QUALCOMM: SIMPLE & SECURE WI-FI CONFIGURATION FOR INTERNET OF THINGS

Jie Luo

Electrical Engineering and Computer Sciences
University of California at Berkeley

Technical Report No. UCB/EECS-2013-193
http://www.eecs.berkeley.edu/Pubs/TechRpts/2013/EECS-2013-193.html

December 1, 2013

QUALCOMM: SIMPLE & SECURE WI-FI CONFIGURATION FOR INTERNET OF THINGS

Hardware Part

JIE LUO

SSID: 24100307
Department: EECS

Abstract:

Wi-Fi Protect Setup (WPS) is a Wi-Fi configuration protocol that provides a secure and simple Wi-Fi setup process by PIN method and Push-Button method. At the moment, hacking activity and complex configuration process of Wi-Fi is still the main barrier for the developing of Internet of Things. A successful secure and simple Wi-Fi configuration is desired by increasing usage of Internet of Things. This paper proposed to introduce a new Wi-Fi configuration method depending on WPS protocol to simplify the connection process and improve the security level. The fundamental concept of configuration approach is using smartphone as the intermedia to connect Internet of Things and Access point (AP). The PIN number is dynamically displaying by external source, then the PIN information would by captured by smartphone to process the Wi-Fi configuration. The whole IoT device Wi-Fi setup depending on WPS would compress the configuration time from average 5 minutes to several seconds, which is drastically reduced complexity. Compared with traditional way of Wi-Fi setup method, a simple & secure Wi-Fi configuration relied relying on the physical signal communication would significantly improve the security level of current pure wireless sign-in method. On the other hand, any passphrase of small network such as home, office would not be necessary at all due to the very ubiquity of the smartphone in the near future.

Introduction:

Currently, 11% of people in the world are using Wi-Fi to connect with the Internet. Furthermore, more than 1 billion Internet of things (IoT) were in use in 2011. But this number is projected to grow to 1.5 billion by 2013.

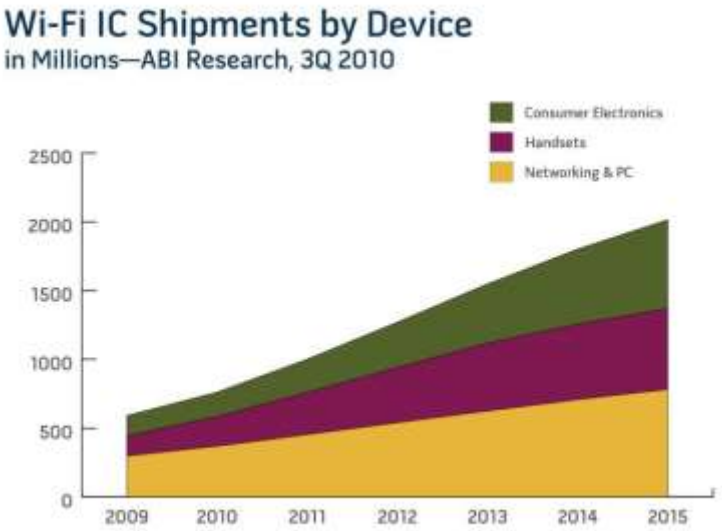

Figure.1 Wi-Fi IC shipments by device in 3Q 2010

Right now, Wi-Fi is the most popular method of wireless networking technology. Based on the current home electric appliance technology, consumers are trying to share content across of multiple digital devices and applications like TVs and printers. Wi-Fi is based on 802.11b wireless standard, which includes Wired Equivalent Privacy (WEP) security protocol, developed by the Institute of Electrical and Electronics Engineers (IEEE). IoT device can detect the “service set identifier (SSID)” number that wireless access point (AP) are constantly radiating to identify the IoT device authorization. But with incredible growing of Wi-Fi, the security problems of wireless network are attracted most people eyeball. There is no additional secure steps of WEP security

protocol needed to access the Wi-Fi network that has caused considerable number of computers were hacked in by the insecure computer networks. Although, current Wi-Fi system have WEP security method, but it is still unable to block the hacker to break into network.

