Secret key Capacity for Wireless Nakagami and Suzuki Fading Channels

Ali Shahzadi1[†] and Masoud Ghoreishi Madiseh[††] and Ali A. Beheshti Shirazi[†††],

Iran University of Science and Technology, Tehran, Iran

Summary
Security of wireless transmission is a great challenge in secure communications. Classical methods are based on cryptographic algorithms. These methods require a secret key that must be generated securely between associated parties in communication. Another approach to security is based on wiretap channel concept and is applicable for wireless communications. Because of rather small secrecy capacity of this method, it is useful for initial secret key establishment process between communication sides. In this paper we introduce a communication model for secret key extraction from fading of channel and calculate the secrecy capacity for Nakagami and Suzuki fadings which are two complicated models having suitable matching with practical measurements.

Key words:
Secret key capacity, mutual information, Nakagami fading, Suzuki fading.

1. Introduction

Nowadays, the widespread use of wireless and mobile communications has stimulated the research on its related subjects. One of the critical problems in wireless communications is security of data transmission. Because of broadcast nature of wireless communication, the channel is accessible by all in the propagation range of radios and this makes new challenges compared with wired communications. Although, the overall security architecture for a complete network covers many aspects, but in this paper we focus on privacy of data transmission.

Classical approaches to data privacy are based on cryptographic methods. These methods can be divided into two main categories as information-theoretic secure and computationally secure. Both of these methods are consist of a public algorithm and a private key. Therefore the key generation and management have particular importance.

In the information-theoretic security, introduced by Shannon [1], the mutual information between plaintext and ciphertext determines the performance of algorithm. Shannon showed that for perfect secrecy, the encryption key must have entropy equal or greater than the plaintext entropy and this requires key length at least equal to plaintext length and makes it useless in many practical situations. In contrast, for practical applications with Limited key lengths, algorithms with tremendous cryptanalysis computations and so, computationally-secure, are used.

But in these methods it is assumed that eavesdropper has full access to ciphertext similar to legitimate party. This situation is violated for wireless communication, because the channel characteristics are non ideal and a noisy and probably erroneous transmission is occurred. So the eavesdropper and legitimate recipient have different copies of transmitted data. This property, motivates a new viewpoint in secure communication which was named wire-tap channel by Wyner [2]. In this scenario, K data bits can be encoded into N > K bits and transmitted. The encoder should be designed to maximize the intruder's uncertainty about the data, subject to the condition that the intended receiver can recover the K data bits perfectly [3]. Later Csiszar et al [4] proved that secrecy capacity can be upper bounded with difference of mutual information between transmitter and two receivers.

Although for wire-tap channels, perfect secrecy with information theory definition is possible, but the secrecy capacity is small and is not suitable for high speed transmission demands of current applications.

Therefore a mixed method that uses perfect secrecy of wire-tap channel for secret key generation and then applying this key in a high speed computationally-secure algorithm (such as symmetric key methods) seems result high degree of security.

In this paper we focus on calculating secrecy capacity of wire-tap channel concept for wireless channels with fast fading. The statistical model for fading is considered as Nakagami and Suzuki that covers both LOS (Rician fading) and NLOS (Rayleigh fading). We proposed the communication model for transmitter, eavesdropper and legitimate receiver and then calculating mutual information based on this model for different conditions of fading. At last secrecy capacity or the maximum number of secret bits per channel use will be calculated.

This paper is organized as follows. In section 2 the required backgrounds about fading and its variety's is presented. Then secrecy capacity of channel is defined that will be used in next sections. In section 3 the problem is stated according to a proposed model for communication scenario and in section 4 the mathematical theory of mutual information calculation for our model is presented.

Manuscript received March 5, 2007
Manuscript revised March 25, 2007

In section 5 mutual information for two common fading probability distributions are calculated and finally in section 6 the simulated results are presented.

