

Robust Encryption for Secure Image Transmission over Wireless Channels

C. Nanjunda, M. A. Haleem and R. Chandramouli

Multimedia System, Networking, and Communications (MSyNC) Laboratory

Department of Electrical and Computer Engineering

Stevens Institute of Technology, Hoboken, NJ 07030

Email: {cnanjund,mhaleem,mouli}@stevens.edu

Abstract—The security of multimedia data transmitted over wireless networks is of increased interest. Encryption mechanisms securely transmit multimedia data over insecure networks. A major issue that has received very little attention so far is that the very same properties that gives ciphers (encryption mechanisms) their cryptographic strength make them sensitive to channel errors as well. In addition, this would enhance the error propagation inherent in compressed data. Therefore provision of security for multimedia transmission over wireless channel results in throughput loss. Nevertheless this lost throughput is traded for increased security. To our knowledge there has been no substantial effort to optimize this tradeoff. Opportunistic encryption proposed in this work is a way to optimize the tradeoff between security offered and the throughput lost due to a cipher. We show that opportunistic encryption methods that adapt to channel variations will lead to an overall increase in the system performance. Two broad scenarios are considered. (a) exact channel state information upto a finite time horizon is known and (b) only the average Signal-to-Noise Ratio (SNR) is known. Proposed opportunistic encryption framework is found to achieve significant gains in throughput compared to fixed block length encryption methods for a wide range of average SNR values. We have shown that applying opportunistic encryption on JPEG compressed image results in a better quality of received image and improved security compared to fixed block length encryption.

I. INTRODUCTION

Due to the growth of wireless networks in recent years and the open nature of the medium, the security of digital multimedia such as image, video, and audio transmitted over wireless networks has become very important. Wireless communication medium is open to intruders and also are highly time varying in quality. As many mobile wireless communication devices are operated with batteries of limited energy, the transmission of the bulky multimedia data, especially video, impose sever restrictions on the applicable security mechanisms.

Cryptography provides the tools to secure sensitive information. The issue of using cryptographically secure ciphers in noisy channel environments is that, the very same properties that gives ciphers their cryptographic strength make them sensitive to channel errors (avalanche effect) [1]. In block ciphers (which operates on the data a fixed block length at a time) a single bit flip in the encrypted data can cause a complete decryption failure. This sensitivity property causes more retransmissions compared to transmission without encryption, reducing the overall throughput. Usually ciphers that do not posses the property of avalanche effect (error propagation property) are weaker and can be broken with ease. Hence there is an inherent tradeoff between security and throughput.

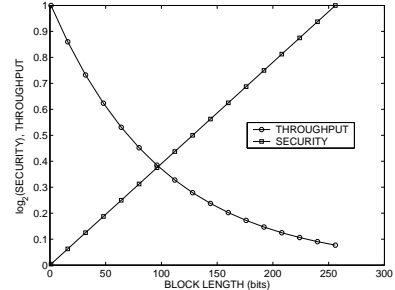


Fig. 1. Throughput (normalized to the maximum) and the log of security (normalized to the maximum) as a function of encryption block length at channel bit error probability, $P_b = 10^{-2}$.

The quality of a wireless channel varies due to time varying path-loss and multi-path fading phenomenon [2]. It has been shown that in order to achieve the capacity of wireless communication systems, opportunistic methods (channel adaptive resource assignment techniques) are necessary. In [3] the authors present channel adaptive transmission rate and power assignment as a way to achieve this. As the ciphers are sensitive to channel errors, the transmission overhead incurred by a cipher also varies with time. In this paper we consider the problem of achieving the optimal tradeoff between the throughput and the security via encryption. As shown in Fig. 1, for a given channel condition the throughput decreases with the encryption block length whereas the security increases with the block length. To the best of our knowledge, so far there has been no effort to optimize this tradeoff. The normalized throughput (with a fixed transmission rate) in this figure is given by $\frac{(1-P_b)^N}{(1-P_b)^{N_{min}}}$ where P_b is the bit error probability, N is the block length in number of bits, and N_{min} is the minimum block length. The set of block lengths used in the plot includes a single bit and from 16 bits to 256 bits in increments of 16 bits. The “security” is defined as 2^N due to the fact that decryption of a cipher of length N by an eavesdropper requires computations in the order of 2^N . The level of security of a cipher should be selected such that the cost of breaking it should be more than what the information it secures is worth. Weak ciphers (lesser security) in general have a higher probability of successful transmission with a given received Signal-to-Noise Ratio (SNR) but can be broken easily. Thus while adapting the security of ciphers to channel conditions, care must be taken to keep the overall security above a minimum security constraint enforced by the value of

the information being protected.

