Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

Capacity Estimation for Error Correction Code-based Embedding in Adaptive Rate Wireless Communication Systems

Peter M. B. Harley
Naval Postgraduate School
pmharley1@nps.edu

Murali Tummala
Naval Postgraduate School
mtummala@nps.edu

John C. McEachen
Naval Postgraduate School
mceachen@nps.edu

Abstract

In this paper, we explore the performance of error correction code-based embedding in adaptive rate wireless communication systems. We first develop a model to illustrate the relationship between the selected modulation and coding scheme index, the current channel state, and the embedding capacity. Extensive simulations facilitate the development of expressions to describe the estimated embedding capacity for the proposed scheme when implemented within the single carrier physical layer of the IEEE 802.11ad, directional multi-Gigabit standard. We further identify and characterize various types of distortion and describe additional constraints that may serve to reduce the available embedding margin and overall embedding capacity.

1. Introduction

Error correction coding is an essential component of modern communication protocols. These techniques provide error detection and correction capabilities which minimize the retransmission of data, facilitating increased throughput and reduced latency. The same redundancy that enables forward error correction (FEC) can be exploited to embed hidden information and develop covert communication channels [1]. An extension of this embedding methodology, previously explored in [2], proposed a novel high-throughput covert channel that leveraged the structure of adaptive-rate wireless communications systems; specifically, the covert channel was implemented within the framework of the IEEE 802.11ad directional multi-gigabit (DMG) standard.

Like many modern wireless communication systems, IEEE 802.11ad utilizes a modulation and coding scheme (MCS) to maximize throughput under varying channel conditions. The MCS construct allows stations to coordinate changes in data rate through the use of a predetermined MCS index, which consists of a modulation type and coding rate. The embedding technique in [2] leveraged the ability of adaptive rate systems to change MCS indices in order to achieve a significant increase in embedding capacity.

Although this embedding scheme was initially envisioned as a method to develop covert channels, there are numerous examples of similar techniques supporting legitimate applications. Information-hiding techniques have been successfully utilized to support watermarking of digital media for digital rights management (DRM) [3], network flow analysis to identify the source of denial-of-service attacks [4], and even to implement security and authentication features within legacy protocols [5]. All of these use cases, along with the traditional information hiding applications, seek to exploit the unused, or underutilized, capacity within a given system, to pass embedded data from a source to a destination [6]. By limiting the amount of degradation caused by the embedding process, these schemes can reduce the detectability of the embedded channel and minimize adverse impacts on the underlying communication system.

This work will seek to build upon the previous results in [2] and develop an estimate to describe the capacity of error correction code-based embedding under varying channel conditions. This capacity will be subject to a variety of constraints and limitations to include the selected modulation type, the coding rate, and the embedding location. It is also necessary to assess the potential impacts of changes in embedding rate and location on the performance of the underlying wireless communication system.

2. Forward Error Correction-based Embedding

In FEC-based information-hiding techniques, the embedded information is comparable to an additional noise source. These schemes are dependent on the availability of excess error correction capacity to support the embedding of hidden data [1]. Unlike

URI: https://hdl.handle.net/10125/64516
978-0-9981331-3-3

traditional stenographic schemes, in which the cover object is irreparably degraded by the insertion of the hidden payload [7], FEC-based embedding can avoid permanent corruption of the legitimate data. If the level of embedding in the underlying communications channel is carefully managed, these techniques will maximize the throughput of the embedded channel while ensuring that the original payload can be recovered without error. To maximize the embedding capacity, we require some information about the quality and state of the communication channel in order to determine how much excess error correction capacity is available.

The novel embedding scheme proposed in [2] recognized that in MCS-based adaptive-rate communication systems, the effective redundancy of the FEC scheme could be increased by intentionally selecting a lower MCS index. Additionally, by observing the MCS index that had been selected by the communication system before embedding, it is possible to gain information about the quality of the channel without needing to measure the channel state explicitly. While this methodology significantly increased the amount of information that could be embedded, it resulted in the underlying system operating with a loss of throughput. Results from this proof-of-concept also indicated that it should be possible to utilize the same embedding mechanism without decrementing the MCS so long as the channel state facilitated a signal-to-noise ratio (SNR) that exceeded the minimum requirements for the current MCS index.

2.1. Error Correction Code-Based Embedding in IEEE 802.11ad

The IEEE 802.11ad physical layer (PHY) and media access control (MAC) amendment for millimeter wave (mmWave) wireless local area networks (WLANs) was formally adopted as the DMG specification in 2012. While IEEE 802.11ad operates in one of six 2.16-GHz channels in the 60 GHz range, DMG is a term for any WLAN operating in channels with a starting frequency above 45 GHz [8]. The combination of high frequency and high channel bandwidth allows DMG to achieve data rates in excess of 8 Gbps. Although DMG was originally specified with both single carrier (SC) and orthogonal frequency-division multiplexing (OFDM) modes, the OFDM PHY is considered obsolete [9].

Initially intended as a cable replacement solution for video applications and computer peripherals, the extremely high data rates and physical characteristics of the mmWave PHY, have led to the development of additional use cases for DMG to include wireless virtual reality hardware [10] and a variety of mobile communication and sensing applications [11]. Development of a follow-on mmWave WLAN implementation continues through the IEEE P802.11 Task Group ay; enhanced DMG (EDMG), will remain backward compatible with DMG, but will utilize channel bonding and aggregation to achieve even higher data rates. Potential EDMG applications include IEEE 802.3 Ethernet replacement or high-capacity backhauls for data centers and telecommunications [12].

