Secrecy Capacity of Symmetric Keys Generated by Quantising Channel Metrics Over a Fading Channel

Srividya.L[1], Dr.P.N.Sudha[2]
[1]Dept of ECE, Dayananda Sagar College of Engineering, Bangalore-560078, India
[1]lsrividyabe@gmail.com
[2]Dept. of ECE, K.S. Institute of Technology, Bangalore-560109, India
[2]pnsudha@gmail.com

Abstract. Physical layer security has become the cornerstone of the wireless communication system. Key generation by channel estimation enables legitimate users to generate keys in a decentralised manner than sharing secret information in open wireless mediums. In this paper we propose secrecy evaluation of symmetric keys which are, generated by channel metrics estimated over the Rayleigh fading channel, encrypted and transmitted over a fading channel in the presence of an eavesdropper . The results are obtained in terms of secrecy capacity and outage probability for various key sizes, different position of eavesdroppers from the source. It is seen that as key size increases and distance of eavesdropper increases from the source the secrecy capacity increases. Also the performance of keys derrived from various channel metrics such as complex channel path gains, EVM rms and complex phase difference are discussed in this paper.

Keywords: Physical layer security, key generation, one time pad encryption, channel metrics, secrecy capacity, quantisation, outage probability.

1 Introduction

Physical layer security has become the cornerstone of the communication system as loss of physical layer security results in the total exposure while other layer results without the catastrophic effect. Hence it has become a prime research area of the recent times. In the information theoretic approach, many works are being carried on implementing cryptographic algorithms at physical layer level [1]. Symmetric key encryption has become attractive due to its simplicity in implementation particularly in restricted environment where memory, processing capacity, power is a constraint. However strong the encryption algorithm might be but if the key is compromised while sharing it, results in data exposure. Hence, now a days there is a shift in the paradigm from developing computationally more complex encryption algorithm to securely generating and sharing symmetric key algorithms. Similarly however strong the key might be it is always prone to malicious attacks as it is shared over a common wireless channel which are open medium and easily accessible [2].

Hence decentralisation of key generation is the solution for this problem. The reciprocity property of the channel between the two legitimate users and its decorrelation in space, makes it secure with respect to possible illegitimate users, is used [8]. The physical layer security is predominantly focused in random time varying component of wireless channel. The physical layer measurements are the typical source of information for two legitimate users and therefore can be processed in order to obtain common bits. Key generation chain consists of channel probing, randomness extraction, quantization, information reconciliation and privacy amplification [6]. Using simple data acquisition process we can probe the channel and get time varying random metrics such as RSSI,CIR, complex channel gains, complex phase difference, EVM rms and so on. Quantization is done on the absolute scales and convert it in processable binary bit sequences[8],[9],[13]. Information reconciliation is essential as imperfect reciprocity and random noise results in mismatch of bits, reconciliation corrects and deletes these using minimum channel data. Privacy amplification is done to select number of secret bits to avoid illegitimate user to deduce the secret bit sequence.

In this paper we focus on the first part of the key generation chain that is channel probing, quantization as we generate a random symmetric key from channel metrics, encrypt, pass it to a fading channel and measure its secrecy capacity and outage probability. Here we have used One time pad encryption scheme as it is proven to achieve Shannon perfect secrecy [13]. Also it is the simplest algorithm which consumes less memory, less computation, perfect for restricted environments [11]. But requires key to be of the same size of the input. Hence we also examine secrecy capacity of the generated symmetric keys from the channel metrics over different key sizes over practical Rayleigh fading.

The rest of the paper is organised this way. Key Generation Phase, Channel Threat Model, Proposed System Model, Simulation Results and Analysis, Conclusion and Future Work.

2 Key Generation Phase

We have implemented simple data acquisition of Rayleigh channel metrics in Simulink model. We have passed an reference binary data from a discrete memory less Bernouli generator into a 16-QAM modulator and Rayleigh channel and acquired three metrics simultaneously in order to compare the results , the acquired random complex data is further processed for quantisation in order to obtain sequence of binary bits of same size of input data as one time pad encryption scheme requirement.

