Security Overhead and Performance for Aggregation with Fragment Retransmission (AFR) in Very High-Speed Wireless 802.11 LANs

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

***Abstract*—In this paper, we study the overhead introduced by the advanced encryption standard cipher in the context of wireless LANs, specifically at the medium access control layer, as described in the 802.11 standard developed by the 802.11n task group. The advanced encryption standard is incorporated into existing aggregation schemes for 802.11 wireless LANs in order to achieve secure transmission of frames. We compute the maximum throughput, optimal frame, and fragment sizes which can be achieved in this context and compare them to the optimal values when encryption is not used. We evaluate the delay performance of such a scheme in the context of encryption and study asymptotic properties of the medium access control layer efficiency, expected frame size, and throughput.**

***Index Terms*—802.11, AES, fragmentation, security overhead, 802.11n.**

I. Introduction

ONE of the main challenges in wireless LANs (WLANs) nowadays is to develop a medium access control (MAC) layer that will not decrease the efficiency of the MAC layer when physical (PHY) rates are increased since as studied by Xiao *et al.* in [1]–[3], a theoretical throughput upper limit exists, indicating that by simply increasing the data rate without reducing overhead, the enhanced performance, in terms of throughput and delay, is bounded even when the data rate goes into infinitely high. Of the existing models, we are particularly interested in Aggregation with Fragment Retransmission (AFR) scheme, which was initially proposed in the IEEE 802.11n task group [4], and then developed more comprehensively in [5]. In this work, multiple frames are aggregated into a larger frame before being transmitted to the physical layer (PHY). If the size of a frame is larger than a pre-established threshold, the frame is divided into fragments before being aggregated. Transmission errors are handled by retransmitting only the fragments of the frame that had been corrupted.

However, the work in [5] does not consider security, i.e., encryption algorithm AES, which is used in IEEE 802.11i. In other words, when IEEE 802.11n and IEEE 802.11i are both adopted, AES over the high speed wireless LANs (WLANs) must be considered. With this motivation, in this paper, we analyze the overhead introduced by AES, when added to the aggregation scheme in [5]. We compute the optimal frame and fragment sizes which render the maximum throughput in this context, and compare the results to the optimal values from [5], where AES encryption is not used. We derive asymptotic results related to the MAC layer efficiency, expected frame size and saturation throughput. Adding security overhead analysis study is very important due to the importance of security as well as the fact that among the current huge number of papers about IEEE 802.11 performance analysis, none of them considers AES overhead in their analysis. The importance of this paper is therefore partially due to the importance of the security.

The rest of the paper is organized as follows. Section II presents significant work related to the problem. In Section III we compute the MAC efficiency with AES overhead and characterize the zero-waiting policy in the context of encryption. Section IV contains a detailed theoretical analysis of the AFR model when encryption is used and Section V presents some numerical results. We draw our conclusions in Section VI.

II. Related Work

With respect to increasing efficiency at the MAC layer, much of the previous work has focused on minimizing the contention time which contributes to the transmission overhead ([6]–[9]). However, Xiao *et al.* in [1]–[3] show that a theoretical throughput upper limit exists, indicating that by simply increasing the data rate without reducing overhead, the enhanced performance, in terms of throughput and delay, is bounded even when the data rate goes into infinitely high. Furthermore, the study in [5] shows that even over a channel with no collisions and no idle slots, the MAC layer efficiency is reduced by approximately half when the PHY rate is doubled. Burst acknowledgement (ACK) ([10]–[12]) and Block ACK ([3], [13]) schemes work to reduce the number of ACKs and short inter-frame spaces (SIFS). However, the PHY header is untouched and eventually dominates the transmission time rendering these type-schemes limited in terms of efficiency.

Li *et al.* [5] provide an aggregation mechanism (AFR scheme) which uses optimum frame sizes to increase efficiency at the MAC layer given high PHY layer rates, even

Manuscript received September 27, 2008; revised April 12, 2009 and September 5, 2009; accepted September 7, 2009. The associate editor coordinating the review of this paper and approving it for publication was D. Tarchi.

A. Olteanu and Y. Xiao (corresponding author) are with the Dept. of Computer Science, Univ. of Alabama, Box 870290, Tuscaloosa, AL 35487-0290 USA (e-mail: aolteanu@cs.ua.edu, yangxiao@ieee.org).

