Opportunistic Encryption: A Trade-Off between Security and Throughput in Wireless Networks

Mohamed A. Haleem, *Member*, *IEEE*, Chetan N. Mathur, *Member*, *IEEE*,
R. Chandramouli, *Senior Member*, *IEEE*, and K.P. Subbalakshmi, *Senior Member*, *IEEE*

Abstract—Wireless network security based on encryption is widely prevalent at this time. However, encryption techniques do not take into account wireless network characteristics such as random bit errors due to noise and burst errors due to fading. We note that the avalanche effect that makes a block cipher secure also causes them to be sensitive to bit errors. This results in a fundamental trade-off between security and throughput in encryption based wireless security.[1] Further, if there is an adversary with a certain attack strength present in the wireless network, we see an additional twist to the security-throughput trade-off issue. In this paper, we propose a framework called *opportunistic encryption* that uses channel opportunities (acceptable signal to noise ratio) to maximize the throughput subject to desired security constraints. To illustrate this framework and compare it with some current approaches, this paper presents the following: 1) mathematical models to capture the security-throughput trade-off, 2) adversary models and their effects, 3) joint optimization of encryption and modulation (single and multirate), 4) the use of Forward Error Correcting (FEC) codes to protect encrypted packets from bit errors, and 5) simulation results for Rijndael cipher. We observe that opportunistic encryption produces significant improvement in the performance compared to traditional approaches.

Index Terms—Stochastic optimization, encryption, wireless security.

1 Introduction

The wireless communication medium is open to intruders. In a wireless network, an eavesdropper can intercept a communication by listening to the transmitted signal. Hence, encrypting the transmitted packets helps to achieve confidentiality. Traditionally, the design of encryption algorithms and their parameters has used only security against an adversary attack as the main criterion. To achieve this goal, the encrypted data or the cipher is made to satisfy several properties including the *avalanche* effect [17].

The avalanche criterion requires that a single bit change to the plain text or the key must result in significant and random-looking changes to the ciphertext. Typically, an average of one half of the decrypted bits should change whenever a single input bit to the decryption device is complemented. This guarantees that there will 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.

1. The channel error probability cannot be made zero but can only be made to approach zero asymptotically. Based on Shannon's theorem, one may in theory find a code that can make the error probability to approach zero asymptotically as long as the transmission rate is below the capacity of the channel and if the block length approaches infinity. In practice, however, block lengths are finite and the probability of error may never be made zero.

- *The authors are with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ 07030.*
E-mail: {mhaleem, cnanjund, rchandr1, ksubbala}@stevens.edu.

Manuscript received 6 Apr. 2006; revised 7 May 2007; accepted 20 June 2007; published online 16 July 2007.
For information on obtaining reprints of this article, please send e-mail to: tdsc@computer.org, and reference IEEECS Log Number TDSC-0041-0406.
Digital Object Identifier no. 10.1109/TDSC.2007.70214.

It is clear that block ciphers that satisfy the avalanche property are very sensitive to bit errors induced by the wireless link. That is, a single bit error in the received encrypted block will lead to an error in every bit of the decrypted block with probability 1/2. Therefore, we have severe error propagation. This leads to a fundamental trade-off between security (with respect to brute force attack) and throughput in encryption-based wireless security, as seen in Fig. 1. In this figure, for a given channel condition, the throughput decreases with the encryption block length, whereas the security increases with the block length. With the assumption that the encryption key length is always equal to or greater than the block length, the level of security of an encrypted block is decided by the block length. Throughput (normalized) is given by $(1 - P_b)^N$, where P_b is the bit error probability, and N is the encryption block length. The security here is defined as $\log_2 N$ (normalized by the maximum). This choice results in a monotonically increasing function capturing the strength of a cipher in a suitable manner and also is a convenience for the optimization. We explore throughput-security trade-off in this paper and investigate a framework called *opportunistic encryption* to optimize it. The term "opportunity" is used to mean channel opportunities, that is, the time durations when channel Signal to Noise Ratio (SNR) is reasonably high (equivalently the bit error rate is low). Note that the channel SNR is a random time-varying parameter. Opportunistic encryption provides a framework that exploits channel opportunities in order to optimize some encryption parameters (for example, encryption block length) based on the security and throughput constraints. It helps to control error propagation due to channel induced bit errors in the received encrypted data. In the process, we exploit the variable encryption block length feature offered in [16]. In Section 1.1 to follow, different modes of cipher in use are discussed, and the specific mode of our interest is

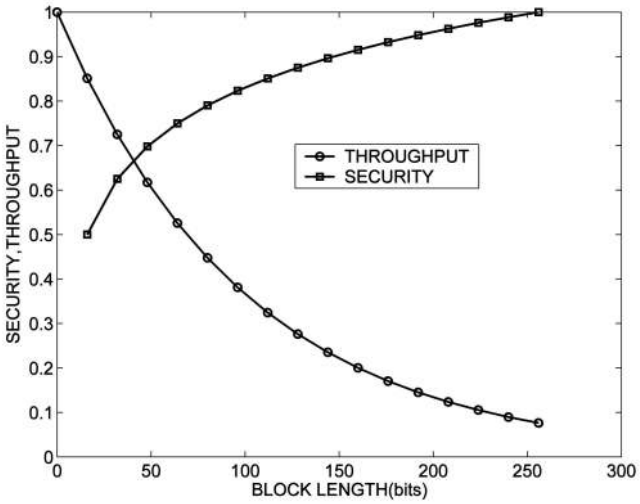

Fig. 1. Throughput (normalized) and security (normalized) as a function of encryption block length at channel bit error probability, $P_b = 10^{-2}$.

explained. Section 1.2 describes the methods of modeling and measure of the security of a cipher.

1.1 Different Modes in Ciphers

There are five basic modes of operation for a block cipher. The Electronic CodeBook (ECB) mode, Cipher Block Chaining (CBC) mode, Cipher FeedBack (CFB) mode, Output FeedBack (OFB) mode, and the CounTeR (CTR) mode. The ECB and CBC modes are referred to as block modes as the plaintext is encrypted a block at a time to produce the corresponding ciphertexts. In CFB, OFB, and CTR modes, some random value (usually a counter) is encrypted, and the resulting ciphertext bits are XORed with the plaintext bits to encrypt the plaintext. Since the encryption here (CFB, OFB, and CTR) can be performed one bit at a time, these modes are considered as stream modes. In the ECB mode, every plaintext block is independently encrypted to a ciphertext block. That is, error in one ciphertext block does not propagate to other ciphertext blocks during decryption. However, for lengthy messages, an ECB mode may not be secure as the cryptanalyst can use structures within the message to break the cipher [15]. In CBC mode, a given plaintext block is XORed with the previous ciphertext block before encryption. This is done to hide the structures within the message; however, due to chaining, an error in one ciphertext block will result in errors in multiple decrypted plaintext blocks. Stream modes of operation do not propagate any errors during transmission. Since the problem of error propagation and the resulting loss of throughput are inherent only to the block modes, in this paper, we consider the security—throughput trade-off with respect to only the block modes of operation. A problem similar to the one studied in this paper is presented in [25]. In it, the authors deal exclusively with the CFB mode of encryption. The overall throughput is formulated as a function of channel bit error rate, encryption block length, and the number of stages in CFB mode. It is shown that, as the number of stages increase, the throughput increases up to a peak value and then gradually decreases. The throughput formulation is used to derive the optimal number of stages for a given channel condition.

1.2 Security of a Cipher

The level of security against cryptanalysis may be measured as the amount of work (computations) required by the adversary to break the cipher. Ideally, a computationally secure encryption system would make it impossible to break the cipher with an exhaustive search approach having exponential order complexity. Nevertheless, practical encryption systems may have vulnerabilities leading to possible short cut attacks making it possible to break the cipher with algorithms of complexities less than an exponential order. Meanwhile, it is reasonable to say that there is no such thing as a completely secure encryption system, and the level of security can only be quantified relative to the strength of the adversary present in the environment. It is possible to model the adversary's "strength" to break a cipher as a random parameter using a probability distribution. It is reasonable to assume that the ability of the adversary to break the cipher becomes less probable as the key length, block length, diffusion, and so forth, increase. In this work, we consider some probability distributions to model the adversary's strength and investigate their effects on the security-throughput trade-off.