Because of the saturation that how heavily people rely on the Wi-Fi Internet, the Wi-Fi security is the most serious problem focused by entire wireless communication. For example, there is a real case of Wi-Fi security problem. A hacker built a Wi-Fi hot spot disguised as free Wi-Fi by himself at a lot places such as airports and hotels. Then enormous sent or received personal information include bank information, personal contact and mail password could be captured by hacker. For the company, once its network is hacked in, the commercial secrets would not be secret any more. So how to improve the Wi-Fi security level became a hot topic be cared by everybody.

Figure 2. the prototype of Wi-Fi Protected Setup

For the security problem, Wi-Fi Protected Setup (WPS) was raised in 2010. It was developed to simple and secure Wi-Fi configuration process what has philosophical differences compared with regular 802.11b WEP. Otherwise, the PIN method is the WPS default in Push Button Configuration in order to initiate an unauthenticated Diffe-Hellman exchange. Indeed, an advanced uplink Wi-Fi configuration method based on WPS technology would be introduced in this report. Uplink Wi-Fi configuration method means that wireless radiation authorized signal would be converted into analog signal such as LED flash what could be captured by smartphone, then smartphone would process the analog signal and send it to the wireless networking access point. Therefore, Wi-Fi connection request and security information would transfer by the third-party media that physically improve the security level of wireless network.

Literature Review

With the development of Internet technology, the high level available security internal network mechanisms are extremely demanded by the user of home and small office networks. At the same time, the function of simple additions and configuration process to the WIFI enable equipment without any passphrase should be added into security internal network mechanisms.

This part would introduce three main aspect of simple & secure Wi-Fi configuration. First part is components and interface. Next one is Wi-Fi protect setup mechanism. Final part is the image process for software.

Core Architecture

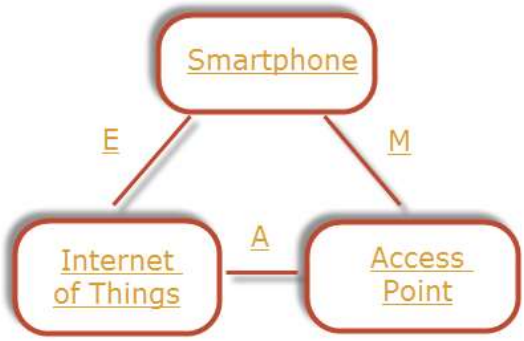

Figure 3. Components and Interface

The figure above shows the WPS protocol architectural consists of three major components: the Access Point (AP), the smartphone (external registrar) and Internet of Things (Enrollee). The Access Point can establish indoor Wi-Fi network, then the next step is to add an Enrollee or Registrar device to the Wi-Fi. Specifically, an new external Registrar is added into network, then the additional external Enrollees can be added relying on that Registrar. New 802.11 information elements are introduced in WPS protocol that involved in beacons, probe, requests and probe responses.

Interface M: the interface between Access Point and Smartphone used to enable an external Registrar to configure a WPS based Access Point. The access point using in interface M is monitoring IEEE 802.11 probe request from smartphone or IoT device, then transfer the request to UPnP message. Moreover, the access point is supporting at least three external Registrar. The smartphone using in interface M is acting as Registrar to process access point discovery information by IEEE 802.11, then capture the MAC address from access point.

Interface A: the interface between access point and IoT device used to enable to discovery WPS configuration information. The access point using in interface A is sending 802.11 beacons and generating Probe Response messages that would help IoT device to recognize the access point need to connect with. The IoT device in interface A is searching for a WPS enabled access point and sending 802.11 probe request to ask for 802.11 beacons indicating the access point information.

Interface E: the interface between IoT device and smartphone used to enable to enable the smartphone to search and authorize WLAN credentials to the IoT device. In this part, the out-of-band channel would be implemented as computer vision demodulation to make a one-way communication between smartphone and IoT device. The IoT device in interface E is sending a unique device PIN number that could authenticate the in-band information exchange. The smartphone in interface E is processing the PIN information sending from IoT device. Then it would also response to access point with the Probe-Request for the IoT device.

Wi-Fi Protected Setup

WPS (Wi-Fi Protected Setup is a certification program what is designed to support 802.11 internet of things such as phones, computers, access points and electronics. Home and small office network is general for all 802.11 devices what included 802.11a/b/g/n, multiple-band IoT device. The Wi-Fi configuration setup option of WPS has two basic methods, one is Personal Identification Number (PIN), other is Push Button Configuration (PBC). In the project, PIN method would select as principle Wi-Fi configuration procedure.