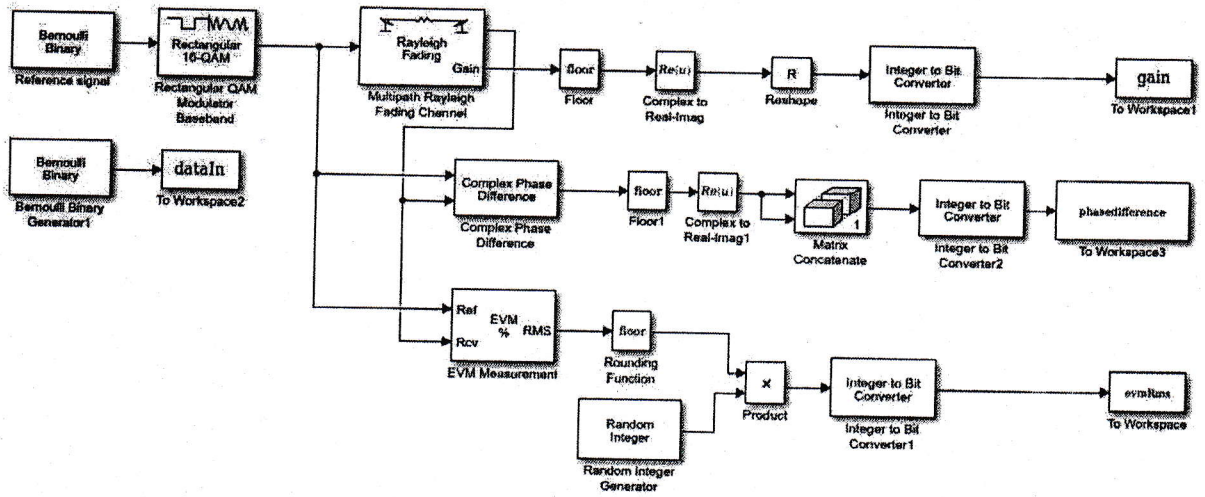


Fig. 1. Key generation from channel metrics.

Fig. 1. shows the Simulink model of the proposed key generation scheme, gain port of the Rayleigh channel block outputs the complex path gain for each path, Complex phase difference block outputs the phase difference between the two complex input signals.This we have measured before and after passing values to the channel. Its range is –pi to pi. EVM rms estimates the RMS Error Vector Magnitude (EVM) between two signals; one is reference signal and a corrupted received signal of the input frame. Power values are expressed in Watts with respect to 1 ohm.

Obtained complex values is quantised on absolute scales and processed to get binary output form. This generated binary bit sequence whose length is equal to the input data of the encryptor is taken as the input to the for OTP encryption as cryptographic symmetric key.

The simulated output is saved in the workspace of the MATLAB which is considered during the execution of the encryption and channel secrecy estimation.

3 Channel Threat Model

Fig. 2 depicts the two hop decode and forward Wyner's wiretap channel model where the information from source to destination reaches in two hops via legitimate relay. Eavesdropper is assumed to be located at a distance d_se from the source. Two legitimate nodes have been assumed to establish a secure link by one time pad encryption [9].The secrecy conditions are measured at one stop relay node which is located at a distance d_sr. Source is assumed to generate output which is the encrypted output of key generated by channel metrics and input data source.The two hop channel is assumed to be a fading wireless channel where each node has decode and forward capability. The eavesdropper channel is assumed to be degraded by a factor a.

Using this Wyner's wiretap channel model we try to evaluate the secrecy capacity by fixing the distance between legitimate relay node, d_sr, as 500m and varying the distance between the eavesdropper and the source, d_se , 50m, 500, and 1000m respectively. The secrecy capacity is further calculated from the received SNR at relay and eavesdropper.