In this paper, we consider two strategies for selecting the optimum security levels (or encryption block lengths). First, by assuming exact channel knowledge over several time slots into the future, we derive a close form optimal solution. Next we propose a frame by frame optimization scheme based on the knowledge of long term average SNR of the channel. This approach assumes a cost function as a weighted combination of “throughput” and “security”. The optimum weights depend on the required security level and the average SNR of the channel. Our simulations in a frequency flat fading wireless channel with Rayleigh probability distribution for the signal envelop shows significant gain in throughput compared to a fixed encryption block length assignment for the same level of security in both approaches. To complete the introduction, we briefly discuss here the error propagation phenomenon in encryption and then mention the important aspects of the Advanced Encryption Standard (AES) [8] which we adopt in our experiments.

Block ciphers operate on plaintexts one block length at a time, converting it to ciphertexts of usually the same length. There have been various block ciphers proposed having different block lengths. Some block ciphers like AES are capable of operating on multiple block lengths. It is found throughout the literature that strong block ciphers exhibit the property of “completeness” and hence avalanche effect. Therefore a single uncorrected channel error can make the entire block of data illegible. This in turn implies that larger the encryption block length higher the probability of loosing the whole block because of a decryption failure. In [1] the authors have derived an expression for average post decryption bit error rate as a function of the encryption block length and the channel bit error rate. The derivation follows the fact that a single bit error in a transmitted data block of length N will cause the transmitted block to be in error. Thus the block error probability is given by

$$P_{bt} = 1 - [1 - P_b]^N \quad (1)$$

where P_{bt} is the channel block error probability, P_b is the channel bit error probability and N is the encryption block length. The error expansion property inherent in cipher causes one bit error to expand to all the bit hence resulting in half of the bits in the decrypted block to be in error. We may write,

$$P_{b,post} = \frac{1 - [1 - P_b]^N}{2} \quad (2)$$

where $P_{b,post}$ is the “post decryption” bit error probability. For $P_b < 10^{-2}$, we can approximate this expression to

$$P_{b,post} \approx \frac{N}{2} P_b \quad (3)$$

This is the post-decryption bit error probability for block ciphers operating in Electronic Code Book (ECB) mode. Interestingly, block ciphers operating in Cipher Block Chaining (CBC) and Cipher Feedback (CFB) modes [6] [7] also have

approximately the same post-decryption bit error probability [9]. Thus the error expansion, δ can be defined as

$$\delta \equiv \frac{P_{b,post}}{P_b} \approx \frac{N}{2} \quad (4)$$

Quantifying the amount of security provided by a cipher is a hard problem. One way to measure the security of a cipher is to measure the work involved to break it by the best known cryptanalysis method (shortcut attack). In the absence of any shortcut attacks to the cipher, the only way to crack it is to use the brute force technique (i.e for a given ciphertext, try decrypting with all possible encryption keys until it decrypts to the corresponding plaintext). A N bit encryption has 2^N possible keys to test, hence the complexity of cracking it is 2^N . For the purpose of this paper we consider the existence of a cipher which can encrypt using block/key lengths ranging from 16 bits to 256 bits in steps of 8. The analysis provided in this cipher can be extended to any cipher which offers flexible block and key lengths and/or any block cipher mode of operation that offers flexible block and key lengths.

The rest of the paper is organized as follows. The concept of opportunistic encryption is introduced in Section II. We formulate the block length selection problem as a Lagrange optimization in Section II-A and proceed to give the optimum solution when the exact channel conditions are known. In Section II-B we propose a cost function and steps to get optimal block lengths when only the average SNR of channel is known. Results from numerical computations/simulations are presented along with the theoretical discussions. We conclude the paper in section III.

