Optimization Between AES Security and Performance for IEEE 802.15.3 WPAN

Alina Olteanu, Yang Xiao, *Senior Member, IEEE,* and Yan Zhang, *Member, IEEE*

***Abstract*—Ultra-wideband (UWB) is a new technology that enables wireless connectivity with consistent high data rates across multiple devices, such as high-definition television (HDTV) receivers, PCs, printers and digital cameras, within the digital home, and the office. In this paper, we focus on UWB transmissions where multiple accesses to the channel are coordinated by the IEEE 802.15.3 medium access control mechanism proposed in the IEEE 802.15.3a task group. Advanced encryption standard (AES), the most popular encryption cipher used nowadays, is used to ensure the security of the transmission. We study the overhead introduced by applying the AES cipher to the transmitted frames. Specifically, we analyze the tradeoff between throughput, payload size, and channel error when AES is used to encrypt the frames.**

***Index Terms*—Advanced encryption standard (AES), bit-error rate (BER), IEEE 802.15.3, medium access control (MAC), ultra-wideband (UWB).**

I. Introduction

ULTRA wideband is a new technology that enables wireless connectivity with consistent high data rates across multiple devices and PCs within the digital home and the office. This emerging technology provides the high bandwidth that multiple digital video and audio streams require throughout the home. The devices among which UWB makes transmissions possible range from HDTV receivers, TV sets, computers, printers and digital cameras, to medical monitoring devices and vehicular radar systems.

One of the critical challenges in UWB networks is coordinating multiple accesses to the channel where, for example, a receiver may need a relatively long time to synchronize with other transmitted signals. In this paper, we consider the IEEE 802.15.3 medium access protocol (MAC) mechanism that was proposed in the IEEE 802.15.3a task group as the protocol used to resolve the timing acquisition problem. The IEEE 802.15.3 MAC protocol has emerged as the result of strong efforts for regulation and standardization. IEEE 802.15.3 supports quality of service (QoS) for real time multimedia applications and insures reliability of delivery by adopting error control techniques under UWB error channel conditions. More precisely, the standard adopts three acknowledgement (ACK) schemes known as: No-ACK, Immediate-ACK (Imm-ACK) and Delayed-ACK (Dly-ACK). The standard is based on the notion of a piconet that is controlled by a piconet coordinator (PNC) and consists of devices (DEVs) which communicate with the PNC within given timeframes. Among these timeframes, we distinguish the contention-free channel time access period (CTAP) and the contention access period (CAP).

In order to ensure secure communication in UWB networks, an encryption mechanism must be employed to protect the transmitted frames from potential attackers. We use AES as our encryption scheme, as it is the most popular encryption cipher adopted in recent years. In this paper, we analyze the overhead introduced by AES when it is used to encrypt frames transmitted at the MAC layer. When working under channel error conditions, large frames need fragmentation to increase throughput given a certain bit error rate (BER). Each small frame, when encrypted by AES, introduces further overhead. Under these conditions, the question becomes: what is the optimum payload size that should be used such that maximum throughput is achieved? We derive formulas for throughput and payload size in both CTA and CAP access periods under the three ACK schemes.

The major contributions of this paper are stated as follows. This paper integrates AES security analysis into performance analysis of IEEE 802.15.3 WPAN under error channels along with three different acknowledgement schemes. Since security is very important nowadays, it is important to consider security overhead in network performance. This paper presents several optimization problems between security and system performance. It then resents theoretical solutions for these optimization problems. These theoretical studies provide deep insights into IEEE 802.15.3 system performance when ASE security overhead is considered.

The rest of the paper is organized as follows. In Section II, we present some related work. Section III provides an analysis of the optimum payload with some constraints in the contention-free period and also presents a solution to a similar optimization problem for the CAP. In Section IV, we solve the unconstrained throughput maximization problem both in the contention-free CTA and in the CAP under the three ACK schemes. Performance results related to our solutions are presented in Section V. We make pertinent observations about future work and draw our conclusions in Section VI.

II. Related Work

The authors in [3] and [6] provided an overhead analysis of AES in the context of network applications. The authors first derived expressions for the total number of processing cycles necessary for encrypting/ decrypting a *block* (a unit

Manuscript received January 6 2009; revised July 27 2009; accepted October 4, 2009. The associate editor coordinating the review of this paper and approving it for publication was M. Guizani.

A. Olteanu and Y. Xiao (corresponding author) are with the Dept. of Computer Science, Univ. of Alabama, USA (e-mail: aolteanu@cs.ua.edu, yangxiao@ieee.org).

Y. Zhang is with Simula Research Laboratory, Norway (e-mail: yanzhang@ieee.org).

Digital Object Identifier 10.1109/TWC.2009.12.090023

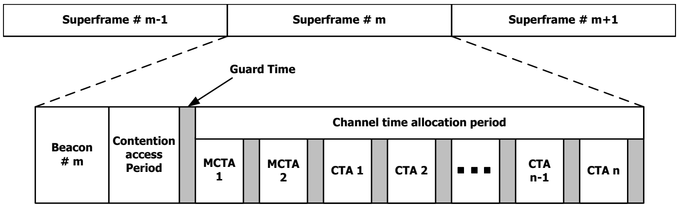
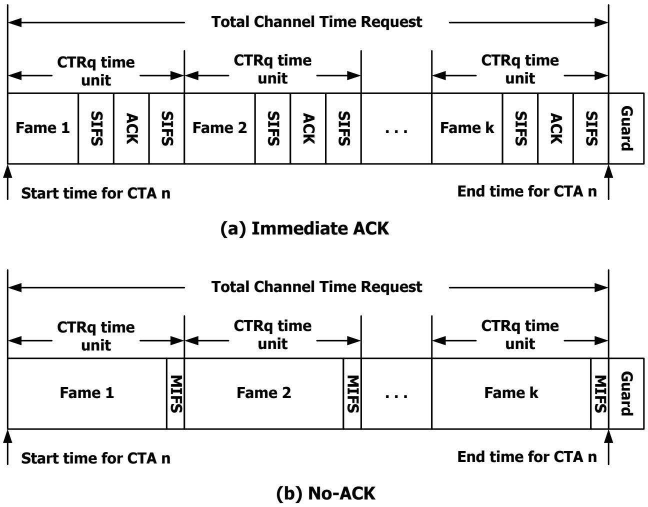


Fig. 1. The basic superframe.



