Exploiting OFDM for Covert Communication

Zaid Hayyeh
Department of Electrical Engineering and Computer Science
University of Kansas, Lawrence, Kansas

Covert Communication

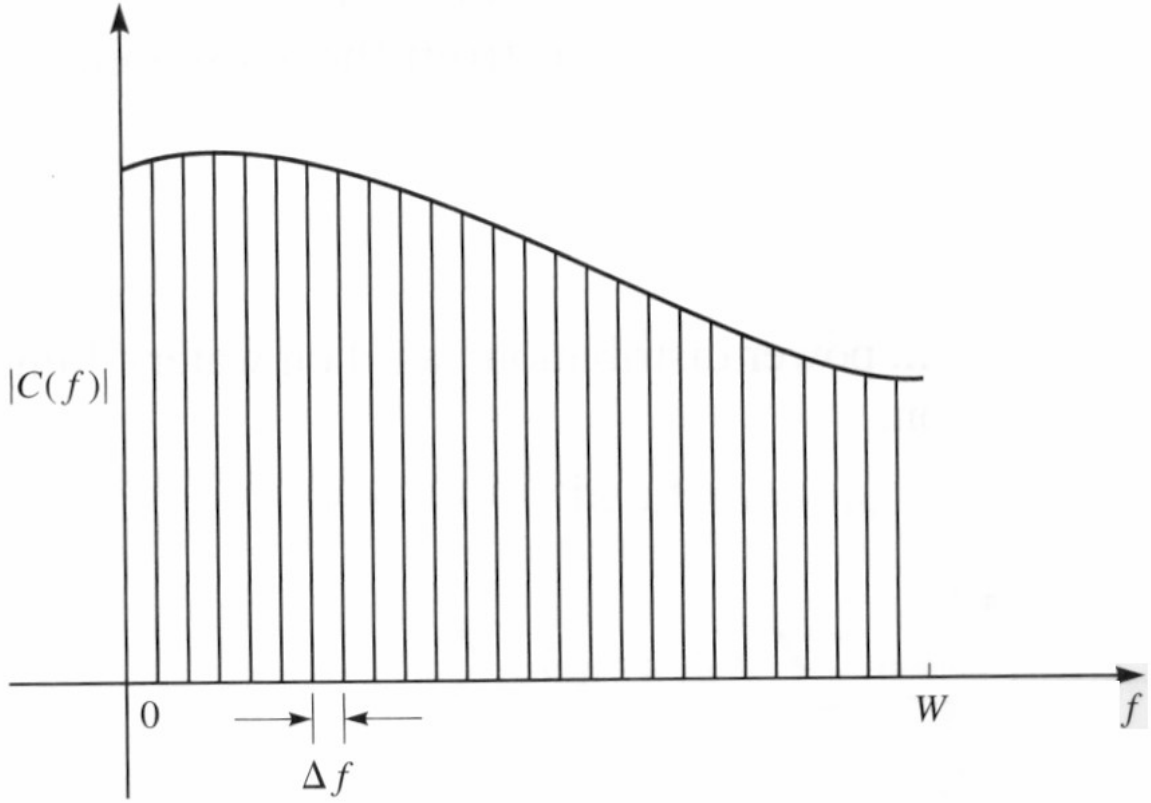
- To hide, with a low probability of detection (LPD), the transmission of information
- A covert signal can be embedded within an existing non-covert communication
- Human scalp to embed a hidden message
- Hidden in the flow of data packets transmitted over the internet

What is OFDM?

- Orthogonal Frequency Division Multiplexing
- Lower rate narrow band as opposed to high rate wide band
- Nearly ideal response across each sub-channel

$$\Delta f = \frac{W}{N}$$

What is OFDM?



What is OFDM?

- Mitigate Intersymbol Interference (ISI)
- ISI caused by multi-path and the non-ideal response of channels
- Sub-carriers are orthogonal, do not interfere with one another

$$\int_0^T \cos(2\pi f_k t + \phi_k)\cos(2\pi f_j t + \phi_j) = 0$$

$$k \neq j$$

Cyclic Prefix Insertion

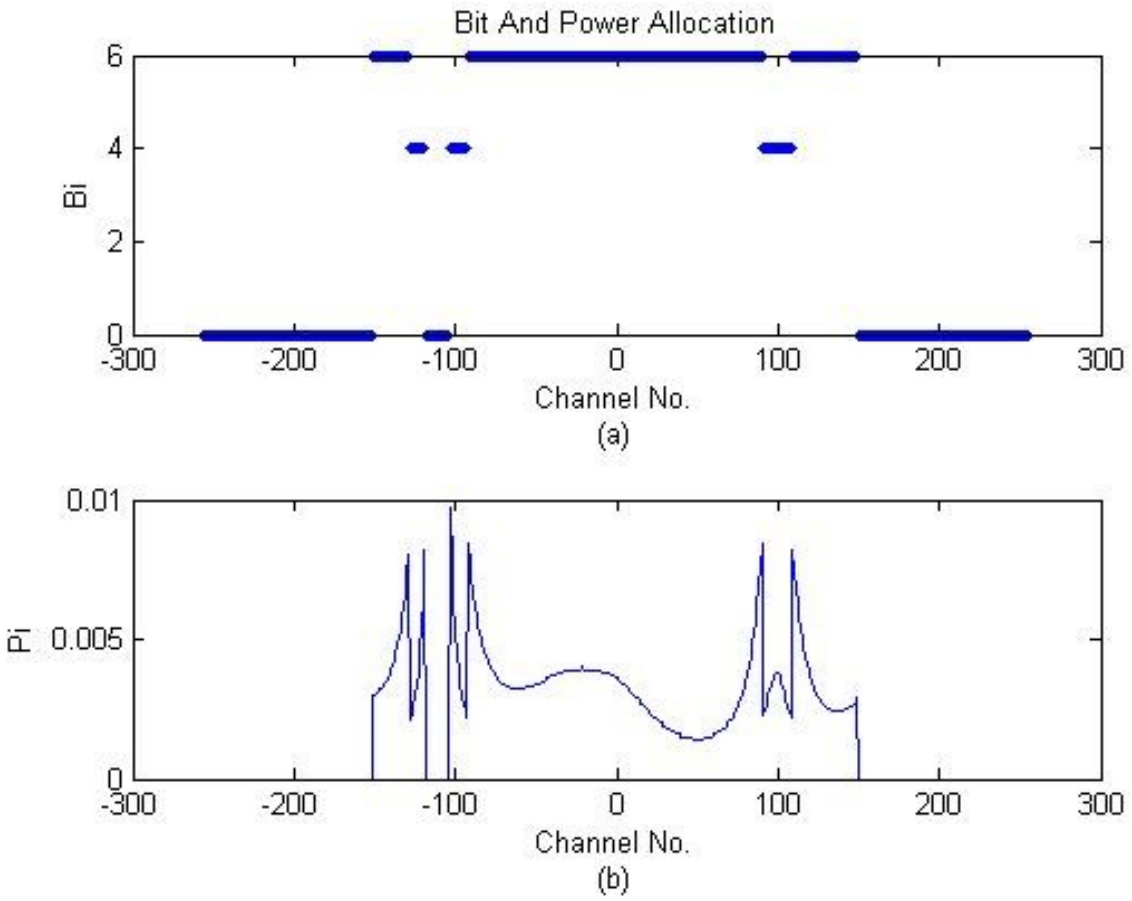
- Cyclic Prefix (CP) or Guard Time (TG)
- Last 6 or 7 samples for extended CP
- Prepended to the front of the OFDM symbol
- Based on channel's time dispersion
- Help to mitigate ISI

Bit & Power Allocation

- QPSK, 16-QAM, 64-QAM
- Divide power equally amongst sub-carriers
- SER below 10^{-4} eliminated
- Adjust bits per channel (B_i)
- Adjust power per channel (P_i)

$$R_b = \frac{1}{T} \sum_{i=1}^{N} B_i \qquad P_{total} = \sum_{i=1}^{N} P_i$$

Bit & Power Allocation



Benefits/Applications of OFDM

- More efficient use of spectrum
- Increase channel capacity
- Mitigate ISI
- LTE (Long Term Evolution)
  - AT&T, Verizon
- WiMAX (802.16)
  - Sprint

