# Frequency Hopped Spread Spectrum Tutorial

DR. KIRAMAT ULLAH, ZAIN UL ABEDIN, MUHAMMAD HASSAN, AHSAN MUKHTAR, MUHAMMAD USMAN IMTIAZ


# ABSTRACT:

This article is about FHSS (Frequency Hopped Spread Spectrum) and one method suggested for Security improvement in it. In this report you can find an in depth information on FHSS from the basic level to the aim of the project. A detailed explanation is given about the Modulation, Frequency Hopping, PN-sequence generation, Frequency table w.r.t PN sequence which form crucial components in generation of the FH-spread signal. And finally demodulation is done and the obtained waveforms are analyzed. The whole process is simulated in the well-known simulator MATLAB. Working code is attached with this report. One method is suggested to improve the security in the FHSS.

# Introduction:

## DEFINITION:

It is the repeated switching of frequencies during radio transmission, often to minimize the effectiveness of "electronic warfare" - that is, the unauthorized interception or jamming of telecommunications.

- Generate a bit pattern.
- The original message modulates the carrier, thus generating a narrow band signal.
- The frequency of the carrier is periodically modified (hopped) following a specific spreading code.
- In FHSS systems, the spreading code is a list of frequencies to be used for the carrier signal.
- The amount of time spent on each hop is known as dwell time.
- Redundancy is achieved in FHSS systems by the possibility to execute re-transmissions on frequencies (hops) not affected by noise.