II. OPPORTUNISTIC ENCRYPTION

Opportunistic encryption is a way to optimize the tradeoff between security offered and the throughput loss due to a cipher. In our discussions and experiments, we consider block ciphers, particularly the AES cipher. As discussed earlier, block ciphers operate on plaintext one block length at a time and usually support different encryption block lengths. We assume that there are no significant operational overheads in changing the block length parameter of the block cipher. We also assume that the key length used by the block cipher is equal to the block length. The above assumptions are made so that we can tweak the block length parameter in each time slot to tradeoff between the security and the throughput provided by the block cipher.

During the allocation of block lengths to K plaintext fragments (corresponding to K time slots), we assume that all the plaintext fragments are equally important and the adversary needs to crack most of the fragments to decode the information. Allowing for the possibility for shortcut attacks, we define the security level of an encrypted block to be $\log_2 N_i$, where N_i is the selected encryption block length for the i^{th} channel slot. The average security over K channel slots is computed as the mean $\frac{1}{K} \sum_{i=1}^K \log_2 N_i$. This is the average work involved for the adversary to crack all K packets. The average security of any allocation should be equal to or greater

than a specified minimum security constraint imposed by the value of the information (for the duration of K time slots). The security constraint can take any value from no security (corresponding to 0) to maximum security that the block cipher under consideration can offer. We further assume the existence of a key management protocol that periodically changes the encryption keys for all the key lengths used. The optimality condition is that the security levels selected should maximize the overall throughput of the system while guaranteeing an average security level equal to or greater than the specified security constraint. The throughput is defined as the useful transmission rate in bits/second accounting for the loss due to channel errors. We have assumed that the time slot durations are flexible.

At the receiver, where the decryption is performed, it is essential to know the encryption block length used. This information can be conveyed in one of the following ways: (a) in this paper, we have made a theoretical assumption that the frame lengths used in each of the time slots are equal to the encryption block lengths. Thus by looking at the frame lengths the receiver gets to know the encryption block lengths used. (b) if the frame lengths are independent of the encryption block lengths, the block lengths should be included as clear text payload in the frames. (c) if the receiver knows the minimum security constraints and the channel conditions, then it can perform the same optimization operations to identify the decryption block lengths.

A. Optimization With Exact Channel Knowledge Over Several Time Slots

Let the channel SNR, γ_i be known for the time slots $i = 1, \dots, n$ into the future. We are required to maximize the throughput subject to an overall security requirement over a finite horizon. For the i^{th} channel, with encryption block length N_i , if the bit error probability is sufficiently low, the block error probability given by (1) can be approximated as

$$P_{bl,i} \approx N_i P_b(\gamma_i, R_i) \quad (5)$$

with $N_i \in Q_N$, where Q_N is the set of available encryption block lengths, γ_i is the channel SNR, $R_i \in Q_R$ is the transmission rate selected from the set Q_R for the i^{th} block, and $P_b(\gamma_i, R_i)$ is the bit error probability. The “throughput” (successful bits/sec) of the i^{th} time slot is given by

$$D_i(\gamma_i, N_i, R_i) = R_i(1 - N_i P_b(\gamma_i, R_i)) \quad (6)$$

We define the security level, as \log_2 of encryption block length N_i normalized to the maximum as

$$S_i(N_i) = \frac{\log_2 N_i}{S_{max}} \quad (7)$$

where S_{max} is given by

$$S_{max} = \log_2 \left(\max_{N_i \in Q_N} (N_i) \right) \quad (8)$$

The definition of “security level” as used in the formulation also avoids domination by the exponential security in the optimization process with the brute force decryption assumption. We are required to maximize the throughput over the n channel slots subject to an overall security requirement given by

$$\frac{1}{n} \sum_{i=1}^n S_i(N_i) = S_{req} \quad (9)$$

We formulate a Lagrange optimization [5] problem as follows. The Lagrangian of the problem, $C^{(n)}$ can be written as weighted sum of the normalized throughput and the normalized security as

