Generation of Simple Symmetric Key Generation Scheme Based on Channel Reciprocity for Wireless Communication

[1]Srividya.L,[2] Dr.P.N.Sudha

[1]Dept of ECE,Dayananda Sagar College of Engineering [2]Dept. of ECE, K.S. Institute of Technology

[1]srividyanag@gmail.com, [2]pnsudha@gmail.com

Abstract.

In this paper we have designed an algorithm to generate a symmetric key for encrypting the data and making it secured to transmit over a mobile wireless channel using physical layer security parameters. The term physical layer security is used as the physical layer parameters of a wireless channel are used to generate the key removing undesirable attributes of the wireless channel such as noise, attenuation, delays etc. The obtained channel parameters are random in nature but are correlated between the sender and receiver channel.[1]

We have designed the key generation algorithm based on reciprocity theorem and the key generated at legitimate receivers have a better BER performances over the adversary's node which is though assumed to have full information about the key generation algorithm and located right next to the legitimate user.

Keywords. symmetric key generation, channel reciprocity, Bit error rate, Wireless mobile communication, Rayleigh channel, MATLAB®, Simulink®.

1. INTRODUCTION

Despite the popularity of wireless systems in every application these days, wireless communication still falls short to fully fledged implementation because of security. Due the broadcast nature of the medium, anyone who is in the vicinity of the transmission range can receive the signal which leads to a serious security issue of eavesdropping. This not only endangers the confidentiality of the information but also integrity between legitimate users. [12]

Key generation and its management play a prime role in secure communication as however strong the encryption algorithm might be but if the key is compromised, strength of the encryption algorithm becomes trivial. Hence our research work is focussed on secured key generation algorithm for symmetric encryption as most of the symmetrical encryption algorithms are complex, low cost and secured but distribution of the key is one a tedious process .Hence this drawback is overcome in this proposed algorithm, here we share the key in a decentralized manner.[2]

Traditional key generation and management schemes suffer either by high implementation cost or complex computational abilities and get compromised when the adversary has higher computational abilities. [3]

Wireless physical layer security approaches can prevent eavesdropping without upper layer data encryption. This technique which is based on channel reciprocity is appealing due to its ease in implementation, less energy consumption and low computational complexity. .[1],[4],[12]

However, such techniques are hindered by time-varying wireless channel conditions and they are typically feasible only when the legitimate partners in the Wyner's wire-tap channel model have an advantage over the source-eavesdropper channels.[4], [5]

We have considered a wireless SISO Rayleigh channel as it is suitable model for urban environment on radio signals, for the correlated measurements between legitimate users, to generate the symmetric key. [6] The impulse response of the channel, which is same when correlated observations are done from both the sender and receiver sides is estimated and converted in to the binary data. This binary data generated is used as key for symmetrical encryption.

Similar key generation setup is made at the adversary's side assuming that it is few meters away from the link.

Sender encrypts the data with its own key and transmits the data over an open wireless medium where the legitimate users and adversaries receive it and tries to decrypt with their respective keys.[9]

Results show a better BER at legitimate receiver's compared to the adversary's who is just few meters away from the legitimate user and assumed to have full information of key generation algorithm.

The rest of the paper is organised in this manner, section 2 describes the proposed system model. Key generation algorithm is shown in the section 3. In Section 4 implementation of the proposed scheme is discussed. We have results in section 5, Conclusions and Future scope is suggested in the last section 6.

2. SYMMETRIC KEY ENCRYPTION

There is a shift in the standard from developing high computationally complex encryption algorithm to secure secret key generation for any simple encryption algorithm.

Symmetric key generation is popular due to its simplicity, less complex especially under restricted environment such as in computation, memory, power etc. The only criterion is that legitimate users has to posses same secret key .

This is really challenging for a open medium such as wireless where the information is broadcasted and can be easily captured by the adversary.

3. WIRELESS CHANNEL CHARECTERISTICS FOR KEY GENERATION

Wireless key generation is based on the channel characteristics and their variation over the various domains like time, frequency and space.

phase ,received signal strength, narrow band channel impulse response, multiple channels, relative node distance, angle of arrival, special equipment like reconfigurable antennas, jamming mechanisms, IR-UWB channel impulse response and so on are the some of the attributes from which the keys are generated.