The MAC layer of DMG also considers the unique characteristics of mmWave. The high signal attenuation and extensive use of beamforming in DMG makes it difficult to implement the carrier sense multiple access with collision avoidance (CSMA/CA) that is traditionally utilized by the distributed coordination function (DCF) [13]. Instead, DMG uses a combination of scheduled access, similar to time division multiple access (TDMA), along with some elements of CSMA/CA [14]. The scheduled access to the communication medium for each DMG station (STA) is known as a scheduled service period (SP); this SP is granted during the data transfer interval (DTI) of the DMG beacon interval (BI) [8].

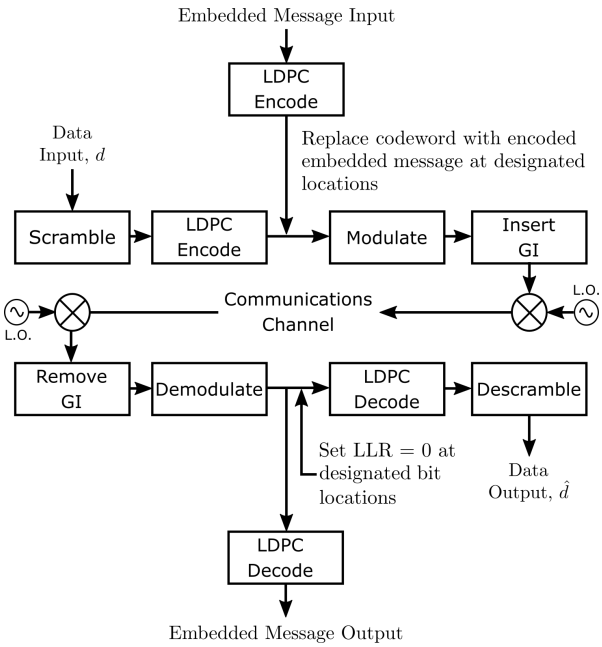

Figure 1. Major components of the embedding process within 802.11ad SC PHY. Adapted from [9].

The major components of the embedding process for DMG from [2] are shown in Figure 1. Embedding is conducted within low-density parity check (LDPC) codewords at the transmitter and the embedded message bits are placed at designated locations within each

codeword before modulation. The embedding locations can be considered a pre-shared key between the transmitted and receiver. The proposed embedding scheme includes the option to utilize an error correction code on the embedded message input; this step would be necessary to ensure reliable delivery of data as the embedded bits are not protected by the normal FEC mechanisms of the underlying channel.

At the receiver, the embedded message bits are recovered from the pre-coordinated locations; in a process similar to that used during the decoding of punctured codewords, the embedded bit locations, which contain log-likelihood ratio (LLR) values, are then set to 0 before being passed to the LDPC decoder. The replacement of the original LLR values is necessary to enable the high embedding rates supported by this scheme.

2.2. Adaptive-Rate Embedding Model

If we consider a general MCS-based communication system, each modulation and coding rate pair supports a different data rate. A description of the available channel throughput is characterized by the relationship between the current channel condition and the number of errors observed at the receiver. An essential component of MCS-based systems is the ability to estimate the current channel conditions and select an appropriate MCS index. While specific rate-adaptation implementations vary, in most cases the selection of an MCS acts like a floor-function; the channel state may exceed the minimum SNR required to support a given MCS index, but the system must select that lower rate to maintain the desired error performance. This error threshold is often defined as a packet error ratio (PER) for a given PHY service data unit (PSDU) length. For 802.11ad, this performance threshold is considered to be a 1% PER for a 4096-octet PSDU [8].

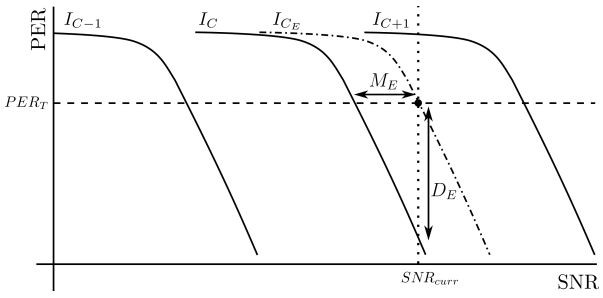

Figure 2. Rate adaptive embedding model, packet error ratio versus SNR

A simplified model was developed to better understand the relationship between the selected MCS, the current channel state, and the available capacity that could be utilized to support FEC-based embedding. In Figure 2 the curves labeled I_{C-1}, I_C, and I_{C+1} represent the PER performance of three MCS indices across a range of SNR values. The MCS index, I_C, is selected based on the current channel state and associated signal-to-noise ratio, SNR_{curr}. In our scenario, the available SNR exceeds the minimum requirements of the communication system, and therefore, some of the error correction capability provided by the selected code rate is redundant; this excess capacity could then be utilized to support the embedding of information within the FEC codewords.

The embedding capacity of each codeword could be increased so long as the PER performance of the communication system remained at or below the specified protocol threshold; this threshold is designated as PER_T and represents the maximum acceptable PER for a given length PSDU. At maximum embedding capacity, the performance of the communication system would be represented by the dashed curve I_{C_E}. This curve would intersect the specified performance threshold, PER_T at SNR_{curr}. The difference between the SNR value at this intersection and the SNR required to maintain PER_T with an unembedded MCS is defined as the embedding margin, M_E.