2. Background

2.1 Fading channels

Fading is a fundamental feature of wireless channels which is random fluctuations of received signal level by temporal or spatial changes. This phenomenon is caused by multipath effects in wireless propagation. fading can be categorized in two major types as short term (small scale) and long term (large scale) [5]. Short term fading is the fast fluctuations that occur very fast in time (typically in range of nanoseconds), but long term fadings occur in much longer periods of time (typically in range of micro seconds). Moreover short term fadings can be divided to LOS (line of sight) and NLOS (non line of sight). Such temporal fluctuations cause the channel to be modeled as a time-variant system with $h(t,\tau)$ impulse response, in which t is time and τ is impulse age. The fourier transform of $h(t,\tau)$ respect to τ is frequency response of channel. This frequency response is also time variant and showing random behavior But in short time interval which is called coherence time, the frequency response can be approximated as a flat response and the width of this flat region which called coherence bandwidth. Hence if signal bandwidth is less than coherence band, the channel response can be modeled as a random gain, otherwise a tapped delay line model should be used.

In this paper we assume flat fading situation. Therefore we consider the channel fading as a simple system with a random gain. The statistical distribution of this random gain is dependent to LOS or NLOS situation. For LOS conditions the Rice distribution has a good matching and for NLOS situations the Rayleigh distribution is suitable. For mixed conditions Nakagami and Suzuki distributions have superior performance because they cover both Rayleigh and Rice distributions.

2.2 Secrecy capacity

Consider a communication system as fig.1.

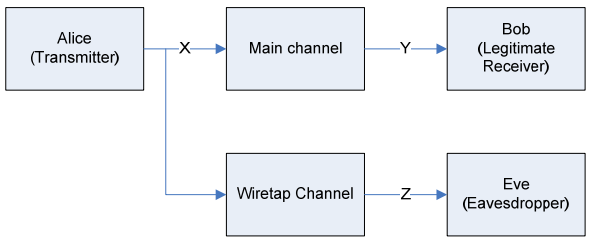

Fig.1 Communication System for a Wiretap Channel manner

Assume the channel behavior is completely specified by the conditional probability distribution $P_{yz|x}$. Note that in Wyner's original setting [2], X, Y, and Z form a Markov chain, i.e., $P_{z|xy} = P_{z|y}$, which implies $I(X;Z|Y) = 0$. The secrecy capacity $C_S(P_{yz|x})$ of the such a channel is defined in [4] as the maximum rate at which Alice can reliably send information to Bob such that the rate at which Eve obtains this information is arbitrarily small. In other words, the secrecy capacity is the maximum number of bits per use of the channel that Alice can send to Bob in secrecy.

Csiszir and Korner [4] proved that

$$C_s(P_{YZ|X}) = \max_{P_X}[I(X;Y) - I(X;Z)] \quad (1)$$

From (1) we can see the upper bound for secrecy capacity is the difference of mutual information between communication end points. Therefore we will calculate this mutual information for proposed communication model.

3. System Model

Fig. 2 shows the system architecture model. Assume that we want to determine the upper bound secret capacity between A and B when E is an eavesdropper who listens to this communication. A and B simultaneously send a raised cosine pulse to each other. We assume they are synchronized before. As it was mentioned in section 2.1, the fading effect is a random gain which multiplied to signal and faded signal is received at each side. This signal will be added by thermal noise and after match filtering and sampling, we have y_a, y_b as follows,

$$y_a = E_s\alpha + z_a \quad (2)$$

$$y_b = E_s\alpha + z_b \quad (3)$$

The eavesdropper could receive this transmission with a different fading as,

$$y_e = E_s\alpha' + z_e \quad (4)$$

In general situation, we assume that α and α' are correlated variables and independent condition is a special case. We try to find out this correlation effect on upper bound secrecy capacity. The correlation has been assumed as,

$$\alpha' = k\alpha + n_\alpha \quad (5)$$

Where k is correlation coefficient and n_α is a Gaussian noise.

