Design and Implementation of Frequency Hopping for Secure Data Communication

Ayman Bassam Nassuora

Department of Management Information Systems, City University College of Ajman (UAE)

Abstract: For the transmission of signals with reliability and security, Frequency Hopping (FH) is one of the well-known techniques. By the use of Frequency Hopping, the signal cannot be intercepted by any device (most of the devices do operate on single frequency) and using Frequency Hopping the carrier frequency is switched to different frequencies by means of a Pseudo- random PN Code only known to the transmitter and the receiver. In the real world there are a number of projects that cannot be implemented because of the different constraints (limited resources and budget). This paper is about novel design and implementation of a prototype for Frequency Hopping Spread Spectrum in Verilog, HDL. The benefit of this is that instead of buying expensive circuits, a programmable Field Programmable Array, FPGA can be chipped to reduce the cost and ability for the modification.

Keywords: Frequency Hoping, Verilog, FPGA, Spread Spectrum, GSM

1. Introduction

This is an evolutionary world. People are enjoying different technologies. One of such examples is cellular communication. These days it is too easy to not only establish calls but also to use high speed data services. The cellular technology was first introduced in late 1970’s and early 1980 are known as the 1G (First Generation). After the technology was introduced to the customers it was realized that the system was limited capacity wise. Lathi stated to overcome the issues specifically the issue of capacity in 1990’s 2G system was introduced to the customers (GSM, Global System for Mobile Communication) [2].

Now we are gifted with 3G Systems and a lot of research is going on for the 4G Systems. What is special in 3G System? It is an introduction to a new technique in which signal is transmitted on a bandwidth considerably larger than the actual frequency content of the original system. Lathi in the same literature and Burr discussed that SS is parallel to CDMA, Code Division Multiple Access technique [1] [2].

Spread spectrum (SS) is a methodology by which the energy is generated for a given bandwidth is spread widely in the frequency domain. The result we get is a signal with a much wider bandwidth. The technique is used widely. The key aspect of this technique is to have a very secure communications because the signal is spread widely and it is very difficult for the jammers to detect it [6]. This is a technique in which a signal is transmitted on a bandwidth considerably larger than the frequency content of the original information. Spread spectrum modulation is parallel to the CDMA technique.

The Spread Spectrum communication is a signal structuring technique that employs direct sequence, frequency hopping, time hopping or a hybrid of these, which can be used for multiple access and/or multiple functions. This technique decreases potential interference to other receivers while achieving privacy [6]. Spread spectrum generally makes use of a sequential noise-like signal structure to spread the normally narrowband information signal over a relatively wideband (radio) band of frequencies. The receiver correlates the received signals to retrieve the original information signal. Originally there were two motivations: either to resist enemy efforts to jam the communications (anti-jam, or AJ), or to hide the fact that communication was even taking place, sometimes called Low Probability of Intercept (LPI).

There are three different types of Spread spectrum, SS Techniques which are given in the figure below.

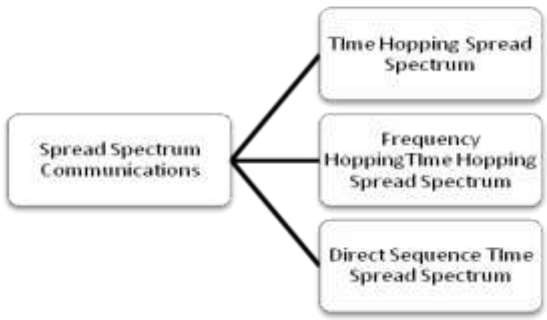

Fig. 1. Different types of Spread Spectrum Communications

2. Significance of Spectrum Technology

There are a number of reasons why we selected the Spread Spectrum technique for our solution:

1. Spread Spectrum communications are Immune to the Noise. The Spread spectrum are like noise since the signal is widely spread in the frequency domain so they are made in much wider band than the actual message signal.