Additionally, this model also provides some insight into a measure of distortion that occurs as a result of the embedded channel implementation. This distortion, labeled as D_E, represents the difference between the expected PER for a given MCS at the current channel state and packet size, and the PER observed when the channel is embedded.

3. Capacity and Distortion Estimation

Results presented in [2] explored the maximum covert channel capacity of the proposed embedding scheme based on selecting a sub-optimal MCS index; during these simulations there appeared to be a relatively predictable increase in the SNR requirement based on the increase in embedding rate but insufficient trials were conducted to fully characterize the relationship. Based on these observations, and the embedding model presented in Section 2.2, additional MATLAB simulations were utilized to conduct embedding trials against each of the DMG SC MCS indices. The goal of these simulations was to gather sufficient data to summarize the error performance of the underlying communication system over the full range of embedding rates; this data would then be used to develop a function to describe the maximum level of embedding that could be conducted at a given channel state.

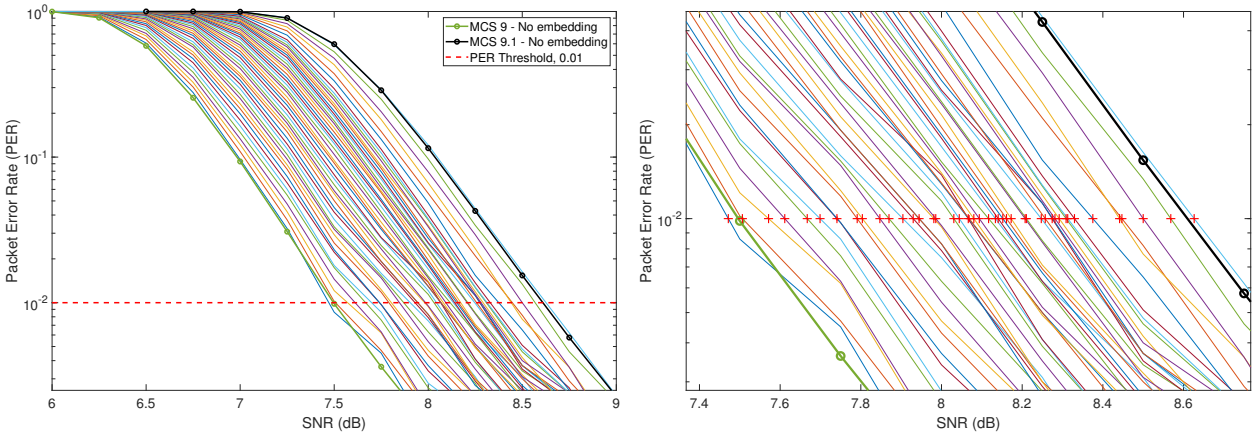

Figure 3. Variable rate embedding trials, DMG PHY simulation under AWGN channel: (a) results for MCS 9, 10000 packets per SNR, 1 to 48 embedded bits per LDPC codeword and (b) estimated SNR requirement to achieve 1% PER for each embedding rate.

As the focus of these trials was to determine the performance of the underlying system, we did not evaluate the bit error rate (BER) performance of the embedded data. The embedding trials in [2] established that the application of FEC techniques to the embedded data was able to deliver acceptable error performance at even the highest embedding rates. While the use of an FEC technique, and the requirement to transmit parity bits, will reduce the number of information bits embedded in each codeword, this reduction can be easily calculated based on the selected FEC code rate.

Expanded embedding trials were conducted for all SC MCS except for MCS 1 and MCS 5. MCS 1 was excluded because it is the only SC MCS that utilizes a repetition factor ($\rho = 2$); MCS 5 was excluded because it is outperformed by MCS 6 under the same channel conditions. Since MCS 6 offers a higher data rate and superior error performance, not only is MCS 5 unlikely to be selected by a link adaptation algorithm, but the MCS would also be a poor candidate for FEC-based embedding.

3.1. Capacity Estimation from Simulation

Simulations to establish the performance of the embedding scheme were conducted in MATLAB and involved modifications to encoder and decoder functions within the WLAN Toolbox. Starting with a script that was developed to determine PER for the SC DMG PHY in an additive white Gaussian noise (AWGN) environment, we evaluated the performance of the underlying communications channel by transmitting a 4096-octet PSDU in AWGN under varying levels of embedding. The embedding ranged from one bit-per-codeword up to the maximum threshold of embedding for each SC MCS; the trials were repeated for 10000 packets at each SNR point to determine the performance of the system as measured in PER. The results of embedding trials conducted at MCS 9, with embedding rates up to the theoretic maximum of 48 bits-per-codeword are shown in Figure 3(a); the embedding was conducted in the first n parity bits of each LDPC codeword. The embedding results are plotted against unembedded trials for MCS 9 and MCS 9.1. Also visible on this plot is a dashed horizontal line that represents the PER threshold established by [8] for a 4096-octet PSDU.

