hJam: Attachment Transmission in WLANs

Kaishun Wu*[†], Haochao Li[†], Lu Wang[†], Youwen Yi[†], Yunhuai Liu[‡], Qian Zhang[†], and Lionel M. Ni[†]

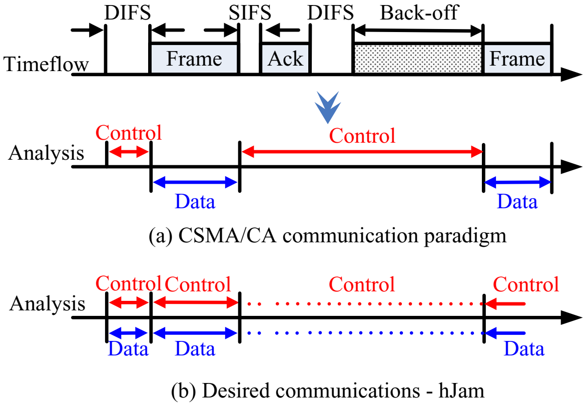
*School of Physics and Engineering, National Engineering Research Center of Digital Life, Sun Yat-sen University
[†]Department of Computer Science and Engineering
Hong Kong University of Science and Technology
[‡]Third Research Institute of Ministry of Public Security

***Abstract*—Effective coordination can dramatically reduce radio interference and avoid packet collisions for multi-station wireless local area networks (WLANs). Coordination itself needs consume communication resource and thus competes with data transmission for the limited wireless radio resources. In traditional approaches, control frames and data packets are transmitted in an alternate manner, which brings a great deal of coordination overhead. In this paper we propose a new communication model where the control frames can be "attached" to the data transmission. Thus, control messages and data traffic can be transmitted simultaneously and consequently the channel utilization can be improved significantly. We implement the idea in OFDM-based WLANs called hJam, which fully explores the physical layer features of the OFDM modulation method and allows one data packet and a number of control messages to be transmitted together. hJam is implemented on the GNU Radio testbed consisting of eight USRP2 nodes. We also conduct comprehensive simulations and the experimental results show that hJam can improve the WLANs efficiency by up to** 72% **compared with the existing 802.11 family protocols.**

I. Introduction

Coordination among stations can effectively reduce radio interference and avoid packet collisions in multi-station wireless local area networks (WLANs). Coordination needs communication and stations have to exchange control messages in order to well coordinate. The control messages can be delivered in an explicit, implicit, or hybrid manner. However, all control messages will consume valuable communication resources such as the communication channel and transmission air time.

In a practical WLAN the transmissions of control messages and data traffic often interleave. As illustrated in Fig. 1 (a), the current CSMA/CA protocols (e.g., 802.11 a/g/n) transmit the control messages and data traffic in an alternate manner. Between data traffic there are always fractions of air time for coordination purposes such as DIFS, SIFS, backoff and packet acknowledgment. It is well-known that such mechanism is quite inefficient when data frames are small [1]. When higher physical layer (PHY) data rates are supported, the efficiency becomes even worse because of the shortened data traffic air time. Off-the-shelf 802.11n products now support up to 300Mbps PHY data rate, while the effective throughput is only 60Mbps [1]. To deal with this issue, a direct way in traditional approaches is to separate the control messages and data traffic. In this approach (e.g., [13]), a dedicated PHY channel is allocated for coordination. This approach consumes an entire channel for control purposes only, which is also too expensive. The separation can also be done in other dimensions. Side Channel [8] transmits the control messages in the code space. It is a customized design for Direct Sequence Spread Spectrum (DSSS) modulation only and does not have general applicability.



(a) CSMA/CA communication paradigm

(b) Desired communications - hJam

Fig. 1: (a) An example of a CSMA/CA communication paradigm and a simple analysis of its performance; (b) Desired communication system with control messages and data packets being transmitted together.

Rather than interleaving or separating the control messages and data traffic, serving them together at the same time is more desirable. As illustrated in Fig.1(b), in this model the data traffic and the control messages are transmitted simultaneously in the same channel. Data traffic accounts for the entire fraction of transmission air time and is allocated the same bandwidth as in traditional systems. In the meanwhile, control messages are transmitted in an attached manner with the data traffic. As such the coordination overhead can be dramatically reduced.

This idea is simple but very challenging to realize. It is mainly because in the Fig.1(b) scenario the control messages and data traffic are transmitted from independent transmitters. These transmitters will have no extra coordination and thus are very likely to collide with each other. It becomes even more challenging when there are several control messages from different transmitters. In a typical WLAN, it is common that when one node is transmitting the data, all others may have the demands to transmit their requests.

978-1-4673-0775-8/12/$31.00 ©2012 IEEE

Recently, Interference Cancellation (IC) technique [2] has been developed well which brings a new hope. Since a practical rate adaptation scheme is unlikely to operate at the ideal bitrate, there will always be a slack for IC to exploit [20]. By a successful application of this technique we propose a new communication architecture called hJam with the core idea in Fig.1(b). hJam is built on top of Orthogonal Frequency Division Multiplexing (OFDM) networks, as OFDM has been widely adopted in modern WLAN protocols (e.g., 802.11 a/g/n) and is becoming the standard for the next generation of WLANs (e.g., WiMAX and 3GPP LTE).

hJam enables two kinds of transmissions in communications. One is the high-throughput transmission for data traffic, which shares the same (de)modulation method, (de)coding algorithm, and the bandwidth with the current OFDM system and thus is fully compatible. The other is the attachment transmission that allows each high-throughput transmission to carry a number of small-sized attachments. The attachments are independent to the high-throughput transmissions, and thus are extremely suitable for control message delivery. Concisely speaking, the attachment transmission supports multiple accesses though the high-throughput transmission supports one flow at a time. The success of hJam is by exploiting a subtle opportunity for channel estimation using packet preamble in current OFDM systems. Actually, the opportunity arises from the redundancy of preamble in different wireless link conditions due to correlation of the channel response of different subcarriers. When this redundancy is smartly utilized, a small amount of information can be delivered by intentionally injecting jamming signals without affecting the data traffic. For control messages, this amount of information is sufficient and is further made use of in our hJam design.