2. The Spread Spectrum signal is hard to intercept [5].

3. The Spread Spectrum signals are difficult to be detected and demodulated.

4. Spread Spectrum are very difficult to be jammed. This was the only reason why this technique is widely used in the military applications. But now due to the advancement of the bleeding edge technologies this technique is a very important feature of 3G communications.

5. Spread Spectrum offers multiple users to access the communications by having the selective addressing capability.

6. Spread Spectrum resists the eavesdropping.

7. The spreading code in Frequency Hopping, Time Hopping and Direct Sequence Spread spectrum communications is only known to the transmitter and the receiver and it is unknown to every one for the case in which the unintended user want to encrypt the signal so it prevents the adversary to sense the signal.

Spread Spectrum shows resistance the fading. Due to the widely spread bandwidth the signal offers some frequency diversity.

Stallings explained that by the use of Frequency Hopping Spread Spectrum (FH-SS) the signal is broadcasted over a seemingly random series of RF Frequencies, Hopping from frequency to frequency at fixed intervals. A receiver switches randomly, hopping between different frequencies in synchronization with the transmitter [5].

FH-SS in reality is a method in which the signal is transmitted by the rapid switching of a carrier among a large number of frequency channels. The rapid switching is done by means of a pseudorandom code or sequence known to the transmitter and the receiver.

Frequency Hopping is mainly used in the military communications. Sutton explained that Military radios use cryptographic techniques to generate the channel sequence under the control of a secret Transmission Security Key (TRANSEC) that the sender and receiver share [5]. By itself, frequency hopping provides only limited protection against eavesdropping and jamming.

3. Design and Implementation

In order to Implement FHSS different methodologies can be adopted, for example using the Discrete Components or Integrated Circuits but before the actual implementation one has to stop and think:

- Availability of strong budget
- Ease and availability of Electronic components
- Availability of testing equipment
- The size of ending product
- Attraction towards the market
- Feasibility of the Design and many more.

One of the solutions can be using one of the famous hardware descriptive languages Verilog, HDL [6]. From the word it is very clear that this language is used to describe a digital system. This language has rapidly become a widely accepted language for VLSI design.

There are four different types of programming that one can do, as shown in Figure 2.

Fig. 02. Different programming modes in Verilog, HDL

In this very implementation the highest level of abstraction is used. The system is designed in terms of the desired/ required Algorithm without concerning the actual circuitry or hardware implementation of the system design.

Padmanbhan and Sundari explained that Designing at this level is very similar to C-programming [3]. An abstract representation helps the designer explore architectural alternatives through simulations and to detect design bottlenecks before detailed design begins. While implementing the biggest hurdle is that Verilog does not support the Analog waves as well as negative values [6].

To achieve the Frequency Hopping Spread Spectrum, FHSS one has to implement the real Analog waves (Sine and Cosine) and then to Generate a Pseudo random, PN Code in order to hop the frequencies. Though very challenging but can be achieved by using a Look UP Table. The threshold level was increased from 0 to get rid of the negative values for the table [7].

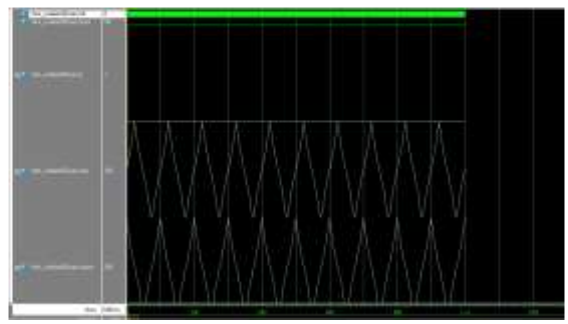

Fig. 3. Sine and Cosine waves

Figure 3 above shows that sine and cosine waves are achieved by using the Look UP table. The sine wave was sampled at different intervals. After drawing a sine wave manually a total of 100 locations/ samples were taken. These samples were stored in a table. The coding was done for the hardware design. A total no of 100 locations/ samples were taken. A clock rate (clk) was provided because the Verilog, HDL introduces no delay as soon as one gives the input gets the output. So when clk=0 the system is stable. When clk =1 the sine wave is achieved and different outputs are achieved for +ve and –ve values of clk. To know the state of the hardware reset functionality is also provided.