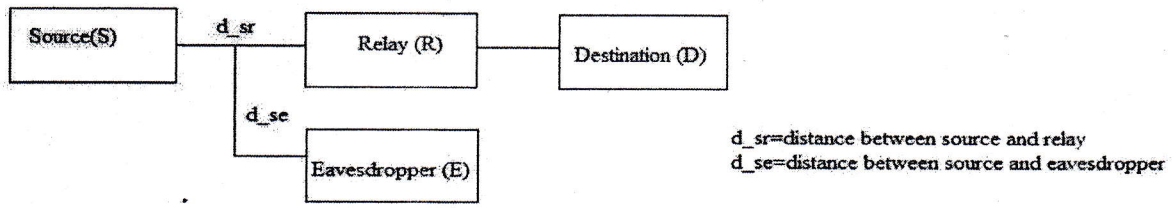


Fig. 2. Two hop DF Wyner's Wiretap Channel Threat Model

4 Proposed System Model

An input data is generated from an random generator, the key generation model is stimulated and three keys are obatained (derived from Complex path gain(gain), complex phase difference (phase difference) and EVM rms(evmRms)).The data with key (Anyone key) is encrypted. A fading legitimate channel with path loss coefficient alpha=3.5,Secrecy Rate *Rs*=0.1, noise variance -60dBm over various global transmit powers ranging from -5dBm to 35dBm is stimulated and *SNR_SR* at first hop relay at a distance of d_sr from the source is measured . We have assumed it to be 500m. Similarly a fading eavesdropper channel with path loss coefficient alpha=3.5, Secrecy Rate *Rs*=0.1, noise variance -60dBm over various global transmit powers ranging from -5dBm to 35dBm is stimulated and *SNR_SE* at first hop relay at a distance of d_se from the source is measured. We have obtained for 50m,500m,1000m and estimated total received at eavesdroppers *SNR_E_linear*. The secrecy capacity of two hop DF relying system is estimated using the formula [5]

$$P(Cs)=(1/2)*\log2((1+SNR\_SR)/(1+SNR\_E\_linear)). \quad (1)$$

The outage probability is estimated using the formula [3]

$$P(outage)=(1-(SNR\_SR/(SNR\_SR+(2\hat{}Rs)*(SNR\_SE)))*\exp(-((2\hat{}Rs)-1)/SNR\_SR)). \quad (2)$$

The graph *P*(*Cs*)Vs Global transmit power in dBm is plotted.Also the graph P(Outage)Vs Global transmit power in dBm is plotted.The above steps, for various key sizes(64,128,256,1000), channel metrics (gain, phase difference, evmRms), d_se (50m,500m,1000m), are repeated .

Here we have to remind that both sides of communication link are running algorithm at the same time but independently, we believe on the channel coherence time to slower transmission time to ensure both ends observe the same fading effects [10].

Secrecy capacity is defined as the maximum transmission rate from the source to the destination where the malicious eavesdropper is not able to access the information [12].According to the information theory to achieve this, the mutual information must satisfy the condition I[*x*:*y*]>I[*x*:*z*] where *x*=input, *y*=legitimate output, *z*=output at the eavesdropper.

Secrecy capacity(*Cs*)is the difference of capacity through the legitimate link(*Cr*) and eavesdropper link(*Ce*), which implies that the system is secure if the values of *Cs* are positive.[5]

$$Cs=[Cr-Ce]+. \quad (3)$$

Cs is a random variable as it is a function of random channel gains .Therefore we study outage probability [14]. It is the probability that the instantaneous secrecy capacity is less than a target secrecy rate *Rs*>0. Source assumes that eavesdroppers capacity *Ce'*=*Cr*-*Rs*. As long as the secrecy rate *Rs*<*Cs* the Eavesdropper channel capacity *Ce* will be worse than source estimate Ce' that is *Ce*<*Ce'*. So the wiretap codes used by the source will ensure perfect secrecy. Else if *Rs*>*Cs* then *Ce*>*Ce'* and information theoretic security is compromised.

When *SNR_SR*>>*SNR_SE*; outage probability is $=(1-\exp(-((2\hat{}Rs)-1)/SNR\_SR))$. (4)

While *SNR_SE*>>*SNR_SR*; outage probability approaches unity [3, 15].

In our proposed model we try to analyse the effect of key size and complexity on the secrecy of the channel. whether we are able to achieve secure transmission still with the trade off of key size and complexity. Also we try to analyse the effect of position of eavesdropper, in this situation, on the secrecy capacity of the channel.