(a) Immediate ACK

(b) No-ACK

Fig. 2. CTA under different ACK policies.

of plaintext in a block cipher). Next, given the IEEE 802.15.4 specification for sensor networks as an example, the number of processing cycles of encrypting and decrypting a *frame* are given in the expressions of O_E and O_D, respectively. Based on this data, formulas for the delay of unacknowledged and acknowledged short and long frames are further derived. The paper does not consider the effects of AES encryption on throughput or payload size. In our study, we use the time of encrypting a frame, O_E, to analyze how it affects the maximum throughput and to find out what payload size should be used to achieve this throughput.

There is also a great deal of research devoted to the UWB technology and the IEEE 802.15.3 MAC protocol [2], [7], [8], [14] . A closed form solution for throughput optimization in the contention free period (CFP) is presented in [2] for all three ACK schemes. A numerical solution for the same problem is also derived in the CAP case. These optimizations do not account for encryption and the overhead that it introduces. Our work extends the one in [2] by incorporating AES overhead when optimizing throughput. In addition, in the CAP, we optimize throughput depending on two factors this time: payload size and the number of frames transmitted during this period.

The channel time is divided into *superframes*, with each superframe beginning with a beacon frame as shown in Fig. 1. The superframe is divided into three main parts: a beacon frame, the optional contention access period (CAP), and channel time allocation period (CTAP).

Figs. 2 (a) and (b) show CTA with the Immediate-ACK policy and the No-ACK policy, respectively. For the Delayed-ACK, the CTA is similar to that for the No-ACK policy except that two additional frames follow the sequence: a delay-request frame from the source and a delay-ACK frame, which are separated by a SIFS (Short Interframe Space) time.

III. Constrained Throughput Optimization

Following the notations in [2], let p_e denote the bit error rate (BER) of the channel. Let L_o , L_a, L_r, and L denote the size of the header and trailer, the ACK frame size in bits, the delay-request frame size in bits, and the payload size, respectively. Let K be the number of frames transmitted during a CTAP, and t_p be the transmission time of the preamble of the frame. Let R_b and R_d be the base rate at which the control frames and the header/trailer are transmitted, and data rate, at which the payloads of data frames are transmitted, respectively.

The probability that a frame is successfully transmitted under the three ACK schemes mentioned is therefore:

$$p_{s,I\_ACK} = (1-p_e)^{L_o+L_a+L}$$

$$p_{s,D\_ACK} = (1-p_e)^{L_o+L_a+L_r+L}$$

$$p_{s,No\_ACK} = (1-p_e)^{L_o+L}$$

.

A. Throughput Optimization for CFP CTA

From [3], we know that

$$O_E = \left\lceil \frac{L}{4B} \right\rceil T_E, \tag{1}$$

where $4B$ represents the size of a block, O_E denotes the number of processing cycles of encrypting a frame, and T_E is the total number of processing cycles for encrypting a block. By the remainder theorem [4], there exist unique integers, x and r, such that

$$L = 4Bx + r, 0 \le r < 4B \tag{2}$$

By replacing L in the expression of O_E, we obtain:

$$O_E = \left\lceil x + \frac{r}{4B} \right\rceil T_E = (x+1)\, T_E \tag{3}$$

The last equality is due to the fact that $0 < \frac{r}{4B} \le 1$. By using the remainder theorem, we have thus eliminated the ceiling function from the encryption time expression (1), which significantly simplifies the following calculus.

We denote by A, D and F in the following expressions that are present in the normalized throughput formula (see [2]) for I_ACK, No_ACK and D_ACK, respectively. Let t_S and t_M denote SIFS (short interframe space) and MIFS (minimum interframe space), respectively, defined in IEEE 802.15.3 [14]. Let t_p denote the transmission time of the preamble. Let

$$A = R_d \left(2t_p + \frac{L_o + L_a}{R_b} + 2t_S \right) \tag{4}$$

$$D = R_d \left(t_p + \frac{L_o}{R_b} + t_M \right) \tag{5}$$

$$F = R_d \left(t_p + \frac{L_o}{R_b} + t_M + \frac{L_r + L_a}{KR_b} + \frac{2t_p + 2t_S}{K} \right) \tag{6}$$

Let S_{I_ACK}, S_{D_ACK} and S_{No_ACK} denote the normalized throughput for the three different ACK schemes. From [2], we have the following expressions for the normalized throughput:

$$S_{I\_ACK} = (1-p_e)^{L_o+L_a} \frac{L(1-p_e)^L}{L+A} \tag{7}$$

$$S_{No\_ACK} = (1-p_e)^{L_0} \frac{L(1-p_e)^L}{L+D} \tag{8}$$

$$S_{D\_ACK} = (1-p_e)^{L_0+L_a+L_r} \frac{L(1-p_e)^L}{L+F} \tag{9}$$

Our goal is to introduce the AES overhead given by (3) into the throughput expressions (7) - (9). By taking into account the derived expression of O_E from (3) and the payload from (2), we obtain the following new throughput expressions as functions of x and r:

$$S_{I\_ACK} = \frac{(1-p_e)^{L_0+L_a}(4Bx+r)(1-p_e)^{4Bx+r}}{(4Bx+r)+A+T_E(x+1)} \tag{10}$$

$$S_{No\_ACK} = \frac{(1-p_e)^{L_0}(4Bx+r)(1-p_e)^{4Bx+r}}{(4Bx+r)+D+(x+1)T_E} \tag{11}$$

$$S_{D\_ACK} = \frac{(4Bx+r)(1-p_e)^{(4Bx+r)}}{(4Bx+r)+F+(x+1)T_E} \tag{12}$$

Next, we introduce three optimization problems, one for each ACK scheme, and find the maximum throughput in each of these cases.

1) Immediate ACK:

Theorem 1. *Let* $x_0^* = (A+R_dT_E)/(-4B\ln(1-p_e))$. *Then the optimization problem:* $\max S_{I\_ACK}(x,r)$, *with constraints* $x \geq \lceil x_0^* \rceil$ *and* $r \geq 0$, *has solution* $S_{I\_ACK}(\lceil x_0^* \rceil, 0)$. *Moreover, the optimization problem* $\min S_{I\_ACK}(x,r)$ *with constraints* $\lceil x_0^* \rceil \leq x \leq \lfloor x_0 \rfloor$ *and* $0 \leq r \leq 4B-1$, *has solution* $S_{I\_ACK}(\lfloor x_0 \rfloor, 4B-1)$, *where* x_0 *is a positive number greater than* x_0^*.