Once the embedding trials were complete, the minimum SNR required to maintain the required 1% PER threshold was calculated using a semi-logarithmic interpolation technique. This technique was selected as the PER curves in the region of interest appeared to be approximately linear when plotted against a logarithmic y-axis scale. After the semi-logarithmic interpolation was complete, the resulting points for each embedding rate were recorded and plotted with cross-shaped markers on the embedding results as shown in Figure 3(b). These markers represent an estimate of the SNR required to embed a specific number of bits-per-codeword.

As shown in Figure 4 this estimate is used to illustrate the relationship between embedding rate and the required SNR for all quadrature phase-shift keying (QPSK)-modulated DMG SC MCS indices. The solid vertical lines in this plot represent the minimum SNR required to maintain 1% PER for each unembedded MCS. The results in Figure 4 confirm the

initial observations in [2] that the embedding capacity predictably increased with SNR; these findings were further confirmed when analyzing the results of the remaining SC MCS indices.

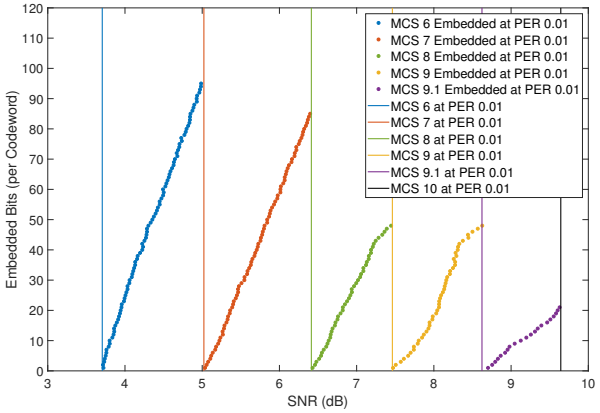

Figure 4. Embedded bits-per-codeword versus SNR for all 802.11ad $\pi/2$-QPSK modulated MCS indices; embedding conducted in first n parity bits of each LDPC codeword.

In an effort to characterize the embedding capacity for each MCS, a linear regression was run against each set of embedding trials with the results being presented in the standard slope-intercept form

$$y = mx + b \tag{1}$$

where y represents the number of embedded bits per codeword, m is the coefficient that describes the slope of the regression, x represents the channel conditions as described by the SNR, and a constant b provides the y-axis intercept and completes the mathematical description of the line. The resulting lines of regression are plotted for the QPSK-modulated DMG SC MCS indices in Figure 5. The most significant element of the linear regression is the slope, which represents the number of bits per LDPC codeword that can be embedded for every decibel (dB) increase in SNR; from this point we will reference this slope as the estimated embedding coefficient, or $\hat{r}_E$.

Once calculated, the estimated embedding coefficient can be utilized to develop a function for the estimated embedding capacity of each codeword, $\hat{C}_{CW}$, measured in bits where

$$\hat{C}_{CW} = \lfloor \hat{r}_E M_E \rfloor, \tag{2}$$

and the embedding margin, M_E, is a measure of the difference in SNR between the current operating condition and the SNR required to maintain a specified PER for an unembedded packet.

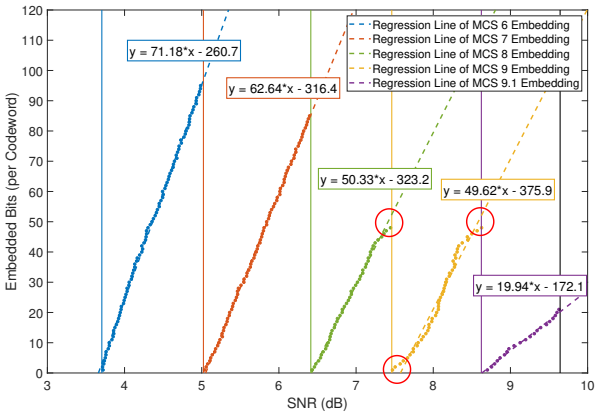

Figure 5. Regression lines for embedded bits-per-codeword versus SNR for all 802.11ad $\pi/2$-QPSK modulated MCS indices

The estimated embedding capacity in each transmitted PSDU, $\hat{C}_{PSDU}$, can then be determined

$$\hat{C}_{PSDU} = N_{CW}\hat{C}_{CW}\,, \tag{3}$$

where N_{CW} represents the number LDPC codewords required for each PSDU. The number of codewords in a PSDU is based on a number of factors including the length of the PSDU (in octets), L_P, and information about the selected MCS to include the length of the LDPC codeword in bits, L_{CW}, the code rate, R_C, and the repetition factor of the code, ρ. If we combine expression for N_{CW} from [8] with (2) and (3) we obtain

$$\hat{C}_{PSDU} = \lfloor \hat{r}_E M_E \rfloor \left\lceil \frac{8\rho L_P}{L_{CW} R_C} \right\rceil\,, \tag{4}$$

which provides the estimated PSDU embedding capacity as a function of the embedding margin, M_E. While this embedding capacity represents the raw number of bits that can be embedded in a given PSDU, it does not factor in the overhead that would be required to support error protection for the embedded information bits.