Hypothesis

- Utilize an unused sub-channel for covert communication
- Edge channel or middle channel
- Show effects of a covert communication signal embedded within an OFDM based wireless waveform
- Show the performance of the covert communications system in the presence of the non-covert OFDM signal

Simulation Methodology

- All simulations in MATLAB
- 10,000 OFDM symbols, approximately 10 minutes to run
- 100 bit errors per simulation for covert/non-covert system
- System performance will be evaluated in bit-error-rate (BER)
- SNR will be given in E_b/N_o

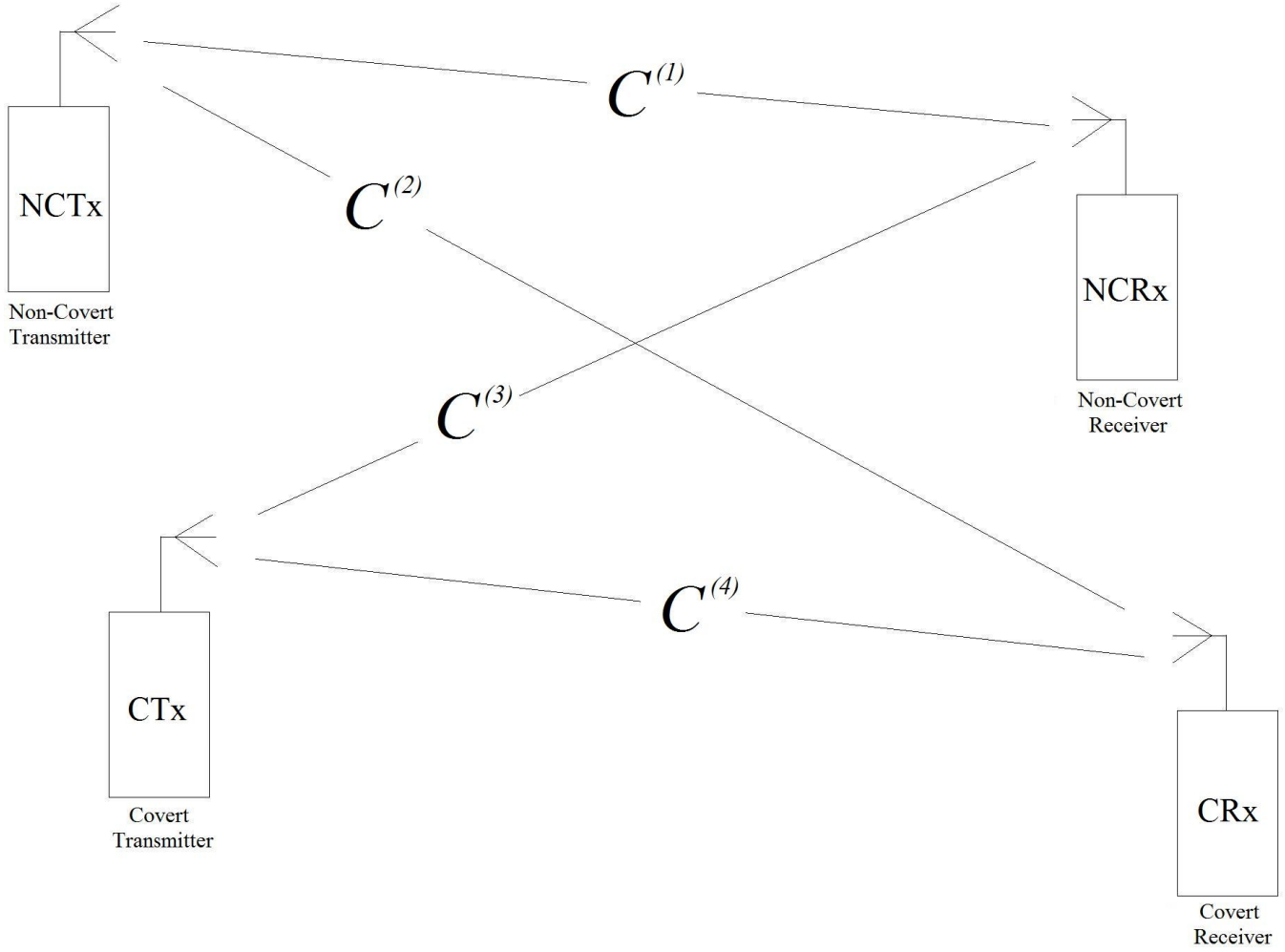
Parameter Values

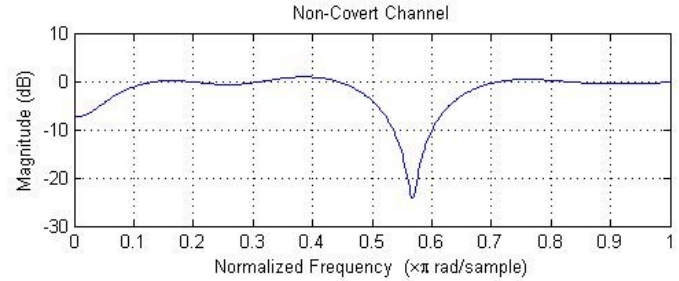
- “Slotted” structure of OFDM
- 5 MHz specification, actual BW = 7.68 MHz
- 512 point IFFT
- 15 KHz sub-channels
- Normal CP
- 301 out of 512 utilized
- 512 samples/symbols
- 518 samples/symbol with CP

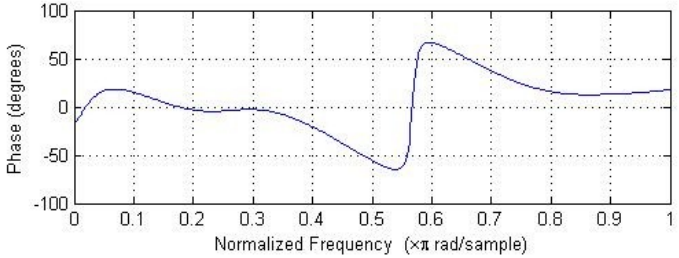
Assumptions

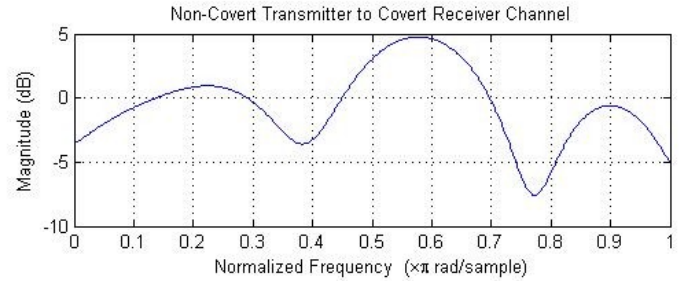
- Known channel state information (CSI)
- Ideal phase/frequency recovery
- Fixed modulation
- Covert system has knowledge of utilized sub-channels
  - Channel spacing
  - Poor performing sub-channels

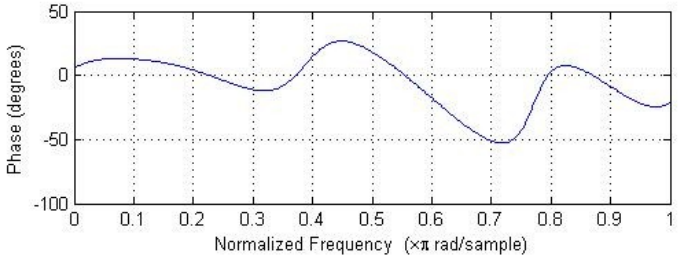
Transmitter/Receiver Pairs & Channels

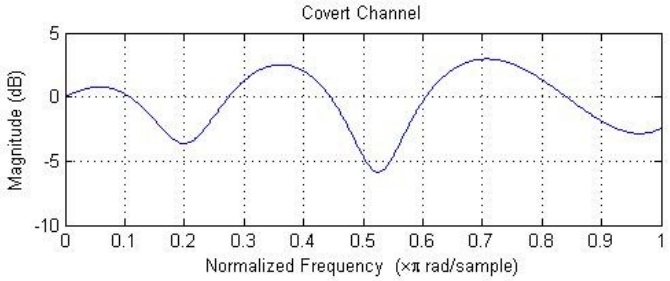


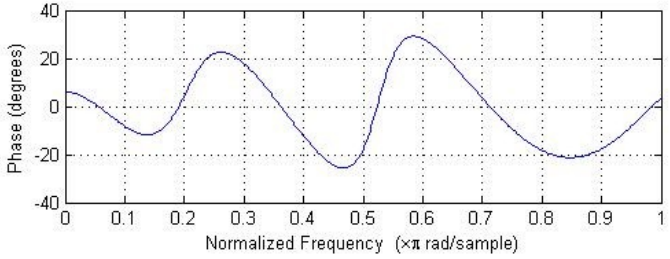

Non-Covert Channel
Magnitude (dB)
Normalized Frequency (×π rad/sample)