Some of the key generation models with wireless channels are Source model, Extended source model, Wiretap channel model, Source-emulation channel model, Reciprocity based channel model , Alternate models.[3]

4. PROPOSED SYSTEM MODEL

The block diagram as show in the Fig: 1. shows the Wyners model for the proposed scheme. At sender's node (Alice) we have an information source which contains the critical data to be transmitted to the legitimate receiver node (Bob), followed by key generation block which is explained in detail in the next section. The generated key is encrypted using one-time padding encryption scheme which is supposed to have perfect secrecy according to Wireless Information-Theoretic Security [5], [8].

Encrypted data is transmitted over a wireless Rayleigh channel which is assumed to be received by both legitimate receiver and the adversary (Eve), who has the same key generation algorithm as legitimate receiver.

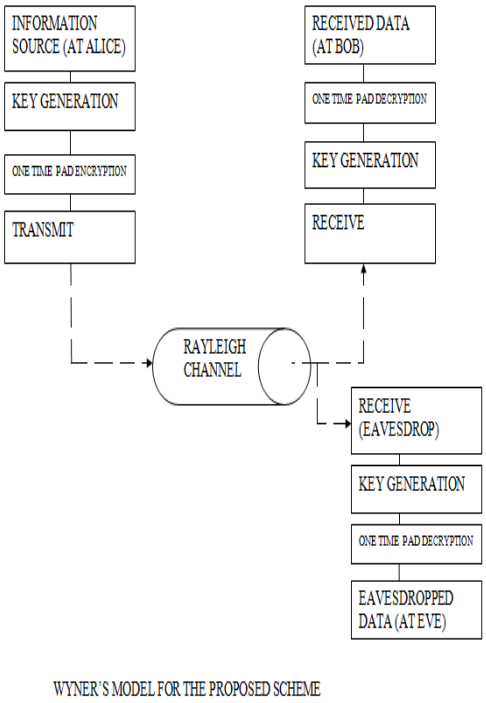


Fig: 1 Proposed scheme

5. KEY GENERATION ALGORITHM

Step1: Send a random binary data (X) into the channel and measure the output(Y).

Setp2: Measure the response H=(Y/X) using inverse Fourier transform.

Step3: Quantize H using a uniform encoder and convert it into bits which are used as key in encryption/decryption process.

Setep4: Repeat for each frame of data.

6. IMPLEMENTATION

The key generation scheme is implemented using Simulink® as we try to measure channel response simultaneously at Alice, Bob and Eve. A random data is generated using Bernoulli random generator block which is modulated by QPSK block and given into a SISO Rayleigh channel.[10] as shown in Fig:2.

Within the key generation block the system impulse response is measured using Discrete Transfer Function Estimator block and converted to time domain using IFFT block (h (t)). The h (t) is quantised using a uniform encoder block and converted into binary data using integer to binary conversion block. The generated output is forwarded to MATLAB® workspace for encryption and transmission. The entire key generation setup is made exactly as Bob at the Eve's except that the channel is multiplied by the variance which is characterized by their respective distances.

Standard deviation of each channel is assumed as 1/distance for a simple transmission.

Channel = sqrt(variance)*(randn(1,N)+j*randn(1,N)); (1)

where N is the random number distributed over a Rayleigh function.

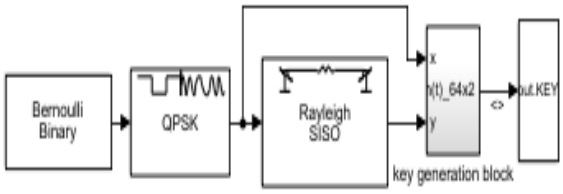


Fig 2: Key generation simulation

The proposed system model is implemented using MATLAB®. [11]

A random binary data is generated and is encrypted using sender's secret key. The encrypted data is modulated and transmitted over a wireless Rayleigh channel. Both at the Bob and Eve, the data is received, demodulated and decrypted using their respective keys.

7. RESULTS AND IMPLICATIONS

The BER of each tranmission for various Eb/N0 levels is measured at both Bob and

Eve. Four different scenerios are studied by placing Eve almost (1)at Alice ,(2)between Alice and Bob (3)at Bob (4)away from both Alice and Bob. Illustration of these cases is as shown in the Fig.3.

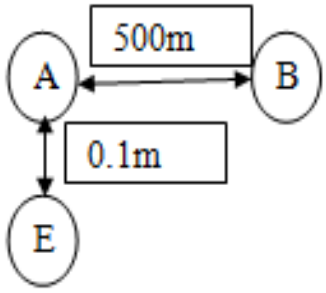
Table. 1. Shows the correlation between the generated keys at Bob and Eve. It is seen that key correlation is of low degree even when she is at Alice and Bob location but experience different channel response and hence derive a different key with low degree or no correlation between them.