When the regression lines obtained for each MCS were plotted against the simulated results, the fit was generally very good. That said, as shown in Figure 5, there were a number of points, highlighted by red circles, where these regression lines deviate from the simulated results. For the SC QPSK MCS, the differences were particularly noticeable as the regression line approached the maximum embedding rate for MCS 8 and at both the maximum and minimum embedding rates for MCS 9. In these cases, alternative bounds were identified to adjust the lines describing MCS 8 and 9 to ensure the capacity estimate was

Table 1. Estimated embedding coefficient, $\hat{r}_E$, for 802.11ad (first n parity bits)

Modulation	MCS	Rate 1/2	MCS	Rate 5/8	MCS	Rate 3/4	MCS	Rate 13/16	MCS	Rate 7/8
$\pi/2$-BPSK	2	78.62	3	66.14	4	46.86	5	N/A	—	—
$\pi/2$-QPSK	6	71.18	7	62.64	8	46.47	9	41.27	9.1	19.94
$\pi/2$-16QAM	10	57.40	11	54.88	12	43.52	12.1	39.02	12.3	19.36
$\pi/2$-64QAM	—	—	12.3	44.02	12.4	37.08	12.5	36.72	12.6	20.52

achievable at the given SNR and within the required PER. The modified slope was then used to determine an updated $\hat{r}_E$; similar discrepancies in the remaining SC MCS were also identified and corrected. The estimated embedding coefficient for all SC MCS are recorded in Table 1.

As shown in Table 1, the value of $\hat{r}_E$ generally decreases as both the code rate increases or the order of modulation increases. This result aligns with our intuition related to FEC-based embedding; $\hat{r}_E$ is a measure of the estimated embedding capacity per codeword for every additional dB of SNR. Therefore as the modulation becomes more complex, or the redundancy of the FEC is reduced, we would expect to see a decrease in the ability to embed data without increasing the PER. The most significant reduction in embedding performance is observed for the MCS that utilize the $R = 7/8$ codes; this extremely poor performance is due to the fact that the $R = 7/8$ code is a punctured version of the $R = 13/16$ LDPC code where the first 48 parity bits have already been removed before any data is embedded.

3.2. Embedding Location

The LDPC codes utilized in DMG are systematic. For the trials conducted in the previous section, embedded bits were inserted into the first n parity bits of the LDPC codewords. This embedding location was originally selected as it mirrored the puncturing location specified in [8] to generate the $R = 7/8$ code needed to support MCS 9.1, 12.3 and 12.6.

Since the mechanism utilized to embed data in FEC codewords closely resembles puncturing, and LDPC puncturing locations can have a significant impact on the performance of the code [15, 16], we conducted embedding trials at various locations within the codeword. A critical factor in the performance of these embedding locations appears to be related to the column weight, w_c, of the parity check matrix, $\boldsymbol{H}$. The impact of changes in w_c on the performance of various embedding locations is likely related to the iterative decoding process for LDPC with LLR inputs. The punctured (or embedded) bit locations where LLR $= 0$ rely upon contributions from the other received symbols to recover the original value; w_c indicates the number of message bits participating in the decode process at each check node [17]. To increase the amount of information which contributes to the recovery of the data lost during the embedding process, locations should be selected that maximize w_c.

The performance of embedding locations, selected within both the data and the parity bits, were compared to determine the impact on embedding capacity. Although we did not conduct an exhaustive search, we determined that embedding in the last n data bits of each codeword generally returned a performance gain over our initial embedding location.

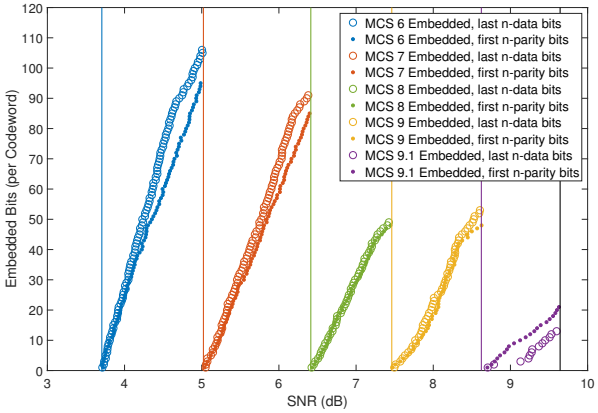

Figure 6. Comparison of embedding capacity for all 802.11ad $\pi/2$-QPSK modulated MCS indices; embedding conducted in first n parity bits versus last n data bits of each LDPC codeword.

Once this alternative location was identified, embedding trials were conducted using the same parameters as described in Section 3.1. The results of embedding in the last n data bits for the QPSK MCS indices is shown in Figure 6; it is clear that this embedding location resulted in a steeper slope for all MCS with the exception of MCS 9.1. This steeper slope corresponds to a larger $\hat{r}_E$ and a higher embedding capacity.

Embedding trials were repeated for all SC MCS with the exception of MCS 1 and MCS 5. The results

Table 2. Estimated embedding coefficient, $\hat{r}_E$, for 802.11ad (last n data bits)

Modulation	MCS	Rate 1/2	MCS	Rate 5/8	MCS	Rate 3/4	MCS	Rate 13/16	MCS	Rate 7/8
$\pi/2$-BPSK	2	86.45	3	71.70	4	48.20	5	N/A	—	—
$\pi/2$-QPSK	6	81.66	7	67.01	8	48.42	9	46.41	9.1	13.33
$\pi/2$-16QAM	10	62.65	11	58.71	12	40.98	12.1	43.70	12.3	13.39
$\pi/2$-64QAM	—	—	12.3	47.15	12.4	37.31	12.5	38.28	12.6	14.94

from these trials were utilized to calculate $\hat{r}_E$ and are summarized in Table 2. When compared to the values for $\hat{r}_E$ obtained from the original embedding location, embedding in the last n data bits resulted in an increased embedding capacity for all MCS indices with the exception of MCS 12, and the MCS that utilize the punctured $R = 7/8$ LDPC code.

