black hat USA 2016

JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS

How to sniff the G3 and Prime data and detect the interfere attack

Abstract

- This topic will talk about how to get the PLC data stream in a PLC communication system which would use G3 or Prime standard, and will also talk about how to detect attacking in the net.
- We will focus on how to identify which kind of standard the system using and how to sniff the PLC data in physical level.

What is PLC?

- PLC is a kind of communication technology which used the power line as the communication medium. This technology ensure power line do the data transfer while supply power.

PLC classification

- Low bandwidth PLC, High bandwidth PLC

Classification	Modulation	Datarate(bps)	Benefit	Application
Low bandwidth	FSK,OFDM	5K~100K	Long communication distance, cross transformer	Power-meter AMR, Municipal facilities, Smart grid
High bandwidth	DMT	Up to 100M	High-speed data access	Internet access

Focus On: Low bandwidth PLC

- Low bandwidth PLC Physical Layer sniff, Physical attack

G3 and Prime Features

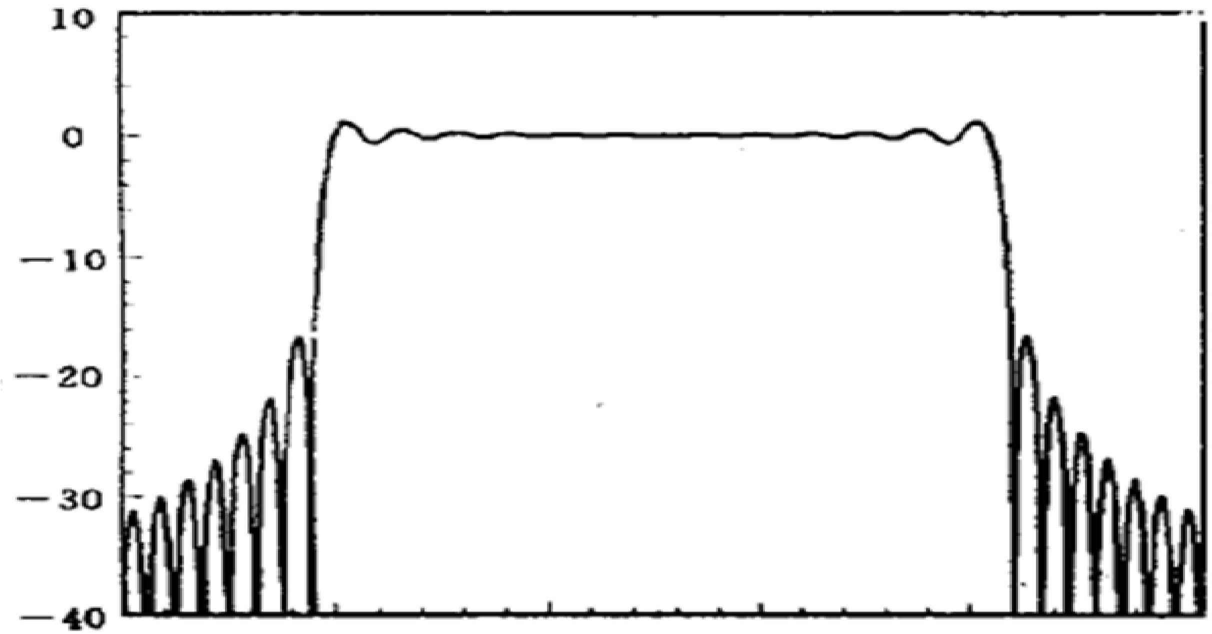
Parameter	PRIME	G3
Base band clock	250kHz	400kHz
Simbol leng	2240 µs	735 µs
Preamble leng	2048 µs	6792 µs
Factors	84（Header）,96（Payload）	36
Modulation	DBPSK / DQPSK	DBPSK / DQPSK
Band	42K~89 kHz	36K~91KHz

How to Identify G3 or Prime

- Power Spectrum Estimation
- With power spectrum estimation, we can get the energy spectrum density distribution. The energy spectrum distribution is related to the signal band, which is different in PRIME and G3.

