRMA) &= C(T, d_{CS}) \setminus C(R, d_{IR}), \\ O_R(ICMR) &= C(T, d_{CS}) \cup C(R, d_{IR}) \setminus E(d). \end{aligned} \tag{27}$$

For the 802.11 standard, nodes in the areas ③ + ④ of Fig. 9(b) satisfy Ineq. (16) and may bring some threats when they receive packets. Both IRMA and ICMR can suppress these threats. Moreover, IRMA and ICMR can exploit the reception opportunity formulated in Ineq. (13) (corresponding to area ②), while ICMR can further exploit the reception opportunities formulated in Ineq. (18) (corresponding to areas ③ + ④ + ⑤) and Ineq. (23) (corresponding to area ⑥, all shown in Fig. 9(b).

3) Comparison: We summarize the opportunities of three protocols in Table I. We use the letters "O" or "T" to indicate whether there exists an opportunity that can be exploited or a threat that can be suppressed in each condition, respectively. "/" indicates the opportunity cannot be exploited or no threat is induced in this condition. "–" indicates a threat is induced and "+" indicates an opportunity can be exploited. The table indicates that IRMA has already exploited four kinds of opportunities and suppressed two kinds of threats, while ICMR can further exploit the remaining three kinds of opportunities, which are marked with red "+" signs.

TABLE I
THE SUMMARY OF OPPORTUNITIES AMONG THREE PROTOCOLS

Condition			O/T	802.11	IRMA	ICMR
Transmission Opportunity	*Tx transmitter-side data-excessive-restriction*	Ineq. (10)	O	/	+	+
	Tx receiver-side data-excessive-restriction	Ineq. (11)	O	/	+	+
	Tx receiver-side data-false-permission	Ineq. (12)	T	–	/	/
Reception Opportunity	*Rx transmitter-side control-excessive-restriction*	Ineq. (13)	O	/	+	+
	Rx receiver-side control-excessive-restriction	Ineq. (15)	O	/	+	+
	Rx receiver-side control-false-permission	Ineq. (16)	O	/	/	+
			T	–	/	/
	Rx receiver-side data-excessive-restriction1	Ineq. (22)	O	/	/	+
	*Rx receiver-side data-excessive-restriction*2	Ineq. (23)	O	/	/	+

C. Backward Compatibility Analysis

ICMR is backward compatible with the 802.11 standards, as the ICMR nodes can coexist with the traditional 802.11 nodes in wireless networks without affecting their performance. Here we use Fig. 1 to analyze this characteristic, while the scenario in Fig. 2 has the similar situation.

In case $T \rightarrow R$ is an ongoing 802.11 transmission link. In Fig. 1(a), the neighboring ICMR nodes T' and R'' should have received T's RTS with the 802.11 format and know that they are within the carrier sense range of an 802.11 transmitter, they are prohibited to transmit data packets at this time. Similarly, the ICMR node R' in Fig. 1(b) is also prohibited to receive data packets as it has received R's CTS with 802.11 format. In summary, the ICMR nodes can distinguish between the 802.11 and ICMR control frames, and act as traditional 802.11 nodes when the 802.11 control frames are received.

In case $T \rightarrow R$ is an ongoing ICMR transmission link. The 802.11 nodes T' and R'' in Fig. 1(a) would keep silence as they determine the channel is busy, and the node R' in Fig. 1(b) is prohibited to receive data packets as it can detect R's CTS successfully. We note that the 802.11 nodes can detect the ICMR control frames (shown in Fig. 3) correctly as the new fields are merely added at the end of the 802.11 control frames, they will keep silence during the ongoing ICMR transmission to avoid interference.

V. FEASIBILITY EVALUATION

In this part, we use hardware experiment results to illustrate the feasibility of using the DIC mechanism to detect data frames when they are collided by control frames.

A. Experiment Setup

The experiments are conducted on Universal Software Radio Peripheral 2 (USRP2) platform and use the GNURadio for the signal processing blocks. The RXF2400 daughter-board is used to make each USRP2 device operate at about 2.4GHz. GNURadio has already implemented the physical layer modulation and demodulation processes. For the receiving process of DIC, we will first restore the received collided samples and make trace-based off-line analysis for the modules in Fig. 6. After that, the recovered data samples will be fed into the GNURadio receiving

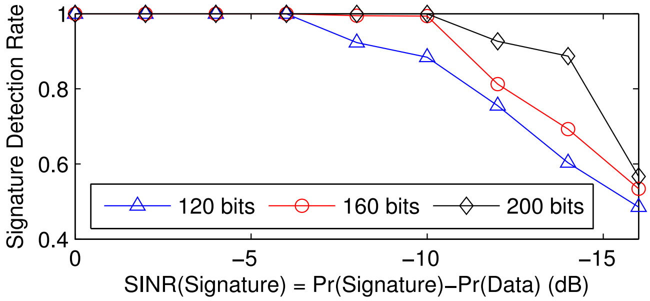


Fig. 10. The signature discernment rate under different SINR environments.