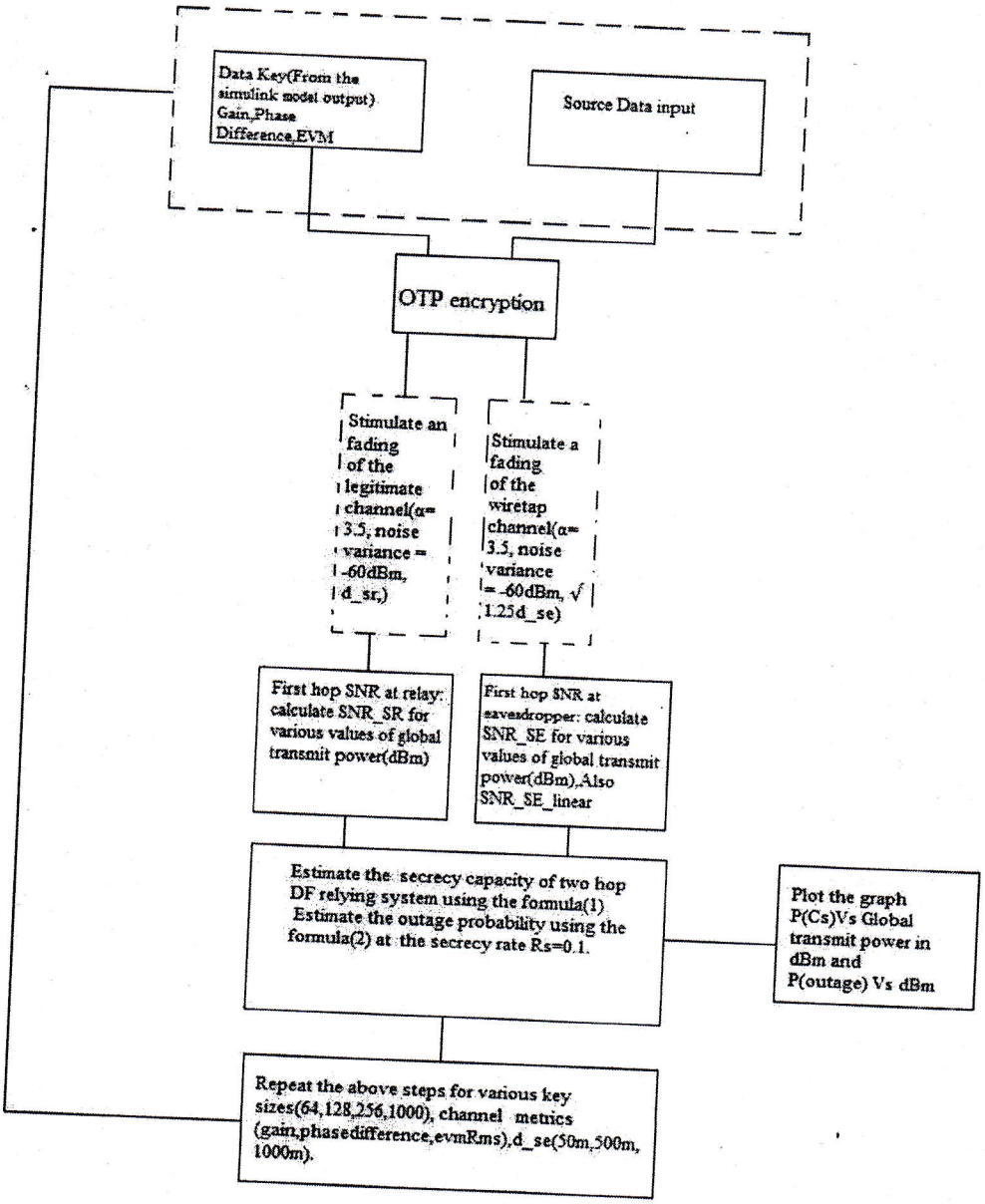
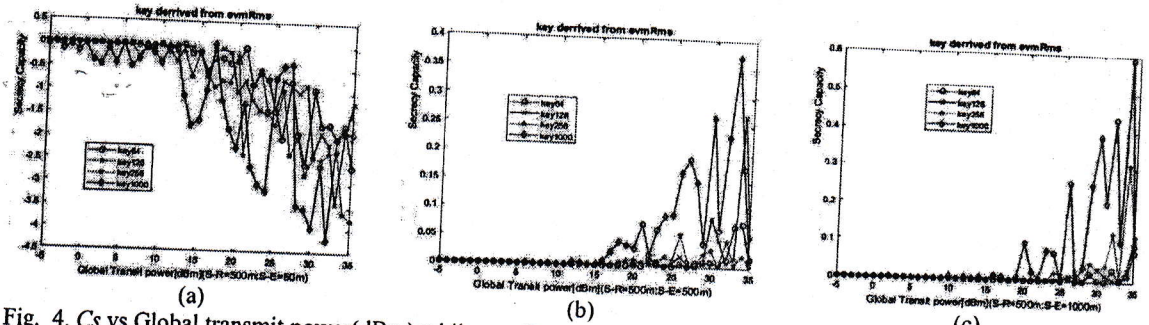