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

Digital Object Identifier 10.1109/TWC.2010.01.081291

under noisy channels. In this scheme, multiple frames are aggregated into a single frame and transmitted to the PHY layer. Rather than retransmitting the entire frame, only the frames/fragments containing such errors are being retransmitted. The optimal frame size is selected dynamically depending on the load condition of the channel, in a scheme called "zero-waiting". In the zero-waiting mechanism, frames are transmitted immediately once the MAC wins a transmission opportunity [5]. The frame sizes adapt automatically to the PHY rate and channel state, thereby maximizing the throughput efficiency while minimizing the holding delay. An analysis of the optimal throughput and delay performance is presented.

Yet another avenue is that involving aggregation schemes ([14]–[17], [24], [25]). The latest 802.11n draft standard [22] proposes two methods with respect to frame aggregation: aggregate MAC protocol service data unit (A-MSDU) and aggregate MAC protocol data unit (A-MPDU). The main distinction between an MSDU and an MPDU is that the MSDU corresponds to the information that is exchanged by the upper part of the MAC sublayer from or to the higher layers, respectively, whereas the MPDU is concerned with the information that is transmitted from or to the PHY by the lower part of the MAC (see [10]). Further optimization is achieved as multiple MPDUs are acknowledged by block ACK using a single extended ACK frame. However, a major drawback of using A-MSDU is under channel error conditions. The transmission of large frames when the channel is error-prone is likely to result in lost or corrupted bits. Based on capabilities of stations, the maximum size of an A-MSDU frame may be up to approximately 4KB or 8KB. If a lost or corrupted transmission the frame has to be resent as a whole frame, the whole the A-MSDU frame ends up being retransmitted even if only one bit has been damaged, and the retransmissions in turn lead to decreased throughput. However, the A-MPDU's scheme also has the capability to resend the part that was not successfully received. The A-MPDU scheme in IEEE 802.11n can reach 64 KB frame size and it has a similar structure (delimiters, sequence numbering, etc.) with the AFR, while the AFR was originally proposed as a proposal for an 802.11n partial draft in 2004 [4] before the 802.11n draft in 2007 that we have read [22]. The AFR scheme can use an arbitrary large frame size and adopt a zero-waiting mechanism. This paper focuses on security analysis of the AFR scheme and the method in this paper can be applied to other mechanisms of the 802.11n draft.

In the AFR scheme, frames are divided into fragments and packets that are also larger than the fragment size are in turn divided. If errors occur, only the damaged fragments are being retransmitted. We will denote the frame, packet and fragment sizes by L_f, L_p and L_{frag}, respectively. All notations used are listed in Table I.

Given a packet size L_p, the PHY rate R, the time to transmit a packet T_p, and the time overhead T_{oh}^p introduced by transmitting a packet, the authors in [5] derive an expression for the per packet MAC efficiency, η_p. Following the notation from [5], let T_{hdr}^{phy} denote the time to transmit the PHY header, T_{hdr}^{mac} the time to transmit the MAC header, T_{CW} the CSMA/CA backoff time, and T_{ack} the time to transmit a MAC acknowledgement (ACK). Let $a = T_{hdr}^{phy} + T_{hdr}^{mac} + T_{CW} + T_{ack}$ and L_1 be the size of a fragment header. m and M represent the number of fragments in a frame and the number of packets in a frame, respectively. In order to decouple the MAC efficiency from the PHY rate R, M is made proportional to R in [5], and therefore we can write $M = bR$, where b is a positive constant. Then, according to [5], $m = m'M$, where m' represents the number of fragments corresponding to a packet. By letting r denote the average number of transmissions before all the fragments in a packet are transmitted successfully, the $perframe$ MAC efficiency is given by:

$$\eta_p = \frac{L_p}{L_p + ra/b + rm'L_1}. \tag{1}$$

In addition, if we consider the time to transmit the payload of a frame to be $T_f = L_f/R$, then the $perframe$ MAC

