The risk from power line- how to sniff the G3 and Prime data and detect the interfere attack

Lei Ji (brianaus@163.com)

Abstract

Power line communication (PLC) is a kind of communication technology which is used the power line as the communication media. The PLC technology is divided with 2 sub-field: narrow-band PLC and wide-band PLC. For the narrow-band PLC, there are 2 very import standards: Prime and G3.

Both the standards are wide used in AMR and electric monitor system and it lead to the rise of threat in AMR system security and electric safety.

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.

The following section will show the outline of white paper:

1 PLC classification

2 The current low bandwidth AMR PLC standard

3 How to Identify the G3 and PRIME in PLC system

4 Demolition G3/PRIME physical layer data

6 Detect interfere attack

PLC classification

PLC is divide into 2 sub-class, Low bandwidth PLC and High bandwidth PLC.

The features are as below:

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

The current low bandwidth AMR PLC standard

PLC has many standards, G3 and PRIME are the most widely used. In many standards, the total of G3 pay more attention to robustness. Consider to the PLC would work on a variety of environment and the environment of the existence of the different kinds of disturbances, with standard G3 tolerance of noise robustness often makes itself become a more global application projects favored by selection.

G3 managed by the G3 alliance. In Europe, G3 works in the CENELEC-A band, and can be extended to the entire FCC band in other countries to provide a high data rate. G3 is a two-way communication standard, with an effective data rate of 20 Kbps to 40 Kbps. It can coexist with S-FSK and other traditional PLC technologies.

Other standards other than G3

While many countries around the G3 implementation of Standardization (especially in France), but some countries (such as Spain) then chose other technologies, such as: PRIME. However, the real standard of competition is just just started. Countries such as China, Indonesia and Japan have not yet shown signs of standardization around the PLC.

G3 and PRIME compare

Parameter	PRIME (OFDM)	G3 (OFDM)

Base band clock	250kHz	400kHz
Simbol leng	2240 μs	735 μs
Preamble leng	2048 μs	715 μs x 9.5=6792 μs
Data sub-carrier frequency	84（Header）,96（Payload）	36
Navigation sub-carrier frequency	84（Header）,1（Payload）	
Modulation	DBPSK / DQPSK/D8PSK	DBPSK / DQPSK/ (D8PSK)
Band	42 ~ 89 kHz	36 ~ 91 kHz
MAC	PRIME MAC	802.15.4/G3
Net	IEC61334-4-32/IPv6	6LoWPAN/IPv6

How to Identify the G3 and PRIME in PLC system

For G3 and PRIME, their symbol length, carrier frequency, communication band are different. So the power Spectrum will be different. The first step will get the Power Spectrum of Communication signal. The A/D of processor will do the time domain, then calculate the power spectrum.

The Power Spectrum can be calculate as:

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

The Second Step will calculate the standard OFDM Power Spectrum:

The $S(f)$ of DBPSK and DQPSK are

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

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

The third step is judge the matching degree of the signal power

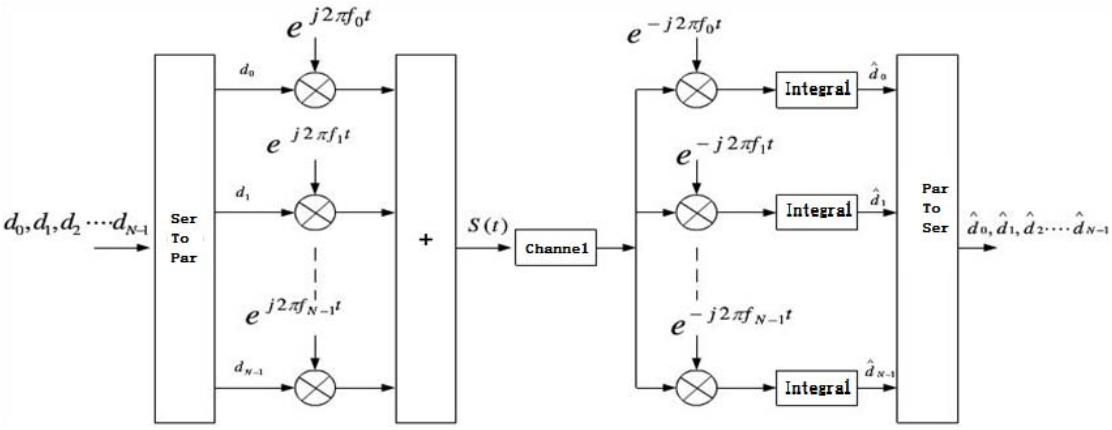
spectrum standard power spectrum.

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

$\rho_{xy}(0)$ is more than a accepted value, two power spectrum matched.

Demolition G3/PRIME physical layer data

After testing the standard to be carried out OFDM demodulation, OFDM is a high-speed serial data through the frequency division multiplexing to achieve parallel transmission of multi carrier transmission technology. The modulation and demodulation system block diagram is as follows



The symbol rate is T, the bit rate is Ts, because the relationship of serial to parallel transform, so T=NTs.

Each subcarrier signal is demodulate by

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

Modulation process can be calculated using FFT and IFFT,

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

We take the $s_l(t)$ equivalent baseband signal. The baseband signal is sampled to obtain the baseband signal $s_l(k)$:

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

So

$$\hat{d}(n)=\sum_{k=0}^{N-1}s_l(k)e^{-j2\pi\frac{nk}{N}},0\le n,k\le N-1$$

Detect interfere attack

In the PLC network, the open broadcast characteristic of the channel makes the data transmission between nodes susceptible to noise or interference. Intentional interference is called interference. This kind of attack only through passive interception to obtain the current network node communication frequency band, can quickly launch attacks, simple and effective.

With checking the signal Power Spectrum, we can detect the interference attack signal.

About Author

Lei Ji is the regional marketing manager in North China worked for Cypress semiconductor. Advisor of Qihu360 Unicorn Team. Before joining Cypress, he took charge of the wireless product supporting for Texas Instrument in North China.

Reference

Wireless Communication Principles and Practices by Theodore S Rappaport.

PLC G3 Physical Layer Specification by G3 alliance

PRIME-Spec (1.3)