Proof: $sign\{\partial S/\partial x\} = sign\{4BA + R_dT_E(4B - r) + 4B\ln(1-p_e)(4Bx+r)[A+R_dT_E(x+1)] + 4B\ln[1-p_e(4Bx+r)^2]\}$. The condition $x \geq (A+R_dT_E)/(-4B\ln(1-p_e))$ in the theorem statement is equivalent to $4B[A+R_dT_E+4Bx\ln(1-p_e)] \leq 0$. This leads automatically to $sign\{\partial S/\partial x\} = -1$. $sign\{\partial S/\partial r\} = sign\{[A+R_dT_E(x+1)][1+(4Bx+r)\ln(1-p_e)] + \ln(1-p_e)(4Bx+r)^2\} = -1$ as the sum of two negative terms.

Now we can apply Lagrange's mean value theorem [5]: $S(x,r) - S(\lceil x_0^* \rceil, 0) = \frac{\partial S}{\partial x}(u_1,u_2)(x-x_0^*) + \frac{\partial S}{\partial r}(u_1,u_2)r \leq 0$ as the sum of two negative terms. Therefore, the maximum throughput is $S_{I\_ACK}(\lceil x_0^* \rceil, 0)$.

The minimum emerges by applying the same Lagrange mean value theorem for the difference $S(x,r) - S(\lfloor x_0 \rfloor, 4B-1)$ and showing that it is positive. The minimum is therefore $S_{I\_ACK}(\lfloor x_0 \rfloor, 4B-1)$. ■

Theorem 1 finds the maximum and minimum throughput when some upper and lower bound constraints are imposed on x. Intuitively, x represents the number of blocks contained in a payload L. It then makes sense to have a lower bound and an upper bound on the number of blocks, which is equivalent to avoiding having too small or too large of a payload.

2) No ACK:

Theorem 2. *Let* $x_1^* = (D+R_dT_E)/(-4B\ln(1-p_e))$. *Then the optimization problem:* $\max S_{No\_ACK}(x,r)$ *with constraints* $x \geq \lceil x_1^* \rceil$ *and* $r \geq 0$, *has solution* $S_{No\_ACK}(\lceil x_1^* \rceil, 0)$. *Moreover, the optimization problem* $\min S_{No\_ACK}(x,r)$ *with constraints* $\lceil x_1^* \rceil \leq x \leq \lfloor x_1 \rfloor$ *and* $0 \leq r \leq 4B-1$, *has solution* $S_{No\_ACK}(\lfloor x_1 \rfloor, 4B-1)$, *where* x_1 *is a positive number.*

Proof: The first order partial derivatives of S_{No_ACK} are the same as in Theorem 1, with the sole difference being that A is replaced by D in this case. The proof follows the one of Theorem 1. ■

3) Delayed ACK:

Theorem 3. *Let* $x_2^* = (F+R_dT_E)/(-4B\ln(1-p_e))$, *where* F *is given by (6). Then the optimization problem:* $\max S_{D\_ACK}(x,r)$ *with constraints* $x \geq \lceil x_2^* \rceil$ *and* $r \geq 0$, *has solution* $S_{D\_ACK}(\lceil x_2^* \rceil, 0)$. *Moreover, the optimization problem* $\min S_{D\_ACK}(x,r)$ *with constraints* $\lceil x_2^* \rceil \leq x \leq \lfloor x_2 \rfloor$ *and* $0 \leq r \leq 4B-1$, *has solution* $S_{D\_ACK}(\lfloor x_2 \rfloor, 4B-1)$, *where* x_2 *is a positive number.*

Proof: See Theorems 1 and 2 for the proof. ■

B. Throughput Optimization for CAP

We again follow the notations from [2]. As in [2], let T_{ACK_TO} be the timeout value waiting for an ACK and τ be the probability that a station transmits during a generic slot time. From [2], we know that the probability that the channel is busy, p_b, is given by: $p_b = 1-(1-\tau)^n$. Also, P_s, the probability that a transmission is successful during a particular slot time is given by:

$$P_s = \begin{cases} n\tau(1-\tau)^{n-1} p_{s,No\_ACK}, \text{for } No\_ACK \\ n\tau(1-\tau)^{n-1} p_{s,I\_ACK}, \text{for } I\_ACK \\ n\tau(1-\tau)^{n-1}(1-p_e)^{L_r+L_a}, \text{for } D\_ACK \end{cases} \tag{13}$$

We denote the duration of a slot time by δ, the time of a successful transmission by T_s, and the time of a failed transmission by T_f. Let t_B denote BIFS (backoff interframe space). According to [2], the equations for T_s and T_f are given by

$$T_s = \begin{cases} t_p + \frac{L_o}{R_b} + \frac{L}{R_d} + t_B, \text{ for } No\_ACK \\ 2t_p + \frac{L_o}{R_b} + \frac{L}{R_d} + t_S + \frac{L_a}{R_b} + t_B, \text{ for } I\_ACK \\ K\left(t_p + \frac{L_o}{R_b} + \frac{L}{R_d} + t_M\right) + 2t_p + t_S + \\ \frac{L_r+L_a}{R_b} + t_B, \text{ for } D\_ACK \end{cases} \tag{14}$$

$$T_f = \begin{cases} t_p + \frac{L_o}{R_b} + \frac{L}{R_d} + t_B, \text{ for } No\_ACK \\ t_p + \frac{L_o}{R_b} + \frac{L}{R_d} + t_{ACK\_TO} + t_B, \text{ for } I\_ACK \\ K\left(t_p + \frac{L_o}{R_b} + \frac{L}{R_d} + t_M\right) + t_p + \frac{L_r}{R_b} \\ +t_{ACK\_TO} + t_B, \text{ for } D\_ACK \end{cases} \tag{15}$$

Accounting for equations (14) and (15), the normalized throughput from [2] is:

$$S_{No\_ACK} = \frac{P_s \frac{L}{R_d}}{(1-p_b)\,\delta + P_s T_s + (p_b - P_s)\,T_f} \tag{16}$$

$$S_{I\_ACK} = \frac{P_s L/R_d}{(1-p_b)\,\delta + P_s T_s + (p_b - P_s)\,T_f} \tag{17}$$

$$\begin{aligned} S_{D\_ACK} &= \frac{P_s \sum_{i=1}^{K} \frac{L}{R_d} (1-p_e)^{L_o+L}}{(1-p_b)\delta + P_s T_s + (p_b - P_s) T_f} \\ &= \frac{P_s K \frac{L}{R_d} (1-p_e)^{L_o+L}}{(1-p_b)\delta + P_s T_s + (p_b - P_s) T_f}. \end{aligned} \tag{18}$$