TABLE I: Notations Used

m	Number of fragments in a frame
M	Number of packets in a frame
m'	Number of fragments in a packet
r	Average number of retransmission attempts until a frame is transmitted successfully
μ	Number of rounds in the Rijndael cipher
T_{hdr}^{phy}	Time duration to transmit the PHY headers of one frame
T_{mac}^{hdr}	Time duration to transmit the MAC headers of one frame
T_{CW}	Contention overhead
T_{ack}	Acknowledgement overhead
T_p	Time duration to transmit one packet
T_{oh}^p	Overhead for transmitting one packet
T_f	Time duration to transmit one frame
T_E	Number of processing cycles for encrypting a block
T_D	Number of processing cycles for decrypting a block
T_{and}	Number of processing cycles for performing byte-wise AND
T_{or}	Number of processing cycles for performing byte-wise OR
T_{shift}	Number of processing cycles for performing byte-wise SHIFT
T_I	Time duration of Idle event in the AFR scheme
T_3	Time duration of Success/Error event in the AFR scheme
T_C	Time duration of Collision event in the AFR scheme
T_{EIFS}	Time duration of Extended Inter-Frame Space (EIFS)
T_{sym}	Time duration for sending a symbol
N_{dbps}	Number of bits contained in each symbol
$4B$	Size of a block in bytes
a	$T_{hdr}^{phy} + T_{hdr}^{mac} + T_{CW} + T_{ack}$
O_E	AES encryption overhead
b	Positive constant, $M = bR$
d	$(rm'L_1)/L_p$
$\eta_{p,AES}$	Per packet MAC efficiency with AES
$\eta_{f,AES}$	Per frame MAC efficiency with AES
P_I	Probability of Idle event
P_3	Probability of Success/Error event
P_C	Probability of Collision event
P_e^{frag}	Fragment error rate
P_b	Bit error rate (BER)
τ	Probability of transmission for a station
n	Number of stations
σ	PHY layer time slot
L_1	Fragment header size
L_f	Payload size in one frame
L_p	Packet size
L_{frag}	Fragment size
L_{hdr}^{mac}	Aggregate size of all MAC headers in one frame
L_{ack}	Size of ACK
L_{FCS}	Size of a Frame Check Sequence (FCS)
α	Real valued factor between 0 and 1, corresponding to the degree of the load
R	Data rate

efficiency is:

$$\eta_f = \frac{T_f}{T_f + a + (rm'L_1/L_p)\,T_f}. \quad (2)$$

Xiao *et al.* [18], [19] analyze the performance of AES by deriving expressions for the total number of processing cycles necessary for encrypting/decrypting a $block$, denoted by T_E and T_D, respectively. From [18], [19], T_E is given by:

$$T_E = (8BT_{and} + 4BT_{or}) + (8BT_{and} + 7BT_{or} + 3BT_{shift}) + [46T_{and} + (31B + 12)\,T_{or} + (64B + 96)\,T_{shift}]\,(\mu - 1),$$

where T_{and}, T_{or}, and T_{shift} represent the number of processing cycles for performing byte-wise AND, OR, and SHIFT operations, respectively, and μ represents the number of rounds in the Rijndael cipher [20].

Next, given the IEEE 802.15.4 specification for sensor networks as an example, the number of processing cycles of encrypting/decrypting a $frame$ are given in the expressions of O_E and O_D, respectively. According to [18], [19], the AES encryption overhead for a frame is thus:

$$O_E = \left\lceil \frac{L_f}{4B} \right\rceil T_E. \quad (3)$$

where $4B$ represents the size of a block in bytes.

For related work about IEEE 802.11 performance analysis, since the middle of the 90's, many research papers have studied performance analysis of 802.11 [26]–[29]. A very popular model is Bianchi's model [30], [31], which evaluates the saturation throughput performance. Many papers are then based on Bianchi's model, e.g., [32]–[37]. There are also many other models, such as [38], [39]. However, none of them considers AES overhead in their analysis. Many related security research can be found in [40-54].

III. Fragmentation with Encryption

After fragmentation, if encryption is needed (i.e., AES is used), each fragment needs encryption. In other words, if a large frame is divided into multiple fragments, the system needs to spend time encrypting each fragment before transmitting it, and decrypting each fragment after receiving it, respectively. Such encryption/decryption introduces more overhead in terms of time.

A. Per packet MAC efficiency with AES encryption

In this section, we account for the AES overhead O_E from (3) and integrate this overhead with the MAC efficiency expression η_p in (1). We obtain a new expression $\eta_{p,AES}$ for the per packet MAC efficiency. For this subsection only, we denote by $O_E = \lceil Lp/(4B) \rceil\, T_E$ the number of processing cycles for encrypting a $frame$.