## FHSS Sender Block Diagram: -

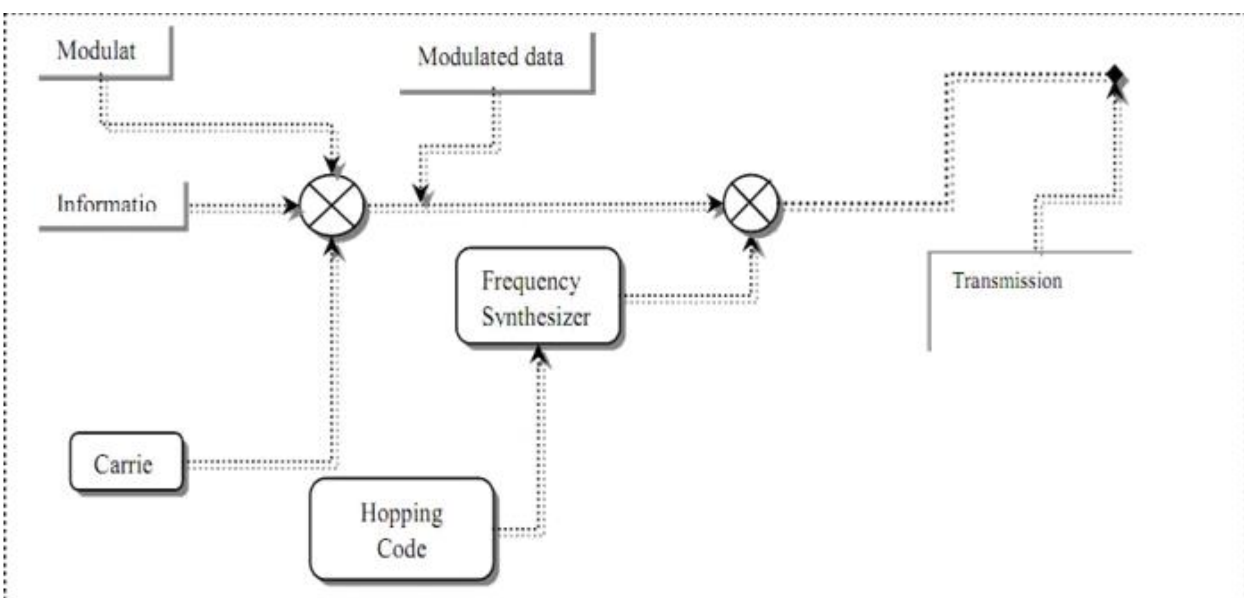



*Figure 1:Simplified Diagram for Transmitter for FHSS*

## FHSS Receiver Block Diagram:

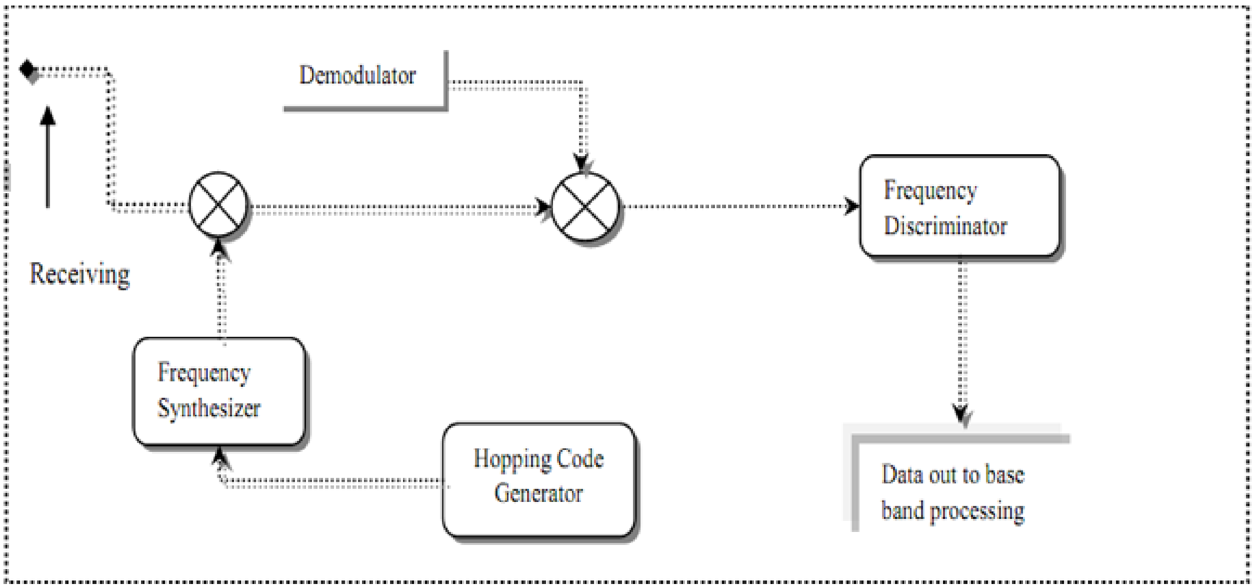



*Figure 2: Simplified diagram for Receiver for FHSS*

## Implemented Block Diagram of FHSS Transmitter: -

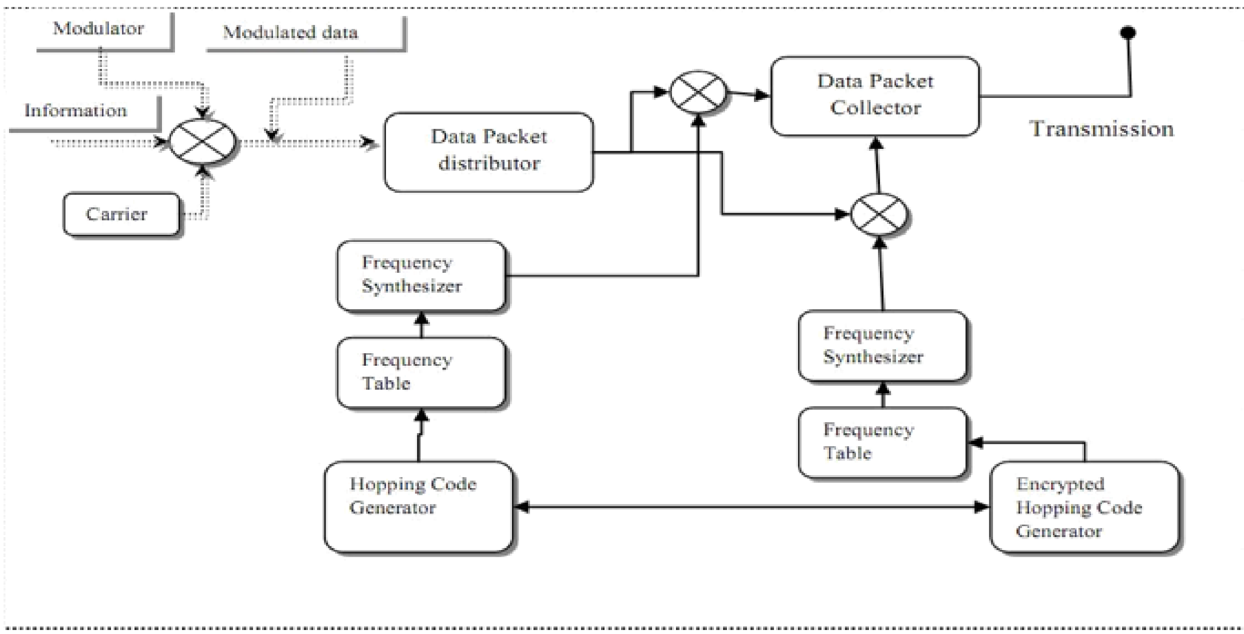



*Figure 3:Transmitter of proposed Technique*

## Explanation:

The above block diagram is the sender block that is used in FHSS. The improvised block diagram is given above where all the odd bits use the PN sequence and the even bits use the encrypted PN-sequence (GRAY CODED) for frequency synthesizing. This makes the jammer harder to find the PN –sequence because the repetition occurs after several iterations than the un improvised one.

## Realization in MATLAB:

With the help of the block diagram we are able to carry out step by step process. Firstly a bit sequence is generated, and then follows the modulation of the signal (BPSK). Then PN-sequence is generated and the even bits are replaced with its gray code and thus now we have an Improvised PN-sequence. This follows the frequency synthesizing with the help of Improvised PN-sequence. Thus finally multiply the frequencies with the modulated signal to give out the FH-spread signal. Using the grid, plot commands we managed to get the plot between frequencies and PN-sequence.