In summary, the main contributions of this paper are as follows.

- We propose hJam, a new PHY architecture for OFDM-based WLANs that enables concurrent transmission of coordination message and traffic data to improve the coordination efficiency. To the best of our knowledge, it is the first of its kind in the literature to enable simultaneous transmissions for control messages and traffic data in OFDM systems.
- We analyze the reliability of hJam theoretically, and numerical results show that multiple attached coordination information can be decoded correctly and the original data traffic is not affected with high probability.
- We demonstrate the feasibility of hJam by implementing it on a GNU Radio testbed of 8 USRP2 nodes. We also simulate hJam performance in a large scale network. hJam shows significant higher efficiency than prior protocols that do not allow concurrent transmission of coordination and data. It can provide up to 2x gain in efficiency, as compared to traditional 802.11 standards.

The rest of this paper is organized as follows. In Section II the system architecture is given. This is followed by the detail design of hJam in Section III. In Section IV, we analyze the performance of hJam. The implementation of hJam is presented in Section V. Experimental evaluations are given in Section VI. In Section VII, the related work is shown. Finally, conclusions are presented and suggestions are made for future research.

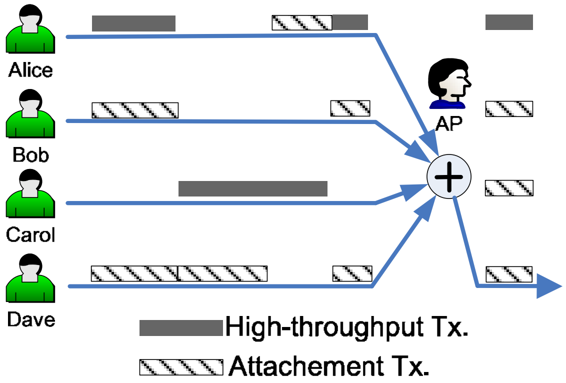


Fig. 2: An illustrative example of hJam communication system

II. Overall System Architecture

In this section, we present the system architecture of hJam which allows simultaneous transmissions for both control messages and data traffic. Challenges in the system design are also presented in this section.

A. hJam communication paradigm

The hJam PHY architecture introduces several new components. At the transmitter end, a jamming generator is designed to enable attachment transmission when necessary. At the receiver end, we introduce a jamming detector to detect the jamming signals, an attachment analyzer to decode the attachment transmission, and an interference cancellation engine to cancel the effects of attachment transmission and recover any high-throughput content.

Consider a simple transmission scenario with four clients Alice, Bob, Carol and Dave, and an AP, as illustrated in Fig. 2, and the architecture of hJam communication system is depicted in Fig. 3. Suppose Alice obtains a high-throughput channel for the next transmission. Alice is in normal mode which transmits the content in the traditional way (High-throughput Tx. in Fig.3 is exactly the same as OFDM Tx.). The others (Bob, Carol and Dave) will then turn to the hJam mode and attempt to use the attachment transmission. Each client in hJam mode will select a unique subcarrier assigned by AP and send jamming signals when Alice is sending. These jamming signals carry the attached information from the hJam clients, combine Alice's signal in the air and are received by the AP. At the receiver end, the AP first applies the jamming detector to determine whether any jamming signals from hJam clients exist. These jamming signals are then analyzed and decoded to recover attachment transmissions (from Bob, Carol or Dave). In the meantime, the interference cancellation technique [2] is applied to cancel the jamming signals and recover the original data for the high-throughput client (Alice).

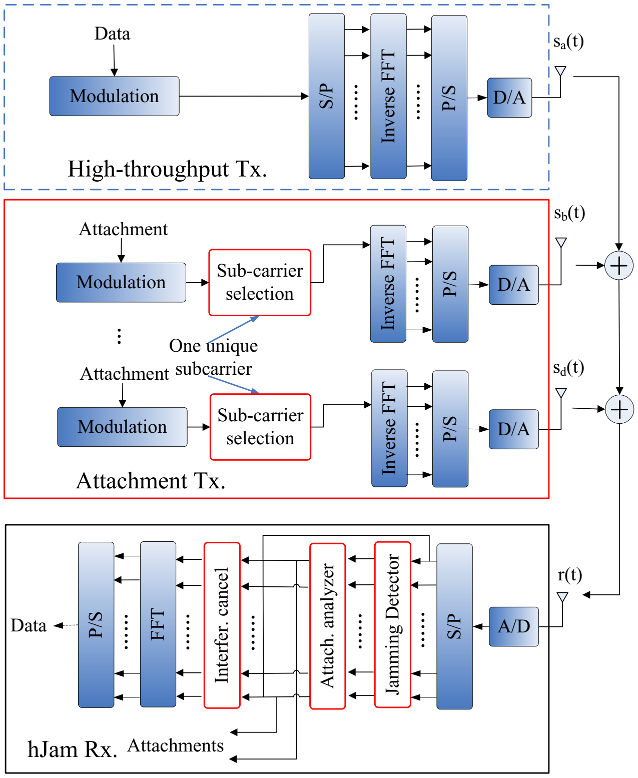


Fig. 3: Architecture of hJam communication system

B. Design challenges

The design principles of hJam are simple and effective. In practice, however, the implementation of hJam design faces many practical challenges.

First, the success of hJam depends highly on whether the generated jamming signals can be reliably identified and decoded. Note that we may not necessarily intend to generate the jamming signals, instead they could be the result of noise. We have to carefully design the jamming signal generator and detector, striking a tradeoff between miss detections and false alarms and strive to reduce both.

Second, the coordination information is attached on the data traffic. The receiver should be able to decode both kinds of data. However, in current mature OFDM-based WLANs, with proper rate adaptation and channel coding, the BER performance is sensitive to the interference. Therefore, it is a great challenge to detect both attached information and original data.