$$C^{(n)} = \frac{1}{n R_{max}} \sum_{i=1}^n D_i(\gamma_i, N_i) + \lambda \sum_{i=1}^n S_i(N_i) \quad (10)$$

where the parameter λ is the Lagrange multiplier and R_{max} is the maximum of the transmission rates. The optimum $C^{(n)}$ is where the partial differentials of (10) w.r.t. N_i are equal to zero. We then obtain the optimal N_i as

$$N_i = \frac{(\prod_{i=1}^n [R_i P_b(\gamma_i, R_i)])^{\frac{1}{n}}}{R_i P_b(\gamma_i, R_i)} e^{(S_{max} S_{req}) \log_e 2} \quad (11)$$

Clearly we see that the optimal encryption block lengths as computed above result in an encryption block length inversely proportional to the *probability of channel bit error*. This implies that “opportunistically” allocating larger block lengths for better channels should improve the performance.

Consider transmission with a fixed rate namely Binary Phase Shift Keying (BPSK) thus the maximum achievable throughput is 1 bit/symbol. The bit error probability of BPSK signaling is given by

$$P_b(\gamma_i) = \frac{1}{2} \text{erfc}(\sqrt{\gamma_i}) \quad (12)$$

and assume the “flat fading” wireless channel where the signal envelop is modeled with Rayleigh pdf leading to an exponential pdf for received SNR. Thus we have

$$p(\gamma_i) = \frac{1}{\bar{\gamma}} e^{-\frac{\gamma_i}{\bar{\gamma}}} \quad (13)$$

where $\bar{\gamma}$ is the average SNR.

In the numerical experiment, we generate a sequence of independent identically distributed (iid) $\{\gamma_i\}$ with the distribution as above at a range of values for $\bar{\gamma}$ and use the close form solution to compute the optimal N_i s. The feasible solutions should comply with the condition $N_i P_b(\gamma_i) < 1$ thus the time slots violating this condition are assumed not used for transmission. The overall security requirement setting is $S_{req} = 0.875$, which is equivalent to the security of 128 bit block encryption. The values of S_{max} is 8 ($\log_2(256)$). The gain in goodput of the opportunistic encryption scheme w.r.t.

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

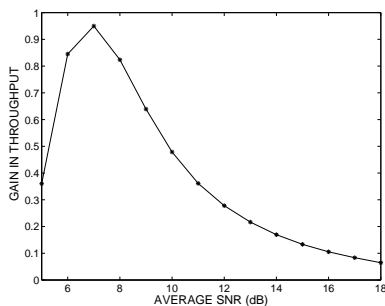


Fig. 2. Gain in goodput of opportunistic encryption with respect to fixed block length encryption for optimization when SNR values are known with BPSK as average SNR varies.

fixed encryption block length of 128 bits corresponding to the security level of 0.875 is given in Fig. 2. We observe a maximum gain of about 95% around 7 dB average SNR. The decline in gain above this level of average SNR is explained by the fact that for the considered range of N_i s the sensitivity of bit error probability to the error expansion is negligible as the bit error probability tends to be extremely low. At lower SNR the approximation used as in (5) is not valid.

B. Optimization With Known Average Channel SNR

In this subsection, we look at an approach when only the mean and the probability distribution of the channel SNR are known. We discuss a way to achieve the desired tradeoff between throughput and security on a frame by frame basis. We define a cost function as a weighted sum of throughput, D and the security, S where the weighted sum is a convex combination [4].

$$C(\gamma, N) = (1 - \lambda)D(\gamma, N) + \lambda S(N) \quad (14)$$

with $0 < \lambda < 1$. This *convex combination* is used to compute the optimal pair of D and S (which are related by N) for a given weighting vector $(\lambda, 1 - \lambda)$. However, the choice of λ is critical to the performance of the method presented herein. In a typical system, the values of R , N and hence D are discrete. When the pdf of the channel SNR and the average SNR are known, it is possible to pre-compute the optimum values of λ as a function of average D , S and C as follows:

- *Step 1:* At each average SNR setting, sufficient number of channel instantiations are generated using the known probability distribution of channel. The initial value of λ is set to 0
- *Step 2:* For each channel instance, the cost function in (14) is computed for each feasible value of N (rate fixed).
- *Step 3:* The maximum of $C(\gamma, N)$ and the corresponding value of D , and S are recorded.
- *Step 4:* Steps 2 – 3 are repeated for all the channel instantiations and the average value of D and S for the maximum C is computed.

