On Optimizing the Security-Throughput Trade-off in Wireless Networks with Adversaries

Mohamed A. Haleem, Chetan Nanjunda Mathur, R. Chandramouli, and K. P. Subbalakshmi

Department of Electrical and Computer Engineering,
Stevens Institute of Technology, Hoboken, NJ 07030, USA,
mhaleem@stevens.edu

Abstract. In this paper, we model the adversary (eavesdropper) present in the wireless communication medium using probabilistic models. We precisely formulate the security-throughput optimization and derive analytical solutions. The effect of different adversary models, and single and multi-rate modulation schemes (BPSK and MQAM) are studied. Simulation results are given to show that significant throughput gain can be achieved by using link (channel) adaptive and adversary adaptive encryption techniques compared to fixed block length encryption.

Key words: Opportunistic, Tradeoff, Optimization, Encryption, Wireless, Security.

1 Introduction

Traditionally, design of encryption algorithms and their parameters has used only the security against an adversary attack as the main criterion. To achieve this goal, the cipher is made to satisfy several properties including the *avalanche* effect [1][2].

The avalanche effect principle requires that a minor change to the plain text or the key must result in significant and random-looking changes to the cipher text. For a given transformation to exhibit the avalanche effect, an average of one half of the output bits should change whenever a single input bit is complemented. This implies that there should not be any noticeable resemblance between two ciphertexts obtained by applying two neighboring keys for encrypting the same plain text. Otherwise, there would be considerable reduction of the keyspace search by the cryptanalyst.

We note that block ciphers that satisfy the avalanche property are very sensitive to bit errors induced by the wireless link. This means that a single bit error in the received encrypted block could lead to about half the decrypted block to be in error (error propagation), resulting in throughput loss when the channel introduces errors. Hence, there is a fundamental trade-off between security and throughput in encryption based wireless networks. We explore this trade-off in this paper and investigate methods to optimize it.

It is customary to measure the level of security in encrypted data against cryptanalysis, as the amount of work (computation) required by the adversary to crack the ciphertext (encrypted information). Computationally secure encryption is achieved if the cost of cracking the information is higher than the value of the information and if the time required to crack the informaiton exceeds the useful time period of the information being sent [1]. Meanwhile, it is reasonable to say that the level of security can only be quantified relative to the strength of the adversary present in the environment. For mobile wireless environment, the adversary's strength also varies with the location and time, and cannot be predicted deterministically. In other words, the adversary's "strength" to crack a cipher is a random parameter that could be modeled using a probability distribution. It is reasonable to assume that the ability of the adversary to crack the cipher text becomes less probable as the computational complexity of attack increases.

In this work, we propose to model the adversary strength probabilistically. The model assumes a finite set of discrete values for the maximum possible block lengths an adversary can crack. Note that the strength of a block cipher is decided by the minimum of the length of key and the length of plaintext, the set of block lengths represent the minima of the lengths of planitext/key pairs. If the adversary is capable of cracking a cipher with a block length of N bits then (s)he is capable of cracking any block length less than or equal to N bits. We associate a probability to each possible attack strength of the adversary. In particular, we consider two probability distributions namely uniform leading to the *linear model* and exponential leading to the *exponential model*. It is reasonable to assume that in a typical communication medium, the probability of the presence of an adversary with certain strength decreases as the strength increases. Such a model is justified from the following fact. In the absence of a shortcut attack (*e.g.* linear and differential cryptanalysis [1]), the computational strength required by the attacker to crack the cipher increases exponentially with the block length. For example, it is exponentially harder to crack 128 bit AES [3] compared to a 64 bit DES [4]. Thus an exponential model is deemed an appropriate one. Nevertheless, the linear model can be considered as the representation of the worst case scenario where we assume that the presence of adversary with a given strength has the same probability for all values of strength. In this case, we assume that the probability of the adversary reduces to zero beyond a maximum defined block length.

The wireless communication channel quality is a highly time varying parameter due to the environmental noise and fading [5]. Traditionally, encryption designs do not consider the effect of bit errors occurring during the transmission of information through the channel and this issue is considered to be an orthogonal problem that should be handled by efficient coding and modulation techniques. In contrast, it is seen in recent work [6] that present and future wireless communication systems and networks can greatly benefit from an encryption design that considers the channel quality. Such an approach makes it possible to achieve a desirable tradeoff between the security and performance. However,

security cannot be merely reduced to increase throughput. The presence of adversaries play a crucial role in security throughput tradeoff.