Consider the case of S_{I_ACK}. By replacing T_s and T_f in the denominator with their expressions from (14) and (15), respectively, and then grouping by P_s and p_b, we obtain the following expressions denoted by A_1 and A_2:

$$A_1 = (1-p_b)\,\delta + P_s\,(t_p + t_S + L_a/R_b - t_{ACK\_TO}) \tag{19}$$

,

$$A_2 = p_b\,(t_p + t_B + L_o/R_b + t_{ACK\_TO})\,. \tag{20}$$

Proceeding in a similar manner for S_{No_ACK} and S_{D_ACK}, we further define constants A_3, and A_4, A_5, respectively:

$$A_3 = (1-p_b)\,\delta + p_b \left(t_p + \frac{L_o}{R_b} + t_B\right), \tag{21}$$

$$A_4 = (1-p_b)\,\delta + P_s \left(t_p + t_S + \frac{L_a}{R_b} + t_{ACK\_TO}\right), \tag{22}$$

$$\begin{aligned} &A_5 = \\ &p_b[K(t_p + \tfrac{L_o}{R_b} + t_M) + t_p + \tfrac{L_r}{R_b} + t_{ACK\_TO} + t_B] \end{aligned} \tag{23}$$

As in the previous subsection, we consider payload L as having the form: $L\,(x,r) = 4Bx + r$, where r is a natural number, $r \le 4B - 1$.

We now have all of the elements needed to define the new throughput in the three ACK schemes while considering for the AES overhead. The throughput is thus given by:

$$S_{I\_ACK} = \frac{P_s (4Bx + r)/R_d}{A_1 + A_2 + \frac{p_b}{R_d}\,(4Bx + r) + (x+1)\,T_E}, \tag{24}$$

$$S_{No\_ACK} = \frac{(4Bx + r)\,P_s/R_d}{A_3 + (4Bx + r)\,p_b/R_d + p_b T_E\,(x+1)}, \tag{25}$$

$$S_{D\_ACK} = \frac{\frac{K P_s}{R_d}\,(1-p_e)^{L_a}\,(4Bx + r)\,(1-p_e)^{4Bx+r}}{A_4 + A_5 + \frac{p_b}{R_d}\,(4Bx + r) + p_b T_E\,(x+1)} \tag{26}$$

1) Immediate ACK:

Consider the throughput expression for the Immediate ACK scheme in CAP, as given by (24).

Theorem 4 finds the maximum throughput, S_{I_ACK}, when an upper bound constraint is imposed on the AES encryption time. This type of constraint is equivalent to the upper bound constraints on the payload (number of blocks in the payload) from the previous subsection.

Theorem 4. *Let $O_{E,MAX}$ be a given positive constant. We use $O_{E,MAX}$ as an upper bound for the permitted encryption time overhead. Consider the following optimization problem: $\max\{S_{I\_ACK}(x,r)\}$, with constraint $O_E \le O_{E,MAX}$. The solution of this problem is given by $S_{I\_ACK}(O_{E,MAX}/T_E, 4B-1)$.*

Proof: $sign\,\{\partial S/\partial x\} = sign\,\{4B\,(A_1 + A_2) + p_b T_E\,(4B - r)\} = sign\,\{4B\,(A_1 + A_2) + 4B p_b T_E\,(1 - r/(4B))\}$. Notice that $(p_b - r/(4B))$ is greater than 0. In addition, in the hypothesis that $p_b - P_s > 0$ ([2]), the expression $A_1 + A_2$ is greater than 1. Therefore, $sign\,\{\partial S/\partial x\} = +1$.

We now consider the signature of the partial derivative of S with respect to r: $sign\,\{\partial S/\partial r\} = sign\,\{4B\,(A_1 + A_2 + p_b\,(x + r)\,T_E)\} = +1$. Therefore, both first order partial derivatives are positive. This implies that S is an increasing function of both x and r, so that S_{I_ACK} is an increasing function of L. Therefore, $\max\{S_{I\_ACK}(x,r)\} = S\,(x^*, r^*)$, where x^* and r^* are the maximum values dictated by the constraints in the theorem statements: $x \le O_{E,MAX}/T_E$ and $r \le 4B - 1$. The constrained extreme point is: $(O_{E,MAX}/T_E, 4B-1)$. We consider $(\lfloor O_{E,MAX}/T_E \rfloor, 4B-1)$ as the actual solution, because we are working with integer values for x, r, and L. ■

The partial order derivatives of S_{I_ACK} with respect to x and r are both positive, which implies that the throughput is an increasing function of L. To find a maximum point, we therefore need some restriction on L, or equivalently on the encryption time O_E which is linear in L.

2) No ACK:

Let S_{No_ACK} be as in (25).

Theorem 5.*The optimization problem: $\max S_{No\_ACK}(x,r)$ with constraints $x \le \lfloor x_3 \rfloor$ and $0 \le r \le 4B - 1$, has a solution $S_{No\_ACK}(\lfloor x_1 \rfloor, 4B-1)$, where x_3 is a positive number.*

Proof: $sign\,\{\partial S/\partial x\} = sign\,\{4B\,(A_3 + T_E) - rT_E\} = +1$ and $sign\,\{\partial S/\partial r\} = sign\{(A_3 + 4BP_b/R_d)\,x + p_b\,(x+1)\,T_E\} = +1$. From the signature of the first order partial derivatives, since A_3 is a positive constant, we infer that S_{No_ACK} is an increasing function of both x and r. Therefore, the maximum is reached with the maximum values of x and r. ■

3) Delayed ACK:

Theorem 6 solves the problem of finding the maximum and minimum throughputs with some constraints on the number of blocks x contained in the payload. Recall that the throughput S_{D_ACK} is given by (26) above. The maximum is reached in the lower left corner of the horizontal strip defined by the constraints, while the minimum is reached in the upper right hand corner of the rectangle defined by the added constraints.

Theorem 6. *Let* $x_4^* = -1/4B\ln(1-p_e)$*. Then the optimization problem:* $\max S_{D\_ACK}(x,r)$ *with constraints* $x \geq \lceil x_4^* \rceil$ *and* $4B-1 \geq r \geq 0$*, has a solution* $S_{D\_ACK}(\lceil x_4^* \rceil, 0)$*. Moreover, the optimization problem* $\min S_{D\_ACK}(x,r)$ *with constraints*$\lceil x_4^* \rceil \leq x \leq \lfloor x_4 \rfloor$ *and* $0 \leq r \leq 4B-1$*, has a solution* $S_{D\_ACK}(\lfloor x_1 \rfloor, 4B-1)$*, where* x_4 *is a positive number greater than* x_4^**.*

Proof: $sign\{\partial S/\partial x\}$ $= sign\{4B(A_4+A_5+T_E)[1+(4Bx+r)\ln(1-p_e)] + 4B(4Bx+r)\ln(1-p_e)[p_b(4Bx+r)/R_d + xT_E] - rT_E\}$. Recall that A_4 and A_5 are constants such that $A_4+A_5>0$ (equations (22) and (23)).