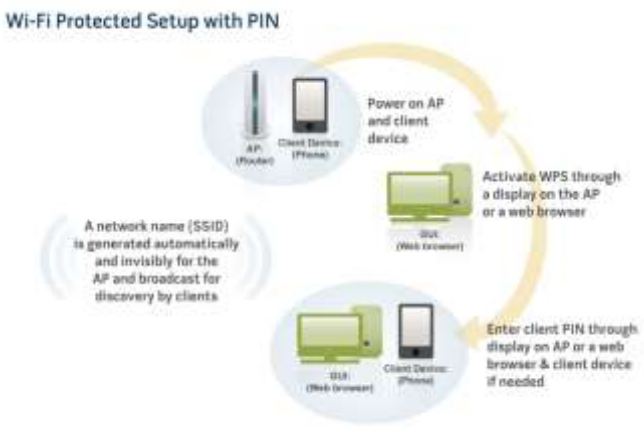

Fig.4 WPS PIN method working process

For the PIN method, every device would be fixed a label or sticker to display the specific PIN number for the user. Otherwise, if the IoT device has screen or monitor, a random PIN would be generated and displayed. This PIN number is provided to ensure that access point (e.g. router) can recognize which device would be connected with and avoid malicious hacker connection. As the project requirement, the PIN number would be sent to the access point by smartphone via a physical way such as LED blinking, buzzer ringing.

At the other hand, WPS provided a security Internet connection for home and small office network as well. WPS Wi-Fi configuration method is based on WPA2 protocols what is developed form Advanced Encryption Standard (AES) and IEEE 802.1X. AES is a top secure internal network protocol for many country governments to prevent hacker attack and protect confidential information. Then IEEE 802.1X is a widely used standard that can ensure the reliability of access control of network.

Image Processing – Object Track

Although, smartphone camera has high shutter speed rely on the new CCD photographic technology. But it still needs smartphone to recognize where is the LED light due to the randomness of user behavior. So a complete object track system should be developed into several steps: 1. Image pre-process, 2. Detect and segment environment, 3. Object characteristic extract and recognize, 4. Analyze object state of motion and track.

1. Image pre-process: in order to reduce the image noise, interference and enhance the contrast ratio between object and environment.
2. Detect and segment environment: this part is the most different in whole object tracking system. It would roughly pin out the possible object area. Then segment this part from the environment to make advanced analysis.
3. Object characteristic extract and recognize: the characteristic of object could be divided into shape, grey scale, area and texture. The different characteristic has different method of extraction. It would satisfy three rules: constancy, uniqueness and stability.
4. Analyze object state of motion and track: after several steps above, the rough object position could be detected and the centroid of object would be computed out. For the image sequence, the object trajectory is already generated. In advance, according to the object moving speed and direction data, the object position in next several frames could be predicted.

Methodology

Wi-Fi communication is depending on the IEEE 802.11 protocol, which is a standard for realizing wireless lock area network. Therefore, the first step of all is enable every Internet of Things (IoT)

with Wi-Fi function. This step would be divided into two parts, the first one is modelling the Wi-Fi PIN mode configuration with smartphone, the second one is creating a wireless library based on WPS PIN setup on Arduino wifishield.

Basically, the IoT device should only active a single configuration mode at that moment. Under such condition, the smartphone used in this project assumed as an external Register. When a Register supposes to setup the Wi-Fi configuration for an IoT device that has already engaged in process with another Register. Therefore this IoT device need to return a NULL message to the new Register. However, the NULL message would be ignored by first connection Register due to the different Nonce value stored.

Indeed, the principle and algorithm converted into Arduino code is extremely different. According to the limitation of Arduino board, it is unable to detect that which Register caught the PIN number. In order to improve the reliability, the unique PIN number of IoT device would be designed to generate randomly by itself. Then, assumed that the delay of PIN number demodulation of smartphone is about 20 seconds. After Access Point (AP) received PIN number sent from smartphone, it still need 5 seconds to setup the connection with IoT device. The total time consumption of PIN mode Wi-Fi configuration is about 25 seconds. In other word, this process should be immune in 25 seconds without second Register interruption. In the result, the IoT device is programming to implement a function that there is a counter inside, IoT device would be active in PIN mode for one second after 25 seconds. If the IoT device do not receive any information of connection request from AP, it would start over again depending on an infinite for loop.