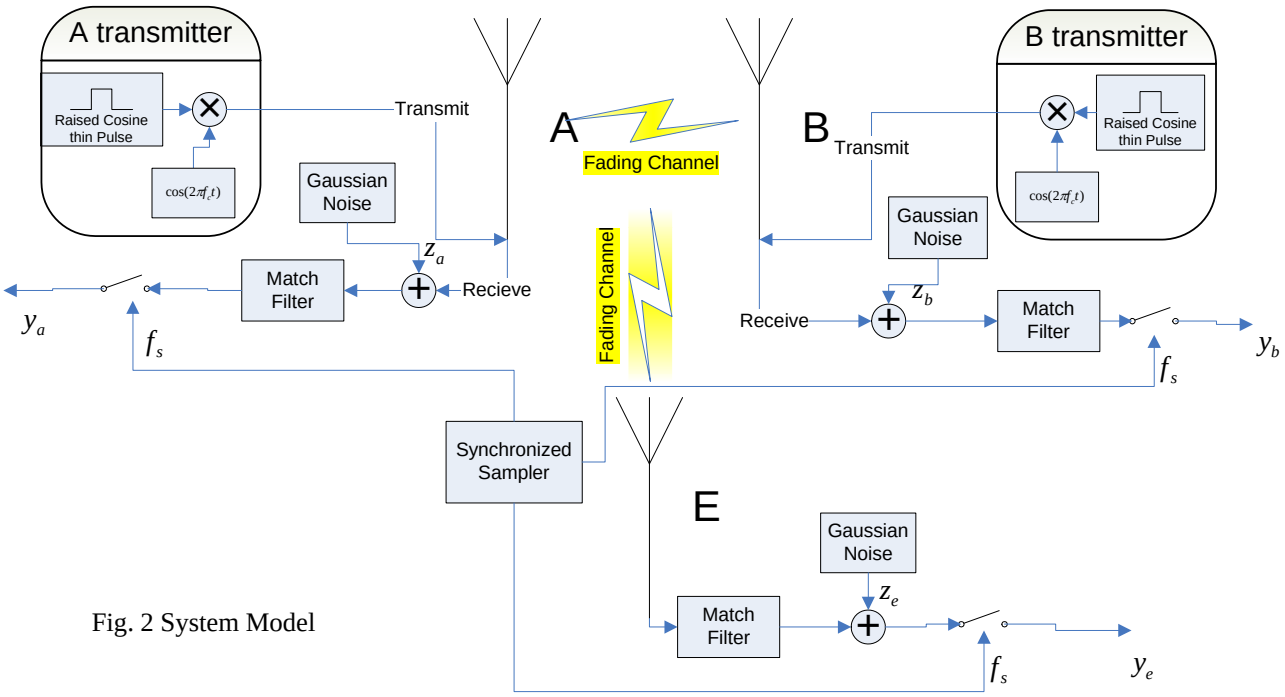

Fig. 2 System Model

When two antennas A and B with no non-linear components radiate identical signals, the outputs of the antennas due to their excitation by the signal originating at the other antenna will also be identical. This behavior, known as the reciprocity theorem, arises from the reciprocity of the radiating and receiving patterns of antennas and applies when the medium between the antennas is linear and isotropic [6]-[7]. When wide bandwidth waveforms are transmitted in cluttered environments, such as homes and offices, the signal observed by a receiving antenna at a remote location is the composite of multiple signals that have traveled over different paths from the transmitting antenna, each signal experiencing different shaping and attenuation, resulting in an output signal that differs significantly from the radiated signal and that changes as the locations of the transceivers is changed. In other words, the output signal contains information about the channel through which the transmitted waveform has propagated, and because of reciprocity this information is a source of common randomness that is available at both ends of the link.

If this common information taken in both side then in each side we have a parameter that is random and base on reciprocity of antennas is unique between the ends of the channel. All of these features direct us to the fact that this parameter is very suitable for secret key extraction of a secure communication. In the other words, the eavesdropper who tries to catch the information could not succeed to receive the data which encrypted by measured secret key, because it doesn't have the secret key that had been calculated by A and B. this is the result of different channels between A, B and E.

The task of generating a secret key from common information has been studied by several authors in particular Maurer [8][9] and Ahlswede et al [10] discovered some fundamental bounds on the so called secret-key rate of system models where the terminals have access to correlated random variables due to some external source (in this case the 'external source' is the channel impulse response). The results in these references show that the secret key rate, upper bounded by the mutual information between the envelopes detected in A and B sides, Y_A, Y_B respectively.

In this paper we argue about this maximum key rate or mutual information for different fading models.