In the sequel, first, we discuss mathematical models to capture the security versus throughput trade-off. Then, maximization of throughput subject to a security constraint is set-up formally as an optimization problem. Several scenarios are considered in the formulations. The effect of modulation and coding on the security-throughput trade-off is studied. At the receiver side, the problem is modeled as a Markov Decision Process (MDP). The proposed analytical techniques are applied and tested on Rijndael cipher using computer simulations. A detailed comparison with a traditional approach is presented.

The rest of the paper is organized as follows: Section 2 discusses the channel model and measures of security used in this work. The concept of opportunistic encryption is introduced in Section 3. In Section 4, we discuss the use of FEC with and without opportunistic encryption. In Section 5, we propose solutions with limited knowledge of channel. Conclusions are presented in Section 6.

2 Channel Model and Security Measure

There are several ways in which one can quantify the strength of an encryption scheme [19]. One way is to measure the work involved in breaking it by the best known cryptanalysis method (or shortcut attack). In the absence of any shortcut attacks (for example, 10 round Advanced Encryption Standard (AES) [16] cipher), the only way to crack the encryption key is to use the brute force technique (that is, for a given ciphertext, try decrypting with all possible encryption keys until it decrypts to the corresponding plaintext). Let us consider a simple example. For an AES cipher with a key length of 128 bits, there are 2^{128} possible key combinations. Assuming unit complexity for testing one key (single decryption), the complexity involved in cracking a 128-bit AES cipher is 2^{128}. Note, however, that this is the worst-case complexity. This motivates a choice of a security measure (with respect to brute force attacks) to be $S(N) = \log_2(N)$, where N is the encryption block length. Note that in many practical encryption schemes, the block length and key length are equal. We will exploit this fact

throughout in this paper. With the maximum block length of N_{max}, we define the normalized security level as $s(N) = \frac{\log_2 N}{S_{max}}$, where $S_{max} = \log_2 N_{max}$.

2.1 Why We Need One Key per Block Length

In this paper, we propose to use a different encryption key for each possible block length in the block cipher. If a common key is to be used for all the block lengths, then an attack on the smaller block length would reveal a part of the key. After a part of the key is revealed, increasing the block length would not exponentially increase the security of the cipher. Since keys are changed only once in every session and thousands of encryption operations are performed before each key change, we expect minimal impact on the complexity of key management due to our requirement of having a separate encryption key per block length.

2.2 Security Quantification for a Brute Force Attack

Packet mode communication can be of fixed frame length or variable frame length. In either case, frame lengths are in general several times as large as encryption block lengths. We assume that each frame has a length (bits) that is equal to an integer multiple of encryption block length used in the frame. The security level of a frame is determined by the block length used in the encryption. Let a message consist of n frames with encrypted block length N_i bits for frame $i = 1, \cdots, n$. N_i is selected by the optimization procedure based on the channel condition. With the block fading [22] assumption of wireless channel, all the information bits in a frame are encrypted using the same encryption block length since the quality of the channel is assumed to be fixed over the frame duration. We make the assumption that every frame of the message (sequence of frames) is equally important to decode the message. In other words, one cannot decode the message unless every frame is decrypted. This applies to a scenario such as encryption of compressed image. Then, a reasonable measure is the mean of the security levels achieved by the individual frames. Thus, we have here

$$\bar{s} = \frac{1}{nS_{max}} \sum_{i=1}^{n} \log_2 N_i, \tag{1}$$

where $N_i \in Q_N$, the set of possible discrete encryption block lengths. Note $0 \leq \bar{s} \leq 1$.

2.3 Security Quantification with an Adversary Model

In addition to the discussion on the measure of security in Section 2.2, in this section, we propose a measure of *vulnerability* having an inverse relationship to security to be used in the optimization process with a probabilistic adversary model. As in the previous case, the amount of work needed to crack a cipher with brute force attack decides the security of a cipher. However, in this case, instead of a security measure based solely on the encryption parameters, we include in it the attacker's behavior. In particular, the attacker's capability to crack a cipher of certain block length is associated with a Probability Mass Function (PMF). Thus, we define the parameter "attacker strength" (denoted by α) having the dimension of block length and write the probability of cracking a cipher of block length N as $Pr(\alpha = N)$. The attacker with strength α has the capability to crack any cipher with block length $\leq \alpha$ within the useful time of the encrypted information and with a cost less than the value of it.

Let there be n frames of length L_i, $i = 1, \cdots, n$ in the message to be transmitted. A frame i is to be encrypted using block length N_i. In the discussion to follow, we assume that there is a fixed integer multiple c of encrypted blocks in a given frame, thus, $L_i = cN_i$. The approach can be easily extended to other cases. Hence, we define the *vulnerability* (which increases as the encryption block length is decreased) $0 \leq \Phi \leq 1$ of a message as the expected fraction of the total message being successfully cracked 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 $K(\leq n)$ distinct encryption block lengths being used and n_k be the number of frames with encryption block length less than or equal to N_k, $k = 1, \cdots, K$, and $Pr(\alpha = N_k)$ be the probability that the attacker's strength α is N_k. Note that $Pr(\alpha = N_k)$ also is the probability with which the n_k frames (in the ordered list) would be cracked by the adversary resulting in the leakage of a fraction $x_k = \sum_{i=1}^{n_k} l_i$ of the total message, where l_i is the frame length normalized by message length

$$\left(l_i = \frac{L_i}{\sum_{j=1}^{n} L_j} \right).$$

Thus, we can define the vulnerability Φ of the message as the expected leakage given by

$$\Phi = \sum_{k=1}^{K} x_k P(x_k), \tag{2}$$

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

$$\Phi = \sum_{k=1}^{K} Pr(x \geq x_k). \tag{3}$$

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

$$\Phi = \sum_{i=1}^{n} Pr(\alpha \geq N_i). \tag{4}$$

3 Optimizing Security-Throughput Trade-Off

As discussed in Section 1, avalanche effect causes one or more errors within an encryption block to propagate within the particular encryption block. Therefore, a single bit error in the received encrypted block will cause the loss of an entire block due to error propagation after decryption. Nevertheless, other blocks in the frame are not effected. Therefore, we make the assumption that a frame is not discarded due to errors in individual encryption blocks in that frame. The problem then is to maximize the

overall throughput while guaranteeing a minimum and/or an average security level(s) for the message. The throughput per block and, hence, a frame is given by $R_i(1-P_i)^{N_i} \approx R_i(1-N_iP_i)$ for $P_i << 1$ and for a given and fixed N_i, where R_i and P_i are, respectively, the transmission rate selected for the frame and the channel bit error probability. The throughput of the message (sequence of frames) can therefore be expressed as

$$T = \frac{1}{nR_{max}} \sum_{i=1}^{n} R_i(1-N_iP_i). \tag{5}$$

Here, the throughput is normalized by the maximum transmission rate $R_{max} = \max_i\{R_i\}$. The discussions on the optimization to follow assume exact channel knowledge over the sequence of frames (message). Let the channel SNR γ_i be known for the frames $i = 1, \cdots, n$. We present here the optimization problems for the two different attack models given in Section 2. The essence of the procedure is to optimally choose the encryption block lengths based on the channel condition and the required security.

Any strategy for optimum block length allocation depends on the knowledge of channel conditions. Further, there should be a mechanism for the receiver to know the encryption block length used during the transmission of each frame. The straightforward approach to achieve this is to include the block length information as a clear text payload in the frame. An alternative would be for the receiver to compute it from the security constraints and the channel state during the reception of the frame. This is feasible as the security constraints are agreed upon a priori, and the receivers usually have the capability to estimate the forward channel. Nevertheless, there could be computational overheads at the receiver. In the case where the frame length is a fixed integer multiple (known to receiver) of the block length, it is trivial for the receiver to compute the block length from the frame length.

The channel adaptive encryption methods presented in this paper heavily depend on the ability to know the channel quality in terms of SNR or the channel Bit Error Rates (BER) in advance. Although beyond the scope of this paper, the sensitivity of the performance to errors in channel knowledge has to be studied. Nevertheless, we mention here published work on channel estimation, tracking, and prediction. Channel estimation techniques for Orthogonal Frequency Division Multiplexing (OFDM) is discussed, for instance, in [26]. A technique for the prediction of channel in the short term for multiuser OFDM scenario can be found in [27]. Similarly, Wong et al. [28] present the methods for long-range channel prediction for OFDM systems.