In the optimization problems formulated in this paper, we make the assumption that the channel states are known for the extent of the message being transmitted. The solution derived with such an assumption provides us an upper bound on the performance. Further, the study presented in this work considers block encryption.

In Section 2 we discuss the measure of security based on the probabilistic models of adversary strength. In Section 3 we present the discussion on the tradeoff between the security and the throughput performance. The optimization problems are formulated and the solutions are derived. Sample numerical results are given in Section 4.

2 Channel Model and Security Measure

In a typical packet mode communication, frames consisting of fixed length of bit stream (with fixed modulation schemes) or symbol stream (variable modulation schemes) are formed. The frame lengths are in general much larger than the encryption block lengths and may consist of multiple encrypted blocks. Let a message be sent by forming n frames of lengths L_i bits for $i = 1, \cdots, n$ and transmitted in distinct time intervals using encryption block lengths $N_i, i = 1, \cdots, n$. N_i is selected by the optimization procedure based on the channel condition. With the block fading [7] assumption on the wireless channel, all the information bits in a frame are encrypted using the same encryption block length as the quality of the channel is assumed to be fixed over the frame duration.

We define the *vulnerability* (which increases as the encryption block length is decreased) $0 \leqslant \Phi \leqslant 1$ of a message as the expected fraction of the total message being successfully decrypted by the adversary. Let the frames be arranged in the ascending order of the respective encryption block lengths. If the adversary's attack strength is α bits, then the adversary can successfully crack all the data frames with encryption block length less than or equal to α. Assume that there are $K(\leqslant n)$ distinct encryption block lengths being used and m_k be the number of frames with encryption block length less than or equal to $M_k, k = 1, \cdots, K$, and $Pr(\alpha = M_k)$ be the probability that the attacker's strength α is M_k. Note that $Pr(\alpha = M_k)$ also is the probability with which the m_k frames (in the ordered list) would be cracked by the adversary resulting in the leakage of a fraction $x_k = \sum_{i=1}^{m_k} l_i$ of the total message, where l_i is the frame length normalized by message length ($l_i = \frac{L_i}{\sum_{j=1}^{n} L_j}$). Thus we can define the vulnerability Φ of the message as the expected leakage given by,

$$\Phi = \sum_{k=1}^{K} x_k P(x_k) \tag{1}$$

where $P(x_k) = Pr(\alpha = M_k)$ is the probability of exposing a fraction x_k of the total message. From a known result in probability theory, this is equivalent to

$$\Phi = \sum_{k=1}^{K} Pr(x \geqslant x_k). \tag{2}$$

Further, if each frame is encrypted with a distinct block length we have $K = n$ and the above equation reduces to

$$\Phi = \sum_{i=1}^{n} Pr(\alpha \geqslant N_i) \tag{3}$$

3 Security-Throughput Tradeoff Optimization

For the discussion in this section, we consider two probability distributions, namely uniform and exponential to model the adversary strength leading to respectively the *linear* and *exponential* adversary strength models. We show in the sequel that with linear model, the optimization problem is equivalent to "fractional knapsack" problem and therefore the optimum algorithm has linear execution time [8]. With the exponential model, the optimal solution resembles "water-filling" algorithm [9], which also has a linear execution time. As discussed in the introduction we assume that a single bit error during the decryption process would cause the loss of entire block of encrypted information. The throughput per block is given by $R_i(1-P_i)^{N_i} \approx R_i(1-P_iN_i)$ where R_i and P_i are respectively the transmission rate selected for the frame and the channel bit error probability. The approximation is valid when the channel bit error probability is sufficiently small. If there is any bit error in an encrypted block within a frame, the avalanche effect would cause propagation of the error to the entire block leading to discarding of such a block of N_i bits. However, blocks of data with no bit errors can be decrypted without any errors and can be accumulated in the receiver as useful data. With such an approach, the throughput of the message (sequence of frames) can be expressed by,

$$T = \sum_{i=1}^{n} R_i(1 - P_iN_i) \tag{4}$$

In the sequel we present the optimization process to compute the optimum values of N_i for a known sequence of channel instantiations. The procedures are presented for the two different adversary models.