4. Mutual Information over Multipath Ultrawideband Channels

In this section we try to present the mutual information calculation in a multipath channel. Suppose that the transmitter, A, sends the narrow band raised cosine pulse with energy E_s to B and vice versa. Let the observed waveform of radio k be represented by,

$$y_k = h(t) * s(t) + n_k(t) \quad (6)$$

Where $h(t)$ is the channel impulse response, $s(t)$ is the pulse transmitted by the other radio, $n_k(t)$ is a Gaussian noise process with power spectral density $\frac{N_{0k}}{2}$ and * indicates convolution.

The nature of the ultrawideband channel is different to that encountered in narrowband systems and deserves some discussion. In narrowband systems, the familiar multipath propagation model assumes the existence of a large number of propagation paths with the same time of arrival but uniformly distributed phase, which results in a Rayleigh distributed amplitude gain by appeal to the central limit theorem. Due to the short duration, typically sub-nanosecond, of an ultrawideband pulse, at most a few paths contribute to the channel impulse response at a given delay (it is often assumed that every path is distinct) and the amplitude is more dependent on the loss that occurs during propagation than on interference between arrivals [11]. The resulting probability distributions for the gains of multipath channel paths are often modeled as log-normal or Nakagami. The other effect of the short pulse width is that the number of resolvable paths in a multipath observation is much larger for ultrawideband signals than for narrower bandwidths.

The analysis of the mutual information between the observations of two radios observing the channel pulse response at opposite ends of a multipath channel will begin by considering the mutual information between the observations due to a single propagation path, and then be extended to multiple paths.

Here, we suppose that the channel has frequency non-selective and slowly fading model. This assumption implies that the multiplicative process may be regarded as a constant during at least one signaling interval. Consequently, if the transmitted signal is $s_l(t)$, the received equivalent lowpass signal in one signaling interval is [4],

$$y(t) = \alpha e^{-j\varphi} s_l(t) + z(t) \quad (7)$$

Where $z_k(t)$ represents the complex-valued white Gaussian noise process corrupting the signal and α defines the channel fading effect on signal. α is a random variable that its distribution changed in different channels.

Let us assume that the channel fading is sufficiently slow that the phase shift φ can be estimated from the received signal without error. In that case, we can achieve ideal coherent detection of the received signal. Thus, the received signal can be processed by passing it through a matched filter. After match filtering and sampling, the received signal, the output sequence in both ends are:

$$y_A = \alpha E_s + z_A \quad (8)$$

$$y_B = \alpha E_s + z_B \quad (9)$$

$$E_s = \int_{-\infty}^{+\infty} {s_l}^2(t)dt \quad (10)$$

E_s is the energy of transmitted pulse and z_A, z_B are white Gaussian noise sequences in side A and B, respectively.

Now base on above assumption the mutual information between A and B defined as the mutual information between y_A and y_B [12]:

$$I(Y_A; Y_B) = \sum_{y_A} \sum_{y_B} p(y_A, y_B) Log_2\left(\frac{p(y_A, y_B)}{p(y_A)p(y_B)}\right) \quad (11)$$

The equation 11 shows that for calculation of mutual information we need to $p(y_A, y_B)$, $p(y_A)$ and $p(y_B)$ then first we try to find these pdfs.

5. Channel fading models

Here we suppose two different distributions for α random variable. First is Nakagami-m model [13] and the other is Suzuki model [14]. Both of these models are in the domain of frequency non-selective and slowly fading.

5.1 Nakagami Model

This pdf is usually used to characterize the statistics of fading channel model. The pdf for this distribution is given by Nakagami (1960) as,

$$P_R(r) = \frac{2}{\Gamma(m)} \left(\frac{m}{\Omega}\right)^m r^{2m-1} e^{-\frac{mr^2}{\Omega}} \quad (12)$$

Where Ω is the second moment of R and defined as,

$$\Omega = \mathrm{E}(\mathrm{R}^2) \quad (13)$$

And the parameter *m* is defined as the ratio of moments, called the fading figure,

$$m = \frac{\Omega^2}{E[(R^2 - \Omega)^2]}, \quad m \geq \frac{1}{2}; \quad (14)$$