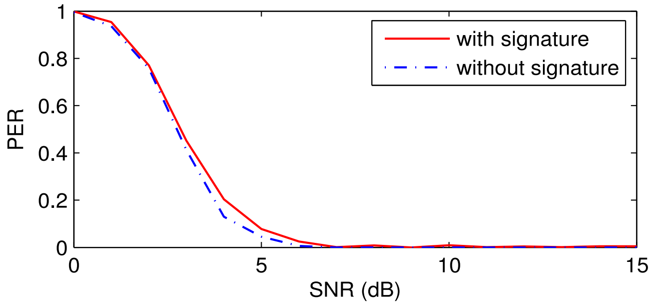


Fig. 11. The packet error rate under different SINR environments.

TABLE II
SIMULATION PARAMETERS

Parameter	Value	Parameter	Value
Preamble	20μs	SIFS	16μs
Time slot	9μs	DIFS	34μs
Signature	13.3μs	CWmax	1023μs
p/q	20/150	CWmin	15μs
m	8	*n*	16

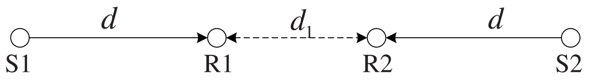


Fig. 12. A linear network topology with four nodes $R1$, $S1$, $S2$, and $R2$.

process to be transformed into bits. The constellation method is BPSK, the bit rate is 1 Mbits/s and the number of samples per symbol is 2.

The experimental network consists of eight USRP2 nodes, and the topology is randomly set up. In each experiment, we choose four nodes to constitute two links like the topology shown in Fig. 4. Each link has a sender and a receiver, their concurrent transmissions are permitted by ICMR. The CTS/ACK transmissions from each receiver may have potential interference on the other link's data frame reception. We let $P_r(Signature)$ and $P_r(Data)$ be the received signal strengths of the signature and data frame respectively, and different $P_r(Signature)$ and $P_r(Data)$ environments are obtained by varying the transmission power of the two receivers while fixing that of the senders.

B. Signature Discernment

One key issue in DIC is to discern signatures in the incoming signal so as to reconstruct the received samples in the following process. Here we first quantify DIC's ability to discern signatures through experiments.

Fig. 10 shows the signature discernment rate under different $SINR(Signature) = P_r(Signature) - P_r(Data)$ and signature length. We can see that a longer signature can have a higher signature discernment rate when the SINR is fixed, and the discernment rate decreases obviously when the SINR is below -6 dB. Especially, when we select signature length to be 160 bits (similar as that in IRMA), the detection rate is almost 100% when SINR is above -10 dB.

C. Data Frame Detection

We also validate the effectiveness of data transmissions when interfered by CTS/ACK transmissions, which is evaluated through the metric packet error rate (PER). We compare the PER of the data frame detection with or without concurrent signature transmissions under different SNR environments. We set the payload of data frame to be 1500 bytes, and evaluate PER when the signature length is 160 bytes.

As shown in Fig. 11, the concurrent transmissions of signatures have little performance degradation on the data packet transmission. Specially, when the SNR is 5dB, DIC will have about 2.5% performance degradation in PER due to the concurrent signature transmission. However, when the SNR is above 8dB, under which environment the normal demodulation process always works, DIC has little performance degradation.

VI. PERFORMANCE EVALUATION

In this section, we evaluate ICMR's performance improvement comparing with IRMA and the 802.11 standard. The 802.11 standard recommends two mechanisms: (1) PCS, which only uses the physical carrier sense to avoid interferences, (2) PCS+VCS, which uses RTS/CTS control frames to coordinate between nodes. We compare ICMR with both mechanisms. All the protocols are implemented in ns-2 with the following basic parameters listed in Table II.

The DIC process in the physical layer is not implemented in the simulation, we just simplify it based on the calculated $P_r(Signature)$ and $P_r(Data)$. The signature detection of the control frames is set as follows: if $P_r(Signature) - P_r(Data) > -10$ dB, the signatures can be obtained successfully; otherwise, the signatures will be ignored. The data frame detection process is set as follows: if $P_r(Data) - P_r(Signature) > -4$ dB, the data frame can be detected successfully; otherwise, the data frame will be discarded. We set the transmission rate be 6 Mbps, the transmission range be 500 m, and the carrier sense range be 700 m.