3.1 Brute Force Attack Model

We are required to maximize the throughput subject to an overall security requirement over a finite horizon. This can be stated as a constrained optimization problem given by

$$\begin{aligned} &\max_{\{N_i\}} \frac{1}{nR_{max}} \sum_{i=1}^{n} R_i(1-N_iP_i) \\ &such\ that\ \ \frac{1}{nS_{max}} \sum_{i=1}^{n} \log_2 N_i = s_{req}. \end{aligned} \tag{6}$$

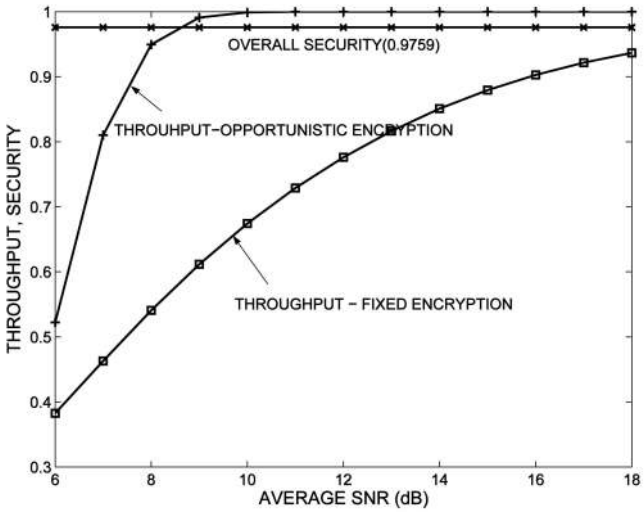

Fig. 2. Normalized throughput and security with opportunistic and fixed block size encryption for known channel SNR sequence and BPSK modulation.

Note that $P_i = P_i(\gamma_i, R_i)$ is a function of channel SNR γ_i and the transmission rate used for the frame R_i, and s_{req} is the required level of security. As shown in the appendices, the optimal block lengths are given by

$$N_i^* = \frac{\left(\prod_{i=1}^{n} R_iP_i\right)^{\frac{1}{n}}}{R_iP_i} e^{\left(S_{max}s_{req}\right)\log_e 2}. \tag{7}$$

In the case where the transmission rate is fixed, the above result reduces to

$$N_i^* = \frac{\left(\prod_{i=1}^{n} P_i\right)^{\frac{1}{n}}}{P_i} e^{\left(S_{max}s_{req}\right)\log_e 2}. \tag{8}$$

Clearly, we see that the optimal encryption block lengths as computed above are inversely proportional to the *probability of channel bit error*. This implies that "opportunistically" allocating larger block lengths for better channels, and vice versa, is the best strategy in the case of fixed rate.

First, we 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[2]

$$P_i = \frac{1}{2}\mathrm{erfc}(\sqrt{\gamma_i}). \tag{9}$$

The assumption of a "flat fading" wireless channel with a Rayleigh probability density function (pdf) for signal envelop and, thus, an exponential pdf for received SNR is

$$p(\gamma_i) = \frac{1}{\bar{\gamma}} e^{\frac{\gamma_i}{\bar{\gamma}}}, \tag{10}$$

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

The comparison of the throughput observed in simulations using opportunistic encryption block lengths computed from (8) and fixed block size encryption is shown in Fig. 2. For the purpose of illustrating the optimization process, we let the block length to assume any positive

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

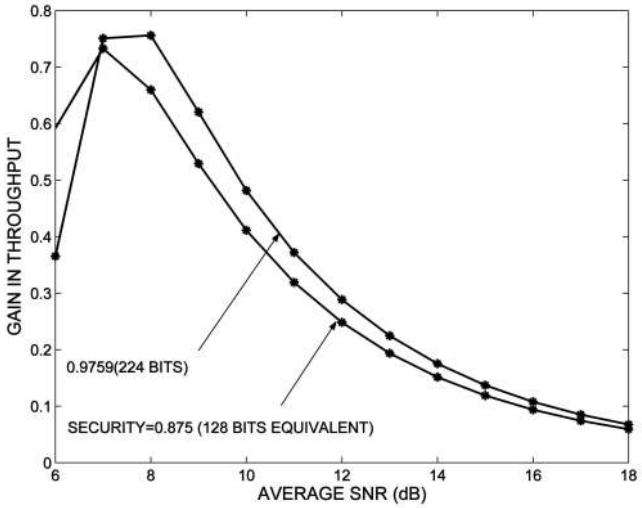

Fig. 3. Throughput gain with opportunistic encryption for known channel SNR sequence and BPSK.

integer value. In the sequel however, we adopt block lengths as per to Rijndael cipher with practically useful block lengths. The overall security requirement setting for this result is $s_{req} = 0.9759$, which is equivalent to the security of a 224 bit fixed block encryption, and

$$S_{max} = \log_2(256) = 8.$$

The gain in throughput was computed as $\frac{T_{opt} - T_{fixed}}{T_{fixed}}$, where T_{opt} and T_{fixed} are the throughput of optimum and fixed block length allocations. Shown in Fig. 3 are gains for two different settings of overall security values of 0.875 and 0.9759. We observe that the gain varies over the range of average SNR values. Maximum gain of about 73 percent is observed at around 7 dB average SNR with $s_{req} = 0.875$. The decline in the gain above a 7-dB average SNR is explained by the low bit error probabilities in this range. The throughput is close to the maximum for all values N_i under consideration. At lower SNR, the BER are high, and in (8), the factor

$$\frac{\left(\prod_{i=1}^{n} P_i\right)^{\frac{1}{n}}}{P_i}$$

approaches unity. Therefore, $N_i \rightarrow e^{(S_{max} s_{req}) \log_e 2}, i = 1, \cdots, n$, which is the fixed block length corresponding to the security level. Hence, the gain in throughput with respect to fixed block length encryption approaches zero.

Fig. 4 compares the throughput of opportunistic and fixed block length Rijndael [16] encryption. For the opportunistic encryption, the encryption block lengths were selected from the set $Q_N = \{128, 160, 192, 224, 256\}$ (bits), and the plaintext block size for fixed block length encryption was 224 bits. It is seen in this figure that the observed throughput gain is smaller than the theoretical gain. This is due to the fact that the number of available block sizes in Rijndael cipher is small. Next, we consider an example with multiple transmission rates including BPSK and higher order Quadrature Amplitude Modulation (QAM) schemes. The probability of a bit error of a M-ary QAM signal is given by the well-known approximation [2]

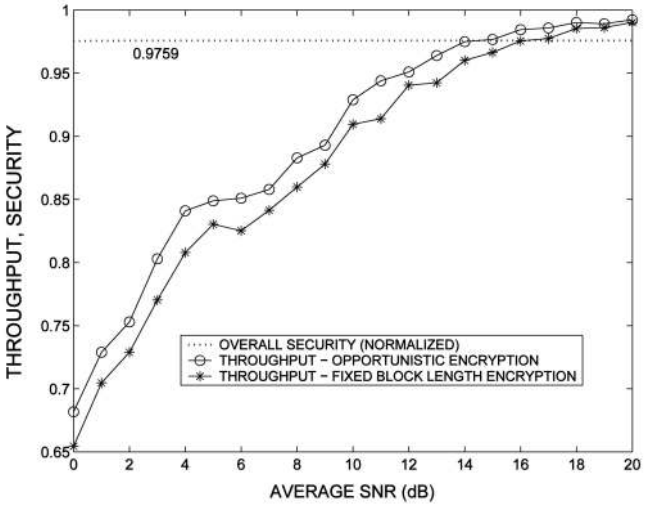

Fig. 4. Throughput comparison of opportunistic and fixed block length Rijndael encryption using BPSK modulation.

$$P_i \approx \frac{\sqrt{M} - 1}{\sqrt{M} \log_2 \sqrt{M}} \operatorname{erfc}\left[\sqrt{\frac{3 \log_2 M}{2(M-1)} \gamma_i}\right], \qquad (11)$$

where M is the constellation size. We use BPSK and the set $Q_M = \{4, 16, 64\}$ in this work. Correspondingly, the set of maximum achievable throughput values are $Q_R = \{1, 2, 4, 6\}$ bits/symbol.

Fig. 5 shows the gain in throughput with variable rates. A gain of 109 percent is observable around 9 dB average SNR. Fluctuation in the gain is observed with increasing SNR, and this is due to the discrete rate control.