Steps 2 – 4 are repeated for all values of λ .

To compare the relative performance of "opportunistic encryption" and the fixed block length encryption we encrypted a 512×512 Lenna image compressed by baseline JPEG compression using both opportunistic and fixed block length encryption. Baseline JPEG compression applies Discrete Cosine Transform (DCT) on the image to be compressed. The DCT transforms generates low frequency values called the DC values and the high frequency AC values. If the attacker captures the DC values, then the entire image can be reconstructed with some reduced quality. Hence while encrypting the image in JPEG compressed domain the lowest frequency components were encrypted using stronger average security equivalent to 192 bit block encryption. The second lowest frequency components were encrypted using average equivalent security of 160 bit encryption, thus reducing the security in steps of 32 bits, the highest frequency component encrypted using average equivalent security of 64 bit block encryption. The block lengths for opportunistic encryption were derived for all the frequency components by assuming the a channel with known average SNR. Block lengths for fixed block length encryption were fixed to be exactly equal to the average equivalent security of the corresponding frequency component. The compressed and encrypted image data was transmitted through a channel with known average SNR. Fig. 6 (a) and (b) shows the received Lenna image decrypted using opportunistic and fixed block length technique respectively. It is clear that Opportunistic encryption has lower post decryption BER and hence better throughput compared to fixed block length encryption. Fig. 3 gives the Peak Signal to Noise Ratio (PSNR) of the received image encrypted using opportunistic and fixed block length encryption for various average SNRs. It can be observed that opportunistic encryption leads to a better performance under all channel conditions.

To measure the resistance of the encryption techniques against brute force attacks we assume adversaries of various strengths. The strength of an adversary is the maximum encryption block length the adversary can crack. For example an adversary of strength 128 bits can crack all block encryptions which use either 128 bit block length or lesser. We consider adversaries with strengths ranging from 64 bit to 192 bit in steps of 32 bits. Fig. 4 gives the adversary strength

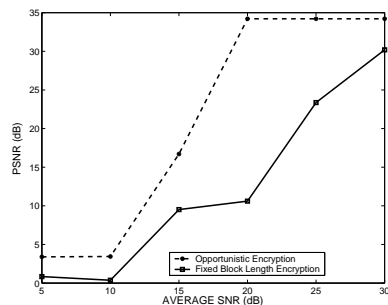


Fig. 3. Average SNR versus Peak SNR of the received Lenna image decrypted using Opportunistic encryption and fixed block length encryption.

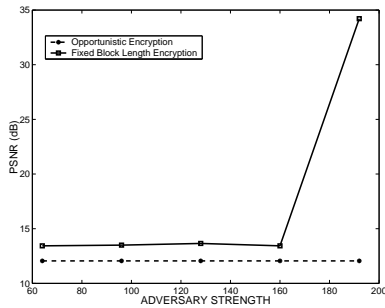


Fig. 4. Adversary strength versus Peak SNR of the cracked Lenna image encrypted using Opportunistic encryption and Fixed block length encryption.

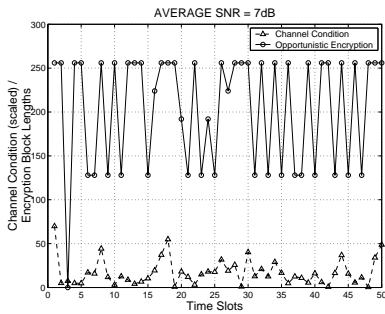


Fig. 5. Encryption block length allocations with respect to raw channel conditions (up-scaled by a factor of 20) for an average SNR of 7dB with the knowledge of probability distribution of SNR.

versus Peak SNR of the cracked Lenna image encrypted using Opportunistic encryption and fixed block length encryption. It is clear from the plot that opportunistic encryption is harder to crack compared to fixed block length encryption. An adversary of strength 192 bits can crack the fixed block length encryption completely but not opportunistic encryption. This is because opportunistic encryption has the flexibility to use block lengths greater than 192 bits for some eblobs but still maintain the same average security. This is evident in Fig 6 (c) and (d) which show the cracked Lenna image by adversary of strength 192 bits.