By the remainder theorem [20], there exist unique integers, x and y_p, such that $L_p = 4Bx + y_p$, and $0 \le y_p < 4B$.

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

$$O_E = \left\lceil x + \frac{y_p}{4B} \right\rceil T_E = (x+1)\,T_E. \quad (4)$$

The last equality is due to the fact that $0 \le \frac{y_p}{4B} < 1$. By further replacing x with $\frac{L_p - y_p}{4B}$, we have:

$$O_E = \left(\frac{L_p - y_p}{4B} + 1 \right) T_E. \quad (5)$$

Then the MAC efficiency incorporating AES overhead is given by:

$$\eta_{p,AES} = \frac{L_p}{L_p + r\left(\frac{a}{b} + m'L_1\right) + rT_E[(L_p - y_p)/(4B) + 1]} = \eta_{p,AES}\,(L_p, y_p)\ . \quad (6)$$

Next, we compute the optimum frame size which maximizes efficiency by calculating the partial derivative with respect to the frame size and equating to zero.

We establish the sign of the partial derivatives: $sign\frac{\partial \eta_{p,AES}}{\partial L_p} = sign\left\{\frac{a}{b} + m'L_1 + T_E\left(1 - \frac{y_p}{4B}\right)\right\} = 1$. The signature of the partial derivative with respect to L_p is given by the signature of the denominator since the numerator is positive. This signature is positive since from the remainder theorem, $y_p < 4B$. $sign\frac{\partial \eta_{p,AES}}{\partial y_p} = sign\left(r\frac{a}{b} + m'L_1\right) = 1$ as the sum of positive quantities.

Therefore the MAC efficiency is an increasing function of L_p, and the maximum is reached at infinity.

We have the following asymptotic result:

$$\lim_{L_p \to \infty} \eta_{p,AES} = \frac{1}{1 + \frac{rT_E}{4B}}. \quad (7)$$

Since we need a finite value for L_p which will render a near optimal throughput, we define a real valued factor α s.t. $0 < \alpha < 1$ to help solve the following problem. Given α, find L_{p_α} such that for any $L_p > L_{p_\alpha}$ we have:

$$\max \eta_{p,AES} > \eta_{p,AES} > \alpha \max \eta_{p,AES}. \quad (8)$$

A small α value stands for a light load, while a large value signifies an increased load.

By combining relations (6) - (8) we obtain:

$$\left(1 + \frac{rT_E}{4B}\right) L_p > \alpha\left[L_p\left(1 + \frac{rT_E}{4B}\right) + r\left(\frac{a}{b} + m'L_1\right) - \frac{y_p}{4B} rT_E\right].$$

Further manipulating and isolating L_p, gives us:

$$L_p \ge \frac{\alpha}{1-\alpha} \frac{r\left(\frac{a}{b} + m'L_1 + T_E\left(1 - \frac{y_p}{4B}\right)\right)}{1 + \frac{rT_E}{4B}}.$$

Since $0 < \alpha < 1$, we can write $\alpha = 1 - \frac{1}{n} \Rightarrow \frac{\alpha}{1-\alpha} = n - 1$. We have:

$$L_p \ge (n-1) \frac{r\left(\frac{a}{b} + m'L_1 + T_E\left(1 - \frac{y_p}{4B}\right)\right)}{1 + \frac{rT_E}{4B}}.$$

We have obtained a lower bound on the packet size. Any size greater or equal to this value used for the packet dimension will render a near optimal throughput.

B. Per frame MAC efficiency with AES encryption

Remember the expression of the per frame MAC efficiency from (2).

In the following, we consider $d = (rm'L_1)/L_p$ to be constant. From (2), accounting for the AES overhead as before, we have:

$$\eta_{f,AES} = \frac{1}{1 + d + (a + T_E(L_p - y_p)/(4B))/(T_f + T_E[(L_p - y_p)/(4B) + 1])}$$

Manipulating, we obtain:

$$\eta_{f,AES} = \frac{T_f + O_E}{(1+d)\,T_f + a + (2+d)\,O_E}, \tag{9}$$

where O_E is given by (5).

This way we have obtained a simplified expression for the per frame MAC efficiency, in which we have isolated the variable T_f.