3.2 Adversarial Attack

For the discussion in this section, we consider two probability distributions, namely, uniform and exponential to model the adversary strength. We show in the sequel that with uniform distribution, the optimization problem is equivalent to "fractional knapsack" problem

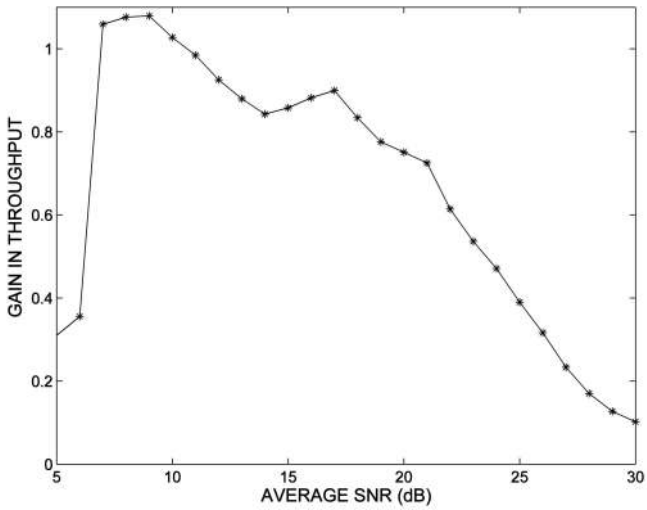

Fig. 5. The gain in the throughput of opportunistic encryption with respect to fixed block length encryption against an average SNR for multiple rate case.

and, therefore, the optimum algorithm has linear execution time. With the exponential distribution, the optimal solution resembles "water-filling" algorithm. As before, we assume that the frames are not discarded due to bit errors in some encryption block in the frame.

3.2.1 Linear Adversary Strength Model

Let the probability mass function (PMS) describing an adversary's strength has a uniform distribution, that is, $\Pr(\alpha = N_i) = \frac{1}{N_{max} - N_{min}}$, for $i = 1, \cdots, n$, where N_{min} and N_{max} are the minimum and maximum block lengths available in the crypto system. That is, the probability that the adversary can successfully attack a ciphertext block (key) length N_i is uniformly distributed. This conclusion leads to

$$\phi_i = \Pr(\alpha \geq N_i) = \frac{N_{max} - N_i}{N_{max} - N_{min}}, i = 1, \cdots, n. \tag{12}$$

Now, we are required to maximize the throughput given by

$$T = \frac{1}{nR_{max}} \sum_{i=1}^{n} R_i(1 - P_i(N_{max} - (N_{max} - N_{min})\phi_i)) \tag{13}$$

subject to the conditions

$$\begin{aligned} \phi_{min} \leq \phi_i \leq \phi_{max}, i = 1, \cdots, n, \\ \frac{1}{n} \sum_{i=1}^{n} \phi_i \leq \Phi_0. \end{aligned} \tag{14}$$

Φ_0 is the maximum allowable average vulnerability level, and ϕ_{min} and ϕ_{max} are the corresponding minimum and maximum allowable values for a frame. It is easily seen that the optimal solution is achieved with equality in condition (14). By expanding (13) and omitting the terms that are independent of ϕ_i, $\forall i$, the problem reduces to the following:

$$\max_{N_i} T' = \sum_{i=1}^{n} w_i \phi_i, \tag{15}$$

where $w_i = P_i R_i$. This problem is a special case of a *fractional knapsack problem*, which is solvable in polynomial time. It can be seen that selecting the ϕ_is in the nonincreasing order of maximum w_i maximizes T' and, hence, T [23]. Observe that for every frame i, we should allocate a minimum vulnerability level, ϕ_{min}, corresponding to the maximum encryption block length, N_{max}. Therefore, the formulation can be modified such that the optimization problem is

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

$$\frac{1}{n} \sum_{i=1}^{n} \phi_i \leq \Phi_0'; 0 \leq \phi_i \leq \phi_{max} - \phi_{min}, \tag{16}$$

where $\Phi_0' = \Phi_0 - n\phi_{min}$. The following algorithm solves the problem optimally [24]:

1. *Initialization*: Allocate a vulnerability level of ϕ_{min} for all frames i, $i = 1, \cdots, n$.
2. Sort the frames in a nonincreasing order of $w_i = P_i R_i$, $i = 1, \cdots, n$.
3. Allocate the additional maximum allowed vulnerability level less than or equal to $\phi_{max} - \phi_{min}$ for each frame i in the sorted order, that is, $w_i > w_{i+1}$. That is, allocate $\phi_{max} - \phi_{min}$ units to frames $i = 1, \cdots, j^* - 1$ for some j^* and fewer than $\phi_{max} - \phi_{min}$ or 0 for frame $i = j^*$ with the sum total of the additional allocation equal to Φ_0'. Frames $i = j^* + 1, \cdots, n$ get no additional allocation above ϕ_{min}.

3.2.2 Exponential Adversary Strength Model

Let the attacker strength be given by

$$\phi_i = \Pr(\alpha \geq N_i) = e^{-kN_i}, \tag{17}$$

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

$$T = \frac{1}{nR_{max}} \sum_{i=1}^{n} R_i \left(1 + \frac{P_i}{k} \log_e \phi_i\right) \tag{18}$$

subject to the conditions

$$\phi_i - \phi_{min} \geq 0, i = 1, \cdots, n, \tag{19}$$

$$\phi_{max} - \phi_i \geq 0, i = 1, \cdots, n, \tag{20}$$

$$\Phi_0 - \frac{1}{n} \sum_{i=1}^{n} \phi_i = 0, \tag{21}$$

where Φ_0 is the maximum allowable overall vulnerability level. The equality in (21) results from the observation that maximum of T is achieved by using the maximum allowed overall vulnerability. The augmented objective function can then be written as

$$\begin{aligned} C = \frac{1}{nR_{max}} \sum_{i=1}^{n} R_i \left(1 + \frac{P_i}{k} \log_e \phi_i\right) + \nu \left(n\Phi_0 - \sum_{i=1}^{n} \phi_i\right) \\ + \sum_{i=1}^{n} \lambda_i(\phi_i - \phi_{min}) + \sum_{i=1}^{n} \mu_i(\phi_{max} - \phi_i), \end{aligned} \tag{22}$$

where ν, λ_i, and μ_i, $i = 1, \cdots, n$, are constants (Lagrange multipliers). The Karush Kuhn-Tucker Conditions (KKC) [6] for this problem are obtained by considering the vanishing point of the first-order derivative of C with respect to ϕ_i and also from the complimentary slackness. Thus, we have

$$\begin{aligned} \phi_i = \frac{R_i P_i}{knR_{max}(\mu_i + \nu - \lambda_i)}, \\ \lambda_i(\phi_i - \phi_{min}) = 0, \\ \mu_i(\phi_{max} - \phi_i) = 0, \\ \lambda_i \geq 0, \\ \mu_i \geq 0, \\ \Phi_0 - \sum_{i=1}^{n} \phi_i = 0, \\ \nu \geq 0, \end{aligned} \tag{23}$$

for $i = 1, \cdots, n$. Therefore, the optimal value of ϕ_i, for $i = 1, \cdots, n$, 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 $\alpha = \frac{1}{k\nu nR_{max}}$, $\nu > 0$ and $w_i = R_i P_i$.

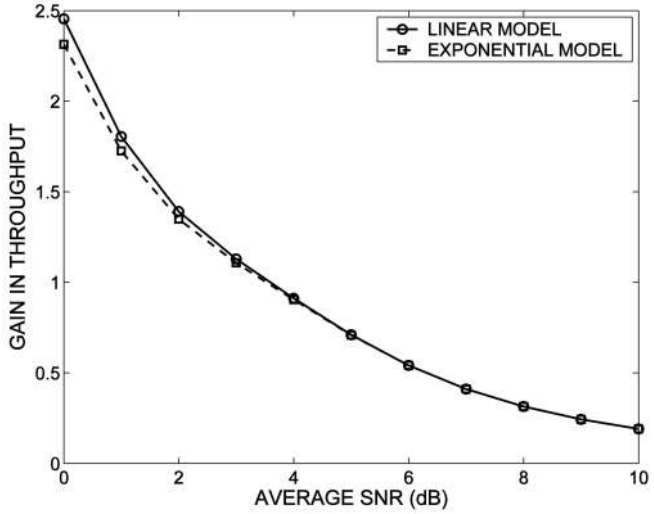

Fig. 6. Throughput gain due to proposed channel adaptive encryption compared to fixed block length encryption for single rate (BPSK) transmission. Both linear and exponential adversary attack models are shown.