The *n*th moment of *R* defined as,

$$E(R^n) = \frac{\Gamma\left(m + \frac{1}{2}n\right)}{\Gamma(m)} \left(\frac{\Omega}{m}\right)^{\frac{n}{2}} \quad (15)$$

If *m=1*, the equation (12) reduces to Rayleigh distribution. For values *m* in the range $\frac{1}{2} \leq m \leq 1$, we obtain pdfs that have larger tails than a Rayleigh distributed random variable. For values of $m > 1$, the tail of the pdf decade faster than that of the Rayleigh. Figure 3 shows the Nakagami distribution for different *m* value.

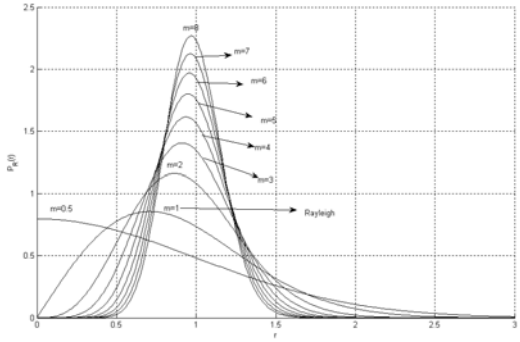

Fig. 3 m-Nakagami Distribution

5.2 Suzuki Model

This distribution is the combination (multiplication) of Rayleigh and Log-normal distributions.

Consider a Rayleigh distributed random variable ζ with the probability density function $P_\zeta(x)$, and a lognormally distributed random variable λ with the probability density function $P_\lambda(x)$. Let us assume that ζ and λ are statistically independent. Furthermore, let R be a random variable defined by the product $R=\lambda\zeta$ Then, the probability density function $P_R(r)$ of R is,

$$E(r) = \sigma_0\sqrt{\frac{\pi}{2}}e^{m_\mu+\frac{\sigma_\mu^2}{2}}$$

$$\sigma_r^2 = E(r^2) - E^2(r) = \sigma_0^2 e^{(2m_\mu+\sigma_\mu^2)}\left(2e^{\sigma_\mu^2} - \frac{\pi}{2}\right)$$

$$P_R(r) = \frac{r}{\sqrt{2\pi}\sigma_0^2\sigma_\mu}\int_0^\infty \frac{1}{y^3} e^{-\frac{r^2}{2y^2\sigma_0^2}} e^{-\frac{(\ln(y)-m_\mu^2)^2}{2\sigma_\mu^2}} dy \quad (16)$$

In this formula σ_0 is the parameter of Rayleigh distribution (variance of Gaussian components), σ_μ and m_μ are the variance and mean values of lognormal distribution respectively.

The following Fig. 4 shows Suzuki distribution respect to $a = \sigma_0\sigma_\mu$,

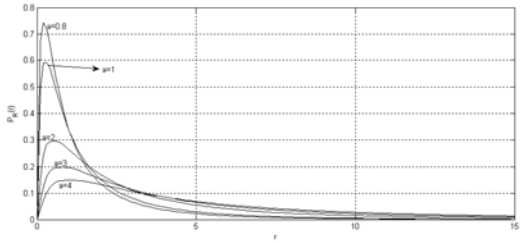

Fig. 4 Suzuki Distribution

As was mentioned before, we should find mutual distribution of y_a, y_b, then we use the concepts of random variables. Suppose that

$$y_A = \alpha E_s + z_A = g_1(\alpha, z_A, z_B) \quad (17)$$

$$y_B = \alpha E_s + z_B = g_2(\alpha, z_A, z_B) \quad (18)$$

$$y_c = \alpha = g_3(\alpha, z_A, z_B) \quad (19)$$

y_c is supplementary random variable for completion of equations.