C. Zero-waiting Scheme, Maximum Efficiency, and Maximum Throughput

The $zero-waiting$ scheme ([5]) is based on the idea that frames should be transmitted at the MAC layer as soon as transmission is possible, without waiting, regardless of the load of the channel. For a detailed description of this policy, please see [5].

In this section, we characterize the maximum efficiency $\eta_{\max}$, and the maximum throughput $S_{\max}$ that any MAC aggregation scheme can support. We first show that $\eta_{\max} = 1/(1+d)$ and $S_{\max} = R/(1+d)$, and then prove that under AES encryption, the zero-waiting aggregation scheme achieves maximum efficiency and can also maximize throughput where it is possible to do so.

Consider the expression of the MAC efficiency (9). Intuitively, the fact that $\lim_{T_f \to 0} \eta_{f,AES} = \frac{O_E}{(2+d)O_E + a}$ and $\lim_{T_f \to \infty} \eta_{f,AES} = \frac{1}{1+d}$ suggests that $\eta_{f,AES}$ increases. Taking the first derivative of (9), we obtain:

$$\begin{aligned}&\tfrac{d\eta_{f,AES}}{dT_f}\\ &\approx (2+d)\,O_E + (1+d)\,T_f + a - (O_E + T_f)\,(1+d)\\ &= O_E + a > 0.\end{aligned}$$

We then have:

$$\frac{O_E}{(2+d)\,O_E + a} < \eta_{f,AES} < \lim_{T_f \to \infty} \eta_{f,AES} = \frac{1}{1+d}. \tag{10}$$

In addition $\eta_{f,AES}$ is concave on $(0,\infty)$ and has a horizontal asymptote; hence $\eta_{f,AES}$ has a finite, stable value when T_f goes to infinity.

We have shown that $\eta_{\max} = \frac{1}{1+d}$ and since, from [5], the maximum throughput, $S_{\max} = R\eta_{\max}$, we have: $S_{\max} = R/(1+d)$.

Next, we reconstruct the analysis from [5] adapting it to our assumption that every fragment is encrypted before being transmitted.

From [5], the mean arrival rate is given by: $\nu = \alpha S_{\max} = \alpha R/(1+d)$ bits per second, where $0 \le \alpha \le 1$. In order to obey the zero-waiting policy the size of the frame is selected to be the same as the queue size $q\,(k)$([5]). During the time $(1+d)\,(T_f + O_E) + a + O_E$ it takes to transmit a frame, there are $\nu\,((1+d)\,(T_f + O_E) + a + O_E)$ expected arrivals at the queue. The mean number of arrivals at the queue during the time in which a frame is transmitted is thus:

$$\begin{aligned}&E\,[q\,(k+1)] = \nu\,[(1+d)\,(Tf + O_E) + a + O_E]\\ &= \nu\,[(1+d)\,E\,[q\,(k)]/R + a + O_E]\\ &= \alpha E\,[q\,(k)] + \tfrac{\alpha R}{1+d}\,[a + O_E]\ .\end{aligned}$$

By induction, we have $E\,[q\,(k+t)] = \alpha^t E\,[q\,(k)] + \sum_{i=1}^{t} \alpha^{i-1} \frac{\alpha R}{1+d}\,[a + O_E]$.

Asymptotically, when $t \to \infty$ and $\alpha < 1$,

$$E\,[L_f] = E\,[q] = \frac{\alpha R}{1+d}\frac{1}{1-\alpha}\,[a + O_E]\,. \tag{11}$$

Next, using the fact that $T_f + O_E = E\,[q\,(k)]/R$, formula (9) and the asymptotic result from (11), we obtain a new expression for $\eta_{f,AES}$:

$$\begin{aligned}&\eta_{f,AES} = \tfrac{E[q]/R}{(1+d)E[q]/R + a + O_E}\\ &= \tfrac{1}{1+d+(a+O_E)R/E[q]}\\ &= \tfrac{1}{1+d+(1+d)(1/\alpha - 1)}\\ &= \tfrac{\alpha}{1+d}\\ &= \alpha\eta_{\max}.\end{aligned}$$

Hence for α close to 1, the maximum frame efficiency, and consequently maximum throughput is achieved under the zero-waiting policy.

IV. Analysis of The Model

In this section, we analyze the saturation throughput, optimal frame and fragment sizes and delay of the AFR scheme over noisy channels, in the context of encryption.