Fig. 3. Flow chart of the proposed system model

5 Stimulation Results And Analysis

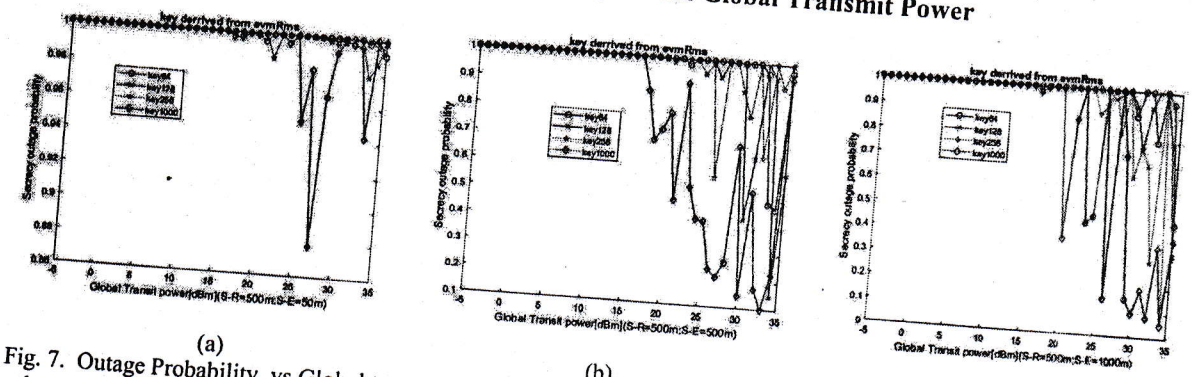
5.1 Stimulation Results for Secrecy Capacity versus Global Transmit Power



(a) (b) (c)

Fig. 4. *Cs* vs Global transmit power(dBm) while evmRms taken as input for key. The graphs a,b,c,shows the variation of *Cs* with respect distance from source to the eavesdropper at 50m,500m and 1000m respectively.

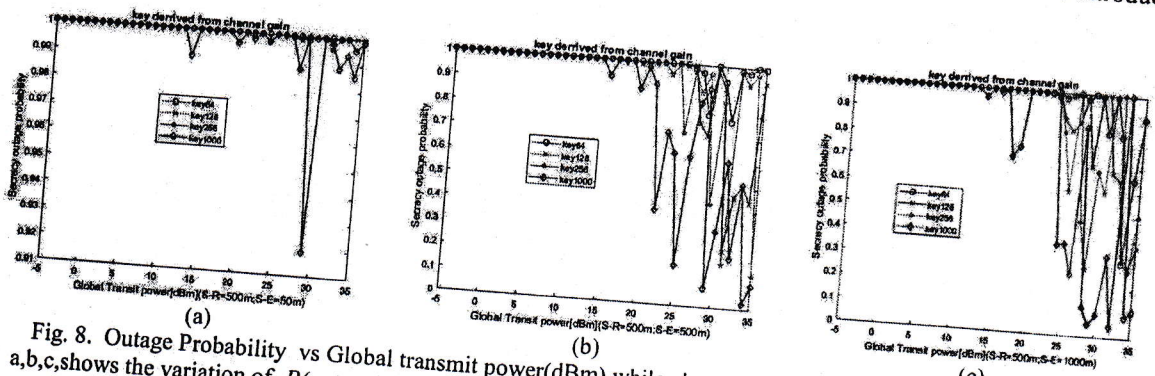
5.2 Stimulation Results For Outage Probability Versus Global Transmit Power



(a) (b) (c)

Fig. 7. Outage Probability vs Global transmit power(dBm) while evmRms taken as input for key. The graphs a,b,c,shows the variation of *P(outage)* with respect distance from source to the eavesdropper at 50m,500m and 1000m respectively.