To find the density function $p_{Y_AY_BY_C}(y_A, y_B, y_C)$, base on [15] we have,

$$p_{Y_AY_BY_C}(y_A, y_B, y_C) = \frac{1}{|J(\alpha,z_A,z_B)|} p_{\alpha z_A z_B}(\alpha, z_A, z_B) \quad (20)$$

Where

$$J(\alpha, z_A, z_B) = \begin{vmatrix} \frac{\partial g_1}{\partial \alpha} & \frac{\partial g_1}{\partial z_A} & \frac{\partial g_1}{\partial z_B} \\ \frac{\partial g_2}{\partial \alpha} & \frac{\partial g_2}{\partial z_A} & \frac{\partial g_2}{\partial z_B} \\ \frac{\partial g_3}{\partial \alpha} & \frac{\partial g_3}{\partial z_A} & \frac{\partial g_3}{\partial z_B} \end{vmatrix} = \begin{vmatrix} E_s & 1 & 0 \\ E_s & 0 & 1 \\ 1 & 0 & 0 \end{vmatrix} = 1 \quad (21)$$

$$\begin{cases} \alpha = y_C \\ z_A = y_A - E_s y_C \\ z_B = y_B - E_s y_C \end{cases} \quad (22)$$

Then,

$$p_{Y_AY_BY_C}(y_A, y_B, y_C) = p_{\alpha z_A z_B}(y_C, y_A - E_s y_C, y_B - E_s y_C) \quad (23)$$

It is obvious that the random variable α is independent of z_A, z_B and the random variables z_A, z_B are independent too then $p_{\alpha z_A z_B}(\alpha, z_A, z_B) = p_\alpha(\alpha)p_{z_A}(z_A)p_{z_B}(z_B)$.

$$p_{Y_AY_BY_C}(y_A, y_B, y_C) = p_\alpha(y_C)p_{z_A}(y_A - E_s y_C)p_{z_B}(y_B - E_s y_C) \quad (24)$$

Now we could find the mutual density function of y_A, y_B as follow,

$$p_{Y_AY_B}(y_A, y_B) = \int_0^\infty p_{Y_AY_BY_C}(y_A, y_B, y_C)dy_C \quad (25)$$

We could find the p_{y_A}, p_{y_B} the same as $p_{y_Ay_B}$ and we could write:

$$p_{y_A}(y_A) = \int_0^\infty p_\alpha(y_C)p_{z_A}(y_A - E_s y_C)dy_C \quad (26)$$

$$p_{y_B}(y_B) = \int_0^\infty p_\alpha(y_C)p_{z_B}(y_B - E_s y_C)dy_C \quad (27)$$

First we calculate equation 25 when α has m-Nakagami distribution and z_A, z_B have zero mean Gaussian distribution with variance $\sigma_{z_A}^2 = \frac{N_A}{2}$ and $\sigma_{z_B}^2 = \frac{N_B}{2}$.

$$P_\alpha(\alpha) = \frac{2}{\Gamma(m)}\left(\frac{m}{\Omega}\right)^m \alpha^{2m-1}e^{-\frac{m\alpha^2}{\Omega}} = A_1\alpha^{2m-1}e^{-B_1\alpha^2} \quad (28)$$

$$p_{z_A}(z_A) = \frac{1}{\sqrt{\pi N_A}}e^{-\frac{z_A^2}{N_A}} = A_2e^{-B_2z_A^2} \quad (29)$$

$$p_{z_B}(z_B) = \frac{1}{\sqrt{\pi N_B}}e^{-\frac{z_B^2}{N_B}} = A_3e^{-B_3z_B^2} \quad (30)$$

Equation 25 has complicated answer in public condition then for simplification we solve it analytically for *m=2* and for the other figures, we compute it with computer simulations (Mont Carlo method). For *m=2* the equation 25 simplifies to,

$$p_{Y_AY_B}(y_A, y_B) = \frac{A_1A_2A_3}{16a^{\frac{7}{2}}}e^{-c}(2\sqrt{a}(b^2+4a) + b\sqrt{\pi}e^{\frac{b^2}{4a}}(6a+b^2)(1-\mathrm{erf}(-\frac{b}{2\sqrt{a}})) \quad (31)$$

Where

$$a = B_1 + E_s^2(B_2 + B_3) \quad (32)$$

$$b = 2E_s(B_2y_A + B_3y_B) \quad (33)$$

$$c = B_2y_A^2 + B_3y_B^2 \quad (34)$$

p_{y_A}, p_{y_B} have the same form as (31) but the parameters *a*, *b* and *c* are different.