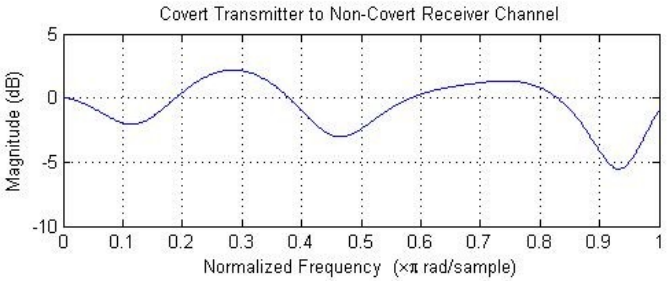

Phase (degrees)
Normalized Frequency (×π rad/sample)

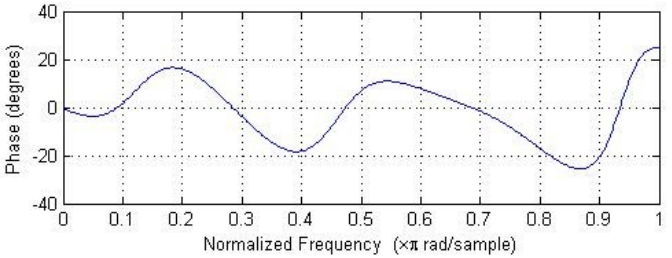

Non-Covert Transmitter to Covert Receiver Channel
Magnitude (dB)
Normalized Frequency (×π rad/sample)


Phase (degrees)
Normalized Frequency (×π rad/sample)


Covert Channel
Magnitude (dB)
Normalized Frequency (×π rad/sample)


Phase (degrees)
Normalized Frequency (×π rad/sample)


Covert Transmitter to Non-Covert Receiver Channel
Magnitude (dB)
Normalized Frequency (×π rad/sample)


Phase (degrees)
Normalized Frequency (×π rad/sample)

Received Signals

$$r(t) = \left(\sum_{k=0}^{N-1} \sqrt{\frac{2}{T}} \left| C_k^{(1)} \right| A_{kc} \cos\left(2\pi f_k t + \phi_k^{(1)}\right) + \sqrt{\frac{2}{T}} \left| C_k^{(1)} \right| A_{ks} \sin\left(2\pi f_k t + \phi_k^{(1)}\right) \right) +$$

$$\left(\sum_{i=0}^{N-1} \sqrt{\frac{2}{T}} \left| C_i^{(3)} \right| B_{ic} \cos\left(2\pi f_i t + \phi_i^{(2)}\right) + \sqrt{\frac{2}{T}} \left| C_i^{(3)} \right| B_{is} \sin\left(2\pi f_i t + \phi_i^{(2)}\right) \right) + n(t)$$

$$A_{vc} \,\&\, A_{vs} = 0 \,;\, B_{ic} \,\&\, B_{is} = 0 \text{ except for } i = v$$

$$r'(t) = \left(\sum_{k=0}^{N-1} \sqrt{\frac{2}{T}} \left| C_k^{(2)} \right| A_{kc} \cos\left(2\pi f_k t + \phi_k^{(3)}\right) + \sqrt{\frac{2}{T}} \left| C_k^{(2)} \right| A_{ks} \sin\left(2\pi f_k t + \phi_k^{(3)}\right) \right) +$$

$$\left(\sum_{i=0}^{N-1} \sqrt{\frac{2}{T}} \left| C_i^{(4)} \right| B_{ic} \cos\left(2\pi f_i t + \phi_i^{(4)}\right) + \sqrt{\frac{2}{T}} \left| C_i^{(4)} \right| B_{is} \sin\left(2\pi f_i t + \phi_i^{(4)}\right) \right) + n(t)$$

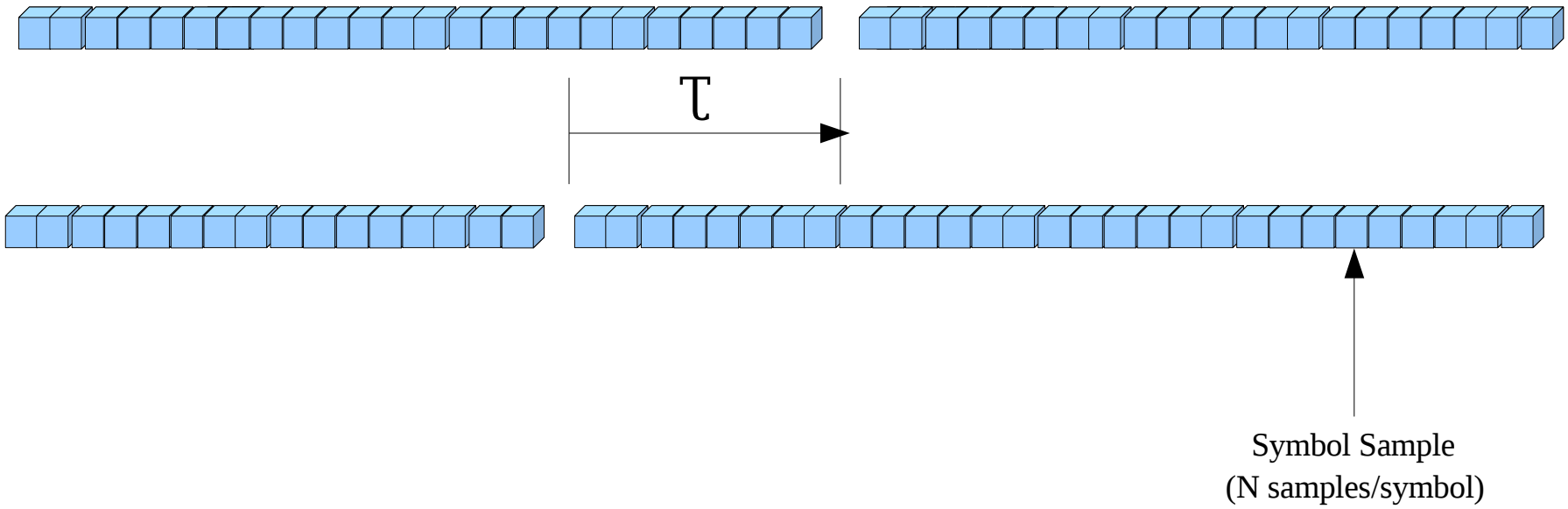
$$A_{vc} \,\&\, A_{vs} = 0 \,;\, B_{ic} \,\&\, B_{is} = 0 \text{ except for } i = v$$

$R_{b,covert}$ = 7.40 kbps, Channel = -152, τ = 128 samples/sym, $E_{b,covert}/E_{b,non\text{-}covert}$ = -10.83 dB