How to Identify G3 or Prime

- Let us see the standard OFDM spectrum distribution



How to Identify G3 or Prime

- Step1: Get the Power Spectrum of Communication signal
- Step2: Calculate the standard OFDM Power Spectrum
- Step3: Match the signal power spectrum and standard power spectrum, identify the carrier band.
-

How to Identify G3 or Prime-Get Signal Power Spectrum

- Communication signal is x(t), after sample, get xa(t).
- According Wiener-Khintchine theorem, the power spectrum density of stationary random process can be obtained by the Fourier transform of the autocorrelation of the discrete sequence.
-

$$P_x(e^{j\omega}) = \sum_{k=-\infty}^{\infty} r_x(k) e^{-jk\omega}$$

How to Identify G3 or Prime-Get Signal Power Spectrum

- We define the process is Mean-Ergodic to simulate the communication process. So
- $$r_x(k) = \lim_{N \to \infty} \frac{1}{2N+1} \sum_{k=-N}^{N} x(n+k)x^*(n)$$
- To cut the signal with N point Rectangular Window, the biased estimation of r(x) is

$$\hat{r}_x(k) = \frac{1}{N} \sum_{n=0}^{N-1} x(n+k)x^*(n)$$

How to Identify G3 or Prime-Get Signal Power Spectrum

The Periodogram is $$\hat{P}_x(e^{j\omega}) = \sum_{k=-N+1}^{N-1} \hat{r}_x(k) e^{-jk\omega}$$

- And $$E\{\hat{P}_x(e^{j\omega})\} = \frac{1}{2\pi} P_x(e^{j\omega}) * W_B(e^{j(\omega+\omega_0)})$$

$W_B(e^{j\omega})$ is the DTFT of Bartlett Window, and

$$W_B(e^{j\omega}) = \frac{1}{N}\left[\frac{\sin(N\omega/2)}{\sin(\omega/2)}\right]^2$$

How to Identify G3 or Prime-Get Signal Power Spectrum

The Resolution of Periodogram is

$$\operatorname{Res}[\hat{P}_{per}(e^{j\omega})] = \Delta\omega = 0.89\frac{2\pi}{N}$$

How to Identify G3 or Prime-Get Signal Power Spectrum

- The carrier band for PRIME is 42KHz~89KHz, and the carrier band for G3 is 36KHz ~ 91KHz. Considering some margin above the Nyquist frequency, set 400KHz as the sample frequency(fs).