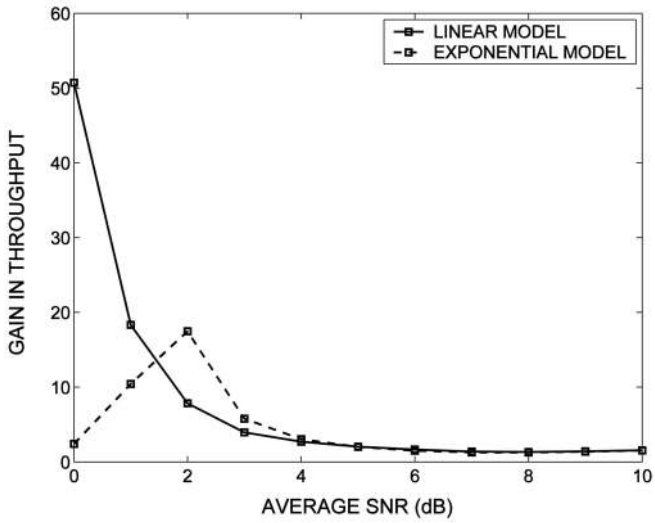

Fig. 7. Throughput gain due to proposed channel adaptive encryption compared to fixed block length encryption for multirate (MQAM) transmission. Both linear and exponential adversary attack models are shown.

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, $i = 1, \cdots, n$, computed complies with one of the three cases above:

1. Sort the channels in a nonincreasing 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 go to step 2; else, go to step 5.
5. If $n\Phi_0 = \sum_{k=1}^{n} \phi_i$, the current set of ϕ_i, $i = 1, \cdots, n$ are optimal; else, go to 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 $\phi_i = \alpha w_i$, $i = 1, \cdots, n$; $\phi_i(\phi_i < \phi_{min}) = \phi_{min}$; $\phi_i(\phi_i > \phi_{max}) = \phi_{max}$; go to the step 8; else, set $l = l - 1$ and go to 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 go to step 7; else, set $l = l - 1$; go to 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 appendices provide an explanation as to how this algorithm indeed provides the optimal solution.

We carried out computations of sample performance curves with certain parameter settings. A case with fixed transmission rate, namely, BPSK and multirate, namely, MQAM were considered. Block length equivalents of the target, minimum, and maximum security levels for this computation are, respectively, 128, 16, and 1,024 bits. For the adversary model with exponential probability distribution, the decay constant k_i was set to 0.0001, for all $i = 1, \cdot, n$. It was assumed that the channel gain remains fixed during the transmission of a frame. For the optimization, $n = 5,000$ channel samples were drawn using a Rayleigh distribution with a given average SNR. The optimum encryption block lengths were assigned based on the algorithm for each of the adversary models. The throughput was computed with an optimum allocation of block lengths and with a fixed block length of 128 bits.

Fig. 6 shows the gain in throughput with respect to fixed block length encryption. The results are given for the two different probabilistic models of the attacker and for single rate (BPSK) signaling. As seen in the results, a throughput gain of 2.5-fold is observable at $\bar{\gamma} = 0dB$. Note in the example that the performance when the adversary is modeled with exponential distribution is slightly inferior to that of uniform distribution at low average SNR, in all cases. With the exponential model, adversary has a larger probability of breaking the encryption with a smaller encryption block length compared to a larger block length. Thus, the optimization process has a tendency to allocate larger block lengths to a larger fraction of frames compared to the case with uniform distribution. Therefore, higher frame error rates results more frequently with exponential probability distribution than in the case of uniform distribution of adversary strength.

Fig. 7 shows the performance with multirate (MQAM) transmissions. It is seen that with the exponential model, the gain has a peak at moderate average SNR values. This is akin to the fact that with exponential model, the optimization algorithms have a tendency to select larger encryption block lengths for a larger fraction of channel instantiations compared to the case with linear model. The fact that transmission rates are optimally selected for the channels and encryption block lengths are mostly large regardless of

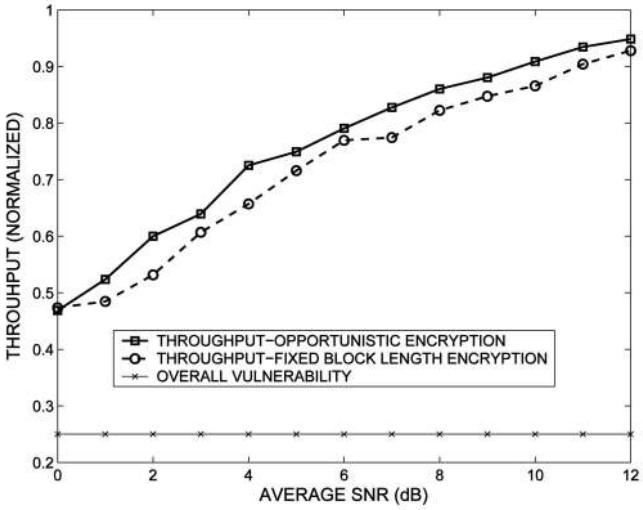

Fig. 8. Throughput comparison of opportunistic encryption and fixed block length encryption for single rate (BPSK) with a linear probability model of attacker strength and Rijndael cipher.

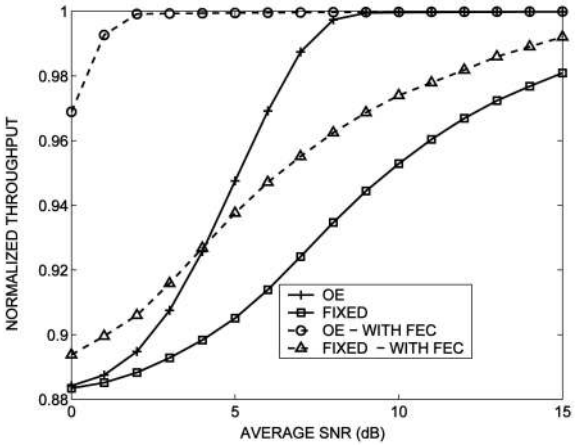

Fig. 9. Throughput of opportunistic encryption and fixed block length encryption with and without FEC (RS code with $t = 15$) as an average SNR varies.

the channel conditions brings the throughput performance close to that of fixed block length encryption. However, there is a range of SNR in which the optimization process has higher gains.

The throughput performance with the probabilistic models of attacker for finite set of encryption block sizes available in the Rijndael cipher is shown in Fig. 8. As with the deterministic models in the previous cases, we observe a marginal gain in throughput due to limited flexibility in the encryption block length sizes.

4 Forward Error Correction Codes

In order to investigate the performance of opportunistic encryption compared to concatenated encryption and forward error correction codes with fixed block length encryption, we used the Read-Solomon (RS) code. In RS, coding redundancy is added to a k symbols of information block to achieve an n symbol codeword leading to (n, k) code. In a $q - ary$ RS code with error correction capability of t symbols, we have $n = q - 1$ and $k = q - 1 - 2t$. Setting the leading l symbols to zero does not change the error correction capability. Thus, deleting this leading l symbols, we obtain the shortened $(q - 1 - l, q - 1 - 2t - l)$ RS code with an error correction capability of t symbols [21]. In the cipher system we consider in this work, information is processed in bytes. Therefore, an RS code with $q = 2^8$ is an appropriate choice. Thus, we adopt a code capable of handling blocks of 255 bytes or less as input. The postdecoding bit error probability of this code can be approximated by

$$P_{bc} \approx \frac{1}{8k}\left(1 - \sum_{i=0}^{t}\binom{255-l}{i}P_s^i(1-P_s)^{255-i-l}\right). \quad (24)$$

$P_s = 1 - (1 - P_b)^8$ here is the byte error probability without coding, and P_b is the bit error probability.

The throughput performance for fixed block length encryption and opportunistic encryption with BPSK with and without FEC (RS code) with $t = 15$ is illustrated in Fig. 9. This result was obtained with the optimization technique based on the deterministic measure of security, as presented in Section 3.1. It is seen that at low SNR values, the throughput performance of a fixed block length encryption with FEC outperforms opportunistic encryption. As the SNR increases, the opportunistic encryption without FEC tends to significantly outperform fixed block length encryption with FEC. At low SNR values, the reduction in block error rate due to FEC has a larger effect than the benefit of adaptive block length selection. However, as the SNR is increased, the opportunistic encryption achieves higher flexibility to optimize the throughput using the large dynamic range in encryption block lengths with minimal effect on throughput.