Because the implementation was on the abstract level/ algorithm level, the data flow graph was also obtained which is shown in the figure 04;

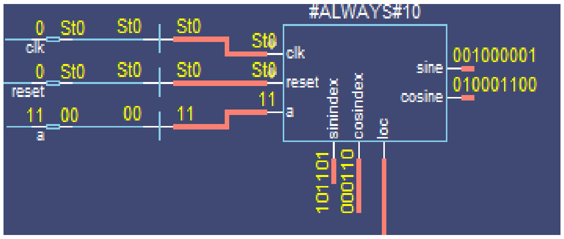

Fig. 4. Data Flow of Sine and Cosine wave

After achieving the sine and cosine waves a 2bit PN Code was also generated. So for the PN of 00 all 100 locations were used. For PN 01 half of the locations were used and so on.

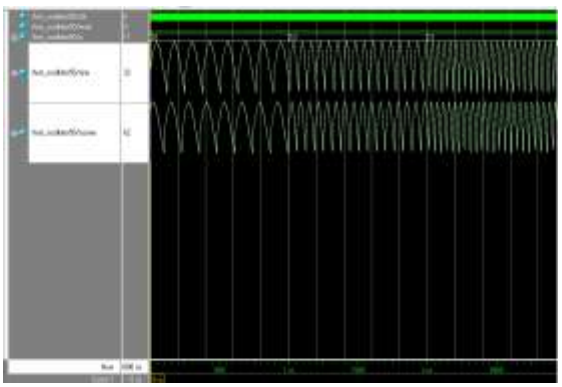

Fig. 5. Frequency Hopping Spread Spectrum

Figure 5 above shows switching of different frequencies. In order to achieve security the signal can be randomly switched on different frequencies. Only the transmitter and the receiver know the PN sequence code [7]. This switching is so fast that no jammer and tracker can intercept with the signal. The code can be increased from 2 bits in order to achieve more security [8].

4. Conclusion

Though to achieve Frequency Hopping Spread Spectrum (FHSS) is challenging as one has to program for the hardware perspective and an extensive research and effort is required to implement but the most promising advantages are:

- Reduction in the cost
- Reduction in the Hardware Design
- Reliability and Security and option of configurability
- Feasibility of Design

Furthermore, there is no need of Testing Equipment as one can develop his/ her own prototype for the testing equipment.

5. References

[1] Burr, A. (2015). Modulation and coding. 1st ed. Harlow, England: Prentice Hall.

[2] Lathi, B. (2014). Modern digital and analog communication systems. 1st ed. New York: Oxford University Press.

[3] Liu, Q., Zhou, S. and Giannakis, G. (2015). Cross-layer combining of adaptive modulation and coding with truncated ARQ over wireless links. Wireless Communications, IEEE Transactions on, 3(5), pp.1746--1755.

[4] Mortara, A., Vittoz, E. and Venier, P. (2014). A communication scheme for analog VLSI perceptive systems. Solid-State Circuits, IEEE Journal of, 30(6), pp.660--669.

[5] Padmanabhan, T. and Bala Tripura Sundari, B. (n.d.). Design through Verilog HDL. 1st ed.

[6] Potop-Butucaru, D., Lallement, C. and Vachoux, A. (2005). VHDL-AMS and Verilog-AMS as alternative hardware description languages for efficient modeling of multidiscipline systems. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on, 24(2), pp.204--225.

[7] Stallings, W. (2014). Data and computer communications. 1st ed. Upper Saddle River, N.J.: Prentice Hall.

[8] Sutton, R. (2013). Secure communications. 1st ed. Chichester: J. Wiley.