A. Linear Topology

We first evaluate the effectiveness of ICMR under a simple four-node linear topology, as shown in Fig. 12. There are two links $S1 \rightarrow R1$ and $S2 \rightarrow R2$ in the network, the transmitter-receiver distances of both links are the same and are denoted by d, the receiver-receiver distance is denoted by d_1. We conduct

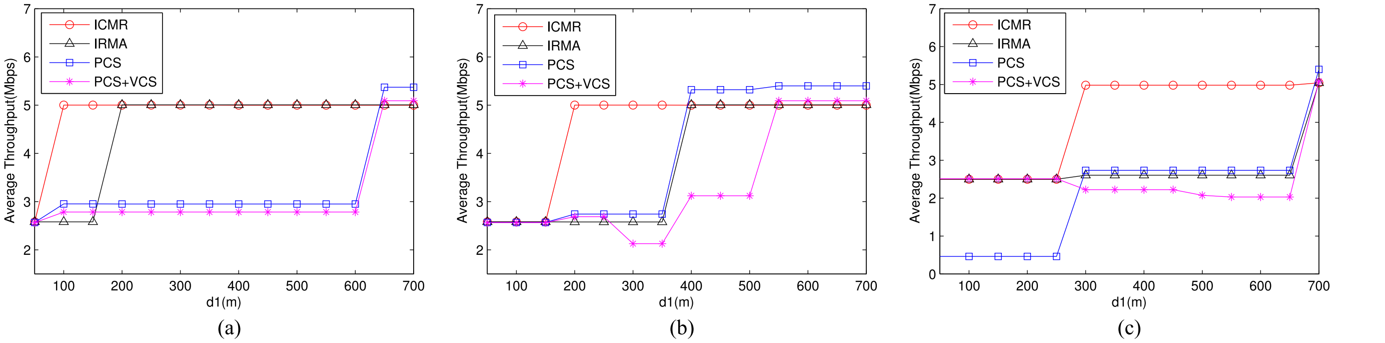


Fig. 13. Average throughput in terms of d_1 in the line topology under three distances d. (a) $d = 100$ m. (b) $d = 200$ m. (c) $d = 400$ m.

the simulation under three scenarios: (1) $d = 100$ m, which is much smaller than the transmission range of 500 m; (2) $d = 200$ m, which is about one-half of the transmission range; (3) $d = 400$ m, which is about the transmission range. For each scenario, we change d_1 from 50 m to 700 m to evaluate how d can affect the performance of each protocol. We set up a CBR (constant bit rate) flow at the sender. The packet length is fixed to be 1500 bytes in the simulation.

We summarize the simulation results shown in Fig. 13 into three main cases:

Case 1: $d + d_1 < d_{IR}$. The corresponding scenarios are $d_1 < 100$ m in Fig. 13(a), $d_1 < 200$ m in Fig. 13(b) and $d_1 < 300$ m in Fig. 13(c), where all the senders and receivers are within the d_{IR} of the other link, concurrent transmissions are prohibited by all the protocols to avoid interferences. Note that when $2 \cdot d + d_1 > d_{CS}$, the two senders cannot carrier sense each other, the performance of PCS degrades dramatically. As shown in Fig. 13(c), the average throughput of PCS is nearly zero when $d_1 < 300$ m, as the two links will "threaten" each other but cannot utilize the physical carrier sense to avoid the interference. This is a typical hidden terminal problem. Instead, ICMR, IRMA and PCS+VCS can solve this problem and have similar performance through coordinating among nodes using control frames.

Case 2: $d_1 < d_{IR} \leq d + d_1$. The corresponding scenarios are 100 m $\leq d_1 < 200$ m in Fig. 13(a), 200 m $\leq d_1 < 400$ m in Fig. 13(b) and 300 m $\leq d_1 < 700$ m in Fig. 13(c), where the senders are outside the interference range of the other link but the receivers are within the interference range. Concurrent transmissions are prohibited by IRMA, PCS and PCS+VCS, but can be exploited by ICMR, leading to a 2× throughput comparing with the other protocols. There are two scenarios that should be discussed separately in this case. When $2 \cdot d + d_1 < d_{CS}$, such as 100 m $\leq d_1 < 200$ m in Fig. 13(a) and 200 m $\leq d_1 < 300$ m in Fig. 13(b), PCS+VCS only has a little performance degradation (about 3%) comparing with PCS, because of the overhead induced by RTS and CTS control frame transmissions. However, when $2 \cdot d + d_1 > d_{CS}$, such as 300 m $\leq d_1 < 400$ m in Fig. 13(b) and 300 m $\leq d_1 < 700$ m in Fig. 13(c), as the two senders are out of carrier sense of each other, the exchange of RTS and CTS may worse affect the other link's data reception, leading to about 22.4% performance degradation comparing with PCS.