The process of PIN mode configuration after AP got the PIN information sending from Register is fantastic complexity. For this part, it raised two method could implement the function, one is

External Registrar trigger first, the other is named IoT device trigger first. Depending on the real situation happened in real world, the smartphone used as a Registrar is always connected with indoor Wi-Fi, which means the AP would trigger Registrar first, then the IoT device would be detected and followed up.

In the next step, the configuration model would be introduced built rely on the Wi-Fi setup of PIN mode. At the first, the IoT device is reset to an unknown state and waiting for the Beacons from AP. Then the IoT device would send Authentication information request with WSC IE and SR to the pre-selected AP or each potential AP sequentially. After the authentication request sending, it would wait for probe response with WSC IE and SR information what is in order to engage with one AP. But the IoT device need to scan all-around Registrar flags in Beacons, probe responses. Once it can detect matched information, it would get into the PIN active mode and prepare to configure the Wi-Fi network.

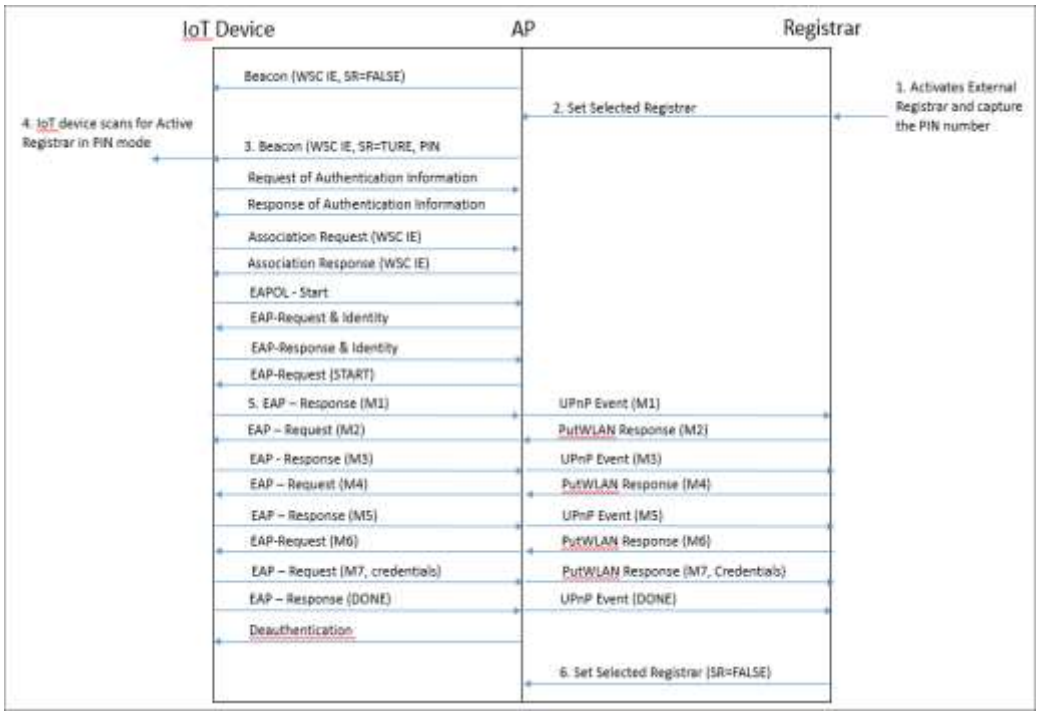

Fig.5 – External Registrar trigger first method model based on PIN mode

According to fig.1 configuration model, the IoT device converts the 8-digit PIN number into LED flashing instead of reading a label. And external Registrar (e.g. smartphone in this project) would capture the information from LED flashing and demodulate it, then send it to the pre-selected AP. In second step of model, the selected Registrar (SR) becomes to TURE that lead the AP into the active mode using Set Selected Registrar UPnP action. Next, AP set WSC IE and SR to TURE in its Beacons and Probe Response after AP get the information from external Registrar through the UPnP action. Once IoT device receives correct WSC IE and SR information, it would start PIN based registration protocol and search for an available AP in range. Then IoT device makes communication with target AP and sends EAP-Response (M1). M1 message means IoT device is accredited the Registrar to receive UPnP event from AP. When the communication between IoT device and AP is set, the main part of Wi-Fi PIN mode configuration is done.