5 Opportunistic Encryption as Stochastic Optimization

Optimal block length selection for encryption with a known sequence of channel gain serves as the way to derive the optimal trade-off in security and performance. Such an approach may be applicable if the current and future channel states are known exactly. In the absence of such knowledge, optimization under uncertainty may be essential. In this section, we present stochastic optimization approaches with two different levels of channel knowledge.

5.1 Optimization Based on Finite State Markov Channel Model

In this section, we present a method applicable when the channel state transitions can be modeled by a *Finite State Markov Chain* (FSMC) [7]. It is assumed that the actual state of the current channel is known prior to each transmission. Then, the selection of encryption block lengths can be considered as the control decisions considering the current and future channel states with the formulation of a finite horizon discrete time MDP [9]. To this end, we are required to define the state space, the transition probabilities, and the control actions.

5.1.1 Finite State Markov Chain Model for the Wireless Channel

For the model, the fading is assumed to be sufficiently slow such that the channel is assumed to remain constant during

the transmission of a data frame. The signal power and, hence, the SNR, γ of Rayleigh fading channel has an exponential pdf given by (10). The bit error probability of BPSK signaling as a function of received SNR is given by (9). Thus, the steady state probability of a state i is defined by a range of SNR from γ_i to γ_{i+1}, as that in [7]:

$$p_i = \int_{\gamma_i}^{\gamma_{i+1}} \frac{1}{\bar{\gamma}} e^{\frac{\gamma}{\bar{\gamma}}} d\gamma = e^{-\frac{\gamma_i}{\bar{\gamma}}} - e^{-\frac{\gamma_{i+1}}{\bar{\gamma}}} \tag{25}$$

and the probability of bit error or the crossover probability in state i is

$$P_b^{(i)} = \frac{[\int_{\gamma_i}^{\gamma_{i+1}} e^{-\frac{\gamma}{\bar{\gamma}}} \mathrm{erfc}(\sqrt{\gamma}) d\gamma]}{[\int_{\gamma_i}^{\gamma_{i+1}} e^{-\frac{\gamma}{\bar{\gamma}}} d\gamma]}. \tag{26}$$

The probability of transition from state i to state $i+1$ (for $i = 1, \cdots, r-1$) is approximately given by

$$P_{i,i+1} \approx \frac{K_{i+1}}{R_{bl} p_i}, \tag{27}$$

whereas the probability of transition from state i to state $i-1$ (for $i = 2, \cdots, r$) is by

$$P_{i,i-1} \approx \frac{K_i}{R_{bl} p_i}. \tag{28}$$

Here, R_{bl} is the transmission rate in number of frames per second, and p_i is the probability the channel is in state i, as in (25). K_{i+1} is the expected number of level crossing per second and is a function of maximum *Doppler frequency*, f_m, and the SNR level, γ_i given by

$$K_i = \sqrt{\frac{2\pi\gamma_i}{\bar{\gamma}}} f_m e^{-\frac{\gamma_i}{\bar{\gamma}}}. \tag{29}$$

The maximum Doppler frequency is defined as $f_m = \frac{v}{\lambda}$ with v, the speed of the vehicle and λ, the wavelength of the carrier. As is the case with practical scenarios, we assume that the probabilities of transition to states other than adjacent are negligible and, therefore, we have

$$P_{i,i} = 1 - P_{i,i+1} - P_{i,i-1} \tag{30}$$

one step transition to states other than self and adjacent states is not possible.

5.1.2 Markov Decision Process (MDP) Formulation

We define the state of the system by a combination of channel state and the amount of data successfully transmitted. Thus, a state is given by the tuple $i \in \{(c_i, b_i) | c_i = 1, \cdots, r; b_i = 1, \cdots, q\}$, where c_i, b_i, r, and q are, respectively, the channel state, the number of bits successfully transmitted, the number of channel states, and the capacity of the receiver buffer in number of bits. Note that two distinct system states i and j such that $i \neq j$ does not imply $c_i \neq c_j$ or $b_i \neq b_j$. However, if $c_i = c_j$ and $b_i = b_j$, then $i \equiv j$. Following a transmission, the success/failure of the correct reception is fed back to the transmitter by an ACK/NACK signal. We define the set of actions as the available encryption block lengths. Then, we can write the receiver buffer occupancy b_i as a sum of a combination of encryption block lengths. Thus, $b_i = \sum_{a=1}^{k} m_a N_a$, where there are k different possible encryption block lengths, and m_a blocks of length N_a were successfully transmitted. It should be noted that there are more than one possible combinations of encryption block lengths resulting in the same b_i. A transition from state i to state j implies that the channel has changed from state c_i to c_j, and the total number of bits transmitted has changed from b_i to b_j. When the channel is statistically stationary, the probability of transition from a state i to state j under action a is independent of the time n and can be expressed as

$$\begin{aligned} P_{ij}(a) = Pr(c(n+1) = c_j, \\ b(n+1) = b_j | c(n) = c_i, b(n) = b_i, a), \end{aligned} \tag{31}$$

where the action a represents the selection of corresponding encryption length N_a. We observe from (27) and (28) that the channel state transition probabilities depend on the frame rate R_{bl}. We discuss here a scenario where the frame length is the same as the encryption block length, N_a, and the extension to the case with fixed frame length is straightforward. Note that the frame rate is inversely proportional to N_a. It is easy to see that (31) can be rewritten as

$$P_{ij}(a) = \begin{cases} Pr(c(n+1) = c_j | c(n) = c_i)(1 - P_{bl,a}(c_i)), \\ b_j = b_i + N_a, |c_j - c_i| \leq 1 \\ Pr(c(n+1) = c_j | c(n) = c_i) P_{bl,a}(c_i), \\ b_j = b_i, |c_j - c_i| \leq 1 \\ 0 \qquad \text{otherwise}, \end{cases} \tag{32}$$

where $Pr(c_{n+1} = c_j | c_n = c_i)$ is the channel transition probability, and the block error probability $P_{bl,a}(c_i)$ in channel state c_i under action a is given by

$$P_{bl,a}(c_i) = 1 - (1 - P_b(c_i))^{N_a}. \tag{33}$$

Here, $P_b(c_i)$ is the channel *bit error probability* in channel state c_i. Equation (32) is written considering the fact that the total number of transmitted bits will increase with number of successfully transmitted frames and remain the same with failures.

Substituting from (27), (28), (29), (30), and (33) into (32) along with the use of the expression for block rate, $R_{bl,a} = \frac{R_b}{N_a}$ in terms of the bit rate R_b and encryption block length, N_a, we get

$$P_{ij}(a) = \begin{cases} \sqrt{\frac{2\pi\gamma_{i+1}}{\bar{\gamma}}} f_m e^{-\frac{\gamma_{i+1}}{\bar{\gamma}} \frac{N_a (1 - P_b(c_i))^{N_a}}{R_b p_i}}, & b_j = b_i + N_a, c_j = c_i + 1, \\ \sqrt{\frac{2\pi\gamma_i}{\bar{\gamma}}} f_m e^{-\frac{\gamma_i}{\bar{\gamma}} \frac{N_a (1 - P_b(c_i))^{N_a}}{R_b p_i}}, & b_j = b_i + N_a, c_j = c_i - 1, \\ \left[1 - \left(\sqrt{\frac{2\pi\gamma_{i+1}}{\bar{\gamma}}} e^{-\frac{\gamma_{i+1}}{\bar{\gamma}}} + \sqrt{\frac{2\pi\gamma_i}{\bar{\gamma}}} e^{-\frac{\gamma_i}{\bar{\gamma}}}\right) f_m\right] \frac{N_a (1 - P_b(c_i))^{N_a}}{R_b p_i}, & b_j = b_i + N_a, c_j = c_i, \\ \sqrt{\frac{2\pi\gamma_{i+1}}{\bar{\gamma}}} f_m e^{-\frac{\gamma_{i+1}}{\bar{\gamma}} \frac{N_a (1 - (1 - P_b(c_i))^{N_a})}{R_b p_i}}, & b_j = b_i, c_j = c_i + 1, \\ \sqrt{\frac{2\pi\gamma_i}{\bar{\gamma}}} f_m e^{-\frac{\gamma_i}{\bar{\gamma}} \frac{N_a (1 - (1 - P_b(c_i))^{N_a})}{R_b p_i}}, & b_j = b_i, c_j = c_i - 1, \\ \left[1 - \left(\sqrt{\frac{2\pi\gamma_{i+1}}{\bar{\gamma}}} e^{-\frac{\gamma_{i+1}}{\bar{\gamma}}} + \sqrt{\frac{2\pi\gamma_i}{\bar{\gamma}}} e^{-\frac{\gamma_i}{\bar{\gamma}}}\right) f_m\right] \frac{N_a (1 - (1 - P_b(c_i))^{N_a})}{R_b p_i}, & b_j = b_i, c_j = c_i, \\ 0, & \text{otherwise}. \end{cases} \tag{34}$$