Last, the bandwidth for attached transmission is limited. Therefore, it is important to modulate multiple coordination messages effectively, and coordinate them to avoid collision. Otherwise collisions in the attachment channel may cause the interference cancellation to fail, resulting in a failed high-throughput channel transmission which may have severe consequence.

In the next section, we give details on how we address these challenges in hJam design.

III. hJam Design

In this section, we detail the design of hJam communication architecture. hJam introduces several new components, namely a jamming generator on the transmitter side, and a jamming detector, interference cancellation and attachment analyzer on the receiver side. We describe the design of each component in detail.

A. Jamming generator and detector

For each hJam mode client (Bob, etc., in Fig. 2), it needs to encode its control messages and transmit them through the attachment transmissions by using our designated jamming generator. As mentioned in Section II-A, each client in hJam will be assigned with a unique subcarrier. To guarantee that different hJam clients do not interfere with each other's jamming signals, we intentionally narrow the jamming signal channel width so that it is completely inclusive of a single subcarrier even in presence of frequency offset.

Accordingly, at the AP side, a jamming detector is carefully designed to identify these jamming signal from the noise. Specifically in our current design, we adopt a simple yet effective scheme by using energy detection. This is based on the simple observation that in general cases, high-throughput transmissions and noise have an even energy distribution over the spectrum. When there is a burst existing in a subcarrier (i.e., the combined signal strength of both the data and jamming signal in our case), it is very likely this is due to intended behavior. More detailed system implementations of the energy detection will be introduced in Section V.

As long as such intentional jamming signals are successfully detected, we are able to cancel corruption effects induced by jamming and recover the high-throughput channel data by leveraging our interference cancellation component.

B. Interference cancellation

The main objective of interference cancellation is to cancel the jamming signals and recover the content in the high-throughput channel. Notice that the raw signal is not directly decodable as it combines both high-throughput transmissions and the attachments.

In OFDM-based WLANs, the time/frequency synchronization and channel estimation are performed by using preambles located in the header of each transmission packet. Due to channel correlation, the channel estimation of some subcarriers can be interpolated with neighboring ones [19] and thus it is sufficient to use only part of the subcarriers to send pilots in preambles. We call the rest vacant subcarriers as clean because ideally no signal except noise is received at these subcarriers. In our attachment transmission design, we exploit this opportunity and make use of those clean subcarriers to record the jamming signal for the purpose of recovering data signal.

In wireless communication, the received signal is typically represented as a stream of discrete complex symbols spaced by the sampling interval T. These symbols are different from the transmitted ones both in amplitude and phase. For example,

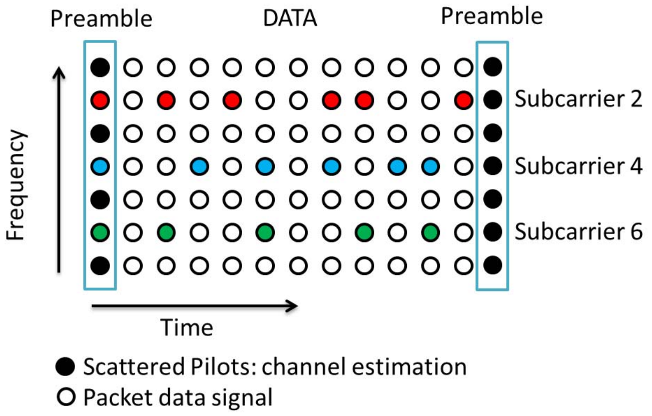


Fig. 4: Example illustration of attached information

the data signal $x[t]$ without jamming on the ith subcarrier can be expressed as:

$$y_i[t] = H_i x[t] + w[t], \tag{1}$$

where $H_i = he^{j\omega}$. The magnitude h refers to channel attenuation and the angle $j\omega$ is a phase shift, and $w[n]$ is a random complex noise.

More specifically in our design, when jamming signals are introduced in those subcarriers not used for sending preambles, the received signal in clean subcarrier can be expressed as:

$$y_i{''}[t] = y_B[t] + w[t] \tag{2}$$

where $y_B[t] = H_B x_B[t]$ refers to the jammer's signals after traversing their corresponding channels to the receiver. Accordingly, the received signal in those data symbol combines the data signal and the jamming signal and can be further expressed as:

$$y_i{'}[t] = y_A[t] + y_B[t] + w[t], \tag{3}$$

where $y_A[t] = H_A x_A[t]$ refers to the transmitter's signals after traversing their corresponding channels to the receiver. Thus the original data signal can be recovered by canceling the jamming signal from the received signal in the data symbol using Equation (2) and (3) as follows:

$$\hat{x}_A[t] = \frac{y_i{'}[t] - y_i{''}[t]}{H_A}, \tag{4}$$

where H_A can be further estimated by the training sequence.

C. Modulation/Demodulation of Attached Information

With the above techniques we are able to correctly identify individual jamming signals that are intentionally generated from an hJam node. In this subsection, we see how to modulate and demodulate the attachment to such jamming signals.

Different from a traditional decoder, we trade the jamming signal as intended information rather than noise. With synchronization, we can decide whether to jam the data at a specific subcarrier for one symbol duration time or not. For the ease of decoding, we use a jamming signal in each symbol to represent one bit of information, i.e., the jammed subcarrier in the symbol is considered to be "1" and the clean one to be "0", or otherwise. Since one packet contains several symbols, and each symbol is modulated on several subcarriers, these jamming patterns can be represented by a bit sequence, which will be the transmitted attachment. As illustrated in Fig. 4, the attached information in subcarrier 2 is "01010011001". Notice that the jamming signals for the attachment transmission starts from the first data symbol in the packet, and ends with the last symbol of the same packet. The jamming signal in the preamble is used by interference cancelation for recovering the original data. Therefore, in such a design, the capacity of attached transmission will be $n \cdot m$ bits per packet, where n is the number of data symbols per packet, and m is the number of hJam nodes.