## Uses:

- Important form of encoding for wireless communication.
- Transmit either analog or digital data
- Analog signal (transmission)
- Developed initially for military and intelligence requirements
- Spread data over wider bandwidth
- Makes jamming and interception harder

# MATLAB CODE:

```
clc

clear all

close all

even=1;

odd=1;

% generate pn sequence
cp=randint(1,20,[1 7]);
%
for k=1:20

   if(mod(k,2))

       dualcode(1,k)=cp(1,k);

       evenbits(1,even)=cp(1,k);

       even=even+1;

   else

       oddbits(1,odd)=cp(1,k);

       odd=odd+1;

      const= bin2gray(cp(1,k),'psk',16);
       dualcode(1,k)=const;

   end

end

s=round(rand(1,20));

signal=[];

carrier=[];
```

```
t=[0:2*pi/119:2*pi];
for k=1:20
if s(1,k)==0
        sig=-ones(1,120);
    else
        sig=ones(1,120);
    end
    c=cos(t);
    carrier=[carrier c];
    signal=[signal sig];
end
subplot(4,1,1);
plot(signal);
axis([-100 2500 -1.5 1.5]);
title('\bf\it Original Bit Sequence');

bpsk_sig=signal.*carrier;
subplot(4,1,2);
plot(bpsk_sig)
axis([-100 2500 -1.5 1.5]);
title('\bf\it BPSK Modulated Signal');

t0=[0:2*pi/4:2*pi];
t1=[0:2*pi/9:2*pi];
t2=[0:2*pi/19:2*pi];
```

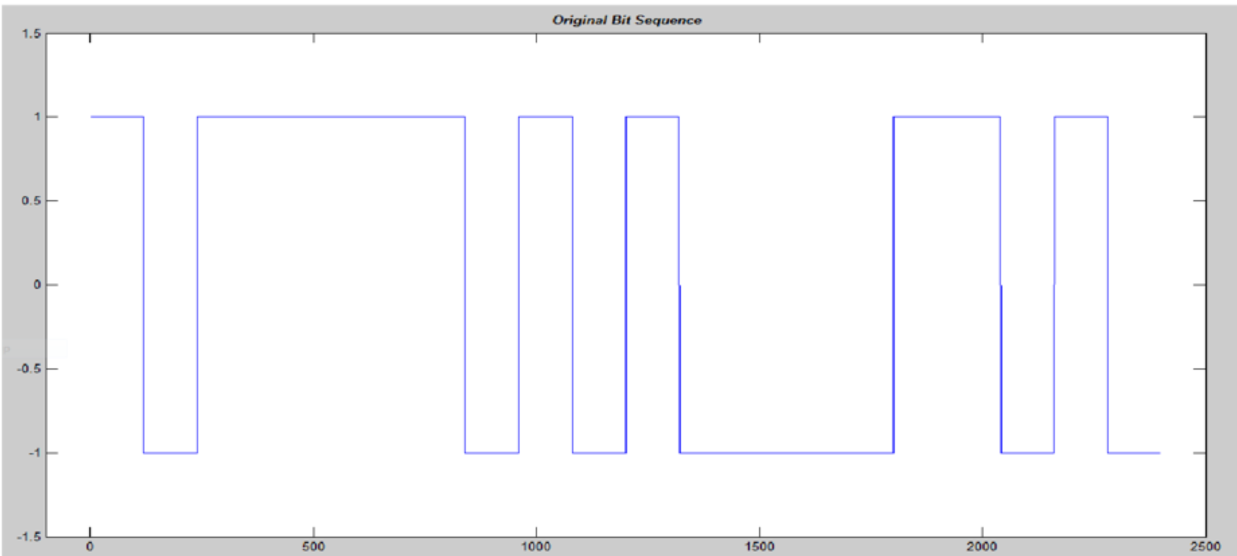
```
t3=[0:2*pi/29:2*pi];

t4=[0:2*pi/39:2*pi];

t5=[0:2*pi/59:2*pi];

t6=[0:2*pi/119:2*pi];


c0=cos(t0);

c0=[c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0

c0 c0 c0 c0];

c1=cos(t1);

c1=[c1 c1 c1 c1 c1 c1 c1 c1 c1 c1 c1
c1]; c2=cos(t2);

c2=[c2 c2 c2 c2 c2 c2];

c3=cos(t3);

c3=[c3 c3 c3 c3];

c4=cos(t4);

c4=[c4 c4 c4];

c5=cos(t5);

c5=[c5 c5];

c6=cos(t6);

% Random frequency hopps to form a spread signal

spread_signal=[];

for n=1:20

    c=dualcode(1,n);

      switch(c)

        case(1)
```

```
            spread_signal=[spread_signal
        c0]; case(2)

            spread_signal=[spread_signal
        c1]; case(3)

            spread_signal=[spread_signal
        c2]; case(4)

            spread_signal=[spread_signal
        c3]; case(5)

            spread_signal=[spread_signal
        c4]; case(6)

            spread_signal=[spread_signal
        c5]; case(7)

            spread_signal=[spread_signal c6];

    end

end

subplot(4,1,3)

plot([1:2400],spread_signal);

axis([-100 2500 -1.5 1.5]);

title('\bf\it Spread Signal with 7 frequencies');

% Spreading BPSK Signal into wider band with total of
12 frequencies freq_hopped_sig=bpsk_sig.*spread_signal;
subplot(4,1,4)
%
plot([1:2400],freq_hopped_sig);
axis([-100 2500 -1.5 1.5]);

title('\bf\it Frequency Hopped Spread Spectrum Signal');

% Expressing the FFTs


rec=freq_hopped_sig.*spread_signal;

lpf=fdesign.lowpass('n,fc',50,0.0168,119);
```