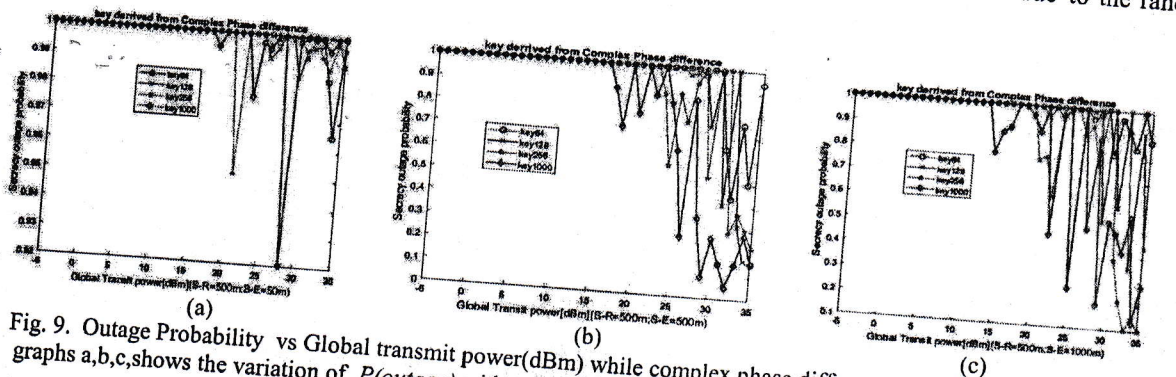
Fig.7. shows the simulation results of the outage probability versus global transmit power(dBm) taking the evmRms as input for key. Also each graph contains four plotting with respect to different key sizes 64bits, 128bits, 256bits, 1000bits. Graph(a) shows that outage probability is unity as theoritical values but dips at higher power level and key sizes . Graph (b) and (c) shows that as the eavesdropper moves away and number of bits increases the outage probability decreases hence giving more probabilty of high secrecy capacity at the given secrecy rate which is taken as 0.1. The spikes in between is due to the random function introduced in fading.



(a) (b) (c)

Fig. 8. Outage Probability vs Global transmit power(dBm) while channel gain taken as input for key. The graphs a,b,c,shows the variation of *P(outage)* with respect distance from source to the eavesdropper at 50m,500m and 1000m respectively.

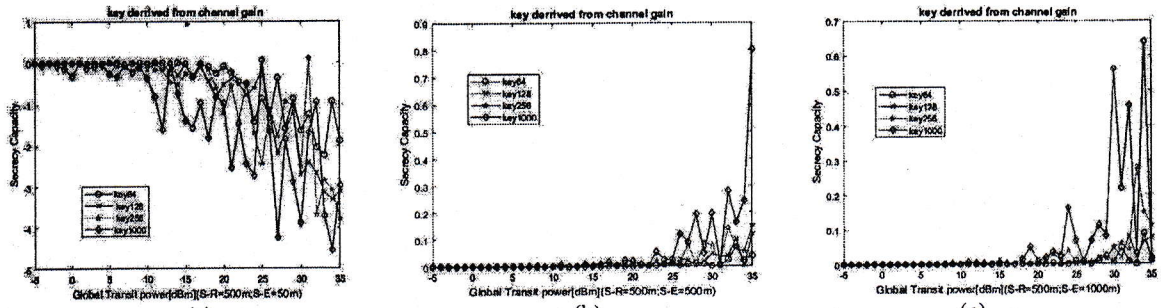
Fig.8. shows the simulation results of the outage probability versus global transmit power(dBm) taking the complex channel path gains as input for key. Also each graph contains four plotting with respect to different key sizes 64bits, 128bits, 256bits, 1000bits. Graph (a) shows that outage probability is unity as theoritical values but dips at higher power level and large key sizes . Graph (b) and (c) shows that as the eavesdropper moves away and number of bits increases the outage probability decreases hence giving more probabilty of high secrecy capacity at the given secrecy rate which is taken as 0.1. The spikes in between is due to the random function introduced in fading.