Fig: 4. show the comparison of BER Vs Eb/N0 at Bob and Eve for the given scenarios.

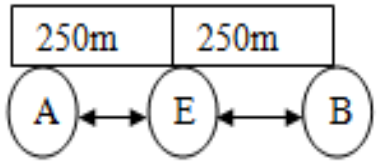
As we can see a typical BER curve for Rayleigh channel at Bob's by successfully decrypting the Alice's data with the Bob's key which was generated in a decentralised manner. Whereas Eve's BER is constantly high as key mismatches with the Alice's.

keysize=256, Doppler frequency=384Hz/70kmph,KGR=6bps				
Case	1	2	3	4
Bob-Alice(distance in m)	500	500	500	500
Eve-Alice(distance in m)	0.1	250	500	750
key correlation(Bob-Eve)	0.0409	-0.0465	0.0127	-0.0013
key correlation(Bob-Alice)	1	1	1	1

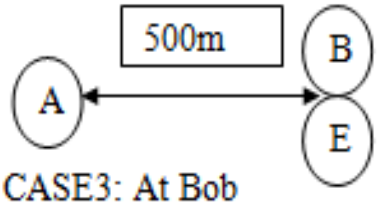
TABLE: 1 COMPARISON OF KEYS FOR CORRELATION



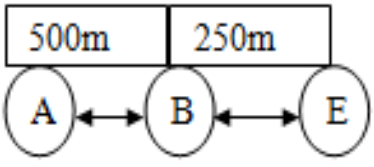
CASE1: At Alice



CASE2: Between Alice and Bob

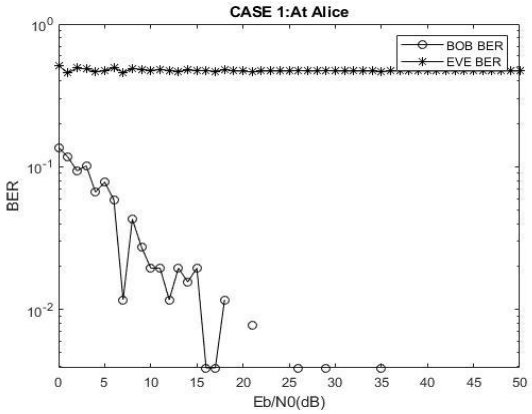


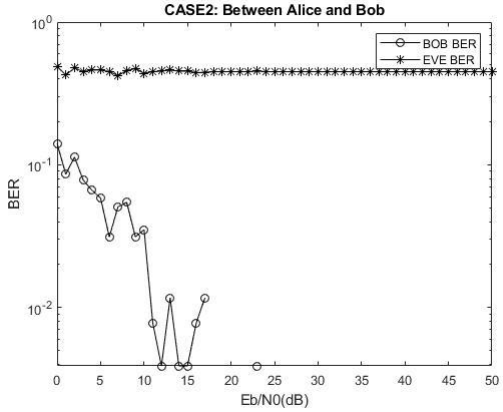
CASE3: At Bob



CASE4: Far from Alice and Bob

Fig: 3 Different scenarios for Eve's location


CASE 1:At Alice
BOB BER
EVE BER
BER
Eb/N0(dB)


CASE2: Between Alice and Bob
BOB BER
EVE BER
BER
Eb/N0(dB)

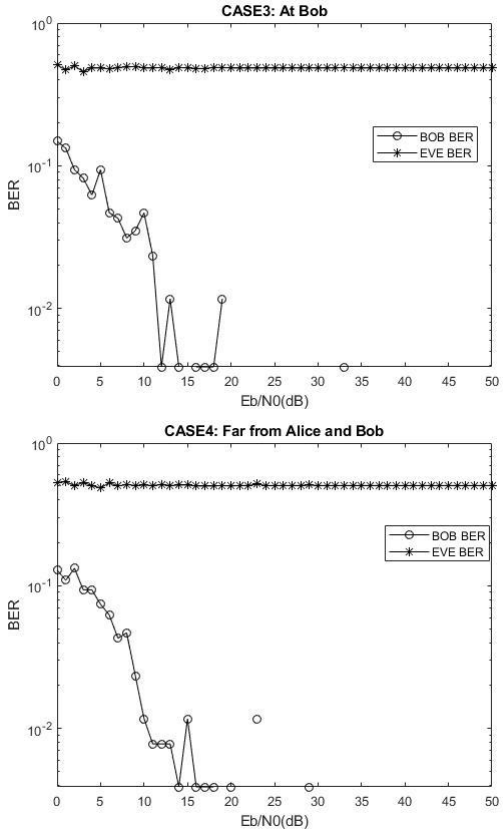


Fig: 4 comparison of BER performance for transmission of encrypted bits at BOB and EVE over Rayleigh channel.