- Define the resolution of frequency is 0.5kHz,

$\Delta\omega=2\pi*\Delta f/fs$

How to Identify G3 or Prime-Get Signal Power Spectrum

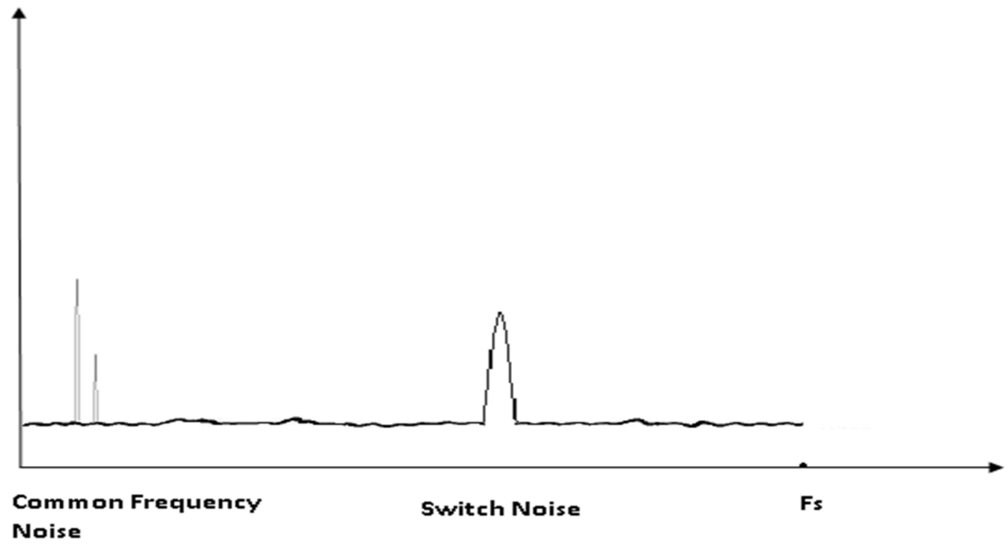
Get N>712,

For FFT, define N= 1024, Δf=0.35KHz

How to Identify G3 or Prime-Get Signal Power Spectrum-How to increase SNR

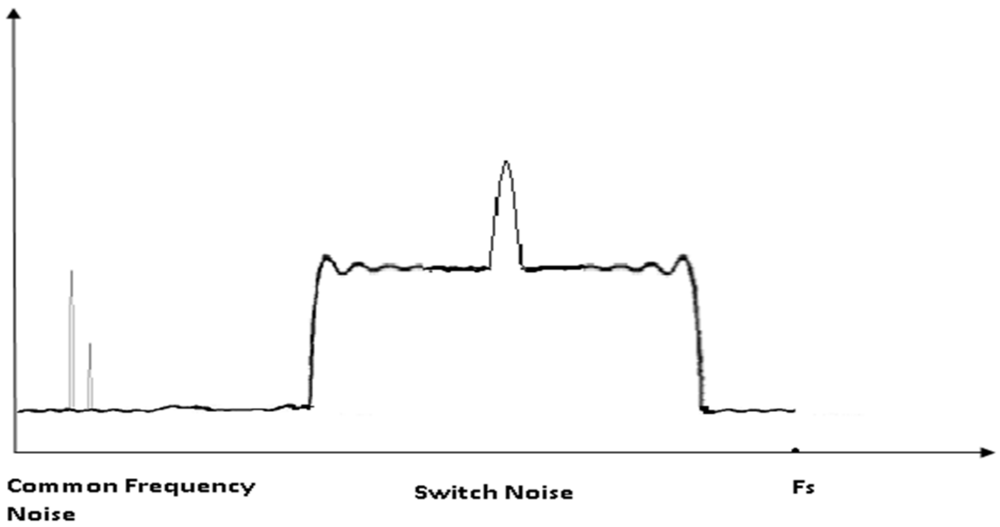
System Noise

- Common Frequency Noise
- Switch Noise
- White Noise



How to Identify G3 or Prime-Get Signal Power Spectrum-How to increase SNR

Signal Power Spectrum would be communication signal power spectrum plus noise power spectrum.



How to Identify G3 or Prime-Get Signal Power Spectrum-How to increase SNR

- Pass Band-Pass-Filter to remove out-band noise
- Calculate base noise power spectrum
- Offset the noise power spectrum in signal power spectrum

How to Identify G3 or Prime-Calculate OFDM Power Spectrum

- The Power Spectrum of OFDM is equal to the sum of sub-factor carrier band power spectrum.

How to Identify G3 or Prime-Calculate OFDM Power Spectrum

- What's is OFDM
- OFDM(Orthogonal frequency-division multiplexing)
- - A method of encoding digital data on multiple carrier frequencies.
- - sub-carrier is modulated with a conventional modulation scheme at a low symbol rate, maintaining total data rates similar to conventional single-carrier modulation schemes in the same bandwidth.

How to Identify G3 or Prime-Prime-Calculate OFDM Power Spectrum

- The Power Spectrum of OFDM is equal to the sum of sub-factor carrier band power spectrum.

$$S_{BPSK}(f) = \sum_{ck=0}^{N-1} T_b \left[\sin c^2((f - f_{ck})T_b) + \sin c^2((f - f_{ck})T_b)\right] / 4$$

$$S_{QPSK}(f) = \sum_{ck=0}^{N-1} T_b \left[[\sin(2\pi(f - f_{ck})T_b)/(2\pi(f - f_c)T_b)]^2 + [\sin(2\pi(f + f_{ck})T_b)/(2\pi(f + f_c)T_b)]^2\right] / 4$$

- Tb for PRIME is 2240uS, for G3 is 735uS

360UNICORNTEAM

How to Identify G3 or Prime-Identify G3 or PRIME

- Crosscorrelation- Measure the degree to which the two signals are similar.