Description of Covert

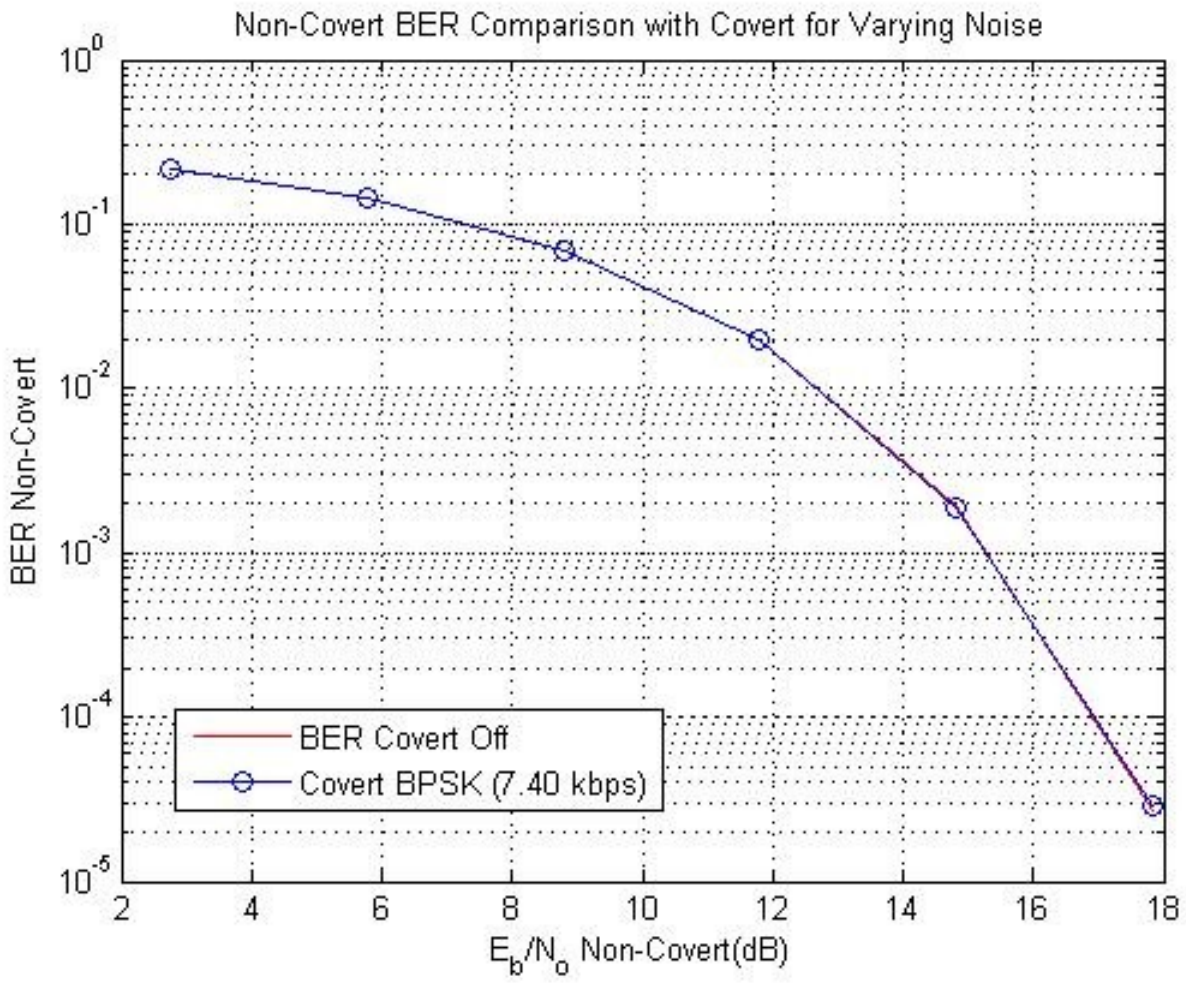
- Symbol/Bit rate for BPSK – R_b
- Synchronous offset – τ
- Location/ Channel number – 256 to +256
- $E_{b,covert}/E_{b,non\text{-}covert}$
- E_b/N_O

Synchronous Offset



Comparison of BER Curve With and Without Covert for Increasing Noise

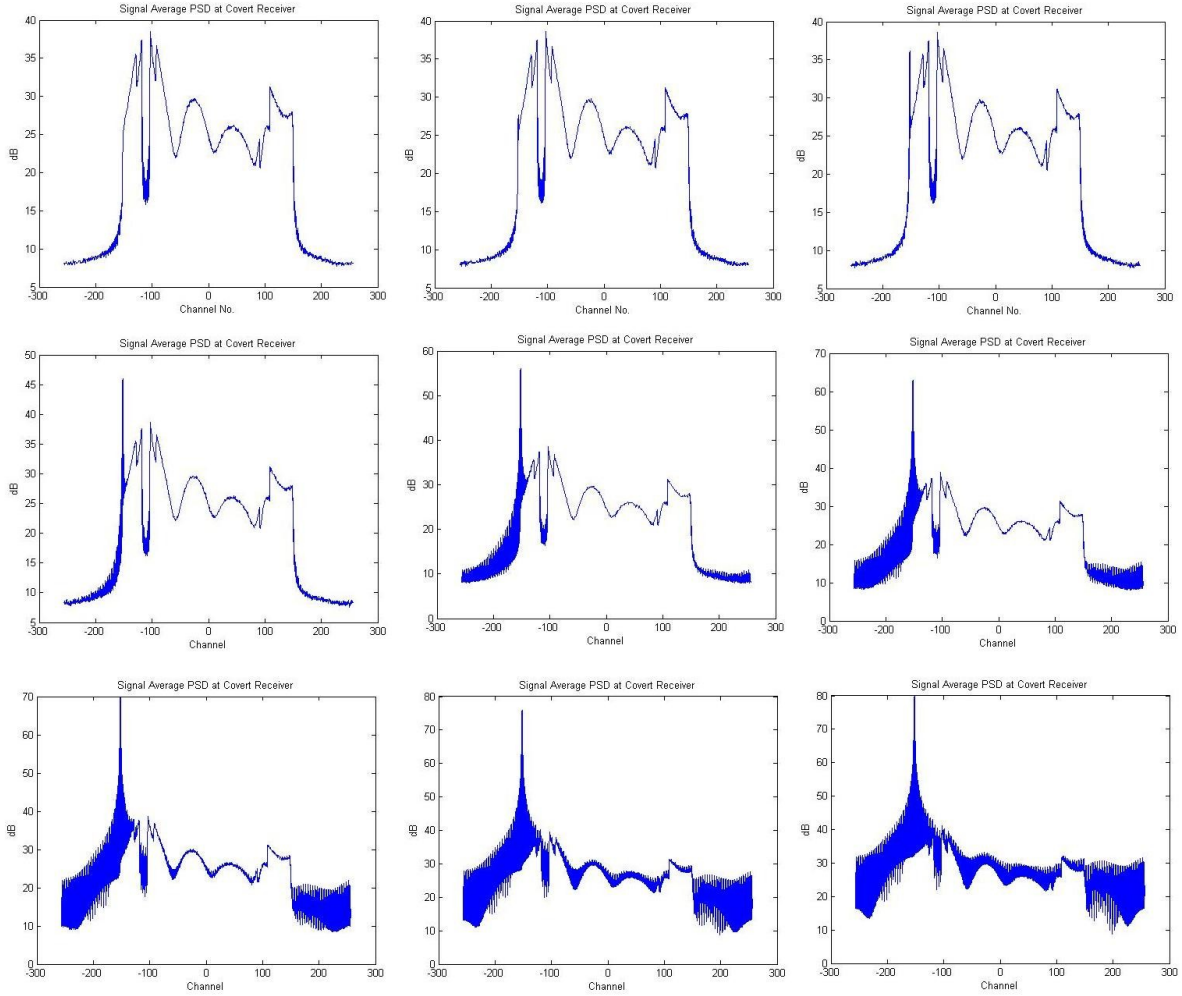
($R_{b,covert}$ = 7.40 kbps, Channel = -152 $E_{b,covert}/E_{b,non\text{-}covert}$ = -10.83 dB, τ = 128 samples/sym)



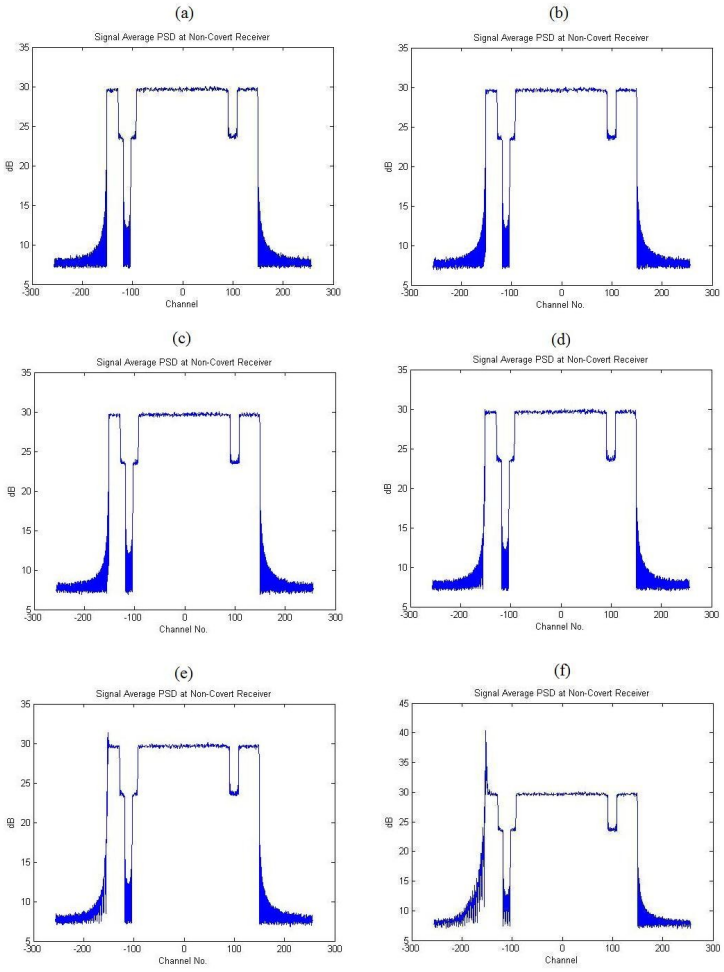
KU INFORMATION & TELECOMMUNICATION TECHNOLOGY CENTER
The University of Kansas