Fig. 5 gives the actual block length allocations for 50 successive channel instances generated by fixing the SNR to 7dB. From Fig. 3 and 5, it is clear that by allocating block lengths (or security levels) proportional to channel condition leads to an optimal solution.

III. CONCLUSION

This paper shows that opportunistic encryption based on wireless channel states could lead to significant gains in the throughput achieved for a specified security constraint. We considered the cases where the channel is exactly known for a finite horizon and only the average and the distribution of the channel SNR is known. Analytical and experimental results are presented. For the case where we assume exact channel knowledge and continuous encryption block length we get an improvement of 95% (around 5dB SNR) in the

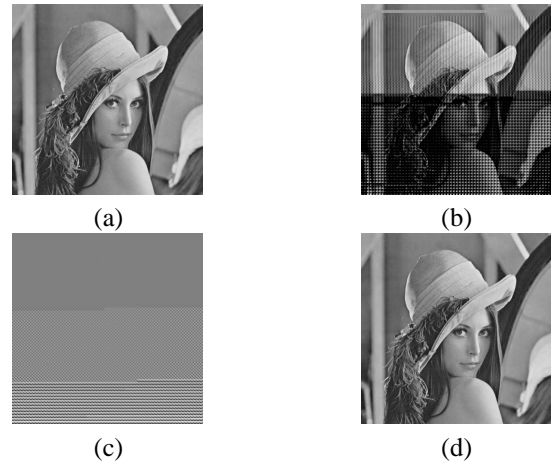


Fig. 6. Images (a) and (b) show recovered Lenna image encrypted using Opportunistic and Fixed block length encryption respectively at an average SNR of 20dB. Images (c) and (d) show cracked Lenna image encrypted using Opportunistic and Fixed block length encryption respectively by an adversary with computational power equivalent to 2^{128} .

throughput over fixed block length encryption. We apply the method obtained for the second case to the transmission of JPEG images in the Rayleigh fading channel. We obtained an improvement upto 25 dB in terms of Peak Signal to Noise Ratio (PSNR) with respect to fixed block length encryption. Further, we showed that the Opportunistic encryption of the same average security is more resistant to a cryptanalytic attack by a strong adversary compared to fixed block length encryption.

IV. ACKNOWLEDGMENT

This work is partially supported by NSF DAS 0242417.

REFERENCES

- [1] J. M. Reason and D. G. Messerschmitt, "The Impact of Confidentiality on Quality of Service in Heterogeneous Voice over IP Networks," *Springer-Verlag*, Berlin Heidelberg 2001.
- [2] W. C. Jakes, "Microwave Mobile Communications", John Wiley & Sons, New York, 1974.
- [3] A. J. Goldsmith and Soon-Ghee Chua, "Variable-Rate Variable-Power MQAM for Fading Channels", *IEEE Trans. Info. Theory*, Vol. 45, No. 10, Oct. 1997, pp. 1218-1230.
- [4] S. Boyd and L. Vandenberghe, "Convex Optimization", Cambridge Univ Press, 2004.
- [5] D. P. Bertsekas, "Dynamic Programming and Optimal Control", Athena Scientific, Belmont, Massachusetts, 1995.
- [6] William Stallings. *Cryptography and Network Security*, Peaterson Education, 2003, pp 27 - 30.
- [7] Bruce Schneier. *Applied Cryptography Second Edition: protocols, algorithms and source code* in C. John Wiley & Sons, Inc.
- [8] AES Proposal: Rijndael Joan Daemen, Vincent Rijmen, <http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf>
- [9] J. Reason, "End-to-end Confidentiality for Continuous-media Applications in Wireless Systems," Doctoral Dissertation, UC Berkeley, December 2000.