3.1 Linear Adversary Strength Model

Let the probability mass function of the attacker strength be a uniform distribution *i.e.*, $\Pr(\alpha = N_i) = \frac{1}{N_{\max} - N_{\min}}$ for $i = 1, \cdots, n$ where $N_{\min}$ and $N_{\max}$ are

the minimum and maximum block length used in the encryption system. Then for the linear model we have,

$$\phi_i = \Pr(\alpha \geqslant N_i) = \frac{N_{\max} - N_i}{N_{\max} - N_{\min}}, i = 1, \cdots, n \tag{5}$$

We maximize the throughput given by,

$$T = \sum_{i=1}^{n} R_i(1 - P_i(N_{\max} - (N_{\max} - N_{\min})\phi_i)) \tag{6}$$

subject to the conditions

$$\phi_{\min} \leqslant \phi_i \leqslant \phi_{\max}, i = 1, \cdots, n \tag{7}$$

$$\frac{1}{n}\sum_{i=1}^{n} \phi_i \leqslant \Phi_0 \tag{8}$$

Here, Φ_0 is the maximum allowable average vulnerability level, and $\phi_{\min}$ and $\phi_{\max}$ are the minimum and maximum allowable values of the vulnerability of a frame corresponding to a maximum and a minimum encryption block length, respectively. Under the assumption of continuous values for ϕ_i, the optimal solution is achieved with the equality in the condition $\frac{1}{n}\sum_{i=1}^{n} \phi_i \leqslant \Phi_0$. By expanding (6) and omitting the terms that are independent of $\phi_i, \forall i$, the problem reduces to the maximization of the following cost function over $\{N_i\}$:

$$T' = \sum_{i=1}^{n} w_i \phi_i \tag{9}$$

where, $w_i = P_i R_i$. This problem is a special case of *fractional knapsack problem* which is solvable in polynomial time. Selecting ϕ_is in the non-increasing order of maximum w_i maximizes T' and hence T [8]. As any data frame in the message should be assigned at least the minimum vulnerability level, $\phi_{\min}$ corresponding to the maximum encryption block length, $N_{\max}$, the formulation can be modified such that the optimization problem is

$$\max_{\phi_1, \cdots, \phi_n} \sum_{i=1}^{n} w_i \phi_i \text{ such that}$$

$$\frac{1}{n}\sum_{i=1}^{n} \phi_i \leqslant \Phi_0'; 0 \leqslant \phi_i \leqslant \phi_{\max} - \phi_{\min} \tag{10}$$

where $\Phi_0' = \Phi_0 - n\phi_{\min}$. The following greedy algorithm optimally solves the problem. The proof of this claim follows along the lines discussed in [10].

1. *Inititalization*: Allocate a vulnerability level of $\phi_{\min}$ for all frames $i, i = 1, \cdots, n$.
2. Sort the frames in the non-increasing order of $w_i = P_i R_i, i = 1, \cdots, n$.

3. Allocate the additional maximum allowed vulnerability level of less than or equal to $\phi_{\max} - \phi_{\min}$ for each frame i in the sorted order, i.e., $w_i > w_{i+1}$. That is, allocate $\phi_{\max} - \phi_{\min}$ units to frames $i = 1, \cdots, j^* - 1$ for some j^*, fewer than $\phi_{\max} - \phi_{\min}$ or 0 for frame j^* and 0 for $i = j^* + 1, \cdots, n$ with the sum total of the additional allocation is Φ_0'.