After the modelling of Wi-Fi PIN mode configuration, the Arduino board using in project should be able to have a Wi-Fi connection. So the Wi-Fi library based on PIN mode would be created. In order to modulate the PIN number into physical signal, Arduino board is enable to blink the LED light. According to the algorithm designed in project, the decimal number would be convert into binary system, which means PIN number represented in 0 or 1. For the corresponding LED blinking, “1” is LED ON and “0” is LED OFF. Then the duty cycle of “1” and “0” is the same. The modulation process consists of three part, flag, PIN number and check sum. The flag signal is defined the beginning signal of the data. Moreover, flag is used for correct and synchronize the data frequency between Arduino broad and smartphone. After the smartphone captured the flag signal and verified it, the read data would be demodulated in process. Each decimal number converts into 4-bit binary number. The Most Significant Bit (MSB) could be decoded in one duty cycle. Next, the second MSB would follow to the next cycle. In the end of PIN number transfer,

the check sum is added into bit stream, which is responsible for the check the reliability of whole signal stream.

Combine the Wi-Fi PIN mode model and PIN number modulation, the hardware part is almost done.

Discussion:

The project was taken from Oct, 2012 to now. The objective and configuration method was changed several times during this period. In the discussion part, the PIN number modulation method and Flag generation/detection would be compared and analyzed based on the computer vision in detail.

PIN number modulation method:

A heavy part of hardware is how to modulate PIN number into analog signal. There are several methods selected for the experiment. The first modulation method is Manchester code, which is specific for low-cost short distance data communication applications. Furthermore, the main feature of Manchester code used in the project is the internal synchronization clock. According to principle of Manchester code, every clock cycle would cause one transition from 1 to 0 or from 1 to 0. Even if the LED blanking is in the different clock domain with smartphone camera, but the principle mentioned above could help smartphone camera to determine and rectify the internal clock matched with hardware clock. Therefore when the smartphone can detect the

transition, the bit number can be read out from comparison between the frame before and after the transition.

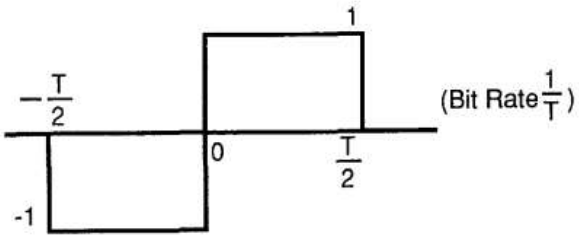

Figure.6 Basic form of Manchester signal

Figure 2 shows the basic transmitting Manchester waveform. The bit rate of this waveform is 1/T. So the Fourier transform equation of this waveform can be derived:

$$\mathrm{F}(\omega) = -\frac{4j}{\omega} sin^2 \frac{\omega T}{4}$$

It is four times the Nyquist rate for a common binary system of 1/T rate when the first null of the equation above occurs at $\omega = 4\pi/\mathrm{T}$. The higher Nyquist rate consumes exorbitant usage of bandwidth. Theoretically, the smartphone can still detect accurately base on four times normal sample frequency. But after implementation, detect accuracy rate is under 30%. According to observation of result, the continuous numbers (e.g. 000 or 111) are unpredictable to demodulate. But the number switching is easily to detect with high accuracy. The camera technical parameter of smartphone is about 20-30 frames per second. Every bit display time is 0.8 second. Therefore it would have at least 16 frames to determine the bit and the transition moment at 0.4 second. However, the most serious error occurs at the transition in same clock cycle. The reason for the error is the LED blanking delay and the halo. During the transition from on to off, the LED was not completely off and it would be suffering nano second delay. Then the

halo of LED would reflect on surrounding objects, which cause chromatism due to different material surface reflectivity. As a result, the smartphone is unable to detect the LED switching in synchronization and the internal clock correction function failed as well. In order to ensure the reliability of demodulation, the traditional modulation method is employed in the project, which presents ON as 1 and OFF as 0 for certain time. Every sampled frame would be compared with pervious frame, if there is some overall difference, the transition happened. Although its transmission rate is relatively lower than Manchester Code. Indeed, the time it stay on the one condition (ON or OFF) is twice of the Manchester Code. Potentially, it would significant increase the reliability of detection.