Because of complexity of Suzuki distribution, we don't find analytic results and only done computer simulation.

6. Simulation Results

The simulation has been done base on equations 23-27 and finally the mutual information computed by (6). We try to show the effect of SNR on mutual information, it means that we increase the amplitude of transmitted pulse and hold the power of noise constant then calculate the mutual information for this increasing. Here we define $SNR = 2E_S/N_0$ and $N_0 = N_A = N_B = 1$.

Figure 3 shows the mutual information in bit for Nakagami distribution. As the figure shows the mutual information decrease when *m* increases but the difference is small for low SNRs and it is increases by SNR (large SNR). For *m=2*, simulation results show very close approximation to analytic results.

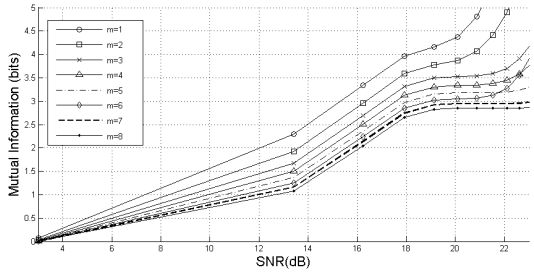

Fig. 5 Mutual Information for m-Nakagami distribution

Figure 4 shows mutual information for Suzuki distribution where $a = \sigma_0\sigma_\mu$. The results show that mutual information increases where *a* increase. Approximately all the plots have the same incline and the difference is a DC shift in vertical position. Greater value of "*a*" shows the wider Log-normal and Rayleigh distribution which multiply and make Suzuki distribution. For small value of "a" the distribution approaches to delta function and this consideration implies the results.

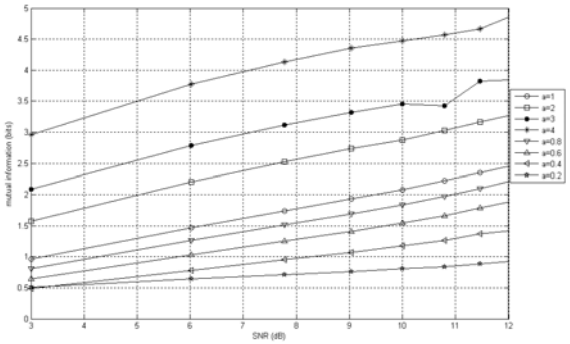

Fig. 6 Mutual Information for Suzuki distribution $a = \sigma_0\sigma_\mu$

Figures 7 to 9 shows the effect of eavesdropper channel correlation on upper bound key rate. The correlation has been supposed as (5). Fig. 7 is for *m=1*

when α is Rayleigh distributed and Fig. 8 and 9 for m=2 and 5, respectively. The results show the smaller values when the correlation coefficient, *k*, approaches to 1.