	BER							
distance from Alice (in m)	500	0.1	500	250	500	500	500	750
Eb/N0 dB	bob	eve	bob	eve	bob	eve	bob	eve
0	0.117188	0.484375	0.15625	0.492188	0.140625	0.53125	0.15625	0.5
5	0.058594	0.496094	0.105469	0.535156	0.0625	0.492188	0.082031	0.464844
10	0.015625	0.523438	0.011719	0.542969	0.0234375	0.5	0.042969	0.464844
15	0.015625	0.507813	0.003906	0.542969	0.00390625	0.488281	0	0.46875
20	0.003906	0.503906	0	0.539063	0.0078125	0.492188	0.007813	0.460938
25	0	0.507813	0	0.539063	0	0.484375	0	0.46875
30	0	0.507813	0	0.539063	0	0.484375	0	0.46875
35	0	0.507813	0	0.539063	0	0.484375	0	0.46875
40	0	0.507813	0	0.539063	0	0.484375	0	0.46875
45	0	0.507813	0	0.539063	0	0.484375	0	0.46875
50	0	0.507813	0	0.539063	0	0.484375	0	0.46875

TABLE:2 . COMPARISON OF BER VS EB/N0 AT BOB AND EVE

8. CONCLUSIONS AND FUTURESCOPE

Based on the channel reciprocity, symmetric keys were generated using the parameters of the mobile wireless channel in a decentralised manner. The symmetric keys of the legitimate users were correlated and identical whereas key generated by adversary's had low degree correlation/no correlation. Hence the overall BER performance at the legitimate receiver node was outstanding compared to that of adversary's.

This work was conducted for a theoretical Rayleigh channel model, further it can be extended to V2V scenario by developing complex channel models and different Doppler's scenarios and taking space dimension into consideration.

Also the BER performance of the legitimate link can be further improvised by suitable adaptable error control coding techniques hence achieving secured and errorless wireless transmissions in mobile scenarios. [13]

9. REFERENCES

[1] Amang Sudarsono, Mike Yuliana, and Prima Kristalina, A Reciprocity Approach for Shared Secret Key Generation Extracted from Received Signal Strength in The Wireless Networks, 2018 International Electronics Symposium on Engineering Technology and Applications (IES-ETA)

[2] Gowda NC, Srivastav PS, Guru M, "StegCrypt (Encryption Using Steganography)", International Journal of Engineering and Advanced Technology (IJEAT), pp. 224-229, May 2019.

[3] S Basha, S. M., Poluru, R. K., & Ahmed, S. T. (2022, April). A Comprehensive Study on Learning Strategies of Optimization Algorithms and its Applications. In *2022 8th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-4). IEEE.

[4] Junqing Zhang, Trung Q. Duong,Alan Marshall, and RogerWoods, Key eneration From Wireless Channels: A Review, VOLUME 4, 2016,IEEE

[5] C. E. SHANNON, A Mathematical Theory of Communication, The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.

[6] KOSTOV,N.:Mobile Radio Channels Modeling in MATLAB, n. kostov, mobıle radıo channels modelıng ın MATLAB.

[7] 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)

[8] Bloch M., Barros.J., Rodrigues,M.,McLaughlin,S..: Wireless Information-Theoretic Security, IEEE transactıons on ınformatıon theory, vol. 54, no. 6 ,2515-2534 (2008)

Books:

[9] Xiangyun Zhou, Lingyang Song,Yan Zhang,Physical layer security in wireless communications, ©2014 by Taylor & Francis Group,LLC.

[10] Arthur A. Giordano & Allen H. Levesque, modeling of digital Communication systems using simulink®, Copyright © 2015 by John Wiley & Sons, Inc. All

[11] John G. Proakis, Masoud Salehi, Gerhard Bauch, Contemporary Communication Systems
Using MATLAB®,third edition,© 2013, 2004 Cengage Learning.

Thesis:

[12] Ahmed, S., Guptha, N., Fathima, A., & Ashwini, S. (2021). Multi-View Feature Clustering Technique for Detection and Classification of Human Actions.

[13] Dr.P.N.Sudha," Speech compression and error correction for mobile communication," JNTU, anantapur, India, August-2012.