3.2 Exponential Adversary Strength Model

Let the attacker strength be given by:

$$\phi_i = \Pr(\alpha \geqslant N_i) = e^{-kN_i} \tag{11}$$

where $k > 0$ is a constant. We are required to maximize the throughput given by

$$T = \sum_{i=1}^{n} R_i(1 + \frac{P_i}{k} \log_e \phi_i) \tag{12}$$

subject to the conditions

$$\phi_i - \phi_{\min} \geqslant 0, i = 1, \cdots, n \tag{13}$$

$$\phi_{\max} - \phi_i \geqslant 0, i = 1, \cdots, n \tag{14}$$

$$\Phi_0 - \frac{1}{n} \sum_{i=1}^{n} \phi_i = 0 \tag{15}$$

where Φ_0 is the maximum allowable overall vulnerability level, and $\phi_{\min}$ and $\phi_{\max}$ are the minimum and maximum values of the vulnerability of a frame corresponding to a maximum and a minimum encryption block length respectively. The equality in (15) results from the observation that maximum of T is achieved by using the maximum allowed overall vulnerability. The augmented objective function can be written as,

$$\begin{aligned} C = \sum_{i=1}^{n} R_i(1 + \frac{P_i}{k} \log_e \phi_i) + \nu(n\Phi_0 - \sum_{i=1}^{n} \phi_i) \\ + \sum_{i=1}^{n} \lambda_i(\phi_i - \phi_{\min}) + \sum_{i=1}^{n} \mu_i(\phi_{\max} - \phi_i) \end{aligned} \tag{16}$$

where $\nu, \lambda_i, \mu_i, i = 1, \cdots, n$ are constants (Lagrange multipliers). The Karush Kuhn-Tucker Conditions (KKC) [11] for this problem are obtained by considering the vanishing point of the first order derivative of C w.r.t. ϕ_i and also from the

complimentary slackness. Thus we have,

$$\begin{aligned}
\phi_i &= \frac{R_i P_i}{k(\mu_i + \nu - \lambda_i)} \\
\lambda_i(\phi_i - \phi_{\min}) &= 0 \\
\mu_i(\phi_{\max} - \phi_i) &= 0 \\
\lambda_i &\geqslant 0 \\
\mu_i &\geqslant 0 \\
n\Phi_0 - \sum_{i=1}^{n} \phi_i &= 0 \\
\nu &\geqslant 0
\end{aligned} \tag{17}$$

for $i = 1, \cdots, n$. Therefore the optimal value of ϕ_i is found from one of the following three cases.

Case 1: $\lambda_i = 0, \mu_i = 0 \Rightarrow \phi_{\min} < \phi_i < \phi_{\max}$ and we have $\phi_i = \alpha w_i$ with $\alpha = \frac{1}{k\nu}, \nu > 0$ and $w_i = R_i P_i$

Case 2: $\lambda_i = 0, \mu_i \neq 0 \Rightarrow \phi_i = \phi_{\max}$

Case 3: $\lambda_i \neq 0, \mu_i = 0 \Rightarrow \phi_i = \phi_{\min}$

The following iterative algorithm provides the optimal solution. Any value of ϕ_i computed complies with one of the three cases above.

1. Sort the channels in the non-increasing order of $w_i, i = 1, \cdots, n$; let $j = 1$
2. Compute $\alpha = \frac{\phi_{\min}}{w_j}$
3. Compute $\phi_i = \alpha w_i$ for $i = 1, \cdots, n$; if $\phi_i < \phi_{\min}$ set $\phi_i = \phi_{\min}$; if $\phi_i > \phi_{\max}$ set $\phi_i = \phi_{\max}$
4. If $n\Phi_0 > \sum_{k=1}^{n} \phi_i$ set $j = j + 1$ and goto step 2); else goto step 5)
5. If $n\Phi_0 = \sum_{k=1}^{n} \phi_i$ the current set of $\phi_i, i = 1, \cdots, n$ are optimal; else goto step 6)
6. The optimum α is in between the two values say α_j and α_{j-1} computed in the last two iterations. Fine tune as follows. Default to the allocation corresponding to $\alpha = \alpha_{j-1}$. Let l be the index of the largest $w_i, i = 1, \cdots, n$ such that $\phi_i < \phi_{\max}$, and $i_{\min}$ is the index of smallest w_i such that $\phi_i > \phi_{\min}$
7. Set $\alpha = \frac{\phi_{\max}}{w_l}$; if $\alpha < \frac{\phi_{\min}}{w_{i_{\min}+1}}$ set $\phi_i = \alpha w_i, i = 1, \cdots, n$; $\phi_i(\phi_i < \phi_{\min}) = \phi_{\min}$; $\phi_i(\phi_i > \phi_{\max}) = \phi_{\max}$; goto the step (8); else set $l = l - 1$ and goto step (9)
8. If $\sum_{i=1}^{n} \phi_i = n\Phi_0$ optimal values are found; else if $\sum_{i=1}^{n} \phi_i < n\Phi_0$ set $l = l+1$ and goto step (7); else set $l = l - 1$; goto step (9)
9. The optimal α is found from $\alpha = \frac{1}{\sum_{i=i_{\min}}^{l} w_i}(n\Phi_0 - (n - i_{\min})\phi_{\min} + (l - 1)\phi_{\max})$; set $\phi_i = \alpha w_i, i = 1, \cdots, n$, $\phi_i(\phi_i < \phi_{\min}) = \phi_{\min}$, and $\phi_i(\phi_i > \phi_{\max}) = \phi_{\max}$