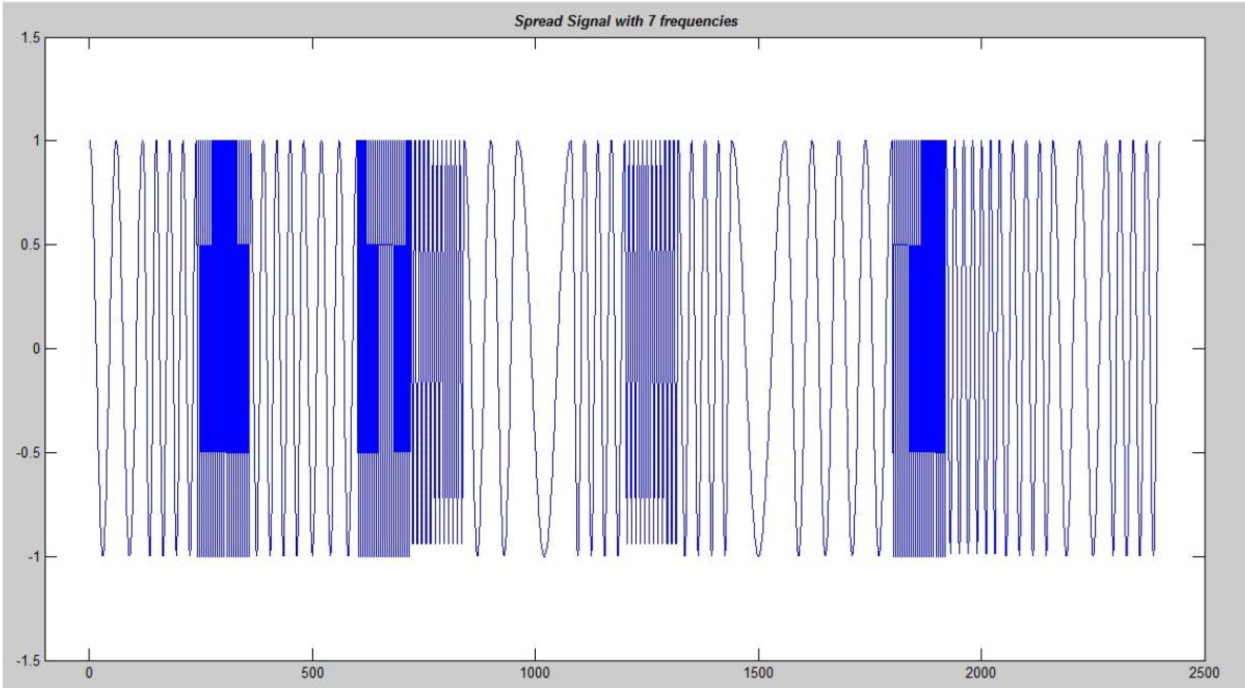
```
d=design(lpf);

j=filter(d,rec);

figure,plot(j);

figure,subplot(2,1,1)

plot([1:2400],freq_hopped_sig);

axis([-100 2500 -1.5 1.5]);

title('\bf\it Frequency Hopped Spread Spectrum signal and its
FFT');

subplot(2,1,2);

plot([1:2400],abs(fft(freq_hopped_sig)));

cc=zeros(size(dualcode));

cc=dualcode;

figure

fit=[];

for k=1:20
        sig=(cc(1,k) -
    0.5)*ones(1,10); fit=[fit sig] ;
end

plot(fit,'oblack','linewidth',8);
axis([-10 200 0 8]); grid on

hold on

for k=10:20:190

stem(k,9,'--','black')

hold on      end
```