Since $\ln(1-p_e)<0$ and $r \geq 0$, in order for this derivative to be negative, it suffices that $1+(4Bx+r)\ln(1-p_e) \leq 0$ for all $r \geq 0$, which is true, since $x \geq \lceil x_4^* \rceil$. This implies:$sign\{\partial S/\partial x\} = -1$ on the considered strip.

$sign\{\partial S/\partial r\} = sign\{[1+(4Bx+r)\ln(1-p_e)](A_4 + A_5 + T_E + xT_E) + p_b(4Bx+r)^2\ln(1-p_e)/R_d\} = -1$. We again apply the Lagrange mean value theorem [5]. $S(x,r) - S(x_4, 4B-1) = \frac{\partial S}{\partial x}(u_1,u_2)(x-x_4) + \frac{\partial S}{\partial r}(u_1,u_2)(r-4B+1)$. The difference is positive as the sum of two positive terms. The conclusion follows. ■

IV. Unrestricted Optimum Throughput

In this section, we derive an unrestricted optimum throughput for each of the three ACK schemes in the contention-free CTA and in the CAP under error channel conditions.

The optimization problem that we propose is: *Given* p_e *and the AES encryption time of a frame given by (1), what is the payload size that maximizes throughput under Immediate ACK, No ACK, and Delayed ACK schemes?*

We derive a close form solution for the throughput in each case. As in [2], this solution has the same format for all three ACK schemes. Moreover, we show that the optimum payload which solves the problem can be upper bounded by the same quantity under all three ACK mechanisms.

Following the notations from Section III, let A, D and F be some rational constants, given by formulas (2), (3) and (4), respectively.

As in Section III, let L be represented by the remainder theorem: $L=4Bx+r$. If we consider the encryption time O_E given by (1), we obtain $O_E = \lceil x + \frac{r}{4B} \rceil T_E = (x+1)T_E$. By further replacing x with $\frac{L-r}{4B}$, we have: $O_E = \left(\frac{L-r}{4B}+1\right)T_E$.

A. Unrestricted Optimum for CFP CTA

1) Immediate ACK:

From [2], taking into account the encryption time overhead and the observations above, we have:

$$S_{I\_ACK} = (1-p_e)^{L_0+L_a}\frac{L(1-p_e)^L}{L+A+T_E(1+(L-r)/(4B))}.$$

Taking the derivative with respect to L, after an elementary calculation, we obtain:$sign\{dS_{I\_ACK}/dL\} = sign\{A + R_dT_E(1-r/(4B)) + L\ln(1-p_e)[L + A + R_dT_E((L-r)/(4B)+1)]\}$. By equating the derivative of S_{I_ACK} to 0, we have: $L_{opt} = \frac{-(A+R_dT_E)}{2(1+R_dT_E/(4B))} + \frac{\sqrt{[A+R_dT_E/(4B)]^2+4R_dT_E(1+R_dT_E/(4B))/(-\ln(1-p_e))}}{2(1+R_dT_E/(4B))}$.

Following the principle$(a+b)(a-b)=a^2-b^2$, the square root in the numerator is eliminated by multiplying it by the conjugate. We further obtain:

$$L_{opt} = \frac{2R_dT_E/(-\ln(1-p_e))}{\sqrt{(4BA+R_dT_E)^2+\frac{4R_dT_E(4B+R_dT_E)}{(-\ln(1-p_e))}}+(4BA+R_dT_E)} \tag{27}$$

Using the fact that the denominator is greater than 2, it results that $L_{opt,I\_ACK} < 1/(-\ln(1-p_e))$.

2) No ACK:

The expression of S_{No_ACK} is given by:

$$S_{No\_ACK} = (1-p_e)^{L_0}\frac{L(1-p_e)^L}{L+D+T_E(1+(L-r)/(4B))}.$$

Since $0 \leq r \leq 4B-1$, and since AES adopts 128-bit blocks ([3]), the value $B=4$ holds. It can then be easily seen that the value of r for which the expression on the right-hand side is maximized is 15. By letting this expression be $S_{No\_ACK,r=15}$, we have: $S_{No\_ACK} \leq S_{No\_ACK,r=15} = (1-p_e)^{L_0}\frac{L(1-p_e)^L}{L+D+R_dT_E(1+(L-15)/16)}$.

We now take the derivative of $S_{No\_ACK,r=15}$ with respect to L: $sign\{\frac{dS_{No\_ACK,r=15}}{dL}\} = sign\{\ln(1-p_e)(16+R_dT_E)L^2 + \ln(1-p_e)(16D + R_dT_E)L + R_dT_E\}$.

By equating the right-hand side to 0, we obtain the optimum payload L_{opt} that maximizes $S_{No\_ACK,r=15}$ and, implicitly, S_{No_ACK}. We then have:

$$L_{opt} = \frac{-(16D+R_dT_E)+\sqrt{(16D+R_dT_E)^2+\frac{4R_dT_E(16+R_dT_E)}{-\ln(1-p_e)}}}{2(16+R_dT_E)}. \tag{28}$$

By simplifying we obtain:

$$\begin{aligned} L_{opt} &= \frac{2R_dT_E/(-\ln(1-p_e))}{\sqrt{(16D+R_dT_E)^2+\frac{4R_dT_E(16+R_dT_E)}{-\ln(1-p_e)}}+(16D+R_dT_E)} \\ &\leq \frac{R_dT_E/(-\ln(1-p_e))}{16D+R_dT_E} \\ &\leq \frac{1}{-\ln(1-p_e)}. \end{aligned}$$

3) Delayed ACK:

$$S_{D\_ACK} = \frac{(1-p_e)^{L_0+L_a+L_r}L(1-p_e)^L}{L+F+LR_dT_E/16+R_dT_E/16}.$$

By following the same approach we obtain:

$$L_{opt} = \frac{-(16F+R_dT_E)+\sqrt{(16F+R_dT_E)^2+\frac{4R_dT_E(16+R_dT_E)}{-\ln(1-p_e)}}}{2(16+R_dT_E)} \tag{29}$$

and $L_{opt} \leq \frac{1}{-\ln(1-p_e)}$.

From (27), (28), and (29), it can be seen that the optimum payloads for the three ACK schemes have the same format. Moreover, L_{opt,I_ACK}, L_{opt,No_ACK}, and L_{opt,D_ACK} can all be upper bounded by the same quantity: $1/-\ln(1-p_e)$.