(a) (b) (c)

Fig. 9. Outage Probability vs Global transmit power(dBm) while complex phase difference taken as input for key. The graphs a,b,c,shows the variation of *P(outage)* with respect distance from source to the eavesdropper at 50m,500m and 1000m respectively.

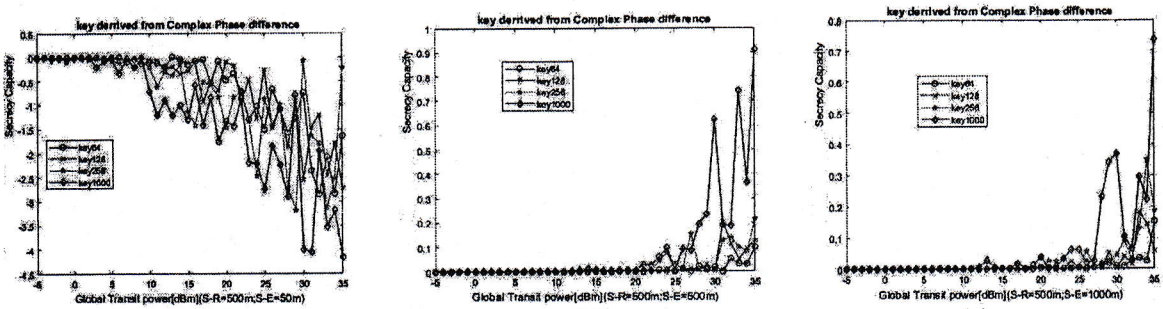
Fig.4. shows the simulation results of the secrecy capacity versus global transmit power(dBm) taking evmRms as input for key. Also each graph contains four plotting with respect to different key sizes 64bits, 128bits, 256bits, 1000bits. Graph (a) shows that secrecy capacity is negative irrespective of power level hence secrecy is lost. Graph (b) and (c) graph shows that as the eavesdropper moves away and number of bits increases the secrecy capacity increases.



(a) (b) (c)

Fig. 5. *Cs* vs Global transmit power(dBm) while channel gain taken as input for key. The graphs a,b,c,shows the variation of *Cs* with respect distance from source to the eavesdropper at 50m,500m and 1000m respectively.

Fig.5. shows the simulation results of the secrecy capacity versus global transmit power(dBm) taking the complex channel path gains as input for key. Also each graph contains four plotting with respect to different key sizes 64bits, 128bits, 256bits, 1000bits. Graph (a) shows that secrecy capacity is negative irrespective of power level hence secrecy is lost. Graph (b) and (c) shows that as the eavesdropper moves away and number of bits increases the secrecy capacity increases.



(a) (b) (c)

Fig. 6. *Cs* vs Global transmit power(dBm) while complex phase difference taken as input for key. The graphs a,b,c,shows the variation of *Cs* with respect distance from source to the eavesdropper at 50m,500m and 1000m respectively .

Fig.6. shows the simulation results of the secrecy capacity versus global transmit power(dBm) taking the complex phase difference as input for key. Also each graph contains four plotting with respect to different key sizes 64bits, 128bits, 256bits, 1000bits. Graph(a) shows that secrecy capacity is negative irrespective of power level hence secrecy is lost. Graph (b) and (c) shows that as the eavesdropper moves away and number of bits increases the secrecy capacity increases.

Analysis for effect of channel metrics on secrecy capacity

As key size increases the secrecy capacity is becoming more positive. At lower transmit powers,secrecy capacity increase above *Rs* when channel gain is taken as input for key. Similarly at higher transmit powers gain and phase difference as the input for key achieves high *Cs* values.