# OUTPUTS:

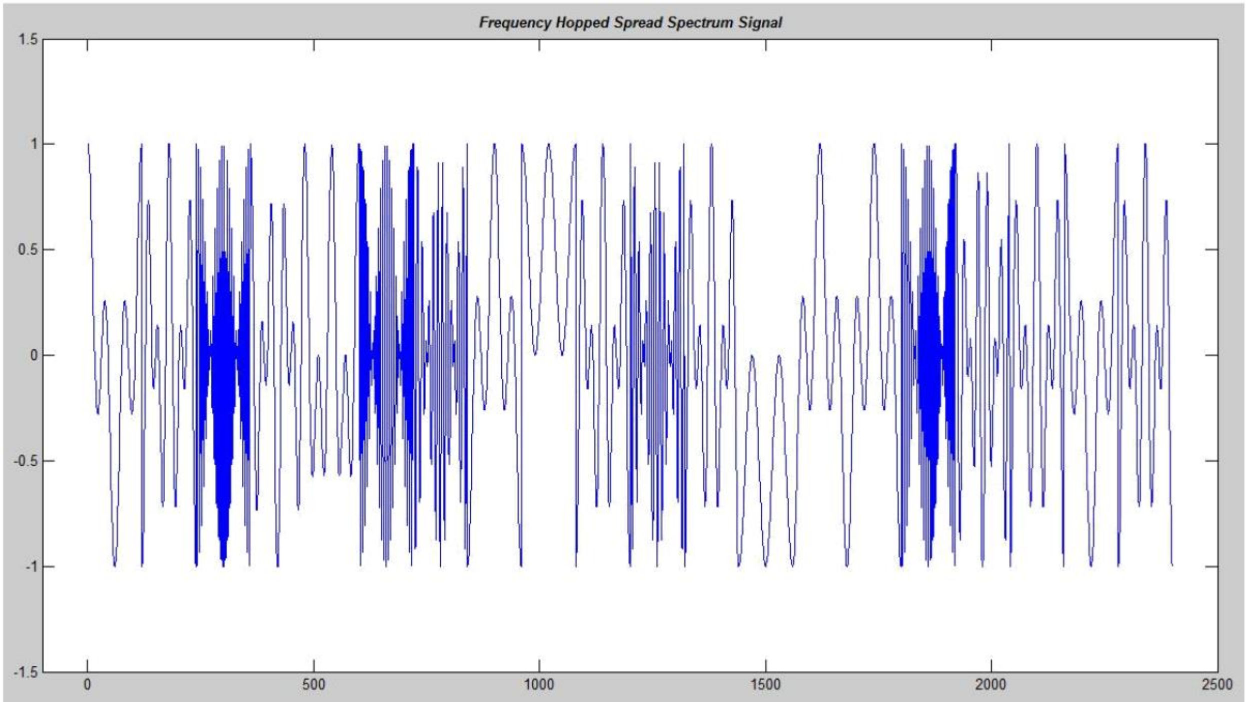
## Bit Sequence:



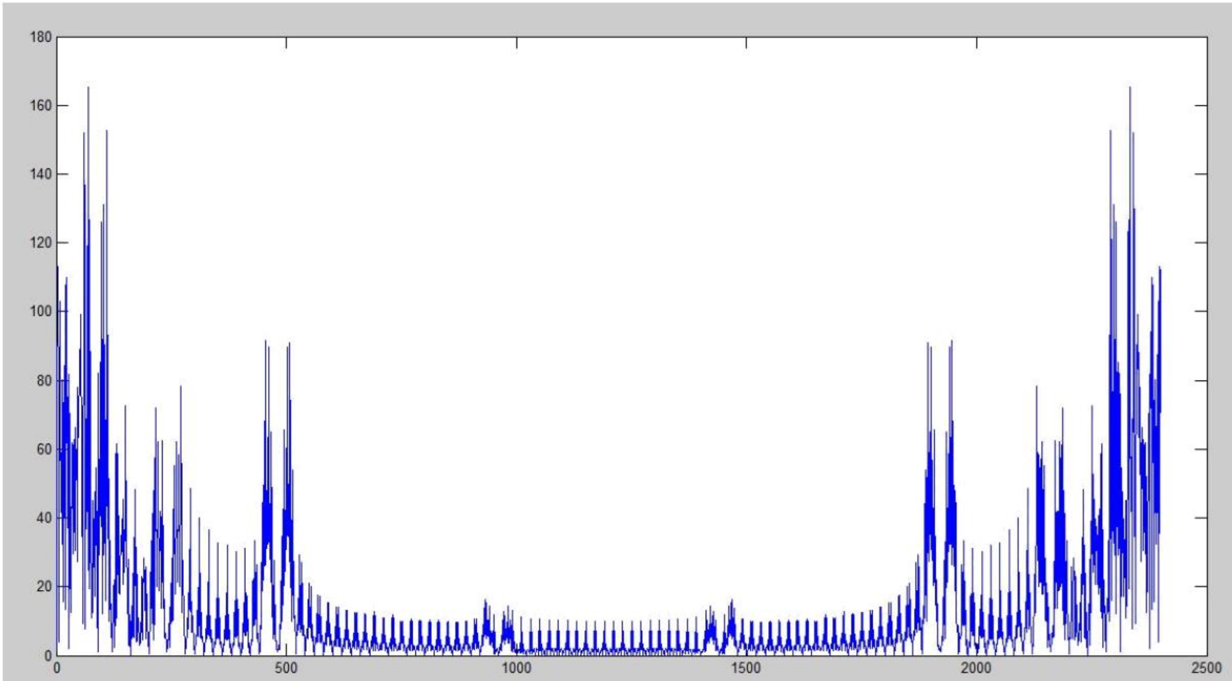
## SPREAD SIGNAL WITH SEVEN FREQUENCIES:



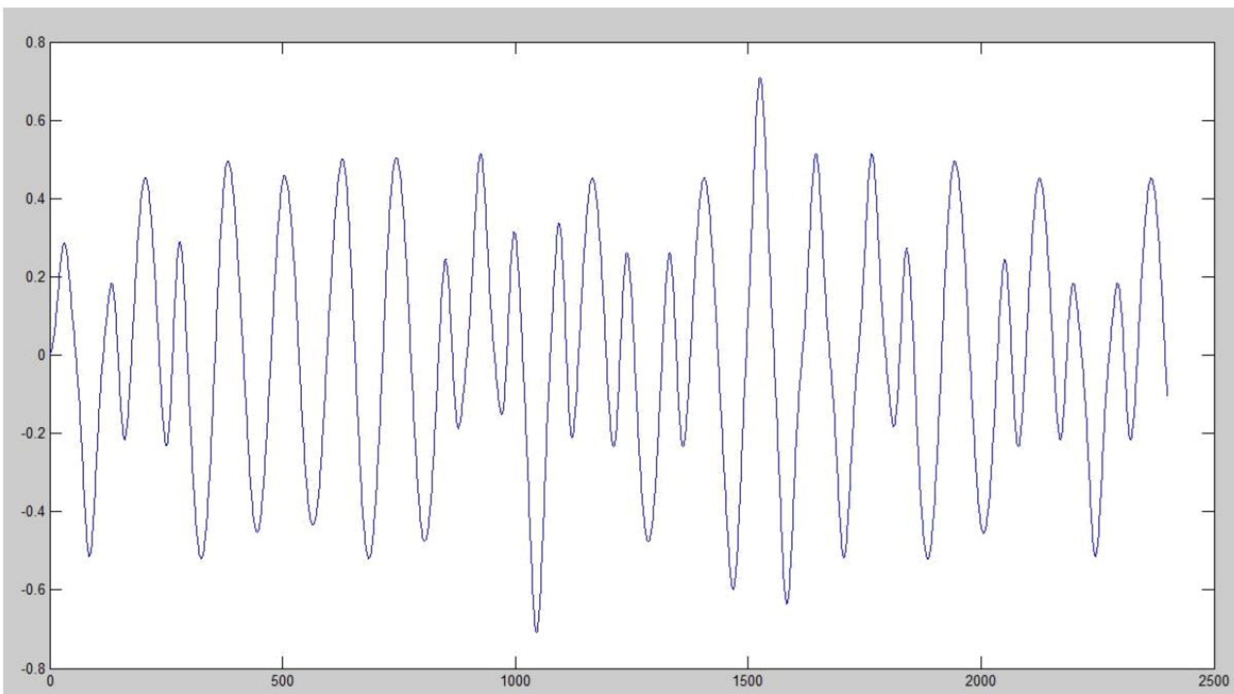

## FH-SPREAD SIGNAL:



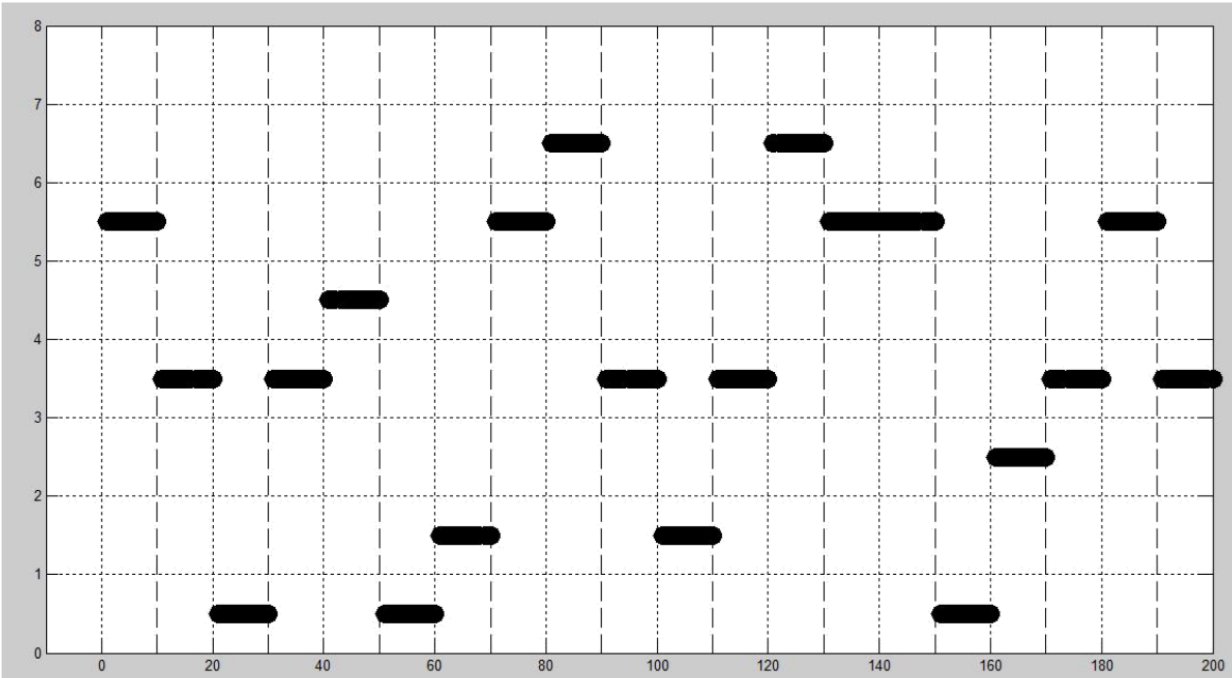
## FFT OF FH-SPREAD SIGNAL:




## DEMODULATED WAVE:



## FREQUENCY vs PN-SEQUENCE:




## BENEFITS OR ADVANTAGES OF FHSS:

Following are the disadvantages of FHSS:

- It provides very robust transmission path in the presence of interferences such as multipath, noise and other wireless transmissions etc. due to support of wide bandwidth.
- It can be employed in point to multipoint applications.
- It supports about ten nearby WLAN compliant APs (Access Points) without any significant interference issues.
- It provides security against any kind of intrusion as only transmitter and receiver are aware of PN codes.

## DRAWBACKS OR DISADVANTAGES OF FHSS:

Following are the disadvantages of FHSS:

- As FHSS relies on carrier frequencies to transmit information bits, it leads to strong bursty errors due to frequency selective fading mainly.

- It supports lower data rate of 3 Mbps compare to 11 Mbps supported by

DSSS.

- It supports lower coverage range due to high SNR requirement at receiver.
- The modulation scheme has become obsolete due to use of emerging wireless technologies in the wireless products.

## RESULT and CONCLUSION:

Thus we have tried hard to reach the aim in getting all the plots as desired and the results match with the theoretical background. FHSS is implemented in MATLAB and its fft plot gave us a clear insight on it regarding the spreading of the signal over the entire spectrum. And the improvised PN sequence is implemented to improve the security in the FHSS transmitted signals and is achieved .frequency vs PN-sequence plot gave a clear picture on how the frequency is allotted for the given PN sequence.