By expressing L with the use of the remainder theorem, and therefore working with integers $(L=4Bx+r)$, we obtain a finite range of values for L_{opt}.

B. Unrestricted Optimum for CAP

1) Immediate ACK:

Recall the constants A_1 and A_2 given by (19), (20). The throughput is:

$$S_{I\_ACK} = \frac{P_s L/R_d}{A_1 + A_2 + \frac{p_b}{R_d} L + \left(\frac{L-r}{4B} + 1\right) T_E}.$$

$$S_{I\_ACK} \leq \tilde{S} = \frac{(1-p_e)^{L_o+L_a+L}\, L}{\tilde{A} + L\left(1 + R_d T_E/(4B)\right)},$$

where

$$\tilde{A} = R_d\left[2t_p + (L_o + L_a)/R_b + 2t_S + T_E/(4B)\right].$$

$$\begin{aligned} sign\left\{\frac{d\tilde{S}}{dL}\right\} &= sign\Big\{\ln(1-p_e)\left(1 + R_d T_E/(4B)\right) L^2 \\ &\quad + \tilde{A}\ln(1-p_e)\, L + \tilde{A}\Big\}. \end{aligned}$$

The positive root of the derivative is:

$$\begin{aligned} &L_{opt} \\ &= \frac{-\tilde{A}\ln(1-p_e) - \sqrt{\left[\tilde{A}\ln(1-p_e)\right]^2 - 4\tilde{A}\ln(1-p_e)(1+R_d T_E/(4B))}}{2\ln(1-p_e)(1+R_d T_E/(4B))} \\ &= \frac{2\tilde{A}/(-\ln(1-p_e))}{\tilde{A} + \sqrt{\tilde{A}^2 - 4\tilde{A}(1+R_d T_E)/\ln(1-p_e)}} \leq \frac{1}{-\ln(1-p_e)}. \end{aligned}$$

2) No ACK:

The throughput in the No ACK scheme is given by:

$$S_{No\_ACK} = \frac{L P_s/R_d}{A_3 + L p_b/R_d + p_b T_E\left(\frac{L-r}{4B} + 1\right)},$$

where A_3 is the constant from (21). Observe that:

$$\begin{aligned} &S_{N_0\_ACK} \\ \geq\ &\hat{S} = \frac{L P_s/R_d}{A_3 + L p_b/R_d + L p_b T_E/(4B) + p_b T_E/(4B)}. \end{aligned}$$

$$sign\left\{\frac{d\hat{S}}{dL}\right\} = sign\left\{A_3 + p_b T_E/(4B)\right\} = +1.$$

This implies that $\hat{S}$ is an increasing function of L, and we can easily see that $\hat{S}$ is concave. We have:

$$\hat{S}(\infty) = \lim_{L\to\infty} \hat{S}(L) = 4BP_s/[p_b(4B + R_d T_E)].$$

$$\hat{S}(\infty) - \hat{S}(L) = c\frac{1}{L},$$

where

$$c = \frac{P_s}{R_d}\frac{A_3 + R_d T_E/(4B)}{\left[p_b\left(1/R_d + T_E/(4B)\right)\right]^2}.$$

The maximum payload L can then be chosen to be sufficiently large such that the fraction c/L is sufficiently small. The throughput is therefore close to the maximum.

3) Delayed ACK:

Let C be a constant denoting:

$$\begin{aligned} &C = (1-p_b)\,\delta + P_s\left(t_p + t_S + \tfrac{L_a}{R_b} + t_{ACK\_TO}\right) + p_b \\ &\left[K\left(t_p + \tfrac{L_o}{R_b} + t_M\right) + t_p + \tfrac{L_r}{R_b} + t_{ACK\_TO} + t_B\right] \\ &+ p_b T_E\left(1 - r/(4B)\right). \end{aligned}$$

The throughput for Delayed ACK scheme in the CAP is given by:

$$S_{D\_ACK} = \frac{P_s K}{R_d}(1-p_e)^{L_a}\frac{L(1-p_e)^L}{C + (Kp_b/R_d + p_b T_E/16)\, L}.$$

By taking the derivative with respect to L and equating to 0, we obtain the optimum payload which maximizes the throughput:

$$\begin{aligned} &sign\left\{\frac{dS_{D\_ACK}}{dL}\right\} \\ =\ &sign\Big\{(1-p_e)^L\,[(1 + L\ln(1-p_e)) \\ &\left(C + Lp_b\left(\frac{K}{R_d} + \frac{T_E}{16}\right)\right) - Lp_b\left(\frac{K}{R_d} + \frac{T_E}{16}\right)\Big]\Big\} \\ =\ &sign\{C + C\ln(1-p_e) + \\ &p_b L^2 \ln(1-p_e)\left(\frac{K}{R_d} + \frac{T_E}{16}\right)\Big\}. \end{aligned}$$

The equation above has only one positive solution. By further observing that the throughput goes to zero when the payload is too small or too large, we can infer that this solution is a maximum point.

This implies:

$$\begin{aligned} &L_{opt} = \\ &\frac{-C\ln(1-p_e) + \sqrt{C^2\ln^2(1-p_e) - 4Cp_b\ln(1-p_e)(K/R_d + T_E/16)}}{2p_b\ln(1-p_e)(K/R_d + T_E/16)} \\ &= \frac{2C/(-\ln(1-p_e))}{\sqrt{C^2 - 4Cp_b(K/R_d + T_E/16)/\ln(1-p_e)} + C} \end{aligned}$$

By observing that the quantity $\frac{4Cp_b\left(\frac{K}{R_d} + \frac{T_E}{16}\right)}{\ln(1-p_e)}$ is positive, we can neglect it and bound the fraction by:

$$L_{opt} \leq \frac{1}{-\ln(1-p_e)}.$$

V. Performance Evaluation

We have plotted the analytical results from Section IV for both CTA and CAP. We used the following parameters for our experiments: BIFS = 9.4 μs, SIFS = MIFS = 8 μs, $L_o = L_a = L_r = 14$ bytes, $t_p = 9.4\mu s$, R_b and $R_d = 54$Mb/s, $B = 4$bytes, $n = 10$ stations, $\delta = 6\mu s$, $K = 5$, $BER = p_e = 0.001$.

A. Constrained Optimum

Note that we used the remainder Theorem to express the payload: $L = 4Bx + r$. Fig. 3 shows the throughput as a function of these two variables, x and r, in the Immediate ACK mechanism. It can be seen that an optimum throughput exists when x reaches its lower bound and $r = 0$.

The graph is consistent with our results from Theorem 1 in Section III.