In the AFR scheme, frames are divided into one or multiple fragments, depending on the frame's size and on some predefined bounds for the fragment sizes (optimally between 128 and 256 bytes, [5]). The fragments created by this way are then aggregated into a single frame before being transmitted. If errors occur, rather than retransmitting the entire frame, only the fragments containing such errors are being retransmitted. The optimal frame size is selected dynamically depending on the load condition of the channel, as seen in Section III-C. For a detailed description and implementation of the AFR scheme, see [5].

A. Saturation Throughput

We compute the saturation throughput based on the insights provided in the previous sections and in paper [5].

According to [5], a station is saturated if it has a frame to transmit at the MAC layer without waiting. From [5], the saturation throughput S is defined as the expected payload size of a frame transmitted successfully $E\,[Lf]$ over the expected time slot duration $E\,[T]$: $S = \frac{E[Lf]}{E[T]}$.

We denote the number of processing cycles necessary for encrypting a fragment by $O_{E,frag} = \lceil L_{frag}/(4B) \rceil\, T_E$.

As in [5], we express the durations T_I, T_3, and T_C corresponding to the tree events in the AFR scheme: Idle, Success/Error, and Collision duration, respectively. They are defined as follows: $T_I = \sigma$, $T_3 = T_{hdr}^{phy} + T_f + T_{ack}$, and $T_C = T_{hdr}^{phy} + T_f + T_{EIFS}$, where σ is the PHY layer time slot.

The expected slot duration from [5], in which we integrate the time to encrypt a fragment, $O_{E,frag}$ is thus:

$$E\,[T] = P_I T_I + P_3 T_3 + P_C T_C, \tag{12}$$

where P_I, P_3 and P_C are the probabilities of Idle, Success/Error and Collision events, respectively. Given a station's transmission probability τ and the number of stations n, these

event probabilities are defined as follows: $P_I = (1-\tau)^n$, $P_3 = \binom{n}{1}\tau(1-\tau)^{n-1}$, and $P_C = 1 - P_I - P_3$.

On the other hand, $E[L_f] = E[q]$ has been computed in the previous section and is given by equation (11).

By combining equations (11) and (12), we obtain the following expression of the saturation throughput in the AFR scheme with AES overhead:

$$\begin{aligned} S_{AFR,AES} &= \frac{P_3 L_f \left(1-p_e^{frag}\right)}{P_I T_I + P_3 T_3 + P_C T_C + O_{E,frag}} \\ &= \frac{P_3 R (T_f + m O_{E,frag})\left(1-p_e^{frag}\right)}{P_I T_I + P_3 T_3 + P_C T_C + O_{E,frag}} \\ &< \frac{R(T_f + m O_{E,frag})}{c + O_{E,frag}}, \end{aligned} \tag{13}$$

where $c = P_I T_I + P_3 T_3 + P_C T_C$ and p_e^{frag} is the fragment error rate.

Taking the first order derivative we obtain:

$$\frac{dS_{AFR,AES}}{dO_E} \approx c - T_f => S_{AFR,AES} < S_{AFR}.$$

This result is consistent with our intuition, since the throughput is diminished by the extra overhead.

The sign of the first order derivative is constant, so we have some intuition upon the function's monotony. From (13) we can see that the AFR throughput increases as the fragment size increases, even under channel error assumptions.

B. Optimal Frame Size

Recall from (5) that we can write the AES overhead of encrypting a frame as: $O_E = ((L_f - y_f)/(4B) + 1) T_E$, where $0 \le y_f < 4B$.

According to [5], equation (20), the AFR throughput is given by:

$$S_{AFR} = \frac{P_3\left(1-p_e^{frag}\right)}{(1-P_I)\,T_f/L_f}.$$

By adding the AES overhead into the above equation, we have:

$$S_{AFR,AES} = \frac{P_3 L_f \left(1-p_e^{frag}\right)}{(1-P_I)\left[T_f + T_E\left((L_f - y_f)/(4B)+1\right)\right]}.$$

We compute the first order derivative of the saturation throughput with respect to L_f.

$$\begin{aligned} & sign\frac{dS_{AFR,AES}}{dL_f} \\ &= sign\left\{T_f + T_E(1-y_f)/(4B) - L_f\frac{dT_f}{dL_f}\right\} \\ &= sign\left\{T_f + T_E(1-y_f)/(4B) - L_f/R\right\} \end{aligned} \tag{14}$$