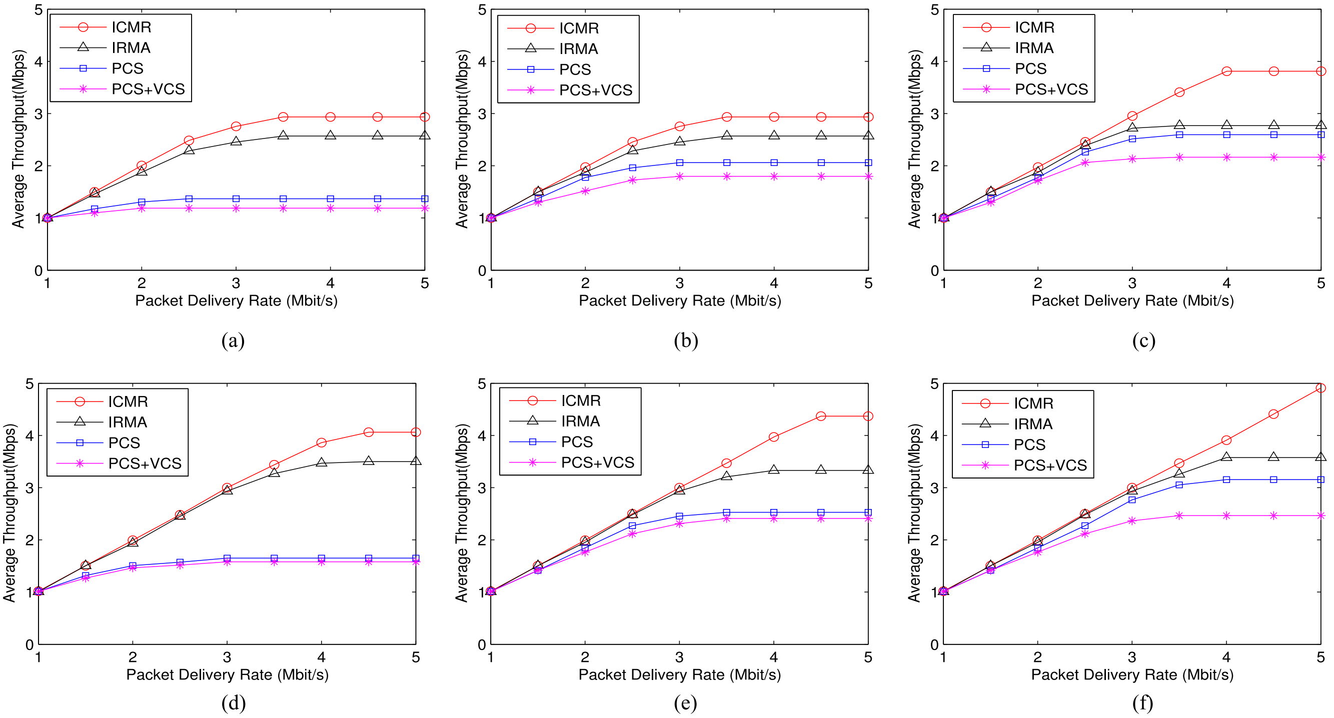
Case 3: $d_1 \geq d_{IR}$. The corresponding scenarios are $d_1 \geq 200$ in Fig. 13(a), $d_1 \geq 400$ m in Fig. 13(b) and $d_1 \geq 700$ in Fig. 13(c), where all the senders and receivers are outside the interference range of the other link. When $2 \cdot d + d_1 < d_{CS}$, such as 200 m $\leq d_1 \leq 600$ m in Fig. 13(a), concurrent transmissions are permitted by ICMR and IRMA, but prohibited by PCS and PCS+VCS because of the physical carrier sense. When $2 \cdot d + d_1 > d_{CS}$, such as $d_1 > 600$ m in Fig. 13(a), $d_1 \geq 400$ m in Fig. 13(b) and $d_1 \geq 700$ m in Fig. 13(c), the two senders cannot carrier sense each other, concurrent transmissions are permitted by ICMR, IRMA and PCS. Both ICMR and IRMA have a little performance degradation (about 6%) comparing with PCS, because of the overhead induced by transmitting control frames and signatures. For PCS+VCS, two scenarios should be discussed separately. When $d_1 < d_{TX}$, such as 400 m $\leq d_1 \leq 500$ m in Fig. 13(b), the two receivers $R1$ and $R2$ can get the CTS from the other link correctly to update their NAV states, making PCS+VCS prohibit the concurrent transmissions. When $d_1 > d_{TX}$, such as $d_1 > 500$ m in Fig. 13(b) and $d_1 > 700$ m in Fig. 13(c), PCS+VCS permits the concurrent transmissions and it has the similar performance as the other protocols.