3.3. Embedding Distortion

In addition to embedding capacity, another important consideration is the impact these techniques have on the underlying communications channel. Similar to the concept of distortion in traditional steganography, which is a measure of the amount of modification that has been performed on the cover object [7], we will examine the impact of our embedding process in terms of observable changes to the performance of the wireless communication system.

Our proposed embedding occurs at the physical layer, and all traces of our embedded data should be removed from the legitimate information bits before they are passed from the PHY. With this in mind, we have identified three potential impacts that would still be observable even if the embedded data is successfully removed at the receiver.

The first impact, designated as Type 1, is the least significant and occurs when embedding is conducted without decrementing the MCS index. In this case, the measured PER is higher than expected for a given SNR; this distortion, previously identified in Figure 2 was labeled as D_E. The second type of distortion, Type 2, is an direct result of the intentional MCS degradation. In this case, the underlying communication system will be operating at a lower throughput than would be expected for the current channel conditions. The final distortion, Type 3, occurs if the embedding impacts the system to such an extent that the PER consistently exceeds the established protocol thresholds. While each vendor implementation of link adaptation methodology is unique, if the PER exceeds the prescribed threshold the communication system will experience excessive re-transmissions and lower overall throughput. It is worth noting that the ability to recognize the presence of Type 1 or Type 2 distortion requires access to accurate channel state information or the ability to estimate the current SNR of the received signal.

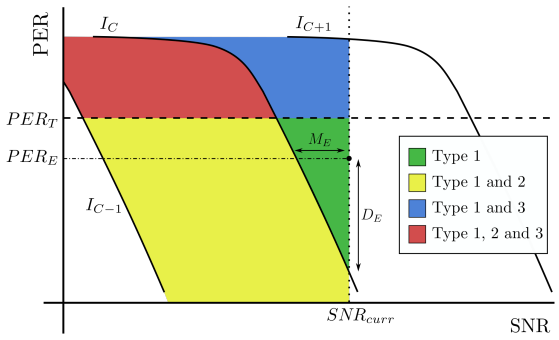

Figure 7. Distortion regions for embedding in adaptive rate communication system

3.4. Distortion Regions

Examining the embedding model outlined in Section 2, it is possible to delineate regions that correspond to each type of distortion. These regions, identified in Figure 7, provide insight into both the amount and types of impact that can be expected on the underlying communication system. If the embedding is being utilized for the purposes of developing a covert channel, the level of distortion can also be an indicator of how vulnerable this channel would be to detection.

The most advantageous region, highlighted in green, is the triangular region where only Type 1 distortion is present. This region offers a lower embedding margin, M_E, than the case where a sub-optimal MCS is selected, but minimizes the impact on the underlying channel. In this particular case the embedding point, identified as the intersection of SNR_{curr} and the embedding PER threshold, PER_E, was selected to reduce the magnitude of distortion, D_E, at the expense of both M_E and the embedding capacity.

If a higher embedded throughput is required, and the MCS is decremented, the channel will move into the yellow region that contains not only Type 1 distortion

but also results in a lower throughput of the underlying channel (Type 2). The final cases, identified as the blue and red regions, occur when the overall PER exceeds the established protocol thresholds. Both of these regions represent the most significant distortion contribution as the underlying system may suffer noticeable disruption and loss of throughput.

4. Capacity Refinements

The final section of this paper examines constraints associated with selecting an embedding rate within the region that only contains Type 1 distortion. Initially, this region is defined by three distinct bounds. The upper horizontal bound, PER_T, represents the protocol threshold for packet error ratio. The vertical bound along the right-side of the region is the current channel state, SNR_{curr}. Finally the diagonal bound on the left-hand edge is the performance of the current MCS index, I_C.

It is important to recognize that our ability to move within this region is entirely dependent upon the selection of an embedding rate. Increasing the embedding rate will cause the performance curve of the current MCS index to move in the direction of the intersection between PER_T and SNR_{curr}. This curve will remain approximately parallel to I_C and will be used to describe the expected PER of the underlying system, quantify the type and magnitude of distortion which results from the embedding, and define M_E which is used to find the embedded channel capacity.

4.1. Constraints

An enlarged version of the embedding region subject to Type 1 distortion is shown in Figure 8. This triangular region, described by the vertices D, E, and F, is subject to three constraints that serve to reduce the size of the embedding region.