Note that $L_f \approx R T_f$ which leads to $\frac{dT_f}{dL_f} \approx \frac{1}{R}$, where R is an average of the rates. By substituting R in (14) we have:

$$sign\frac{dS_{AFR,AES}}{dL_f} = sign\left\{T_E(1-y_f)/(4B)\right\} = +1.$$

The conclusion is that $S_{AFR,AES}$ is an increasing function of the frame size and its maximum is reached when $L_f \to \infty$. In addition, $S_{AFR,AES}$ as a function of L_f is concave (Fig. 5(b)). We have:

$$\begin{aligned} & \max S_{AFR,AES} \\ &= \lim_{L_f \to \infty} S_{AFR,AES} \\ &= \frac{P_3\left(1-p_e^{frag}\right)}{(1-P_I)(1/R + T_E/(4B))}. \end{aligned} \tag{15}$$

C. Optimal Fragment Size

From [5], equation (20), and accounting for AES encryption, we have the following expression for $S_{AFR,AES}$:

$$\begin{aligned} S_{AFR,AES} &= \frac{b'\left(1-p_e^{frag}\right)L_{frag}}{(L_{frag}+c')(T_{Sym}+O_E)} \\ &= \frac{b'(1-p_b)^{L_{frag}}L_{frag}}{(L_{frag}+c')(T_{Sym}+O_E)} \end{aligned}$$

where $b' = \frac{P_3 N_{dbps}}{1-P_I}$, $c' = L_{FCS} + L_{frag}^{hdr}$ are positive constants, T_{Sym} and N_{dbps} are the time duration for sending a symbol and the number of bits contained in each symbol, respectively, and L_{FCS} represents the size of a Frame Check Sequence (FCS) ([5]).

In order to find the optimal fragment size which renders the maximum throughput, we have to study the monotony of a function of the type:

$$S_{AFR,AES}(x) = \frac{x(1-p_b)^x}{x + c'}, \tag{16}$$

where x stands for L_{frag}.

We have:

$$\begin{aligned} & sign\frac{dS_{AFR,AES}}{dx} \\ &= sign\left\{\ln(1-p_b)\,x^2 + c''\ln(1-p_b)\,x + c'\right\}. \end{aligned}$$

In the above expression, we have a second degree polynomial; we compute its roots in order to determine its signature. The roots are:

$$x_{1,2} = \frac{-c'\ln(1-p_b) \pm c'^2\ln(1-p_b)^2 - 4c'\ln(1-p_b)^{1/2}}{2\ln(1-p_b)}.$$

The positive root is:

$$\begin{aligned} x_2 &= \frac{-c' + \left(c'^2 - 4c'/\ln(1-p_b)\right)^{1/2}}{2} \\ &= \frac{-2c'}{\ln(1-p_b)\left[c' + \left(c'^2 - 4c'/\ln(1-p_b)\right)^{1/2}\right]} < -\frac{1}{\ln(1-p_b)}. \end{aligned}$$

This implies that $S_{AFR,AES}$ increases on interval $[0, x_2]$ and then decreases. x_2 is thus a maximum point for $S_{AFR,AES}(L_{frag})$. From (16) we can also infer:

$$S_{AFR,AES}(0) = 0;\ S_{AFR,AES}(\infty) = 0.$$

D. MAC Delay Analysis

According to [5], the MAC layer delay of successfully transmitting one frame is given by:

$$\frac{E[T]}{E[number\,of\,frames]} = r\frac{P_I T_I + P_3 T_3 + P_C T_C}{P_3},$$

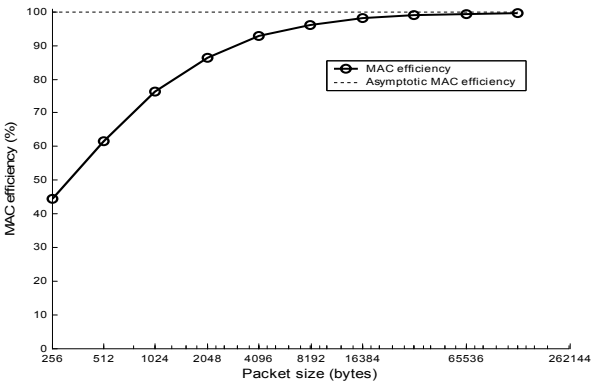
where r represents the expected number of retransmission attempts.