Obviously, the attached information able to transmitted by a specific user is bounded by the number of data symbols per packet n. However, the number of subcarriers for jamming is not limited by the total number of OFDM subcarriers, but the performance degradation of the original data link that can be tolerated due to the existence of these jamming signals. In the next section, we analyze the effect of the jamming signals on performance of the high-throughput transmission.

D. Multiple access by hJam

To demonstrate the effectiveness of hJam in this section, we show how to use hJam to benefit transmissions in WLANs in the infrastructure mode [12]. The high-throughput transmission is used for application data traffic and the attachment is used for control message delivery.

Consider the single AP scenario. Upon receiving a data packet from a client, AP first decodes both the high-throughput and attachment transmissions. Then the high-throughput content is delivered to the upper layer application directly while the attachments are collected for coordination purpose. These attachments carry the transmission requests from the clients and can be further used to build a potential sender list. By having this list, the AP is responsible for whole channel coordination and assign the next sender. Specifically, the AP attaches the senders' IDs in order in the ACK and broadcast it. At the client end, by receiving the ACK from AP, the client can check its order in the sender list and determines whether it is the next sender of the high throughput channel. Then the next data transmission continues. It will be similar when the transmission is from the AP to the client due to that each client knows its sending order.

In addition, clients may join and leave. At the initialization step, the AP is responsible for allocating the subcarriers to the existing clients in the network. Afterward, a Client being inactive for too long time is automatically kicked out by the AP. To the contrary, a new comer should first listen to the AP's broadcast ACK packet (indeed, the ACK is for other clients). This packet carries the sub-channel utilization information and the new comer simply selects a random un-used subcarrier to delivers its request.

TABLE I: Notations for BER calculation

k/n	number of information/coded bits in convolutional code
r	$r = k/n$ is defined as channel coding rate
d	hamming distance
d_{free}	free distance of the convolutional code
B_d	total number of information bit ones on all weight d paths
P	the uncoded probability of bit error in AWGN under the effect of jamming
B_j/B_o	bandwidth of jamming signal/OFDM symbol
ρ	$\rho = N_u * B_j/B_o$ is the total jamming portion
E_b/N_0	ratio of average energy per bit-to noise power spectral density
N_j	jamming power spectral density

IV. Performance Analysis

In this part, we analyze the performance of hJam. The first issue is to find out the conditions under which the attachment transmission is nearly harmless to the performance of original data transmission in terms of Packet Reception Rate (PRR), so that data traffic can be guaranteed under hJam. The second issue is to evaluate the performance of attachment transmission in terms of Jamming Detection Rate (JDR), so that control messages can also be guaranteed. To this end, a key parameter N_u, which is the maximum number of subcarriers we can totally jam, is derived for different channel conditions.

Except the data transmission, the performance of the attachment transmission itself should also be evaluated in terms of the JDR, so that the probability of missing a jamming signal when one is present (miss detection), and the probability of falsely detecting a jamming signal when it is absent (false alarm), is designed to be as small as possible. We mainly focus on these two factors in the following subsections.

A. Performance for data symbol

The first influential factor used to measure the quality of original data transmission is PRR. According to [16], we can depict the relationship between PER and Bit Error Rate (BER) in Fig. 5, where left axis is BER and right axis is the corresponding PRR. For example, if we require PRR to exceed 99.6%, then the desired BER should be less than 10^{-5}.

BER has a direct connection with the encoding/deco-ding scheme applied by original data transmission. In order to be safe, the joint effect of intended jamming and noise should not go beyond the error correction capability of that coding/decoding scheme. Here we adopt convolutional encoder as the channel coding scheme and accordingly Viterbi hard decision decoder as the channel decoding scheme.

Lemma: For a hard decision, the Viterbi algorithm is a minimum Hamming distance decoder. An upper bound on the BER is used in order to examine its performance [16]:

$$P_b = \frac{1}{k} \sum_{d=d_{free}}^{d_{free+4}} B_d P_d \tag{5}$$

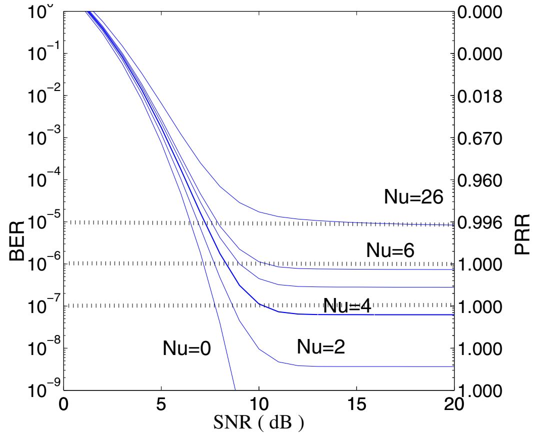


Fig. 5: Relationship between BER, PRR, # of clients and SNR(AWGN with noise and jamming, $SIR = 17$dB).

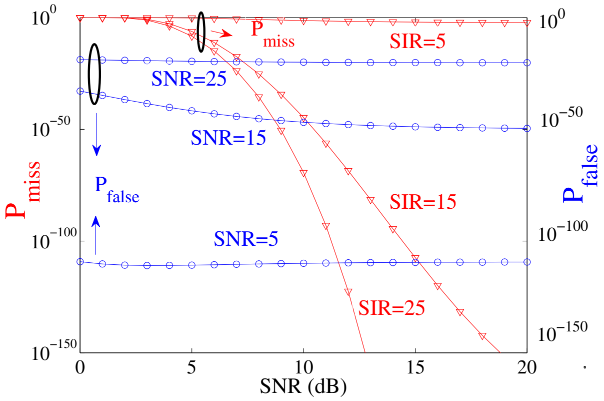


Fig. 6: Relationship between SIR, P_{miss}, P_{false} and SNR ($N_u = 1$)