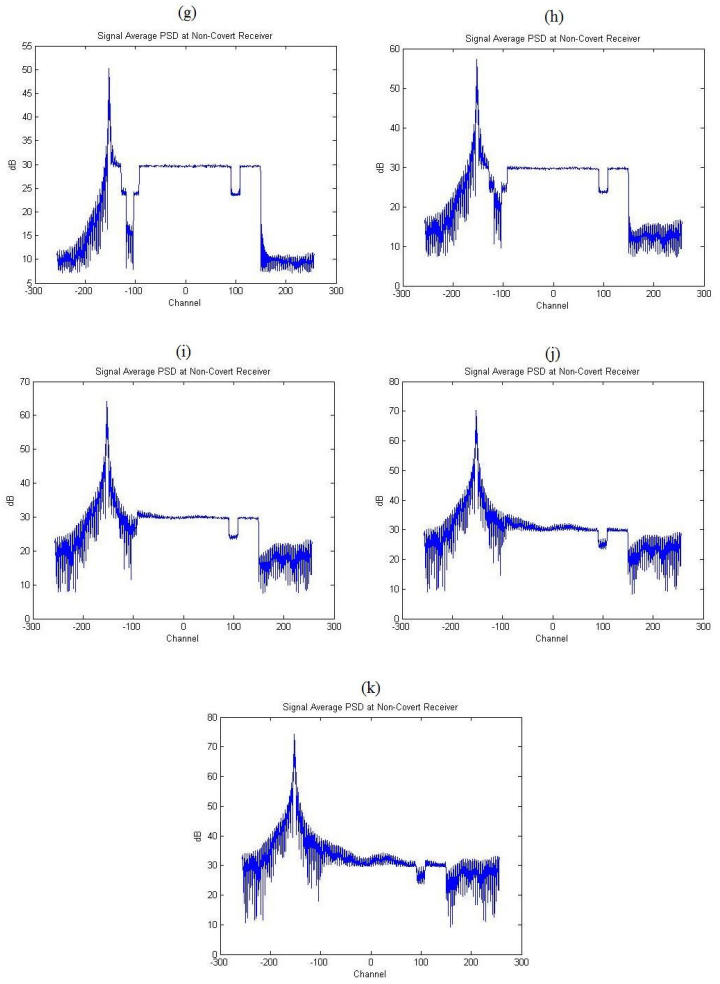
Effect of Increasing Covert Power on Non-Covert OFDM Signal

($R_{b.covert}$ = 7.40 kbps, Channel = -152, ϒ = 128 samples/sym)