The first constraint is based on the inherent limitations of channel estimation and the impact of this uncertainty on our embedding limits. The IEEE 802.11ad DMG PHY utilizes a preamble composed of a Short Training Field (STF) and a Channel Estimation Field (CEF); these fields employ Golay sequences to perform synchronization, automatic gain control and channel estimation in the time and frequency domain [9]. While the use of Golay sequences provide robust channel estimation, it has been observed that the reliability of SNR estimates can be impacted by factors related to the specific environment and equipment calibration [18, 19]. As a result, when evaluating the embedding region we propose establishing an offset, ϵ, from the estimated SNR_{curr}; lowering the

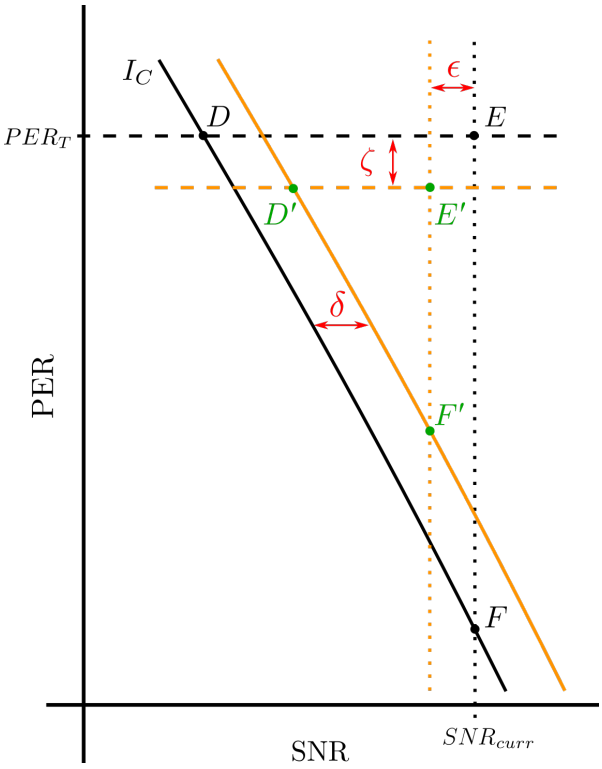

Figure 8. Visualization of practical embedding region subject to additional constraints

SNR value will reduce both M_E and the maximum embedding capacity, but will also reduce the chance of unintentionally introducing uncorrectable errors. Revisiting (2), the embedding capacity per codeword due to this offset, $\hat{C}_{CW_\epsilon}$, can be represented as

$$\hat{C}_{CW_\epsilon} = \lfloor \hat{r}_E \left(M_E - \epsilon \right) \rfloor \ . \tag{5}$$

The second constraint is a user-defined factor of safety that imposes a more restrictive error threshold than that specified by the protocol standard, PER_T. Lowering the upper acceptable PER limit by ζ reduces the embedding capacity of the channel but also reduces the likelihood that embedding will cause the underlying system to exceed the established PER. The PER performance of the underlying channel in the vicinity of PER_T is approximately linear on a semi-logarithmic plot; as long as $PER_{T-\zeta}$ remains within this log-linear region, $\hat{r}_E$ will remain relatively consistent. Assuming a fixed value for $\hat{r}_E$, we can update (5) to reflect the reduced margin of embedding, M_{E_ζ}, at the new PER threshold, $PER_{T-\zeta}$,

$$\hat{C}_{CW,max} = \left\lfloor \hat{r}_E \left(M_{E_\zeta} - \epsilon \right) \right\rfloor \ , \tag{6}$$

where $\hat{C}_{CW,max}$ is the new maximum embedding

capacity, measured in bits-per-codeword, based on the constraints ϵ and ζ.

The final constraint on the embedding region is governed by the minimum required throughput for the embedded channel. Using the length of the DMG beacon interval in seconds, T_{BI}, the required throughput of the embedded channel in bits-per-second, U_E, and the number of PSDU transmitted during each beacon interval, N_{PSDU}, we can develop an expression for $C_{PSDU,min}$, the minimum number of embedded bits required in each PSDU

$$C_{PSDU,min} = \left\lceil \frac{U_E T_{BI}}{N_{PSDU}} \right\rceil . \tag{7}$$

This minimum embedding capacity then needs to be translated into a minimum embedding margin, $M_{E,min}$, to define the offset, δ, shown in Figure 8. Using insight from (2) and (3), we can specify the minimum required embedding capacity per codeword, $C_{CW,min}$, while also establishing the relationship with, $M_{E,min}$, and $\hat{r}_E$

$$C_{CW,min} = \left\lceil \frac{C_{PSDU,min}}{N_{CW}} \right\rceil = \lfloor \hat{r}_E M_{E,min} \rfloor . \tag{8}$$

Since $C_{CW,min}$ is an integer value, and $\hat{r}_E > 0$, we find the bounds of the embedding margin

$$\frac{C_{CW,min}}{\hat{r}_E} \leq M_{E,min} < \frac{C_{CW,min}+1}{\hat{r}_E} , \tag{9}$$

and then define the required offset, δ, to ensure sufficient capacity to support U_E

$$\delta = \frac{C_{CW,min}+1}{\hat{r}_E} . \tag{10}$$

Combining elements from (7), (8), and (10) yields an expression for δ based on U_E

$$\delta = \frac{1}{\hat{r}_E} \left\lceil \frac{U_E T_{BI}}{N_{PSDU} N_{CW}} \right\rceil + \frac{1}{\hat{r}_E} , \tag{11}$$

which can be further expanded with the expression for N_{CW} from [8]

$$\delta = \frac{1}{\hat{r}_E} \left\lceil \frac{U_E T_{BI}}{N_{PSDU} \left\lceil \frac{8\rho L_P}{L_{CW} R_C} \right\rceil} \right\rceil + \frac{1}{\hat{r}_E} . \tag{12}$$

4.2. Region Bounds

The vertical boundary between vertices E' and F' on the edge of the reduced region in Figure 8, represents an estimate of the current channel state after adjusting for the required offset and the location that will maximize the embedding margin, M_E, for a given PER. The horizontal edge of the region, connecting D' and E', identifies the maximum permissible PER based on both the protocol standard and any specified factor of safety. Finally, the diagonal segment connecting D' and F' is the expected performance of the underlying communications system while supporting the minimum embedded channel requirements.