P_d is the probability of selecting a code word what is Hamming distance d from the correct word. When d is even:

$$P_d = \sum_{i=\frac{d+1}{2}}^{d} \binom{d}{i} p^i (1-p)^{d-i} \tag{6}$$

When d is odd:

$$P_d = \frac{1}{2}\binom{d}{\frac{d}{2}} p^{\frac{d}{2}} (1-p)^{\frac{d}{2}} + \sum_{i=\frac{d+1}{2}}^{d} \binom{d}{i} p^i (1-p)^{d-i} \tag{7}$$

Table I lists the notations used for calculating P_b. Here we consider different type of modulation schemes for a single OFDM subcarrier, including BPSK, QPSK, 16QAM and 64QAM. for simplicity we only compute BPSK/QPSK, 16/64 QAM will be showed in Fig. 5 below. With the presence of noise and jamming in the original data transmission, p with BPSK/QPSK can be expressed as:

$$p = \rho \cdot Q\left(\sqrt{\frac{2rE_b}{N_0 + N_j/\rho}}\right) + (1-\rho) \cdot Q\left(\sqrt{\frac{2rE_b}{N_0}}\right) \tag{8}$$

We depict Equ. 5 in Fig. 5, which shows the relationship between BER, PRR and SNR when different number of

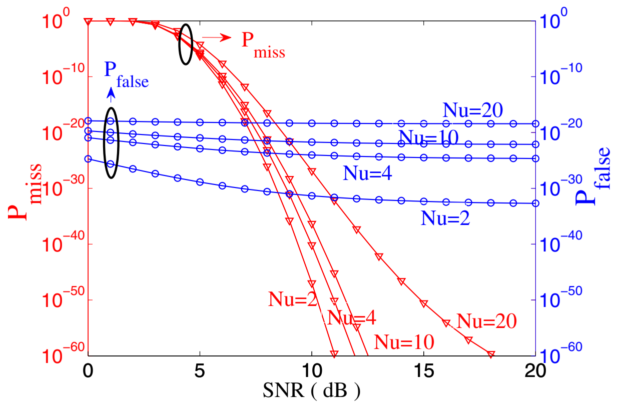


Fig. 7: Relationship between # of clients, P_{miss}, P_{false} and SNR (SIR=17dB)

attachment transmissions exist. The figure shows that when the channel condition exceeds a certain threshold (e.g., SNR $>$ 10dB), BER hardly changes as SNR increases. BPSK/QPSK shows robust performance even with $N_u = 20$ attachment transmissions, where hjam obtain a desired BER$< 10^{-9}$ and a corresponding $PRR > 100\%$. While with 16/64QAM, BER increases as the number of concurrent transmission increases. In the range from 20 to 30 dB which is the typical working range of 802.11 [18], BER remains stable at 10^{-7} for the worst case (64QAM with 20 concurrent transmissions), resulting in a $PRR > 99.7\%$. This is acceptable, and further confirms that the performance degradation induced by the attachment transmission can be ignored. Therefore we can come to the conclusion that in theory hjam is harmless and can be safely used in WLANs.

B. Performance for attachment transmission

Now we evaluate the performance of attachment transmission in terms of Jamming Detection Rate, which is dominated by the probability of miss detection P_{miss} and false alarm P_{false}. According to our Jamming Detection algorithm, when the energy strength of received signal $R(d)$ exceeds certain threshold (λ), we determine the presence of a jamming signal at instant d.

Lemma: Given a certain threshold value λ, P_{miss} and P_{false} can be expressed as [17]:

$$P_{miss}(\lambda) = 0.5erfc\left(\frac{\mu_M - \lambda}{\sqrt{2\sigma_M{}^2}}\right) \quad (9)$$

$$P_{flase}(\lambda) = e^{-\lambda G^2/D^2} \quad (10)$$

Here μ_M and σ_M are mean and variance of $R(d)$ inside jamming signal, while D and G^2 are mean and variance of $R(d)$ outside jamming signal. According to [17], the total SIR has a reverse impact on P_{miss} and P_{false}. We depict this feature in Fig. 6. As is shown below, P_{miss} decreases while P_{false} increases as the total SIR increases. Based on this observation, the total SIR should be set appropriately to meet the requirements of both P_{miss} and P_{false}. For example, if SNR is around 10dB, we can get a miss detection rate of $P_{miss} < 10^{-45}$ and false alarm rate $P_{false} < 10^{-48}$ by setting $SIR = 15$dB, when the number of attachment transmission $N_u = 1$, which is small enough for 802.11 specifications.

Now we derive how to calculate N_u using Equ. 9 and 10, which are depicted in Fig. 7. When the channel condition is above 10dB, we can set $N_u = 20$ to obtain a desired miss detection rate of $P_{miss} < 10^{-25}$ and false alarm rate of $P_{false} < 10^{-18}$. This result also agrees with N_u calculation under BER factor. Taking P_{miss} and P_{false} together into consideration, we can evaluate the probability that successful detecting the whole packet of attachment transmissions P_h:

$$P_h = (\frac{1}{2}(1 - P_{miss}) + \frac{1}{2}(1 - P_{false}))^{P_L} \quad (11)$$

where P_L is the packet length of one attachment transmission, with $P_L = 40$ bits for example, the probability that correctly detecting an attachment transmission packet is 99.99%. Therefore we can conclude that hJam, in theory, is not only harmless but reliable in typical working range of 802.11.

V. System Implementation

Building an operational communication system, however, involves many practical challenges. We use GNU Radio testbed for our experiments. We have implemented hJam using Software Defined Radios (SDRs). The SDRs are from the open source GNU Radio project [4], which implement signal processing blocks of wireless communication system in software. We use the Universal Software Radio Peripheral 2 (USRP2) [5] for our RF frontend, and use the RFX2450 daughterboard which operate in the 2.4-2.5GHZ range. Our implementation uses BPSK as the modulation. We have implemented the basic mechanisms of hJam on the USRP2.