The following discussion establishes that this algorithm is indeed optimal. Consider the quantity to be maximized namely $T = \sum_{i=1}^{n} R_i(1 + \frac{P_i}{k} \log_e \phi_i)$ subject to the constraints as in (13)-(15). This is equivalent to maximizing $S = \sum_{i=1}^{n} w_i \log_e \phi_i$ where $w_i = R_i P_i$ with the set of constraints. Each of the terms in the summation expression of S is concave and therefore the optimum allocation of ϕ_i resembles "water-filling" solution. Let $y_i = w_i \log_e \phi_i$. The marginal gain of additional allocation to the ith channel is given by $\frac{\partial y_i}{\partial \phi_i} = \frac{w_i}{\phi_i}$. Let the channels be ordered such that $w_1 \geqslant w_2 \geqslant \cdots \geqslant w_n$. The optimal allocation procedure should first allocate $\phi_i = \phi_{\min}$ for $i = 1, \cdots, n$. Next, starting with the first channel in the ordered list, ϕ_1 should be increased from the initial value of $\phi_{\min}$ until the condition $\frac{\partial y_1}{\partial \phi_1} = \frac{\partial y_2}{\partial \phi_2}$ is reached which is equivalent to $\frac{\phi_1}{w_1} = \frac{\phi_2}{w_2}$ with $\phi_2 = \phi_{\min}$. From this point onward both ϕ_1 and ϕ_2 should be increased such that $\frac{\phi_1}{w_1} = \frac{\phi_2}{w_2}$ until the common ratio is equal to $\frac{\phi_3}{w_{\min}}$. The procedure continues including more and more channels while maintaining equal marginal gains for all channels under consideration. Due to the upper limit of $\phi_{\max}$ on ϕ_i, they may be capped at $\phi_{\max}$. The procedure continues until the condition $n\Phi_0 = \sum_{i=1}^{n} \phi_i$ is met. Our formulation of the algorithm is to carry out this allocation process in discrete values for computational efficiency.

The algorithm starts by allocating $\phi_i = \phi_{\min}, i = 1, \cdots, n$ and proceeds with the iteration by selecting increasing values for α so that to assign $\phi_i > \phi_{\min}$ to more and more channels in the increasing order of w_i until the condition $n\Phi_0 \geqslant \sum_{k=1}^{n} \phi_i$ is achieved. If the equality of constraint is not achieved, the subsequent steps performs fine tuning to achieve the optimal solution.

4 Numerical illustrations

We carried out computations of sample performance curves with parameter settings as follows. Cases with fixed transmission rate namely BPSK and multi-rates namely MQAM were considered. Block length equivalents of the target, minimum, and maximum security levels for these computations were respectively 128, 16 and 1024 bits. For the exponential adversary model, the decay constant k_i was set to 0.0001 for all $i = 1, \cdots, n$. It was assumed that the channel gain remains fixed during the transmission of a frame. For the optimization, $n = 5000$ channel samples were drawn from Rayleigh distribution with each setting of average signal to noise ratio (SNR). The optimum encryption block lengths were assigned based on the algorithm for each of the adversary models. The throughput was computed with optimum allocation of block lengths and with fixed block length of 128 bits. The gain in throughput was computed as $\frac{T_{\text{opt}} - T_{\text{fixed}}}{T_{\text{fixed}}}$, where T_{opt} and T_{fixed} are throughput with respectively the optimum and fixed block length allocations.