Requirements for PIN value:

For IoT device without display function, the 8-digit PIN number should be used. The last digit in the 8-digit PIN is a kind of checksum. According to limitation of manufacture, the fixed PIN number could be susceptible to a potential attack. In this condition, the PIN number needs to regenerate periodically. The first 7-digit PIN number could be generated randomly, but the checksum is used to validate based on pervious 7-digit of PIN number.

```
bool Checksum(unsigned long int PIN)
{
        unsigned long int accum = 0;
        accum += 3*((PIN / 10000000) % 10);
        accum += 1*((PIN / 1000000) % 10);
        accum += 3*((PIN / 100000) % 10);
        accum += 1*((PIN / 10000) % 10);
        accum += 3*((PIN / 1000) % 10);
        accum += 1*((PIN / 100) % 10);
        accum += 3*((PIN / 10) % 10);
        accum += 1*((PIN / 1) % 10);

        return (0 == (accum % 10 ));
}
```

Flag Detection:

Flag bit stream would be employed in every communication system to indicate the start of the data transmission. Initially, a flag is set by 1000001 combined with Manchester Code. It was failed in testing due to the big stream is too short that is easily confused with read data stream. Therefore, an extended flag bit stream is implemented into data transmission. According to worst case, 000000+111111 would never happened in 32 bit decimal-binary number system. Then a binary number 0 as checksum would add into the last of flag bit stream to ensure the smartphone detect the correct number sending from the IoT device.

Further Improvement:

The method introduced in this report is mainly based on the computer vision what is most visual way for WPS protocol Wi-Fi configuration. Alternatively, pulse-width modulation or phase-shift keying based on the buzz is an improved method, but it is significantly complex for encoding and decoding process. Because the sampling rate of smartphone audio recorder is 128kbps for high sound quality, which is much higher than camera sampling rate.

Conclusion:

The Wi-Fi Protected Setup protocol based on PIN number method significantly simplify the process of IoT Wi-Fi configuration. At the same time, it implemented with most advanced Wi-Fi protocol that improved the security level compared with WPA2 protocol. Currently, the prototype of this project still has several issues what could be further improved, such as efficiency, reliability. However, it is a good start point for a simple and secure Wi-Fi configuration. With the increasing demand of IoT device, a simple and secure Wi-Fi configuration method would be attract more attention in the future.

Reference:

1) Wi-Fi Alliance. "*Wi-Fi Certified Wi-Fi Protected Setup*"

2) Tim Higgins. "*How is WPS supposed to work?*". Sourced on Dec. 11th, 2012, http://www.smallnetbuilder.com/wireless/wireless-features/30345-how-is-wps-supposed-to-work

3) Stefan Viehbock. "*Wi-Fi Protected Setup made easier to brute force*", Sourced on Dec. 11th,2012. http://www.h-online.com/open/news/item/Wi-Fi-Protected-Setup-made-easier-to-brute-force-Update-1401822.html

4) Stallings William. 2004. "*Data and Computer Communications (7th ed).*" Prentice Hall. pp.137-138. ISBN 0-13-100681-9.

5) ATMEL. "*Manchester Coding Basics Application Note*", sourced on Dec. 12th, 2012. http://www.atmel.com/Images/doc9164.pdf

6) Alper Yilmaz, Omar Javed and Mubarak Shah. " *Object Tranksing: a survey*", sourced on Dec. 12th 2012. http://crcv.ucf.edu/papers/Object%20Tracking.pdf

7) David Horner, Su Yi. (2004). "*Development of an Automic Object Tracking Camera System Using Multiple Metrics*", sourced on Dec. 12th, 2012, http://dave.thehorners.com/personal/projects/tracking/AutomaticCameraTrackingAbstractFinal.pdf

8) Wi-Fi Alliance., 2011, "*Wi-Fi Simple Configuration Technical Specification*" Version

2.0.2,

9) Barr M. “Pulse width modulation[J]. Embedded Systems Programming”, 2001, 14(10): 103-104. Sourced on March. 10th , 2013. http://homepage.cem.itesm.mx/carbajal/Microcontrollers/ASSIGNMENTS/readings/ARTICLES/barr01_pwm.pdf

10) De Buda R. “*Coherent demodulation of frequency-shift keying with low deviation ratio[J]*.” Communications, IEEE Transactions on, 1972, 20(3): 429-435.