One challenge during the implementation is the strict timing requirements due to synchronization (measured in micro seconds). If the clients and AP are not synchronized, the misalignment between the jamming signal and data signal may lead to the failure of the interference cancellation. However, the unpredictable latency caused by signal processing in software makes precise time control impossible in GNU Radio and thus software radios are incapable of real synchronization. To compensate for this latency, we import the USRP2 timestamps derived from the radio hardware [9] to record the packet receiving time. Thus upon receiving the ACK, we are able to control the data/jamming transmission time of all clients by adding a constant delay after the ACK's receiving time, so that all the senders can transmit the data at the same time.

Another challenge is the threshold setting for the jamming detection. According to our system design, either false alarm or missing detection will cause misbehavior in the interference cancellation procedure and thus lead to performance degradation. As the distance and the transmission power vary, how to dynamically adjust the threshold for accurate detecting jamming becomes the key issue in our system design. Currently, we have applied exponential averaging to track the mean (μ) and standard deviation (σ) of normal power level

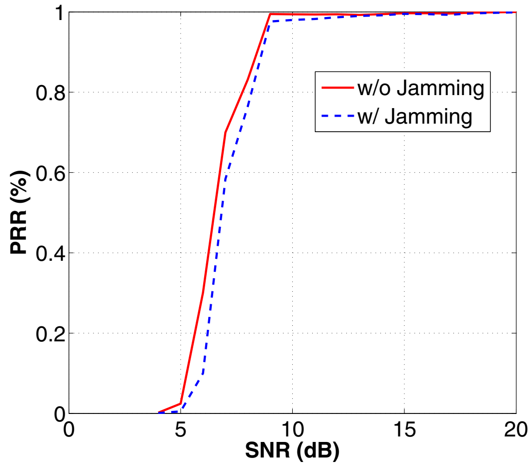


Fig. 8: Decodability of hJam under different SNRs

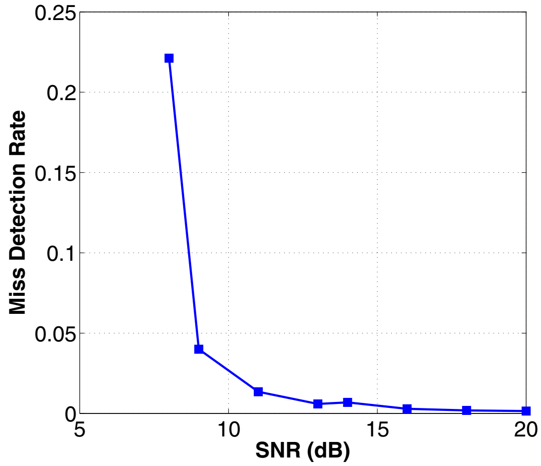


Fig. 10: Miss detection rate under different SNRs

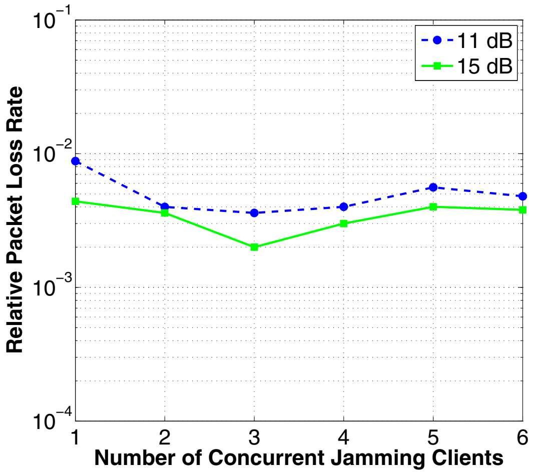


Fig. 9: Impact of number of concurrent jamming clients under different SNRs

(w/o jamming) and set the threshold as $\mu + \lambda \cdot \sigma$. A peak exceeding this threshold is recognized as the jamming signal.

Finally, the last challenge is the spectrum leakage and the phase offset. During the experiment, we observed that the subcarrier signal often has some spectrum leakage. Also the phase offset will cause jamming misalignment. We have noted that as mentioned in [10], the channel width can be adaptive. We then narrowed down the subcarrier channel width as it becomes a portion of the original one.

VI. Experimental Evaluation

A. Experiment

The feasibility of hJam is the focus of our experiments and mainly consists of two aspects. First, hJam is feasible only if the jamming signal can be cancelled out and thus the normal data packets can be recovered. Second, due to the coordination of the whole system design highly depending on the control message encoded in the jamming signals, the decodability of the attachment transmission becomes essential and dominates the effectiveness of hJam. Thus we have conducted realtime experiments by using USRP2 nodes with RFX2450 daughterboards operating in the 802.11 frequency range in our office, which is a typical real world environment with size 5m×8m shown in Fig. **??**. Unless otherwise specified below, we use the default configuration, e.g., a packet size 400 bytes. Specifically, we use 52 subcarriers and a bandwidth of around 2MHz. We make these changes because we want to make the inter subcarrier spacing comparable to 802.11 (0.3125MHz) while still maintaining the normal transmission of USRP2, which is limited by the hardware itself [**?**]. All of our experiments run on the 2.425GHz.

1) Is hJam harmless?: In order to answer this question, experiments are conducted to examine the decodability of hJam and the impact of the number of concurrent jamming clients respectively.

For measuring the decodability, we use a three-node setting, i.e., a sender, an AP and a jamming client. Upon receiving an ACK from AP for acknowledgement and coordination, the sender sends a normal packet while the jamming client sends the jamming signal simultaneously. Then we evaluate this by comparing the PRR under various SNRs. Each run transfers 2500 packets, first without jamming, then with jamming. For each value of SNR, we repeat the experiment 10 times.