Fig. 1 shows the throughput gains of proposed adaptive encryption with respect to fixed block length encryption for single rate (BPSK) signaling. For the optimization process, the anticipated bit error probabilities during channel

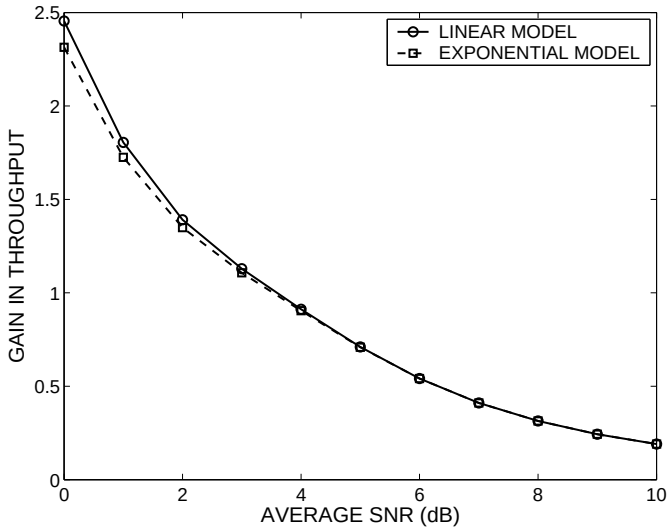

Fig. 1. Throughput gain of proposed channel adaptive encryption compared to fixed block length encryption for single rate (BPSK) transmisision. Linear and exponential adversary attack models are compared.

instantiations were evaluated using the following expression.

$$P_i(\gamma_i) = \frac{1}{2}\text{erfc}(\sqrt{\gamma_i})^1 \tag{18}$$

Here γ_i and $\bar{\gamma}$ are the frame-wise SNR and the average SNR. A throughput gain of 2.5 fold is observable with $\bar{\gamma} = 0dB$. Note that in this example the performance with exponential adversary model is slightly inferior to that of linear adversary model at low average SNR values. With exponential model, the probability of presence of an adversary increases as the encryption block length decreases. Thus the optimization process has a tendency to allocate larger block lengths to a larger fraction of frames compared to the case with linear model. Therefore, throughput loss is higher with exponential model compared to linear model. Nevertheless, the optimization process has its advantage with respect to fixed block length encryption, both with linear and exponential models. As the SNR increases the throughput gain with both models approaches a fixed value of about 0.2. Such a convergence is justified as follows. With large SNR values it is possible to use the largest possible block length for significantly large fraction of frames without causing much performance degradation. However, as we are interested in achieving a level of security equivalent to that with fixed block length encryption, the optimization algorithm is constrained to maintain

[1] $\text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-t^2} dt$

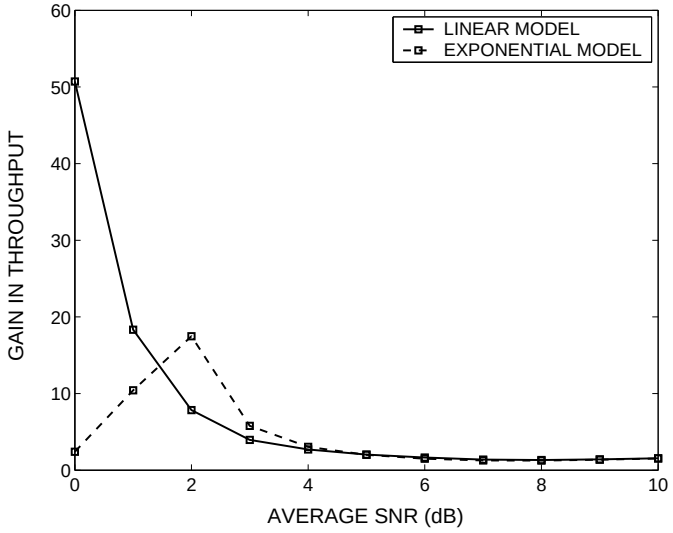

Fig. 2. Throughput gain of proposed channel adaptive encryption compared to fixed block length encryption for multi- rate (MQAM) transmisision. Linear and exponential adversary attack models are compared.

the allocation of large block lengths within a limit. Therefore the achievable throughput gain with respect to fixed block length encryption saturates at large SNR values.