B. *Random Topology*

We further compare the performance of ICMR with the other protocols in the random topology with different network densities.

We set up three networks, each of which has 100 nodes deployed in a 10 × 10 grid. We set the side length d of each grid cell to 100 m, 200 m and 400 m, making the networks have three different densities. For each network, we randomly select 10 transmitter-receiver links: we first randomly select one node as a transmitter, then select an adjacent node as its receiver. A CBR flow is set up at each sender to generate data packets.

As shown in Fig. 14, the average throughput of all the protocols increases when the packet delivery rate or the packet length l_p increases. The throughput of PCS+VCS is the lowest nearly in all the scenarios. Different from the results in the line topology, PCS has a better performance than PCS+VCS in the random topology even when $d = 400$ m, as shown in Fig. 14(c) and Fig. 14(f), as PCS has a critical unfairness issue, which largely avoids collisions and makes the network achieve



(a) (b) (c) (d) (e) (f)

Fig. 14. Average throughput in terms of packet delivery rate in the random topology, under three transmission rates and two packet lengths. (a) $l_p = 500$ bytes, $d = 100$ m. (b) $l_p = 500$ bytes, $d = 200$ m. (c) $l_p = 500$ bytes, $d = 400$ m. (d) $l_p = 2000$ bytes, $d = 100$ m. (e) $l_p = 2000$ bytes, $d = 200$ m. (f) $l_p = 2000$ bytes, $d = 400$ m.

a higher throughput in average. Fig. 14 also indicates that the performance of the four protocols increases along with the increase of l_p. This is because the overhead induced by control frames is much larger when the packet length is shorter, leading to a lower performance.

We can see from Fig. 14 that both ICMR and IRMA can improve the network throughput due to exploiting concurrent transmissions, and ICMR has the highest throughput comparing with the other protocols in all cases. The throughput gain of ICMR over IRMA increases along with the increases of d, that means the throughput gain increases along with the deceases of network density. When $l_p = 2000$ bytes, ICMR's throughput gain is about 16.1% over IRMA when $d = 100$ m. This value increases to 31.2% when $d = 200$ m, and increases to 37.3% when $d = 400$ m. The situation is similar when $l_p = 500$ bytes. Meanwhile, the throughput gain of both ICMR and IRMA over PCS or PCS+VCS decreases along with the increase of d. As shown in Fig. 14, when $l_p = 2000$ bytes, ICMR's throughput gain is about 146.2% over PCS and 157.8% over PCS+VCS when $d = 100$ m. These values decrease to 55.6% and 99.1% respectively when $d = 400$ m.

As a conclusion, in the unsaturated situations, all the protocols have similar performance as the channel bandwidth is sufficient for the required data transmission, as shown in Fig. 14 when the packet delivery rate is about 1 Mbits/s. In the saturated situations, ICMR has the highest throughput comparing with other protocols in all cases because concurrent transmission opportunities are effectively exploited by this protocol. The throughput gain over PCS or PCS+VCS will be larger in a denser network, and the throughput gain over IRMA will be larger in a sparser network.

Although the performance in this paper is just evaluated based on the CBR traffic, we also conduct simulations using the VBR (variable bit rate) traffic and find that both have similar average throughput when VBR's average bit rate is equal to the CBR value in the saturated networks. This is reasonable as in both scenarios there are always data packets in the buffer waiting for transmission, the features of different traffic patterns are counteracted in this way. Due to the page limit, we do not include the simulation results about VBR in the paper.

VII. Related Work

Prior related work mainly falls into two categories.

A. Avoid Interference and Exploit Concurrent Transmissions

Many research works exploit concurrent transmissions by either effectively utilizing control frames or solving the varied-IR problem.