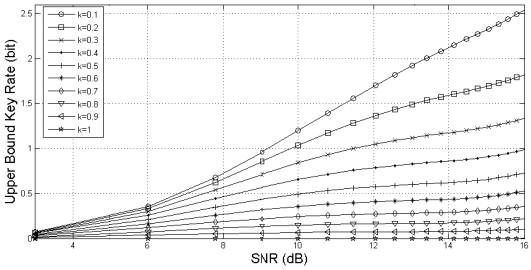

Fig. 7 Upper bounded Secret Key Rate, m=1

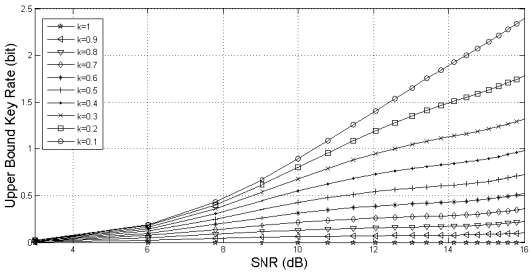

Fig. 8 Upper bounded Secret Key Rate, m=2

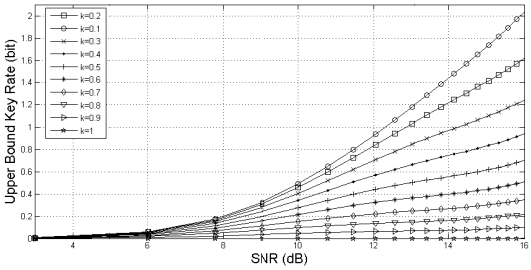

Fig. 9 Upper bounded Secret Key Rate, m=5

7. Conclusion

A practical communication model for secret key extraction from fading of channel is proposed. Based on this model, two types of fading in form of Nakagami and Suzuki was evaluated. For Nakagami fading both analytical and numerical results in secrecy capacity was presented but in Suzuki case only numerical results was mentioned. These results show maximum secret bits per each channel use. The obtained capacity rates show this method of key establishment is practical in wireless applications but the proper coding method that achieves capacity rate is a open problem.

Acknowledgments

This work is partly supported by Iran Telecommunication Research Center.

References

[1] C. Shannon, “Communication theory of secrecy systems,” Bell Syst. Tech. J., vol. 29, pp. 656–715, 1949
[2] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, pp.1355–1387, 1975.
[3] L. H. Ozarow and A. D. Wyner, “The wire-tap channel, II,” Bell Syst. Tech. J., vol. 63, pp. 2135–2157, 1984.
[4] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” IEEE Trans. Inform. Theory, vol. IT-24, pp. 339–348, May 1978.
[5] J. G. Proakis, “Digital Communications”, 4th ed. New York, NY: McGraw-Hill, 2001.
[6] C. A. Balanis, Antenna Theory: Analysis and Design, 2nd ed. New York: John Wiley & Sons, 1997.
[7] G. S. Smith, “A direct derivation of a single-antenna reciprocity relation for the time-domain,” Trans. on Antennas and Propagation, vol. 52, pp. 1568–1577, Jun. 2004.
[8] U. M. Maurer, “Secret key agreement by public discussion from common information,” Trans. on Information Theory, pp. 733–742, 1993.
[9] “Unconditionally secure key agreement and the intrinsic conditional information,” Trans. on Information Theory, pp. 499–514, 1999.
[10] R. Ahlswede and I. Csiszar, “Common randomness in information theory and cryptography – part i: secret sharing,” Trans. on Information Theory, pp. 1121–1132, July 1993.
[11] A. F. Molisch, J. R. Foerster, and M. Pendergrass, “Channel models for ultrawideband personal area networks,” Wireless Communications, pp. 14–21, Dec. 2003.
[12] Thomas M. Cover, “Elements of Information Theory”, John Wiley & Sons, Inc., 1991.
[13] M. Nakagami, "The m-Distribution-A General Formula of Intensity Distribution of Rapid Fading", in Statistical Methods of Radio Wave Propagation, W. C. Hoffman (ed.), pp.3-36, Pergamon Press, New York.
[14] H. Suzuki, "A Statistical Model for Urban Multipath Channels with Random Delay", IEEE Trans. Communication vol. COM-25, pp. 673-680, July, 1977.
[15] A. Papoulis, “Probability, Random Variables, and Stochastic Processes”, 3rd Edition, McGraw-Hill, 1991.

Ali Shahzadi. received the B.S. and M.S. degrees in Electronic Engineering from Iran University of Science and Technology (IUST) in 1997 and 2000, respectively. He is currently working toward the Ph.D. degree in the Department of Electrical Engineering, IUST. His research interests include: the wireless communication, communication security and statistical digital signal processing.

Masoud Ghoreishi Madiseh. Received the B.S. in Communication System Engineering from Iran University of Science and Technology (IUST) in 2005. He is currently working toward the MS. degree in the Department of Electrical Engineering, IUST. His research interests include: the wireless

communication, estimation and detection and statistical digital signal processing and wireless location systems.

Ali Asghar Beheshti Shirazi. received the B.S. and M.S. degrees in Communication Engineering from Iran University of Science and Technology (IUST) in 1984 and 1987, respectively and Ph.D. from Okayama University, Japan in 1995. In 1995, he joined the Department of Electrical Engineering, IUST, where he currently is an Assistant Professor. His research interests include Digital Image Processing, Data Communication Networking and Secure Communication.