The vertices of this reduced region that intersect the adjusted SNR limit represent locations of either minimum distortion or maximum embedding capacity. Specifically, F' represents the lowest Type 1 distortion while supporting the lowest allowable embedding capacity. Conversely, E' represents the maximum possible M_E and the highest embedding capacity, but achieves this capacity at the highest level of distortion.

5. Conclusion

In this paper, we extended our investigation into the performance of error correction code-based embedding within an adaptive rate wireless communication system. Through extensive simulation we successfully characterized the performance of FEC-based embedding in the IEEE 802.11ad SC PHY under a range of embedding rates, channel conditions, and embedding locations. We developed the concept of an embedding coefficient which provides an estimate for embedding capacity when combined with information about the current channel state. In many cases, the monotonic relationship between the embedding margin and the embedding capacity was linear; therefore, the constant-valued slope from a line of regression provided a reasonable estimate for this coefficient. We then described three potential sources of distortion and detailed the conditions under which each type of distortion would be present. Finally, we focused on the embedding region that resulted in the least significant distortion and investigated the impact of additional constraints on the overall embedding capacity.

While this paper focused on IEEE 802.11ad, these capacity estimation techniques should be applicable to other adaptive rate communication protocols. Changes to embedding location within the LDPC codeword resulted in significant variations in the embedding capacity for a given PER threshold. Selecting embedding locations through the use of

existing puncturing optimization algorithms and search techniques may yield even higher embedding rates and associated increases in channel capacity.

References

[1] K. S. Subramani, A. Antonopoulos, A. A. Abotabl, A. Nosratinia, and Y. Makris, "INFECT: INconspicuous FEC-based Trojan: A hardware attack on an 802.11a/g wireless network," in *2017 IEEE Int. Symp. Hardware Oriented Security and Trust (HOST)*, pp. 90–94, May 2017.

[2] P. M. B. Harley, M. Tummala, and J. C. McEachen, "High-throughput covert channels in adaptive rate wireless communication systems," in *2019 International Conference on Electronics, Information, and Communication (ICEIC)*, pp. 1–7, Jan. 2019.

[3] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. 3.4, pp. 313–336, 1996.

[4] E. Jones, O. L. Moigne, and J. Robert, "IP traceback solutions based on time to live covert channel," in *Proceedings. 2004 12th IEEE International Conference on Networks (ICON 2004) (IEEE Cat. No.04EX955)*, vol. 2, pp. 451–457 vol.2, 2004.

[5] W. Mazurczyk and Z. Kotulski, "New security and control protocol for VoIP based on steganography and digital watermarking," *Annales UMCS Informatica*, vol. 5, pp. 417–426, 2006.

[6] W. Mazurczyk, S. Wendzel, S. Zander, A. Houmansadr, and K. Szczypiorski, *Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures (IEEE Press Series on Information and Communication Networks Security)*. Wiley-IEEE Press, 2016.

[7] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press, 2009.

[8] "IEEE standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pp. 1–3534, Dec. 2016.

[9] B. Schulz, "White Paper: 802.11ad - WLAN at 60 GHz - Solution," tech. rep., KG, Rohde & Schwarz GmbH & Co, 2017.

[10] P. Bright, "Intel to stop making WiGig cards for laptops but still pushing 60ghz for VR [Updated]," Sept. 2017.

[11] P. Kumari, N. Gonzalez-Prelcic, and R. W. Heath, "Investigating the IEEE 802.11ad standard for millimeter wave automotive radar," in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, pp. 1–5, Sept. 2015.

[12] B. Su, "The next generation wireless LAN standard and overcome the test challenges," tech. rep., Keysight, June 2017.

[13] T. S. Rappaport, R. W. Heath, R. C. Daniels, and J. N. Murdock, *Millimeter Wave Wireless Communications*. Pearson Education (US), 2014.

[14] C. Hemanth and T. G. Venkatesh, "Performance analysis of service periods (SP) of the IEEE 802.11ad hybrid mac protocol," *IEEE Transactions on Mobile Computing*, vol. 15, pp. 1224–1236, May 2016.

[15] J. Ha, J. Kim, and S. W. McLaughlin, "Rate-compatible puncturing of low-density parity-check codes," *IEEE Trans. Inf. Theor.*, vol. 50, pp. 2824–2836, Sept. 2006.

[16] Y. Xu, Y. Wei, and W. Chen, "On the performance evaluation of quasi-cyclic LDPC codes with arbitrary puncturing," in *2010 IEEE 71st Vehicular Technology Conference*, pp. 1–5, May 2010.

[17] S. Lin and D. J. Costello, *Error Control Coding (2nd Edition)*. Pearson, 2004.

[18] M. Vutukuru, H. Balakrishnan, and K. Jamieson, "Cross-layer wireless bit rate adaptation," in *Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication*, SIGCOMM '09, (New York, NY, USA), pp. 3–14, ACM, 2009.

[19] J. Zhang, K. Tan, J. Zhao, H. Wu, and Y. Zhang, "A practical SNR-guided rate adaptation," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, pp. 2083–2091, Apr. 2008.