Fig. 2 shows the performance with multi-rate (MQAM) transmission. The bit error probability of M-arry QAM is given by the well known approximation

$$P_i(\gamma) \approx \frac{\sqrt{M}-1}{\sqrt{M}log_2\sqrt{M}}\text{erfc}\left[\sqrt{\frac{3log_2M}{2(M-1)}\gamma}\right] \tag{19}$$

where M is the constellation size. In this computation we include BPSK and $M = 4, 16$, and 64 with which we have the set of transmission rates $R = 1, 2, 4$, and 6 bits/symbol. Rate and block length allocation in this case was performed in two steps. The maximum feasible rate R_i was selected from this set such that $R_i \leqslant \log_2(1+\gamma)$. The block length allocation followed with the optimization algorithms. Gain of 50 fold is observable at low SNR with linear models. However, with exponential model, the gain is maximized at moderate values of SNR around 2 dB, but decreases both at smaller and larger SNR values. The fact that transmission rates are optimally selected for the prevailing channel conditions by the channel adaptive rate selection procedure reduces the room for further optimization of throughput. In addition, the fact that the flexible encryption algorithm for exponential model has the tendency to select larger block lengths for a larger fraction of channel instantiations compared to the case with linear

model, brings the throughput performance close to that of fixed block length encryption. However for a range of intermediate SNR values, the optimization process shows significant performance improvement. As in the case of fixed rate transmission, the throughput gain converges to a fixed value of about 2 with both adversary models.

5 Conclusions

In this paper, we proposed and studied probabilistic models for adversary strength to crack a cipher. Based on these models, we formulated techniques where the encryption strength is a variable matched to the time varying channel, thereby improvement was brought to the throughput performance of wireless link with data encryption compared to using a fixed encryption block length. We presented optimal block length allocation algorithms with uniform and exponential distributions for the attacker strength leading to respectively the linear adversary model and the exponential adversary model. With linear model, the optimal allocation process uses fractional knapsack algorithm. We developed an algorithm resembling "water-filling" process for the case with exponential model. Numerical results were presented showing significant gains in throughput for a range of practical average SNR values. Results were presented for single rate (BPSK) transmission and channel adaptive multi-rate (MQAM) transmission. Different trends in throughput gains were observable with the two different adversary models and the associated optimization algorithms. This work shows the advantage of a channel adaptive flexible block length encryption scheme which is achievable with probabilistic models for adversary strength.

References

1. Stinson, D.R.: Cryptography: Theory and Practices. Discrete Mathematics and its Applications. CRC Press Inc., 2000 Corporate Blvd., N.W., Boca Raton, Florida 33431 (1995)
2. Schneier, B.: Applied cryptography: protocols, algorithms, and source code in C. 2nd edn. Wiley, New York (1996)
3. FIPS: Specification for the advanced encryption standard (AES). Federal Information Processing Standards Publication 197 (2001)
4. FIPS: Specification for the data encryption standard (DES). Federal Information Processing Standards Publication 46-2 (1988)
5. Stein, S.: Fading channel issues in systems engineering. IEEE Journal on Selected Areas in Communications **5**(2) (1987) 68–89
6. Y.Xaio, Guizani, M.: Optimal stream-based cipher feedback mode in error channel. IEEE Globecom Conference (Globecom 2005) (2005)
7. Ozarow, L.H., Shamai, S., Wyner, A.D.: Information theoretic considerations for cellular mobile radio. IEEE Trans. Veh. Tech. **43**(2) (1994) 359 – 378
8. Cormen, T.H., Leiserson, C.E., Rivest, R.L., Stein, C.: Introduction to Algorithms. Second edition edn. The MIT Press,, Cambridge, MA, (2003)
9. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley Series in Telecommunicatons. Wiley-Interscience, New York (1991)

10. Bapatla, S., Chandramouli, R.: Battery power optimized encryption. IEEE International Conference on Communications **27**(1) (2004) 3802–3806
11. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge University Press (2004)