Some approaches are proposed to improve the network throughput through utilizing control frames effectively. MACA-P [11] schedules the transmissions centrally to avoid the control frames' collisions through the exchanges of RTS/CTS. CSMA/CN [9] utilizes this technology to notify the collision information, which can be detected under strong interference and thus make the transmitter suspend its data transmission immediately. Side Channel [12] utilizes DSSS systems which have the ability to resist interferences to make the control information transmitted with the original data packet simultaneously. RTS/S-CTS [13] proposes to solve the hidden terminal problem through presenting a symbol-level detection mechanism, it designs new CTS which uses the symbol sequences to carry the coordination information and detects the CTS even when the SINR is very low, thus can avoid interference efficiently. 802.11ec [14] uses known sequences to deliver the control information, so as to reduce the transmission overhead of the control frames. hJam [15] and Attached-RTS [16] allow the control information to be transmitted simultaneously with the data packet, so as to both reduce the coordination overhead and solve the exposed terminal problem, however, nodes nearby the receiver cannot get correct control information to make proper decisions. FAST [17] uses a full duplex paradigm [18] to solve the problem existed in Attached-RTS. It makes the control information be transmitted by the receiver simultaneously with the transmitter. These schemes cannot solve the varied-IR problem.

Many other approaches are proposed to exploit concurrent transmissions through solving the varied-IR problem. Some approaches design mechanisms to find the links that have no mutual interference to permit their concurrent transmissions and increase the network throughput. SDN [4] constructs an interference graph for each node through periodical control packets exchange among nearby nodes. CMAP [19] makes each node build a conflict map to distinguish the interfering and non-interfering links through empirical observations on packet loss. RTSS/CTSS [20] achieves this goal through an offline training, which can only be applied in the line topology. These schemes cannot solve the CA-CF problem.

Some approaches utilize the joint information from multiple APs connected by wired network to increase concurrency. TRACK [21] tunes the bit rate of concurrent links to make the transmissions succeed based on online channel measurements that account for SINRs. OpenTDMF [22] brings TDMA in enterprise WLANs through a centralized controller. COAP [23] extends the centralized method in home APs for coordination and management. These schemes are hard to be applied to real networks currently as they need a great number of information exchange and stringent time synchronization among APs.

B. Signal Recovery Under Interferences

Recent years have seen a great number of research works that improve the network performance through recovering the collided signals.

Besides IRMA [6], the cross correlation technology adopted in this paper has already been exploited in many previous works to improve the network performance. CSMA/CN [9] exploits this technology to make the transmitter detect the collision notification information, which is sent by the receiver when a collision occurs, so as to defer the data transmission to avoid further interference. RTS/S-CTS [13] and 802.11ec [14] propose the symbol-level detection mechanism to combat the collision of the RTS/CTS/ACK frame transmission, thus to solve the hidden terminal problem. ZigZag [8] makes each packet in a n-packet collision retransmitted n times, and utilizes the partially clean symbols to recover all the collided packets. Symphony [24] extends the Zigzag-like decoding process in the multiple-AP scenario. It encourages packets collision at APs and decodes all the packets through the collaboration among the APs, thus improve the throughput of WLANs. This technology has also been utilized in other systems to improve the network performance, such as RFID [25]. However, these works can only exploit the cross correlation technology to detect either the collided control message or the data packet, while DIC in this paper can detect both kinds of signals at the same time.

Some approaches try to recover the collided signal through exploiting the well-known capture effect. SIC [26] makes nodes first detect the strong interfering signal through normal demodulation process, then subtract it from the received signal to obtain the inferior strong signal. The nodes can then detect this signal if its SINR is above the threshold. Coco [27] permits simultaneous transmissions of multiple nodes based on the requirement of capture effect, thus enhances the channel utilization. This mechanism can be used in the data-gathering scenario to improve the performance. However, this kind of mechanisms have a limit on the received signal power to detect the signal correctly.

Comparing with the previous works, the DIC proposed in this paper can detect the collided control and data signal without the limit of both the packet length and signal power.

VIII. Conclusion and Future Works

In this paper, we conclude that the 802.11 standard degrades the network performance from two aspects, including the CA-CF problem and the varied-IR problem. Comparing with IRMA, we propose ICMR to further solve the CF-CA problem through permitting the data frame being collided by the control frames, and propose the DIC mechanism to detect the data frame in this situation, so as to maximize the network performance. We formulate the concurrent transmission opportunities, then analyze and compare the opportunities among ICMR, IRMA and the 802.11 standard theoretically. We show the feasibility of the DIC mechanism through hardware experiments, and demonstrate ICMR's significant throughput improvement over other protocols by ns-2.