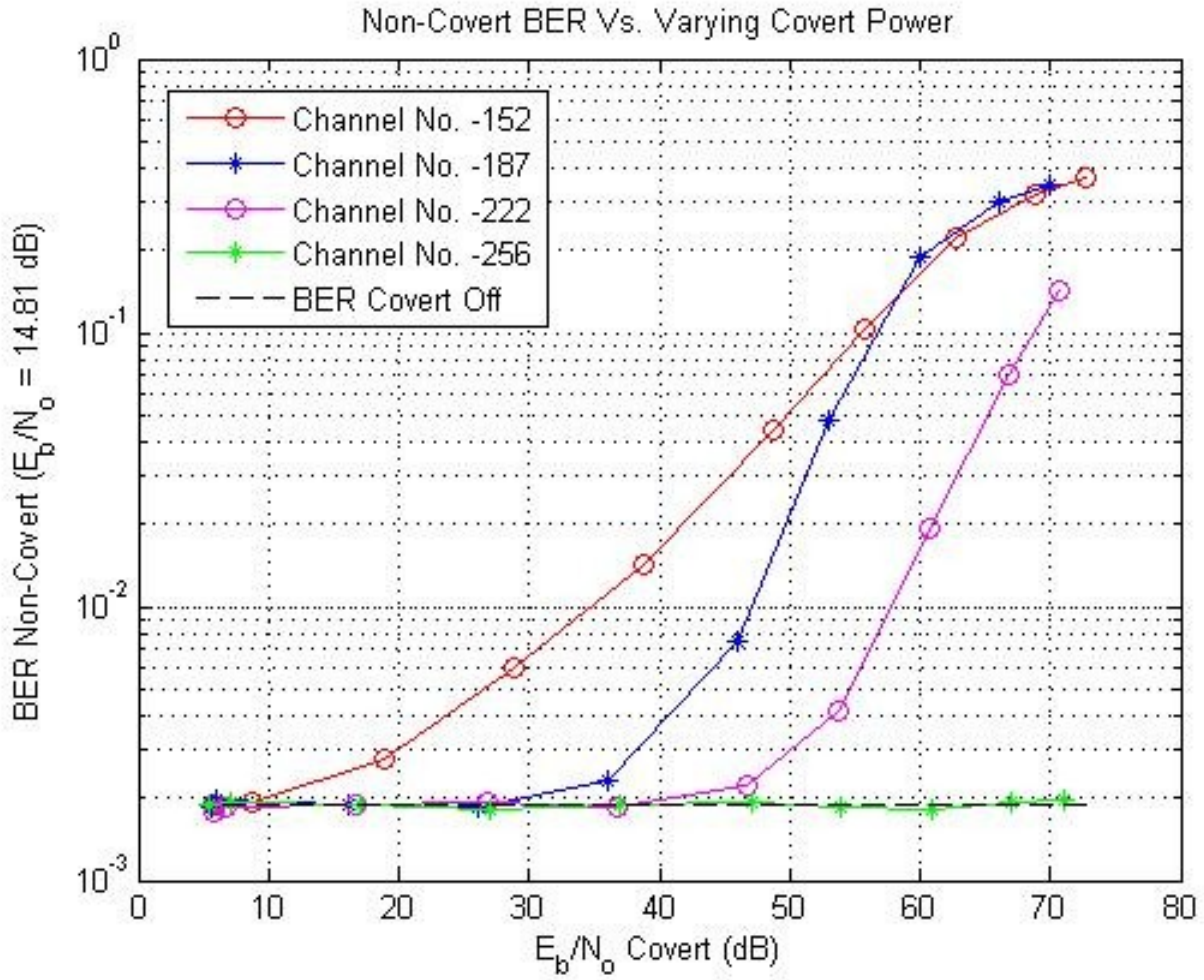


Effect of Increasing Covert Power on Non-Covert OFDM Signal





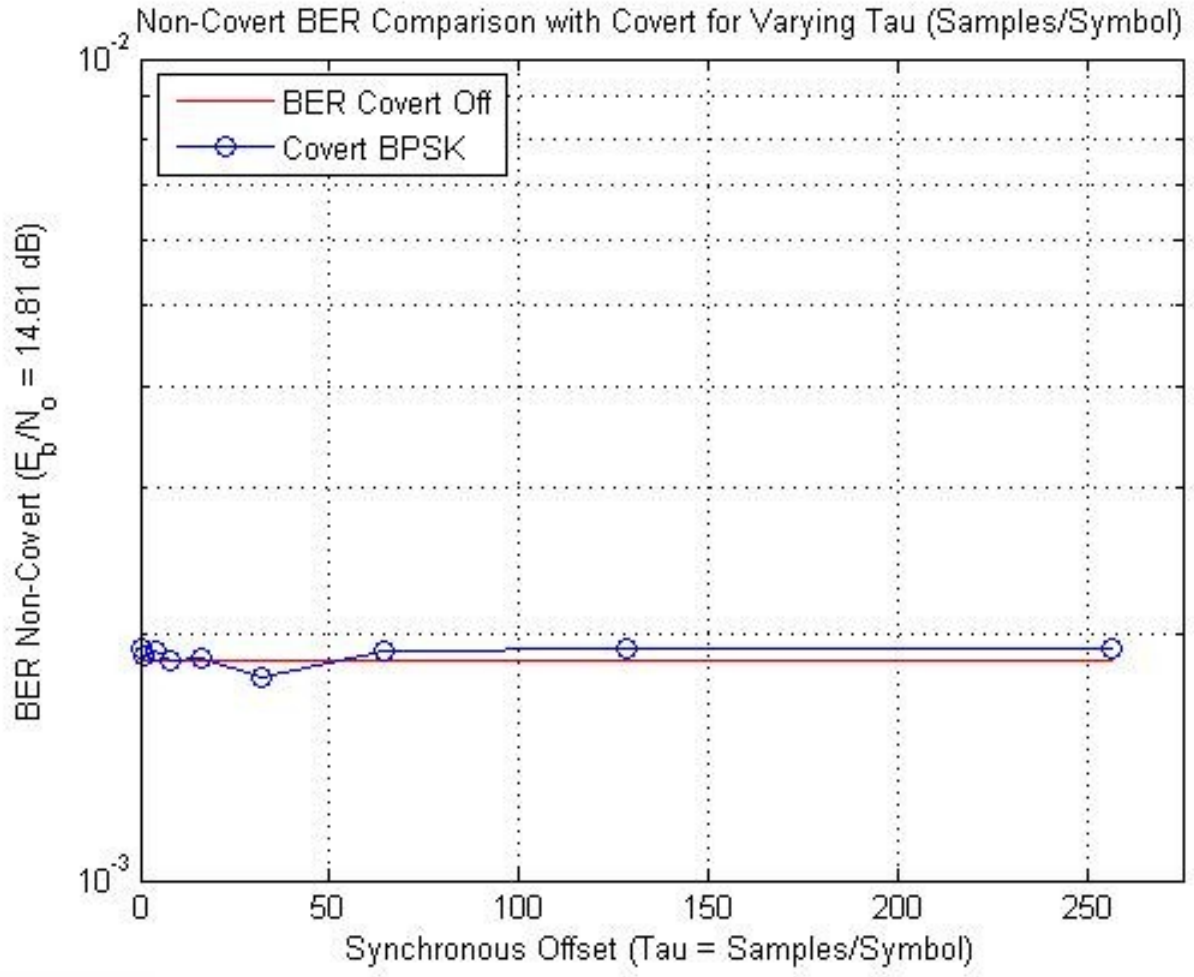
Effect of Increasing Covert Power on Non-Covert OFDM Signal



KU INFORMATION & TELECOMMUNICATION TECHNOLOGY CENTER
The University of Kansas

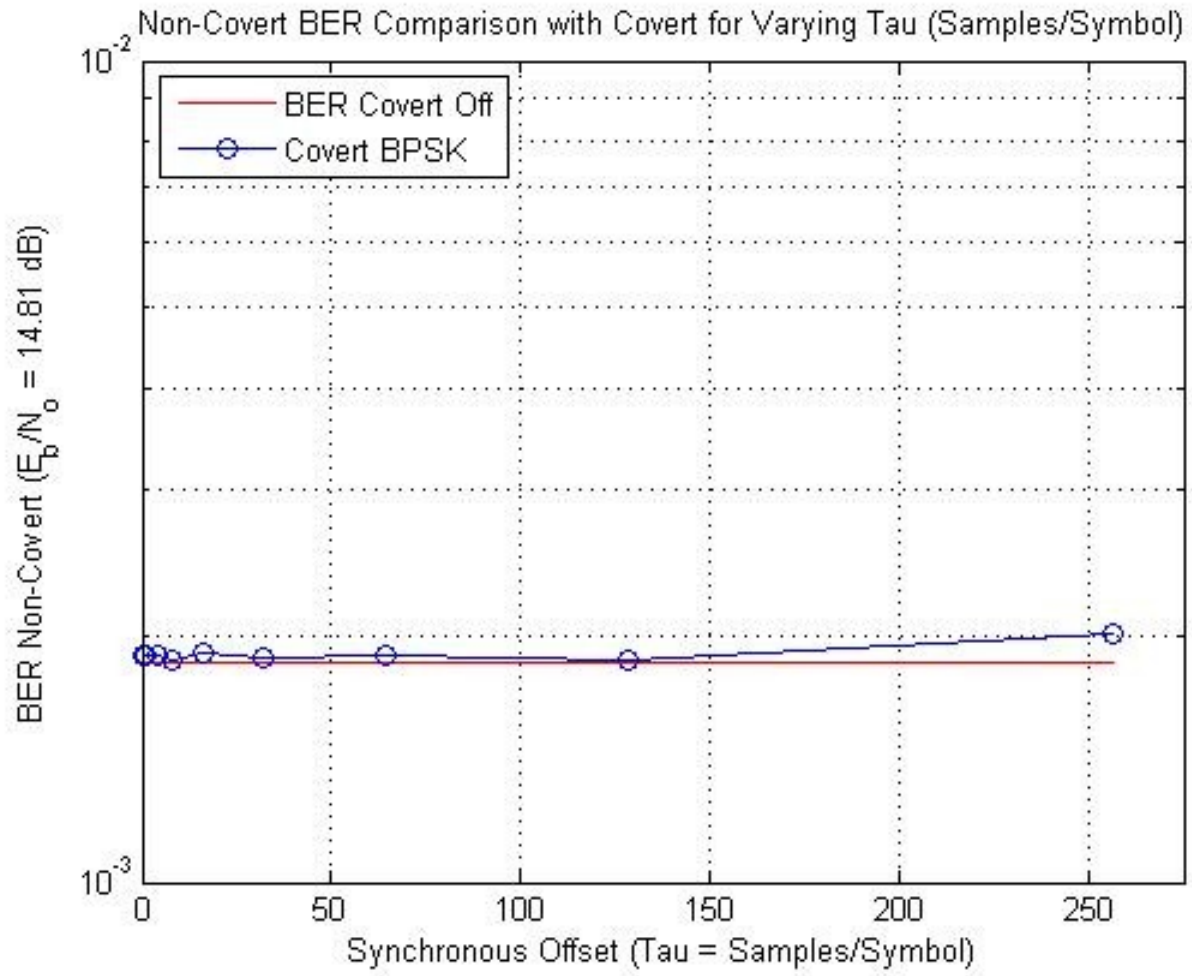
Effect of Synchronous Offset on Non-Covert OFDM Signal

Synchronous Offset (τ) Vs. Non-Covert BER ($R_{b,covert}$ = 7.40 kbps, Channel = -152, $E_{b.covert}/E_{b.non-covert}$ = -10.83 dB)



Effect of Synchronous Offset on Non-Covert OFDM Signal

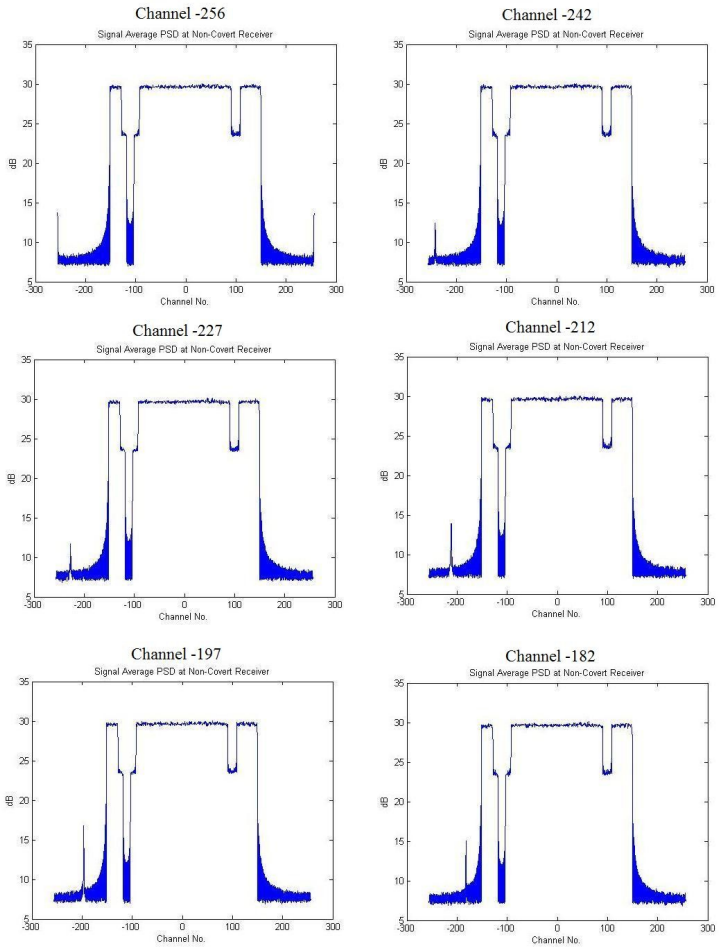
Synchronous Offset (Ƭ) Vs. Non-Covert BER ($R_{b,covert}$ = 7.40 kbps, Channel = -105, $E_{b,covert}/E_{b,non\text{-}covert}$ = -9.15 dB)