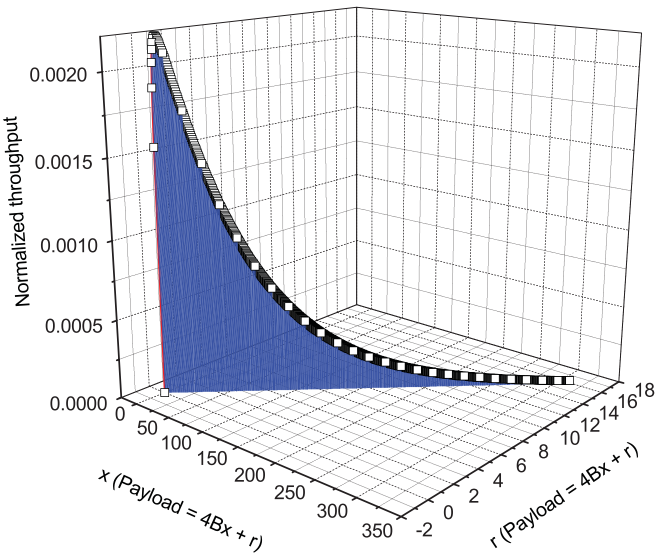


Fig. 3. Throughput versus payload size in Imm-ACK in the contention free CTA period.

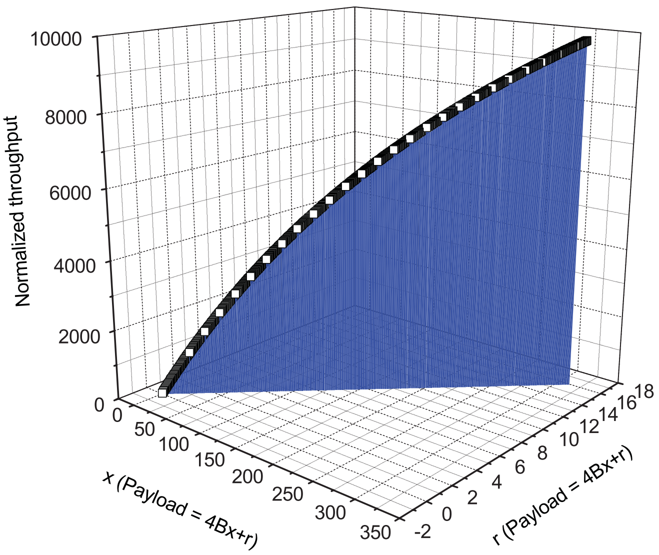


Fig. 4. Throughput versus payload size in No-ACK in the CAP.

Fig. 4 shows the optimal throughput in the No-ACK scheme in the contention access period. In this case, the maximum throughput is reached for the upper bound of x, and when $r = 4B - 1$.

B. Unrestricted Optimum

Figs. 5, 6, and 7 show the throughput for different payload sizes in the Imm-ACK, No-ACK and Dly-ACK mechanisms, respectively. It can be seen that adding AES encryption overhead in each case (Imm-ACK, No-ACK and D-ACK) results in a decreased throughput compared to when encryption is not used. Also, the optimal payload size and throughput decrease as BER increases.

Fig. 6 shows that No-ACK has better throughputs than both imm-ACK and Dly-ACK. Fig. 7 shows that the lowest throughputs are recorded in the Delayed ACK scheme.

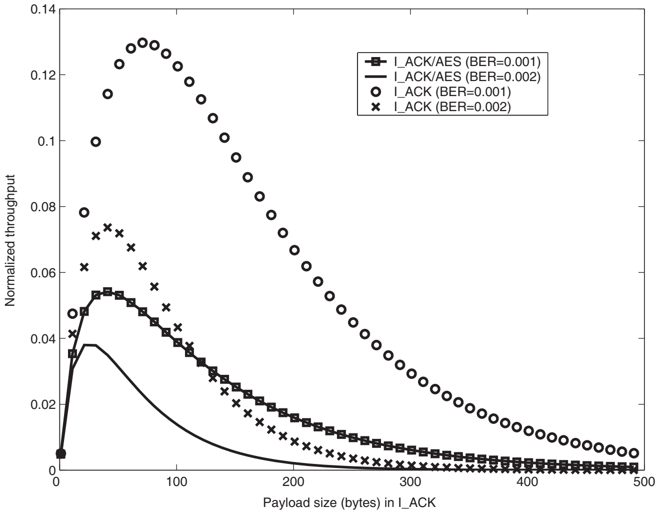


Fig. 5. Throughput versus payload size in Imm-ACK in the contention free CTA.

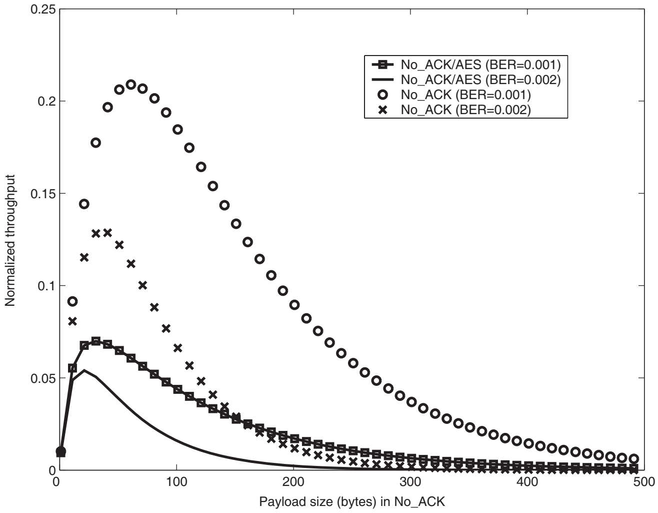


Fig. 6. Throughput versus payload size in No-ACK in the contention free CTA.

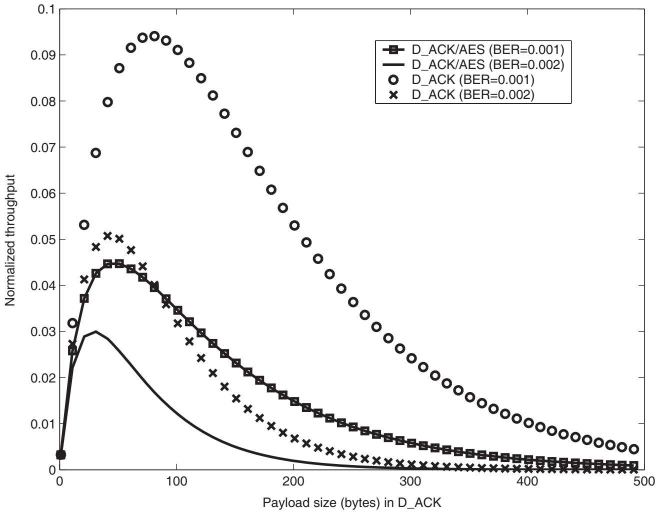


Fig. 7. Throughput versus payload size in Dly-ACK in the contention free CTA.