Fig.9. shows the simulation results of the outage probability versus global transmit power(dBm) taking the complex phase difference as input for key. Also each graph contains four plotting with respect to different key sizes 64bits, 128bits, 256bits, 1000bits. Graph (a) shows that outage probability is unity as theoritical values but dips at higher power level and large key sizes . Graph (b) and (c) shows that as the eavesdropper moves away and number of bits increases the outage probability decreases hence giving more probabilty of high secrecy capacity at the given secrecy rate which is taken as 0.1. The spikes in between is due to the random function introduced in fading.

Analysis for effect of channel metrics on outage probability

As key size increases the outage probability dips at the earliest compared to lower key sizes,which means that even at low power levels and $SNR\_SE > SNR\_SR$ we are able to achieve transmission rate greater than secrecy rate hence acheiving secrecy with larger key sizes.The performance while taking phase difference as input for key at lower transmit powers (around 15dBm)and evmRms, gain at relatively high transmit power(around 20dBm) is at its best comparatively.

6 Conclusion And Future Work

A key generation scheme was proposed using channel metrics which was acquired by stimulating Rayleigh fading channel and encrypted with the information data and transmitted over an fading channel. The performance evaluation of various keys sizes, channel metrics and d_se were conducted and analysed under various global transmit powers.

Higher key sizes resulted in better secrecy capacity compared to low sized keys and also in case of outage probability it resulted in better performances.It is affirmed that as the distance between eavesdropper and source increases secrecy capacity increases and outage probability decreases.

The performances as various channel metrics as a key input were evaluated and each proved better at various combination of transmit power levels and d_se. The performance while taking phase difference as key input at lower transmit powers (around 15dBm)and evmRms, gain at relatively high transmit power(around 20dBm) was having better secrecy capacity. In case of outage probability, phase difference as key input had less outage probability at lower power levels (around 15 dBm)while gain, evmRms had better performance at 20dBm.

Further this work can be improvised by information recounciliation and privacy amplification. Also can be extended by improvising its BER performances over fading channels by error control coding mechanisms[7].

References

1. Srividya.L, Dr.P.N.Sudha.: literature survey on recent audio encryption techniques, International Journal of Electronics and Communication Engineering and Technology (IJECET) Volume 7, Issue 6, Article ID: IJECET_07_06_013, pp. 91–95 (2016)
2. Srividya.L, Dr.P.N.Sudha.: Physical Layer Secret Symmetric Key Generation and Management Techniques for Wireless Systems-A Study, JASC: Journal of Applied Science and Computations, ISSN NO: 1076-5131,Volume VI, Issue II (2019) .
3. Bloch M., Barros.J., Rodrigues,M.,McLaughlin,S..: Wireless Information-Theoretic Security, IEEE transactions on information theory, vol. 54, no. 6 ,2515-2534 (2008)
4. Barros,J.,Rodrigues,M..: Secrecy Capacity of Wireless Channels,IEEE transaction.
5. Nosrati,E., Wang,X., Khabbazibasmenj,A..: Secrecy Capacity Enhancement in Two-hop DF Relaying Systems in the Presence of Eavesdropper, IEEE ICC - Communication and Information Systems Security Symposium 7365-7369 (2015)
6. Tunaru,I.:Physical layer secret key generation for decentralized wireless networks, Signal and Image processing, Université Rennes1, Europe (2015)
7. Dr.P.N.Sudha.:Speech compression and error correction for mobile communication, JNTU, anantapur, India (2012)
8. Wang,T.,Liu,Y.,Vasilakos,A..: Survey on channel reciprocity based key establishment techniques for wireless systems, Published online: 13 January 2015 Springer Science+Business Media New York (2015)
9. Sahin,C.,Katz,B.,Dandekar,K..:Secure and Robust Symmetric Key Generation Using Physical Layer Techniques Under Various Wireless Environments,IEEE 211-214 (2016)
10. KOSTOV,N.:Mobile Radio Channels Modeling in MATLAB, n. kostov, mobile radio channels modeling in MATLAB.
11. Harrison,W.:Physical-layer security: practical aspects of channel coding and cryptography, Georgia Institute of Technology,(2012)
12. Padala,A.,Kommana,K.:Performance of Physical Layer Security with Different Service Integrity Parameters, Blekinge Institute of Technology SE-37179 Karlskrona, Sweden.