We consider this paper may have some future works worthy for study. At first, this work just evaluates the feasibility of DIC through experiments, we may implement an ICMR real-world testbed which is sure to help further optimize the mechanism design; at second, this work only exploits DIC to increase concurrent transmissions in wireless networks, we consider the DIC process can be exploited to benefit other wireless communication systems, such as cellular networks [28], [29] and wireless sensor networks [30]; at last, we also consider exploiting the physical layer techniques utilized in this paper for wireless smart sensing [31], [32].

References

[1] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Computer Society. 802.11, '2007.

[2] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[3] T. Rappaport, *Wireless Communications: Principles and Practice*. Englewood Cliffss, NJ, USA: Prentice-Hall, 2002.

[4] L. B. Jiang and S. C. Liew, “Improving throughput and fairness by reducing exposed and hidden nodes in 802.11 networks,” *IEEE Trans. Mobile Comput.*, vol. 7, no. 1, pp. 34–49, Jan. 2008.

[5] J. Yao, T. Xiong, and W. Lou, “Elimination of exposed terminal problem using signature detection,” in *Proc. 9th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw.*, 2012, pp. 398–406.

[6] J. Yao, T. Xiong, J. Zhang, and W. Lou, “On eliminating the exposed terminal problem using signature detection,” *IEEE Trans. Mobile Comput.*, vol. 15, no. 8, pp. 2034–2047, Aug. 2016.

[7] M. S. Gast, “802.11ac: A survival guide,” Sebastopol, CA, USA: O’Reilly Media, 2013.

[8] S. Gollakota and D. Katabi, “Zigzag decoding: Combating hidden terminals in wireless networks,” in *Proc. ACM SIGCOMM*, 2008, pp. 159–170.

[9] S. Sen, R. R. Choudhury, and S. Nelakuditi, “CSMA/CN: Carrier sense multiple access with collision notification,” in *Proc. ACM MOBICOM*, 2010, pp. 25–36.

[10] X. Zhang and K. G. Shin, “DAC: Distributed asynchronous cooperation for wireless relay networks,” in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[11] A. Acharya, A. Misra, and S. Bansal, “Design and analysis of a cooperative medium access scheme for wireless mesh networks,” in *Proc. ICST BROADNETS*, 2004, pp. 621–631.

[12] K. Wu, H. Tan, Y. Liu, J. Zhang, Q. Zhang, and L. M. Ni, “Side channel: Bits over interference,” in *Proc. ACM MOBICOM*, 2010, pp. 13–24.

[13] T. Xiong, J. Zhang, J. Yao, and W. Lou, “Symbol-level detection: A new approach to silencing hidden terminals,” in *Proc. IEEE Int. Conf. Netw. Protocols*, 2012, pp. 1–10.

[14] E. Magistretti, O. Gurewitz, and E. W. Knightly, “802.11ec: Collision avoidance without control messages,” in *Proc. ACM MOBICOM*, 2012, pp. 65–76.

[15] K. Wu *et al.*, “HJam: Attachment transmission in WLANs,” in *Proc. IEEE INFOCOM*, 2012, pp. 1449–1457.

[16] L. Wang and K. Wu, “Attached-RTS: Eliminating exposed terminal problem in wireless networks,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 7, pp. 1289–1299, Jul. 2013.

[17] L. Wang, K. Wu, and M. Hamdi, “Combating hidden and exposed terminal problems in wireless networks,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 4204–4213, Nov. 2012.

[18] M. Jain *et al.*, “Practical, real-time, full duplex wireless,” in *Proc. ACM MOBICOM*, 2011, pp. 301–312.

[19] M. Vutukuru, K. Jamieson, and H. Balakrishnan, “Harnessing exposed terminals in wireless networks,” in *Proc. ACM NSDI*, 2008, pp. 59–72.

[20] K. Mittal and E. Belding, “RTSS/CTSS: Mitigation of exposed terminals in static 802.11-based mesh networks,” in *Proc. IEEE Workshop Wireless Mesh Netw.*, 2006, pp. 3–12.

[21] J. Huang, G. Xing, and G. Zhou, “Unleashing exposed terminals in enterprise WLANs: A rate adaptation approach,” in *Proc. IEEE INFOCOM*, 2014, pp. 2481–2489.

[22] Z. Yang, J. Zhang, K. Tan, Q. Zhang, and Y. Zhang, “Enabling TDMA for today’s wireless LANs,” in *Proc. IEEE INFOCOM*, 2015, pp. 1436–1444.

[23] A. Patro and S. Banerjee, “Outsourcing coordination and management of home wireless access points through an open API,” in *Proc. IEEE INFOCOM*, 2015, pp. 1454–1462.