TABLE 1
Channel States and SNR Ranges at 10 dB Average SNR

state	SNR range
1	$-\infty$ - 1.2558
2	1.2558 - 4.5891
3	4.5891 - 6.7210
4	6.7210 - 8.4083
5	8.4083 - 9.9159
6	9.9159 - 11.4186
7	11.4186 - 13.1795
8	13.1795 - ∞

Having defined the state space, the action set, and the transition probabilities, the iterative *value function* of the MDP is given by the Bellman's equation and can be written as

$$v_{\alpha,T}(i) = \max_a \left\{ r(i,a) + \alpha \sum_j P_{ij}(a) v_{\alpha,T-1}(j) \right\}, \qquad (35)$$

where $v_{\alpha,T}(i)$, the optimal *function value* computed using T steps into the future, is the optimal *reward*. We define the reward for taking the action a at state i as $r(i,a) = b_i + N_a(1 - P_{bl,a}(c_i))$. Here, the first term is the reward for the total number of bits successfully transmitted. The second term is the reward of achieved encryption strength (on successful transmission). $0 < \alpha < 1$ is a discount factor to give a desired weight to the future rewards. We do not assume a termination reward. The computation of optimal function values along with the optimal action is performed recursively.

Numerical simulations for the MDP formulation were carried out as follows: The SNR regions for each state were selected with the assumption of equal steady state probabilities for the states. The state transition probability matrix of (34) was computed for the parameter settings, $f_m = 10$Hz, $r = 8$, $\bar{\gamma} = 0$, 5, 10 dB, and $p_i = \frac{1}{r}$ for all i. Table 1 shows the SNR ranges corresponding to each state at $\bar{\gamma} = 10dB$ as an example. We have used the Rijndael ciphers with encryption block lengths $N_a \in \{128, 160, 192, 224, 256\}$. The encryption block lengths for various channel instances for the Rijndael cipher were calculated using the MDP-based approach, with the set of N_as as the set of control actions and the channel transition probability matrix as discussed above. In the MDP, we set $r = 8$, $q = 30$, $T = 1,000$, and $\alpha = 0.5$. As a baseline of comparison, we consider a 224-bit fixed block length encryption for all channel instances. We observed that (Fig. 10) using opportunistic encryption and the knowledge of the channel model, we can achieve higher throughput when compared to the present encryption method, where the selection of encryption block length is independent of the channel conditions. Fig. 10 gives the comparison of throughput achieved by opportunistic encryption and the fixed block length allocation (224 bit) over a range of average SNR, $\bar{\gamma}$. We can observe a gain in the throughput over all SNR values. Moreover, for low SNR values, the throughput gain using opportunistic encryption is observed to be higher than that at high SNR values, which is explained by the optimal selection of smaller block sizes at low SNR.

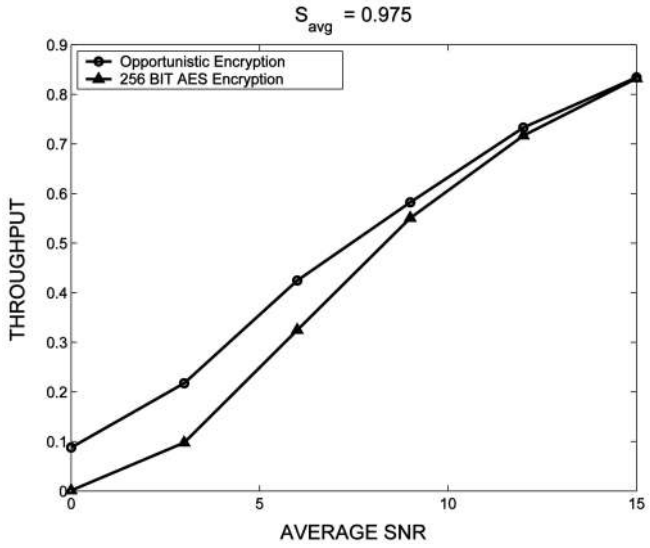

Fig. 10. Throughput comparison between opportunistic encryption and the fixed block length allocation over all average SNRs for a fixed security requirement of $\frac{\log_2(224)}{\log_2(256)} = 0.975$ with the MDP approach.

6 Conclusion

The work presented in 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. Three different approaches are presented each with varying levels of channel knowledge. Both analytical and experimental results are presented. For the case where we assume the exact channel knowledge and continuous encryption block length, we get an improvement of 95 percent (around 5dB SNR) in the throughput over fixed block length encryption. For the case where only the average SNR and the probability distribution are known, we get an improvement of 32 percent (around 5 dB SNR) in the throughput variable block length encryption. Finally, for the case when a Markov channel model is available, using MDP techniques we observe an improvement of 50 percent (around 5 dB SNR) in the throughput over the fixed encryption.

Appendix A
Optimum Solution with Brute Force Attack

We are required to maximize the throughput subject to an overall security requirement over a finite horizon. This can be stated as a constrained optimization problem given by

$$\begin{aligned} &\max_{\{N_i\}} \frac{1}{nR_{max}} \sum_{i=1}^{n} R_i(1 - N_i P_i) \\ &such\ that \quad \frac{1}{nS_{max}} \sum_{i=1}^{n} \log_2 N_i = s_{req}. \end{aligned} \qquad (36)$$

Note that $P_i = P_i(\gamma_i, R_i)$ is a function of channel SNR γ_i, and the transmission rate used for the frame R_i and s_{req} is the required level of security. This constrained optimization problem can be converted to an unconstrained optimization problem using the Lagrange optimization technique, where the object function can be written as

$$C = \frac{1}{nR_{max}} \sum_{i=1}^{n} R_i(1 - N_i P_i) + \lambda \left(\frac{1}{nS_{max}} \sum_{i=1}^{n} \log_2 N_i - s_{req} \right), \tag{37}$$

where the parameter λ is the Lagrange multiplier. Taking partial derivatives of (37) with respect to N_i and setting them equal to zero, we obtain

$$N_i^* = \frac{\lambda}{\log_e 2} \frac{R_{max}}{S_{max}} \frac{1}{R_i P_i}, i = 1, \cdots, n, \tag{38}$$

where the superscript $*$ indicates the optimality. Constraint in (36) and (38) leads to

$$N_i^* = \frac{\left(\prod_{i=1}^{n} R_i P_i\right)^{\frac{1}{n}}}{R_i P_i} e^{\left(S_{max} s_{req}\right) \log_e 2}. \tag{39}$$

In the case where the transmission rate is fixed, the above result reduces to

$$N_i^* = \frac{\left(\prod_{i=1}^{n} P_i\right)^{\frac{1}{n}}}{P_i} e^{\left(S_{max} s_{req}\right) \log_e 2}. \tag{40}$$

APPENDIX B

OPTIMALITY OF THE ALGORITHM UNDER EXPONENTIAL ATTACK MODEL

The following discussion establishes that the algorithm presented in Section 3.2.2 is indeed optimal. Consider the quantity to be maximized, namely, $T = \frac{1}{nR_{max}} \sum_{i=1}^{n} R_i(1 + \frac{P_i}{k} \log_e \phi_i)$ subject to the constraints as in (19), (20), and (21). 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 summands in S is concave and, therefore, the optimum allocation of ϕ_i resembles "water-filling" solution [20]. If $y_i = w_i \log_e \phi_i$, then 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 $w_1 \geq w_2 \geq \cdots \geq w_n$. 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 ϕ_{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 ϕ_{max} on ϕ_i, they may be capped at ϕ_{max} as the procedure continues. 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 as to assign $\phi_i > \phi_{min}$ to more and more channels in the increasing order of w_i until the condition $n\Phi_0 \geq \sum_{k=1}^{n} \phi_i$ is achieved. If the equality of constraint is not achieved, the subsequent steps perform fine tuning to achieve the optimal solution.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for the valuable comments. Part of this work was presented in the *Proceedings of the Fifth International Conference on Applied Cryptography and Network Security (ACNS)*, 2006. This work is supported by grants from the US Army and the US National Science Foundation.