Fig. 8 plots the PRR with/without the jamming client as a function of the received SNR at AP ranging from [4, 20]dB. The figure shows that when the SNR exceeds a threshold, i.e., larger than 10dB, the PRRs almost have no difference between the cases with and without a jamming client. This little performance degradation is acceptable because the typical range of SNR region defined for 802.11 is 10-30dB [18], where our hJam works well. Though, such results are comparable but less than the theoretical optimum. We infer this is due to two reasons. First, the software-defined signal processing may limit the USRP2's ability of the strict timing and accurately sampling. Second, our implementation runs in a public user-space in the unlicensed 2.4GHz range, some external interferences can not be avoided.

Though we have proved the feasibility of the hJam's

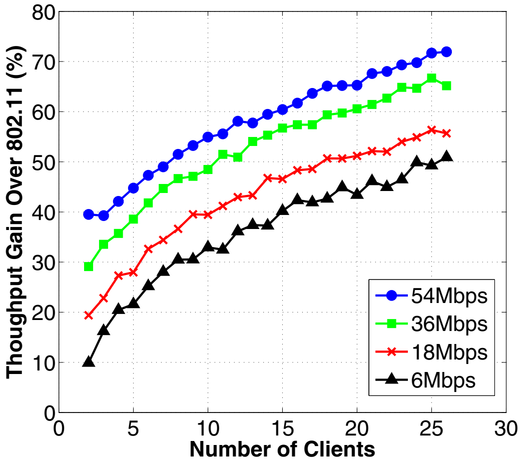


Fig. 11: Performance gain of hJam over 802.11 a/g under different number of clients

decodability in the presence of jamming signal, it is also interesting to ask whether the number of concurrent jamming clients has impact on the system performance. To investigate this influence, we use a similar setting to evaluate the PRR of the normal sender but with the number of concurrent jamming clients varying from 1 to 6. More precisely, we have 52 subcarriers (from 0 to 51) and those subcarriers with odd number are not used for channel estimation. The six subcarriers we have used for jamming in this experiment are Subcarrier $1, 3, 5, 7, 9$ and 17.

Fig. 9 plots our results under different number of jamming clients with SNR 11dB and 15dB respectively. We expected that the performance loss would increase when the number of the concurrent jamming clients increases as shown in our theoretical analysis (Fig. 5). Surprisingly, we observe that the relative performance loss varies randomly under different number of concurrent jamming clients, though they are so small that can be negligible. In theoretical analysis, even when SNR is 11dB with 20 jamming clients, the BER is below 10^{-6}, which would lead to merely no performance loss. We infer that the difference between the practical and the theoretical results may due to the processing capability of USRP2 hardware.

2) Is the attachment transmission reliable?: This question refers to the detection accuracy problem, i.e., whether we can accurately detect the jamming signal and decode the attached information correctly. It is mainly affected by the miss detection and false alarm rate. Note that hJam apply the interference cancellation only when it detects a jamming signal. So both cases will cause misbehavior in interference cancellation procedure and result in the decoding failure.

In this part of the experiment, we use similar three-node setting but varying the SNR of the jamming signal. For each run, the sender sends 2500 packets in total while the jamming client keeps sending attached information encoded in the jamming signal upon receiving an ACK. The AP logs all the attachment information for calculating the results. For each SNR value ranging from [8, 20]dB, we repeat the experiment 10 times.

TABLE II: Configuration Parameters

Parameters	**Values**	**Parameters**	**Values**
SIFS	10μs	DIFS	28μs
PIFS	19μs	Slot time	9μs
Preamble	20μs	Symbol time	4μs
CW_{min}	16	CW_{max}	1024

From the experimental results, we find out that there is no false alarm which is consistent with the theoretical analysis. Fig. 10 shows that when SNR> 13dB, the miss detection rate is controlled within 1%, resulting in a detection accuracy more than 99%. The detection algorithm will also impact the results. Therefore, one of our future works is to design a more precise detection algorithm.

B. Performance Evaluation

The latency constraint of USRP2 disallows the realtime evaluation of the system throughput. Thus we implement a simulator to understand the performance of hJam primarily under a single AP network with varying number of total clients. In order to focus on the performance on the channel utilization by each method, we assume that the packet reception failure is only caused by the collisions and the network is saturated. In this subsection, we mainly compare the performance of hJam with CSMA/CA [6], which is used by the current IEEE 802.11 Standard.

Our simulations model the CSMA MAC. For scheduling of hJam, we just simply use Round Robin as an example to demonstrate its performance. For the evaluation of hJam, Equation. 12 gives a simple model for hJam's throughput efficiency.

$$E_{hJam} = \frac{t_{data}}{t_{preamble} + t_{data} + t_{ACK}} \tag{12}$$

Unless otherwise stated, the default packet size is 1500 bytes, which is around the maximal transmit unit (MTU). Table II summaries the configuration parameters used in our simulators. Specially, for the simulation of high data rates with 802.11n, the total number of subcarriers is set to 114, of which 108 are used for data transmission and 6 for equalization.

Fig. 11 plots the throughput gain of hJam over 802.11 as a function of total clients under different data rates. It shows that hJam outperform 802.11 CSMA MAC at all cases and its throughput gain is significant, e.g., when the data rate is 54Mbps, the relative throughput gain over 802.11 a/g is up to around 72%. This significant improvement is due to two reasons. First, hJam eliminates the coordination overhead in each transmission while the proportion of coordination overhead in CSMA increases as the data rate increases. The second reason is due to that hJam is collision free while the collision probability of CSMA in IEEE 802.11 increases with the number of clients. Thus hJam has better utilization of the channel.

VII. Related Work

In order to address the radio interference issues and reduce the transmission collisions well, a large amount of coordination schemes have been proposed. The existing approaches can be classified as out-of-band and in-band.

The out-of-band coordination approaches are more suitable for multi-channel/radio environments. In these approaches, they often allocate a dedicated PHY channel to control messages [13], [14]. Stations switch in and off the control channel during transmissions, leading to significant switching overhead. In addition, these approaches consume an entire channel for control purpose only, which is too expensive.