$$\rho_{xy}(0) = \sum_{n=N1}^{N2} x(n)y(n) / \sqrt{rx(0) * ry(0)}$$

How to Identify G3 or Prime-Identify G3 or PRIME

Frequency sample,

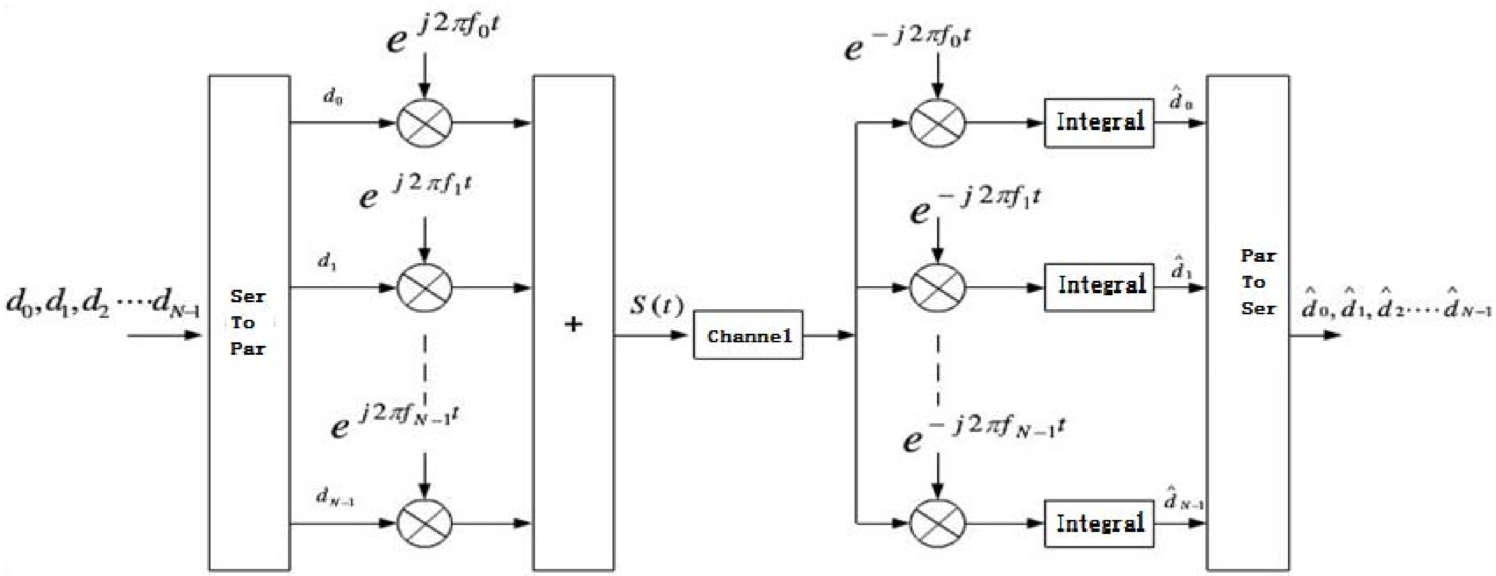
$fs = 400KHz, \omega_0 = 2\pi * 0.35KHz/fs$

Focus on band of 32KHz~95KHz for some margin,

Calculate the $\rho_{xy}(0)$, $\rho_{xy}(0)$ >0.9 is acceptable correlation.

360UNICORNTEAM

How to sniff Physical layer data- OFDM Modulation and Demodulation structure



360UNICORNTEAM

How to sniff Physical layer data- OFDM Demodulation

- The modulation signal is

$$s(t) = \sum_{n=0}^{N-1} d(n) e^{j2\pi f_n t}$$

- after demodulation, the signal is

$$\hat{d}(m) = \frac{1}{NT_s} \int_0^{NT_s} \sum_{n=0}^{N-1} d(n) e^{j2\pi f_n t} e^{-j2\pi f_m t} dt = \frac{1}{NT_s} d(n) \sum_{n=0}^{N-1} \int_0^{NT_s} e^{j2\pi \frac{n-m}{NT_s} t} dt = d(m)$$

How to sniff Physical layer data- OFDM Demodulation

$$s(t) = \sum_{n=0}^{N-1} d(n) e^{j2\pi(f_0 + \frac{n}{NT_s})t} = \underbrace{[\sum_{n=0}^{N-1} d(n) e^{j2\pi \frac{n}{NT_s} t}]}_{s_l(t)} e^{j2\pi f_0 t}$$

$s_l(t)$ is the base band, sample to the base band signal get $s_l(k)$

$$s_l(k) = \sum_{n=0}^{N-1} d(n) e^{j2\pi \frac{n}{NT_s} t} \Big|_{t = kT_s} = \sum_{n=0}^{N-1} d(n) e^{j2\pi \frac{nk}{N}}, 0 \le n, k \le N-1$$

360UNICORNTEAM

How to sniff Physical layer data- OFDM Demodulation

$\hat{d}(n)$ is the FDT of $s_l(k)$,Need to calculate with FFT.

How to detect the interfere attack

Interfere Attack will takes the communication channel and block the node to do the service.

OFDM Interfere attack will be in several slave carrier frequency or the wide band.

The attacker will generate a strong enough interference signal which will cause to receiver cannot modulate the digital signal correctly.

With checking the signal Power Spectrum, it would detect the attack signal.

Thanks!