REFERENCES

[1] J.M. Reason and D.G. Messerschmitt, *The Impact of Confidentiality on Quality of Service in Heterogeneous Voice over IP Networks.* Springer, 2001.
[2] B. Sklar, *Digital Communications: Fundamentals and Applications.* Prentice Hall, 1988.
[3] W.C. Jakes, *Microwave Mobile Communications.* IEEE, 1974.
[4] A.J. Goldsmith and P.P. Varaiya, "Capacity of Fading Channels with Channel Side Information," *IEEE Trans. Information Theory,* vol. 43, no. 6, pp. 1986-1992, Nov. 1997.
[5] A.J. Goldsmith and S.-G. Chua, "Variable-Rate Variable-Power MQAM for Fading Channels," *IEEE Trans. Information Theory,* vol. 45, no. 10, pp. 1218-1230, Oct. 1997.
[6] S. Boyd and L. Vandenberghe, *Convex Optimization.* Cambridge Univ. Press, 2004.
[7] H.S. Wang and N. Moayeri, "Finite-State Markov Channel-A Useful Model for Radio Communication Channels," *IEEE Trans. Vehicular Technology,* vol. 44, no. 1, pp. 163-171, Feb. 1995.
[8] C.C. Tan and N.C. Beaulieu, "On First-Order Markov Modeling for the Rayleigh Fading Channel," *IEEE Trans. Comm.,* vol. 48, no. 12, pp. 2032-2040, Dec. 2000.
[9] L.I. Sennott, *Stochastic Dynamic Programming and the Control of Queueing Systems.* John Wiley & Sons, 1999.
[10] D.P. Bertsekas, *Dynamic Programming and Optimal Control.* Athena Scientific, 1995.
[11] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* second ed. Wiley, 1996.
[12] Federal Information Processing Standards Publication 197, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, Nov. 2001.
[13] J. Kam and G. Davida, "Structured Design of Substitution-Permutation Encryption Networks," *IEEE Trans. Computers,* vol. 28, no. 10, pp. 747-753, 1979.
[14] W. Trappe and L. Washington, *Introduction to Cryptography: With Coding Theory.* Prentice Hall, 2002.
[15] W. Stallings, *Cryptography and Network Security,* pp. 27-30. Peaterson Education, 2003.
[16] J. Daemen and V. Rijmen, AES Proposal: Rijndael, http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf, 2006.
[17] J. Reason, "End-to-End Confidentiality for Continuous-Media Applications in Wireless Systems," PhD dissertation, UC Berkeley, Dec. 2000.
[18] S. Stein, "Fading Channel Issues in Systems Engineering," *IEEE J. Selected Areas in Comm.,* vol. 5, no. 2, pp. 68-89, Feb. 1987.
[19] D. Stintson, *Cryptography Theory and Practice,* third ed. CRC Press, 2005.
[20] T.M. Cover and J.A. Thomas, *Elements of Information Theory.* Wiley Series in Telecomm., Wiley-Interscience, 1991.
[21] S. Lin and D.J. Costello Jr., *Error Control Coding,* second ed. Prentice Hall, 2004.
[22] L.H. Ozarow, S. Shamai, and A.D. Wyner, "Information Theoretic Considerations for Cellular Mobile Radio," *IEEE Trans. Vehicular Technology,* vol. 43, no. 2, pp. 359-378, May 1994.
[23] T.H. Cormen, C.E. Leiserson, R.L. Rivest, and C. Stein, *Introduction to Algorithms,* second ed. The MIT Press, 2003.
[24] S. Bapatla and R. Chandramouli, "Battery Power Optimized Encryption," *Proc. IEEE Int'l Conf. Comm. (ICC '04),* pp. 3802-3806, June 2004.
[25] Y. Xiao and M. Guizani, "Optimal Stream-Based Cipher Feedback Mode in Error Channel," *Proc. IEEE Global Telecomm. Conf. (Globecom '05),* pp. 1660-1664, Nov. 2005.

[26] S. Coleri, M. Ergen, A. Puri, and A. Bahai, "Channel Estimation Techniques Based on Pilot Arrangement in OFDM Systems," *IEEE Trans. Broadcasting,* vol. 48, no. 3, pp. 223-229, Sept. 2002.
[27] Z. Shen, J.G. Andrews, and B.L. Evans, "Short Range Wireless Channel Prediction Using Local Information," *Proc. Conf. Record 37th Asilomar Conf. Signals, Systems, and Computers,* vol. 1, pp. 1147-1151, Nov. 2003.
[28] I.C. Wong, A. Forenza, R.W. Heath, and B.L. Evans, "Long Range Channel Prediction for Adaptive OFDM Systems," *Proc. 38th Asilomar Conf. Signals, Systems and Computers,* vol. 1, pp. 732-736, Nov. 2004.
[29] X. Wu and P.W. Moo, "Joint Image/Video Compression and Encryption via High-Order Conditional Entropy Coding of Wavelet Coefficients," *Proc. IEEE Int'l Conf. Multimedia Computing and Systems,* vol. 2, pp. 908-912, June 1999.

Mohamed A. Haleem received the BSc Eng degree with the specialization in electrical and electronic engineering from the University of Peradeniya, Kandy, Sri Lanka, in 1990, the MPhil degree in electrical and electronic engineering from the Hong Kong University of Science and Technology, Hong Kong, in 1995, and the PhD degree in electrical engineering from the Stevens Institute of Technology, Hoboken, New Jersey, in 2005. He was with the Department of Electrical and Electronic Engineering, University of Peradeniya, Sri Lanka, from 1990 to 1993 and has held the position of lecturer. He was with the Wireless Communications Research Department, Bell Laboratories, Lucent Technologies Inc., Crawford Hill, Holmdel, New Jersey, from 1996 to 2002, as a consultant and a member of technical staff. He is currently a postdoctoral researcher in the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, New Jersey. He is a member of the IEEE.

Chetan N. Mathur received the BE degree in computer science from the Visveshwaraiah Institute of Technology, Bangalore, India, in 2002 and the MS and PhD degrees in computer engineering from the Stevens Institute of Technology, New Jersey, where a part of his MS thesis was patented by the Stevens Institute of Technology. In the past few years, he has published several research papers in the fields of cryptography, coding theory, and dynamic spectrum access. He has also received numerous awards including the IEEE Best Student Paper Award presented at the IEEE Consumer Communications and Networking Conference (CCNC '06) and the IEEE Student Travel Grant Award presented at the International Conference on Communications (ICC '05). He is a member of the IEEE and is on the advisory board of Tau Beta Pi, the national organization of engineering excellence.

R. Chandramouli is the Thomas E. Hatfrick Chair and an associate professor of information systems in the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, New Jersey. Prior to joining the Stevens Institute of Technology, he was on the faculty of the Department of Electrical and Computer Engineering, Iowa State University, Ames. His research interests include steganography, steganalysis, encryption, wireless networking, and applied probability theory. His research in these areas is sponsored by the US National Science Foundation (NSF), the Air Force Research Laboratory, the US Army, the US Office of Naval Research, the US Department of Justice, and industry. He is a recipient of the NSF CAREER Award. He is also involved with several conference organization committees, as a Technical Program Committee member. He is a senior member of the IEEE.

K.P. Subbalakshmi is an associate professor in the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, New Jersey, where she codirects the MSyNC: Multimedia Systems Networking and Communications Laboratory. She is the program chair of the IEEE Global Telecommunications Conference (Globecom) 2006 Symposium on Information and Communication Security and a guest editor of the *IEEE Journal on Selected Areas of Communication*'s special issue on cross-layer wireless multimedia communications. She is the chair of the Special Interest Group on Multimedia Security within the IEEE Multimedia Communication Technical Committee. She leads research projects in information security, error resilient encryption, joint source-channel and distributed source-channel coding. She has been an active participant in several international conference program committees and organizations. She is a senior member of the IEEE.