## Glossary

### PN Sequence:

(A pseudo noise code (PN code) or pseudo random noise code (PRN code) is one that has a spectrum similar to a random sequence of bits but is deterministically generated.)

### Gray Code:

a numerical code used in computing in which consecutive integers are represented by binary numbers differing in only one digit.
Binary Phase Shift Keying (BPSK) is a two phase modulation scheme, where the 0's and 1's in a binary message are represented by two different phase states in the carrier signal: $\theta=0\circ$

for binary 1 and θ=180∘ for binary 0.

# References


[1] Z. Haider, M. Saleem, and T. Jamal, "Analysis of Interference in Wireless", in Proc. of ArXiv, arXiv:1810.13164 [cs.NI], Oct. 2018.

[2] T. Jamal and P. Mendes, “Relay Selection Approaches for Wireless Cooperative Networks”, in Proc. of IEEE WiMob, Niagara Falls, Canada, Oct. 2010.

[3] T. Jamal, P. Mendes, and A. Zúquete, “Opportunistic Relay Selection for Wireless Cooperative Network”, in Proc. of IEEE IFIP NTMS, Istanbul Turkey, May 2012.

[4] T. Jamal and P. Mendes, “Cooperative relaying in user-centric networking under interference conditions”, in Proc. of IEEE Communications Magazine, vol. 52, no. 12, pp. 18–24, Dec 2014.

[5] P. Mendes, W. Moreira, T. Jamal, and Huiling Zhu, “Cooperative Networking in User-Centric Wireless Networks”, In: Aldini A., Bogliolo A. (eds) User-Centric Networking. Lecture Notes in Social Networks. Springer, Cham, ISBN 978-3-319- 05217-5, May 2014.

[6] T. Jamal, P. Mendes, and A. Zúquete, “Relayspot: A Framework for Opportunistic Cooperative Relaying”, in Proc. of IARIA ACCESS, Luxembourg, June 2011.

[7] T. Jamal, and SA Butt, "Malicious Node Analysis in MANETS", in Proc. of International Journal of Information Technology, PP. 1-9, Springer Publisher, Apr. 2018.