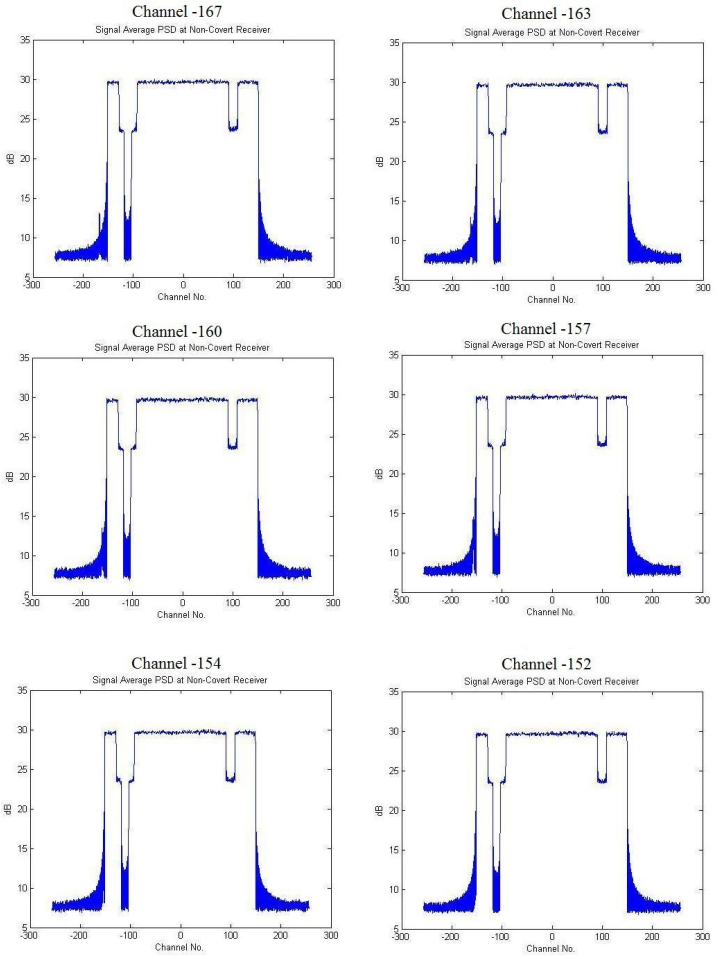


KU INFORMATION & TELECOMMUNICATION TECHNOLOGY CENTER
The University of Kansas

Effect of Spectral Position on Covert Signal

($R_{b,covert}$ = 7.40 kbps, ϒ = 128 samples/sym)