VI. Conclusion

In this paper, we analyzed the overhead introduced by AES when used to encrypt frames transmitted at the MAC layer. When working under channel error conditions, large frames need fragmentation to increase throughput given a certain bit error rate (BER). Each small frame, when encrypted by AES, introduces further overhead. Under these conditions, the question becomes: what is the optimum payload size that should be used such that maximum throughput is achieved? We derived formulas for throughput and payload size in both CTA and CAP access periods under the three ACK schemes.

So far we have found constrained maxima and minima for the throughput under the three MAC ACK schemes.

In future work, we would like to find conditions such that a free, unconstrained maximum is reached, either locally or globally. This maximum can be found by equating the first order partial derivative of S to 0.

A second avenue would be to study the relationship between x and r when we want to achieve a given maximum throughput. We can use the data from [2] for such values of the maximum throughput. By applying the implicit function theorem in this case, we can express x as a function of r. If an explicit expression cannot be derived for x, we can still provide some insights to the problem by studying other properties, such as the functions of monotony and convexity.

Acknowledgement

This work is supported in part by the US National Science Foundation (NSF) under the grant numbers CNS-0716211, CNS-0737325, and CCF-0829827.

References

[1] G. Racherla, J. L. Ellis, D. S. Furuno, and S. C. Lin, “Ultra-wideband systems for data communications,” in *Proc. IEEE International Conference on Personal Wireless Communications*, Dec. 2002, pp. 129-133.

[2] Y. Xiao, X. Shen, and H. Jiang, “Optimal ACK mechanisms of the IEEE 802.15.3 MAC for ultra-wideband systems,” *IEEE J. Sel. Areas Commun.*, vol. 24, no. 4, pp. 836-842, 2006.

[3] Y. Xiao, B. Sun, H. Chen, S. Guizani, and R. Wang, “Performance analysis of advanced encryption standard (AES),” in *Proc. of GLOBECOM 2006*.

[4] Remainder (2008, 21 Mar.) [Online]. Available: http://en.wikipedia.org/wiki/Remainder.

[5] Lagrange Mean Value Theorem. (Feb. 2008). [Online]. Available: http://en.wikipedia.org/wiki/Mean_value_theorem.

[6] Y. Xiao, H. Chen, B. Sun, R. Wang, and S. Sethi, “MAC security and security overhead analysis in the IEEE 802.15.4 wireless sensor networks,” *EURASIP J. Wireless Commun. and Networking*, vol. 2006, Article ID 93830, 12 pages, 2006. doi:10.1155/WCN/2006/93830.

[7] Y. Xiao, “MAC layer issues and throughput analysis for the IEEE 802.15.3a UWB,” *Dynamics of Continuous, Discrete and Impulsive Systems, Series B: Applications & Algorithms*, vol. 12, no. 3, pp. 443-462, June 2005.

[8] X. Chen, Y. Xiao, Y. Cai, J. Lu, and Z. Zhou, “An energy Diffserv and application-aware MAC layer scheduling for multiple VBR video streaming over high-rate WPANs,” *Computer Commun.*, vol. 29, no. 17, pp. 3516-3526, Nov. 2006.

[9] R. C. Qiu, H. Liu, and X. Shen, “Ultra-wideband for multiple access communications,” *IEEE Commun. Mag.*, vol. 43, no. 2, pp. 80-87, Feb. 2005.

[10] X. Shen, W. Zhuang, H. Jiang, and J. Cai, “Medium access control in ultra-wideband wireless networks,” *IEEE Trans. Veh. Technol.*, vol. 54, pp. 1663-1677, Sep. 2005.

[11] G. Bianchi, “Performance analysis of the IEEE 802.11 distributed coordination function,” *IEEE J. Sel. Areas Commun.*, vol. 18, pp. 535-547, Mar. 2000.

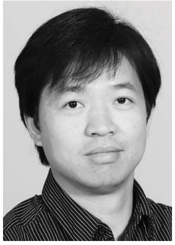
[12] Q. Ni, T. Li, T. Turletti, and Y. Xiao, “Saturation throughput analysis of IEEE 802.11 wireless networks in error environments,” *Wireless Commun. Mobile Comput. J.*, vol. 5, no. 8, pp. 945-956, Dec. 2005.

[13] T. Li, Q. Ni, D. Malone, D. Leith, Y. Xiao, and T. Turletti, “Aggregation with fragment retransmission for very high-speed WLANs,” *IEEE/ACM Trans. Networking*, vol. 17, no. 2, pp. 591-604, Apr. 2009.

[14] IEEE 802 Part 15.3: wireless medium access control (MAC) and physical layer (PHY) specifications for higher rate wireless personal area networks (WPAN), 2003.

Alina Olteanu received her B.S. degree in Computer Science and her M.S. degree in Applied Mathematics from the University of Bucharest and Polytechnic University of Bucharest, Romania in 2003 and 2005, respectively, and earned her Ph.D. degree in Computer Science from the University of Alabama, Tuscaloosa in 2009. Her research interests are in the areas of wireless network security, network performance optimization and lightweight cryptography.

Yang Xiao (SM'04) is currently with Department of Computer Science, The University of Alabama, Tuscaloosa. He currently serves as Editor-in-Chief for International Journal of Security and Networks, International Journal of Sensor Networks, and International Journal of Telemedicine and Applications. His research interests are security, telemedicine, robots, and sensor/wireless networks. Dr. Xiao serves as an Associate Editor for several journals, e.g., IEEE Transactions on Vehicular Technology. He was a voting member of the IEEE 802.11 Working Group from 2001 to 2004.



Yan Zhang received a Ph.D. degree from Nanyang Technological University, Singapore. From Aug. 2006, he is working with Simula Research Laboratory, Norway. He is currently serving the Book Series Editor for the book series on “Wireless Networks and Mobile Communications” (Auerbach Publications, Taylor and Francis Group). He is a regional editor, associate editor, on the editorial board, or guest editor of a number of international journals. He serves as organizing committee chairs for many international conferences, including WICON 2010, IWCMC 2010/2009, BODYNETS 2010, BROADNETS 2009, ACM MobiHoc 2008, IEEE ISM 2007. His research interests include resource, mobility, spectrum, energy, and data management in wireless communications and networking.