[24] T. Bansal, B. Chen, P. Sinha, and K. Srinivasan, “Symphony: Cooperative packet recovery over the wired backbone in enterprise WLANs,” in *Proc. ACM MOBICOM*, 2013, pp. 351–362.

[25] J. Yao, T. Xiong, and W. Lou, “Beyond the limit: A fast tag identification protocol for RFID systems,” *IEEE Trans. Mobile Comput.*, vol. 21, no. 1, pp. 1–18, Aug. 2015.

[26] D. Halperin, T. Anderson, and D. Wetherall, “Taking the sting out of carrier sense: Interference cancellation for wireless LANs,” in *Proc. ACM MOBICOM*, 2008, pp. 339–350.

[27] X. Ji *et al.*, “On improving wireless channel utilization: A collision tolerance-based approach,” *IEEE Trans. Mobile Comput.*, vol. 16, no. 3, pp. 787–800, Mar. 2017.

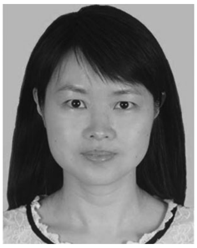
[28] R. Ruby, S. Zhong, H. Yang, and K. Wu, “Enhanced uplink resource allocation in non-orthogonal multiple access systems,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1432–1444, Mar. 2018, doi: 10.1109/TWC.2017.2778105.

[29] J. Xu, J. Yao, L. Wang, Z. Ming, K. Wu, and L. Chen, “Narrowband Internet of Things: Evolutions, technologies and issues,” *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1449–1462, Jun. 2018, doi: 10.1109/JIOT.2017.2783374.

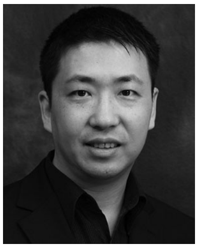
[30] Z. Wang, Q. Cao, H. Qi, H. Chen, and Q. Wang, “Cost-effective barrier coverage formation in heterogeneous wireless sensor networks,” *ELSEVIER Ad Hoc Netw.*, vol. 64, no. 1, pp. 65–79, Sep. 2017.

[31] Y. Zou, W. Liu, K. Wu, and L. M. Ni, “Wi-Fi radar: Recognizing human behavior with commodity Wi-Fi,” *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 105–111, Oct. 2017.

[32] Y. Xie, Z. Li, and M. Li, “Precise power delay profiling with Commodity WiFi,” in *Proc. ACM MOBICOM*, 2015, pp. 53–64.



Junmei Yao received the B.E. degree in communication engineering from Harbin Institute of Technology, Harbin, China, in 2003, the M.E. degree in communication and information system from Harbin Institute of Technology, China in 2005, and the Ph.D. degree in computer science from The Hong Kong Polytechnic University, Kowloon, Hong Kong, 2016. She is currently an Assistant Professor with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, China. Her research interests include wireless networks, wireless communications, and RFID systems.



Dr. Wei Lou received the B.E. degree in electrical engineering from Tsinghua University, Beijing, China, in 1995, the M.E. degree in telecommunications from Beijing University of Posts and Telecommunications, Beijing, China, in 1998, and the Ph.D. degree in computer engineering from Florida Atlantic University, Boca Raton, FL, USA in 2004. He is currently an Associate Professor with the Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong. His current research interests are in the areas of wireless networking, mobile ad hoc and sensor networks, peer-to-peer networks, and mobile cloud computing. He has worked intensively on designing, analyzing and evaluating practical algorithms with the theoretical basis, as well as building prototype systems. His research work is supported by several Hong Kong GRF grants and Hong Kong Polytechnic University ICRG grants.

Lu Wang received the B.S. degree in communication engineering from Nankai University, Tianjin, China, in 2009 and the Ph.D. degree in computer science and engineering from Hong Kong University of Science and Technology, Hong Kong, in 2013. She is currently an Assistant Professor with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, China. Her research interests focus on wireless communications and mobile computing.

Kaishun Wu received the Ph.D. degree in computer science and engineering from Hong Kong University of Science and Technology (HKUST), Hong Kong, in 2011. After that, he was a Research Assistant Professor with HKUST. In 2013, he joined SZU as a Distinguished Professor. He has coauthored two books and authored or coauthored more than 90 high-quality research papers in international leading journals and primer conferences, like IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, *ACM MobiCom*, IEEE INFOCOM. He is the inventor of six U.S. and more than 70 Chinese pending patent. He was the recipient of the 2012 Hong Kong Young Scientist Award, the 2014 Hong Kong ICT Awards: Best Innovation and 2014 IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award.