[8] T. Jamal, and P. Mendes, “COOPERATIVE RELAYING FOR DYNAMIC NETWORKS”, EU PATENT, (EP13182366.8), Aug. 2013.

[9] T. Jamal, and P. Mendes, “802.11 Medium Access Control In MiXiM”, in Proc. of Tech Rep. SITILabs-TR-13- 02, University Lusófona, Lisbon Portugal, Mar. 2013.

[10] T Jamal, M Alam, and MM Umair, "Detection and Prevention Against RTS Attacks in Wireless LANs", in Proc. of IEEE C-CODE, Islamabad Pakistan, Mar. 2017.

[11] L. Lopes, T. Jamal, and P. Mendes, "Towards Implementing Cooperative Relaying", In Proc. of Technical Report COPE-TR-13-06, CopeLabs University Lusofona Portugal, Jan 2013.

[12] T. Jamal, P. Mendes, and A. Zúquete, “Interference-Aware Opportunistic Relay Selection”, In Proc. of ACM CoNEXT student workshop, Tokyo, Japan, Dec. 2011.

[13] T. Jamal, "Cooperative MAC for Wireless Network", In Proc. of 1st MAP Tele Workshop, Porto, Portugal, 2010.

[14] T. Jamal and P. Mendes, “Analysis of Hybrid Relaying in Cooperative WLAN”, In Proc. of IEEE IFIP Wireless Days (WD), Valencia, Spain, November 2013.

[15] T. Jamal, and P. Mendes, “Cooperative Relaying for Wireless Local Area Networks”, In: Ganchev I., Curado M., Kassler A. (eds) Wireless Networking for Moving Objects. Lecture Notes in Computer Science, vol 8611. Springer, Cham, (WiNeMo), Aug. 2014.

[16] T. Jamal, and SA Butt, “Cooperative Cloudlet for Pervasive Networks”, in Proc. of Asia Pacific Journal of Multidisciplinary Research, Vol. 5, No. 3, PP. 42-26, Aug 2017.

[17] T. Jamal, P. Mendes, and A. Zúquete, “Wireless Cooperative Relaying Based on Opportunistic Relay Selection”, in Proc. of International Journal on Advances in Networks and Services, Vol. 5, No. 2, PP. 116-127, Jun. 2012.

[18] SA Butt, and T. Jamal, “Frequent Change Request from User to Handle Cost on Project in Agile Model”, in Proc. of Asia Pacific Journal of Multidisciplinary Research 5 (2), 26-42, 2017.

[19] T. Jamal, and P. Amaral, “Flow Table Congestion in Software Defined Networks”, in Proc. of IARIA 12th ICDS, Rome Italy, Mar. 2018.

[20] R. Sofia, P. Mendes, W. Moreira, A. Ribeiro, S. Queiroz, A. Junior, T. Jamal, N. Chama, and L. Carvalho, “Upns: User Provided Networks, technical report: LivingExamples, Challenges, Advantages”, Tech. Rep. SITI-TR- 11- 03, Research Unit in Informatics Systems and Technologies (SITI), University Lusofona, Lisbon Portugal, Mar. 2011.

[21] T. Jamal, and P. Mendes, “Cooperative Relaying in Wireless User-Centric Networks”, Book Chapter In: Aldini, A., Bogliolo, A. (eds.) User Centric Networking. Lecture Notes in Social Networks, Springer, Cham, pp. 171–195, 2014.

[22] T. Jamal, P. Mendes, and A. Zúquete, “Design and Performance of Wireless Cooperative Relaying”, PhD Thesis MAP-Tele, University of Aveiro, Oct. 2013.

[23] T. Jamal, P. Mendes, and A. Zuquete, “RelaySpot: Cooperative Wireless Relaying”, in Proc. of MAP-Tele Workshop, Aveiro, Portugal, May 2011.

[24] T. Jamal, and P. Mendes, “Cooperative Wireless Relaying, Key Factors for Relay Selection”, in Proc. of MAP- Tele Workshop, Porto, Portugal, Dec. 2009.

[25] SA Butt, and T. Jamal, “Study of Black Hole Attack in AODV”, in Proc. of International Journal of Future Generation Communication and Networking, Vol. 10, No.9, pp. 37-48, 2017.

[26] T. Jamal, and SA Butt, “Low-Energy Adaptive Clustering Hierarchy (LEACH) Enhancement for Military Security Operations”, In Proc. Of Journal of Basic and Applied Scientific Research, ISSN 2090-4304, 2017.

[27] T. Jamal, and P. Mendes, “RelaySpot, OMNET++ Module”, Software Simulator Extension In Proc. of COPE- SW-13-05, 2013.

[28] T. Jamal and Z. Haider, "Denial of Service Attack in Cooperative Networks", in Proc. of ArXiv, arXiv: CoRR Vol. abs/1810.11070 [cs.NI], Oct. 2018.