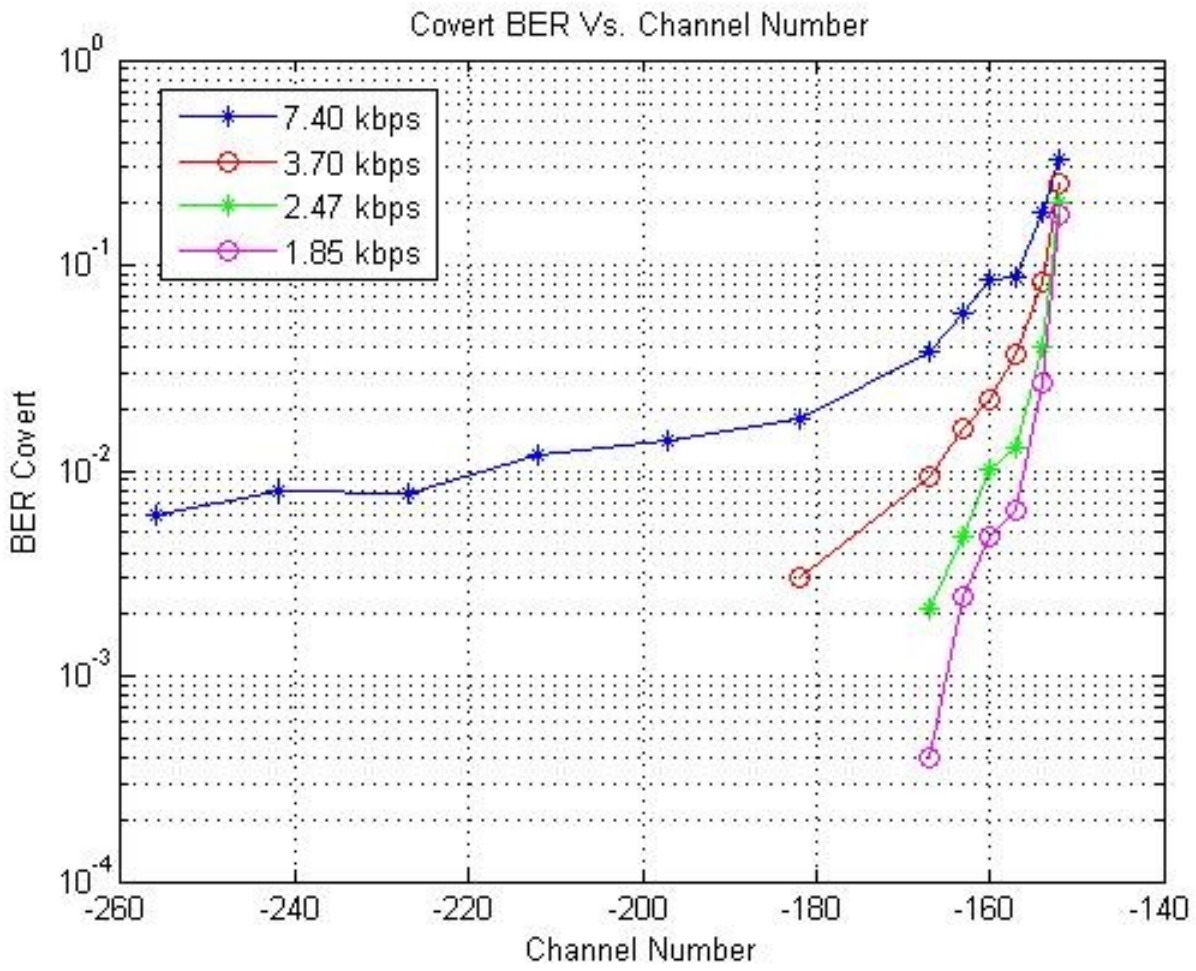




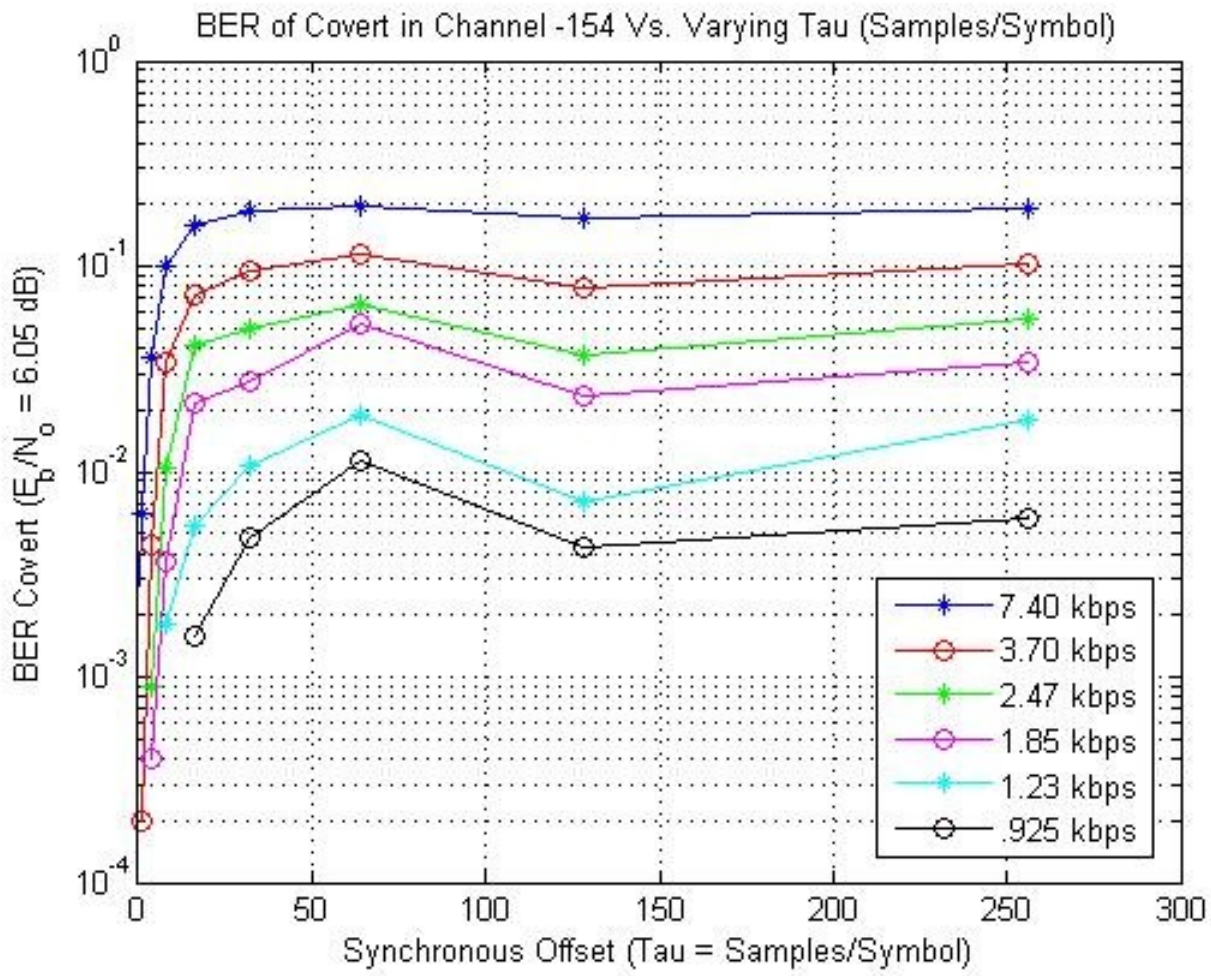
KU INFORMATION & TELECOMMUNICATION TECHNOLOGY CENTER
The University of Kansas

Effect of Spectral Position on Covert Signal

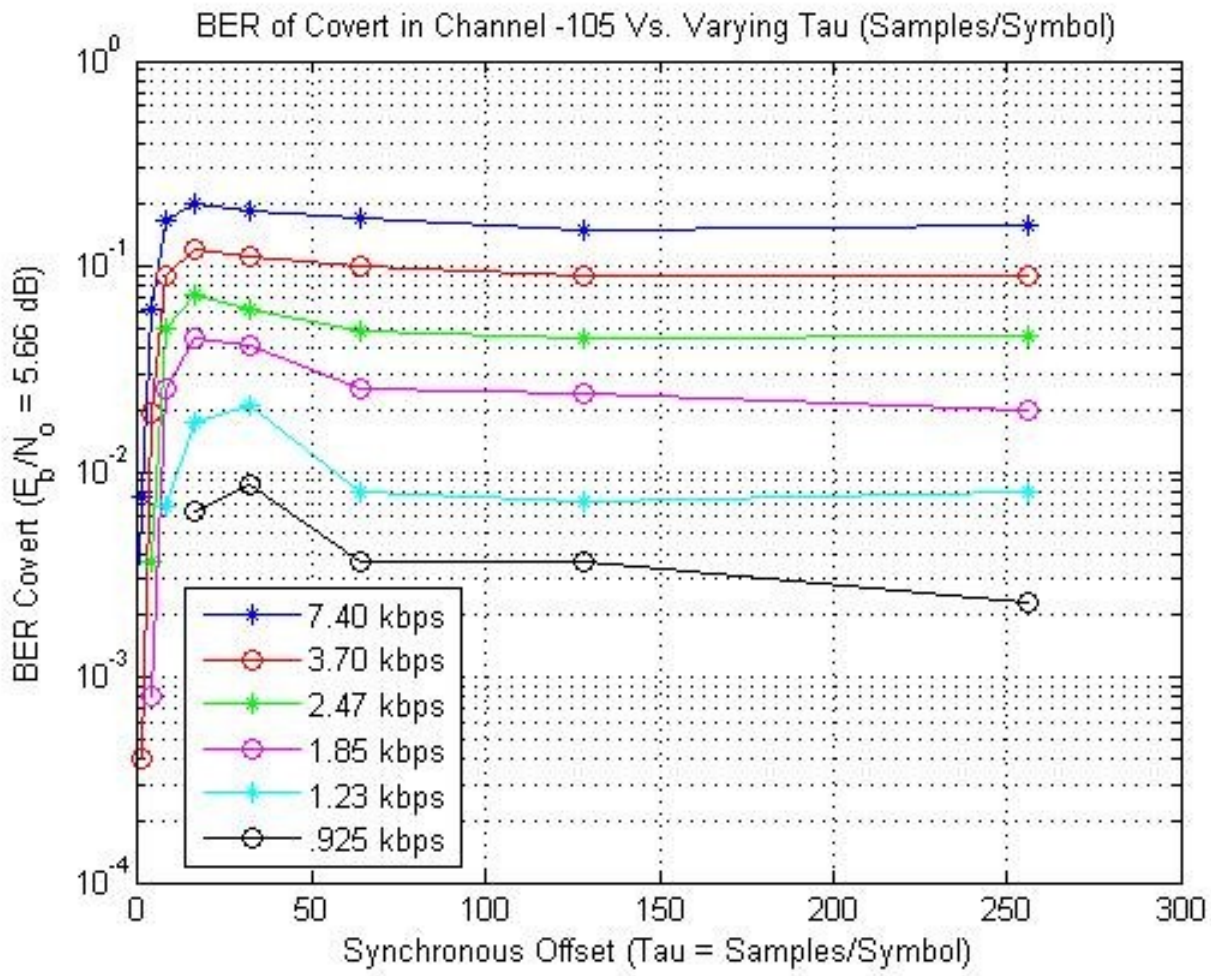
(Ƭ = 128 samples/sym)



Effect of Synchronous Offset on Covert (Channel -154, $E_{b,covert}/E_{b,non\text{-}covert}$ = -8.76 dB)



Effect of Spectral Synchronous Offset on Covert (Channel -105, $E_{b,covert}/E_{b,non\text{-}covert}$ = -9.15 dB)



Received PSD at Non-Covert Receiver for Channel -105
($E_{b,covert}/E_{b,non-covert}$ = -10.83 dB, R_b = .925 kb/s)

Covert Channel -105

Conclusion

- Demonstration of the feasibility of the concept
- Covert is hidden or difficult to detect
- Covert has little or no effect on non-covert system
  - Location of covert is an unused sub-channel
  - Synchronous offset has negligible effect
  - Power of covert can achieve SER less than or equal to non-covert

Conclusion

- Effective covert system
  - Covert synchronous offset can be ignored if....
  - Covert power is set to achieve SER equal to or less than SER of non-covert system (10^{-4})
  - This also aids in maintaining covert characteristic
  - Bit rate several times below max allowed by sub-channel (935 bps)
  - At least a few sub-channels away from utilized non-covert OFDM sub-channels
  - BER of covert is too high for sub-channels next to those utilized by the non-covert OFDM system

- These conditions will allow covert communication to be successful

Future Work

- System for adjusting synchronous offset to achieve improved BER
- Study effect on most adjacent sub-carriers
- Study covert signal utilizing other symbol constellations
- Adaptive coding and modulation to enhance ability to hide covert

Thank You

Questions?