The in-band approaches deliver the control traffic in the same channel as the data traffic. It will also consume the communication resources. In the current 802.11 legacy protocol design [6], [15], the coordination is scheduled along the temporal space, which introduces great overhead such as the DIFS, SIFS and random back-offs. Some recent work also reveal the need for optimal CSMA by experimental results [11]. In [7], they propose a minimum controlled coordination by reducing the DCF overhead. However, in our hJam, we remove such coordination overhead. Also different from CDMA [16] using PN code in code space, our hJam exploits the opportunity in frequency domain.

In some recent works, researchers begin to think of improving the channel utilization by PHY designs. In FICA [1], a fine grained channel access system is proposed. It has improved the channel utilization by increasing the data transmission time in each subchannel and but still needs DIFS, SIFS and random back-offs between transmissions. In hJam, we propose a different approach which focus on eliminating the coordination overhead. Side Channel [8] transmits the control messages in the code space but works for DSSS [21] modulation only. For the high data rate modulations such as OFDM, it is not applicable. To enable coordination information delivery in more general environments, we design hJam on the modern OFDM modulation schemes.

VIII. Conclusion

Coordination is a well-known problem in wireless networks that causes significant performance degradation. We find that fundamentally it is because of the interleaved control messages and data traffic account for too much of the transmission air time. Rather than separating or interleaving them, we propose a new communication model that transmit them together and develop hJam to realize it on top of OFDM-networks. Intended jamming signals and interference cancellation techniques are used with the explored preamble redundancy in OFDM modulations. As such, in hJam the application data can obtain the full air time. Theoretical analysis confirms the general applicability of hJam in practical environments. We implement hJam on GNU Radio testbed. The performance evaluations as well as the simulations show that hJam outperforms IEEE 802.11 protocols by up to 72% under different traffic patterns.

IX. Acknowledgement

This research was supported in part by Pearl River New Star Technology Training Project, Hong Kong RGC Grants 617710, 617811, 623209 and 622410 and China NSFC Grants 60933011, 60933012, 61170247, 61073180 and Huawei-HKUST joint lab, and National High Technology Research and Development (863) Program of China under Grant No.2011AA010500, National Science and Technology Supporting Program 2012BAH07B00 and NSFC-Guangdong Joint Fund of China under grant (No.U0735001, U0835004 and U0935004).

References

[1] K. Tan, J. Fang, Y. Zhang, S. Chen, L. Shi, J. Zhang, and Y. Zhang, “Fine Grained Channel Access in Wireless LAN” in *ACM SIGCOMM*, 2010.

[2] S. Katti, S. Gollakota, and D. Katabi, “Embracing Wireless Interference: Analog Network Coding”, in *ACM SIGCOMM*, 2007

[3] K. Ramachandran, E. Belding-Royer, K. Almeroth, M. Buddhikot: “Interference-Aware Channel Assignment in Multi-Radio Wireless Mesh Networks”, in *IEEE INFOCOM*, 2006.

[4] Blossom, “Gnu software defined radio”,
http: //www.gnu.org/software/gnuradio.

[5] M. Ettus,“The Universal Software Radio Peripheral or USRP, 2008.”

[6] IEEE standard for local and metropolitan area networks part 11; amendment 5: Enhancements for higher throughput. IEEE Std 802.11n-2009.

[7] Z. Zeng, Y. Gao, K. Tan, and P. Kumar, “CHAIN: Introducing Minimum Controlled Coordination into Random Access MAC”, in *IEEE INFOCOM*, 2011.

[8] K. Wu, H. Tan, Y. Liu, J. Zhang, Q. Zhang and L. Ni, “Side Channel: Bits over Interference”, in *ACM MobiCom*, 2010.

[9] G. Nychis, T. Hottelier, Z. Yang, S. Seshan, P. Steenkiste. “Enabling MAC Protocol Implementations on Software-Defined Radios”, in *Proc. of NSDI*, 2009.

[10] R. Chandra, R. Mahajan, T. Moscibroda, R. Raghavendra, and P. Bahl. “A case for adapting channel width in wireless networks”, SIGCOMM Comput. Commun. Rev., 2008.

[11] B. Nardelli, J. Lee, K. Lee, Y. Yi, S. Chong, E. Knightly, and M. Chiang, “Experimental Evaluation of Optimal CSMA”, in *IEEE INFOCOM*, 2011

[12] Y. Bejerano, H. Choi, S. Han, T. Nandagopal, “Performance tuning of Infrastructure-Mode wireless LANs”, in *WiOpt*, 2010.

[13] G. Zhou, C. Huang, T. Yan, T. He, J. Stankovic and T. Abdelzaher. “MMSN: Multi-Frequency Media Access Control for Wireless Sensor Networks”, in *IEEE INFOCOM*, 2006.

[14] J. Zhao, H. Zheng, and G. Yang, Distributed coordination in dynamic spectrum allocation networks”, in *IEEE DySpan*, 2005.

[15] Y. Cheng, H. Li, P. Wan, X. Wang Capacity region of a wireless mesh backhaul network over the CSMA/CA MAC”, in *IEEE INFOCOM*, 2010.

[16] J. G. Proakis, Digital Communications, 4th ed. New York: McGraw-Hill, Inc., 2001.

[17] M. Marey and H. Steendam, “Analysis of the narrowband interference effect on OFDM timing synchronization”, IEEE Trans. Signal Processing, 2007.

[18] M. Souryal, L. Klein-Berndt, L. Miller, and N. Moayeri, “Link assessment in an indoor 802.11 network”, in *IEEE WCNC*, 2006.

[19] M. Ozdemir and H. Arslan, “Channel Estimation for Wireless OFDM Systems”, Communications Surveys & Tutorials, IEEE, 2007.

[20] S. Sen, N. Santhapuri, R. Choudhury, and S. Nelakuditi, “Successive interference cancellation: a back-of-the-envelope perspective”, in *ACM HOTNETS*, 2010.

[21] K. Wu, H. Tan, Y. Liu, L. Ni, “Chip Error Pattern Analysis in IEEE 802.15.4”, in IEEE Transactions on Mobile Computing, 2012.