On the other hand, since a frame is composed of m' fragments, some of which needing retransmission, we also know from [5] that the probability of transmitting a frame in exactly r' attempts is given by:

$$r = \sum_{r'=1}^{\infty} r'\left[(1-p_e^{frag^{r'}})^{m''} - (1-p_e^{frag^{r'-1}})^{m''}\right].$$

Making use of some known approximations, we can express the fragment error rate linearly:

$$\begin{aligned} p_e^{frag} &= 1 - (1-p_b)^{L_{frag}+L_{FCS}} \\ &\approx 1 - (1 - p_b(L_{frag} + L_{FCS})) \\ &= p_b(L_{frag} + L_{FCS}). \end{aligned}$$



(a) MAC efficiency

L_1 (bytes)	8
B (bytes)	4
L_p (bytes)	256 , ··· ,262144
M	64
m'	8
T_{hdr}^{phy} (μs)	6
Basic rate (Mbps)	6
PHY rate (Mbps)	54
Retry limit	4

(b) Parameters

Fig. 1: (a) Per frame MAC efficiency. (b) MAC and PHY parameters used.

Combining the last two equations, we have:

$$r = \sum_{r'=1}^{\infty} \left\{ r' p_b^{(r'-1)m'} \left(L_{frag} + L_{FCS}\right)^{(r'-1)m'} \bullet \left[p_b^{m'} \left(L_{frag} + L_{FCS}\right)^{m''} - 1 \right] \right\}.$$

From [5], given the encryption overhead of a fragment $O_{E,frag} = \lceil L_{frag}/(4B) \rceil T_E$ and (5), the per frame MAC delay is:

$$D_{AFR}^{mac} = r \frac{P_I T_I + P_3 T_3 + P_C T_C + m'(\frac{L_{frag} - y_{frag}}{4B} + 1) T_E}{P_3}.$$

If the frame size is chosen to be directly proportional to the PHY rate, than the delay becomes independent of the increasing frame size and PHY rate. This way, the MAC delay and efficiency are approximately constant while the throughput becomes significantly larger.

V. Model Evaluation

In this section, we provide some numerical results. From Fig. 1 to Fig. 6, all results are numerical results.

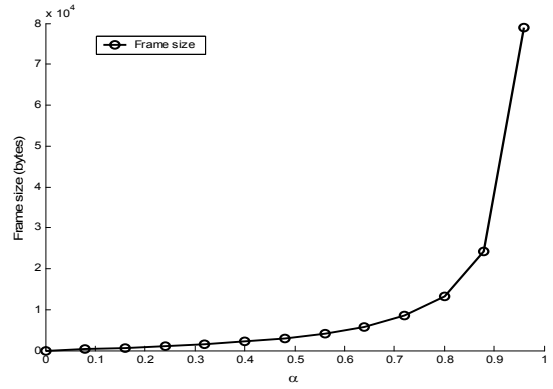


Fig. 2: Adapting the frame size to the level of the load, α. $R = 54$Mbps. The other parameters are listed in Fig. 1(b) and Table II.

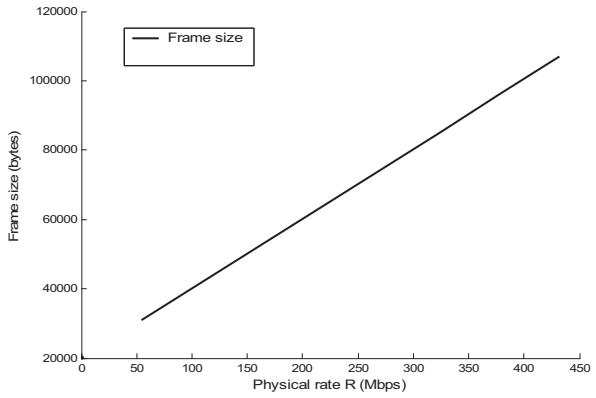


Fig. 3: Frame size scales with the PHY rate R. $\alpha = 0.5$. The other parameters are listed in Fig. 1(b) and Table II.

Fig. 1(a) shows the per packet MAC efficiency with AES overhead. The asymptotic efficiency given by (7) is marked by the dotted line. Moreover, η_p is a concave, increasing function on $(0, \infty)$ and has a horizontal asymptote, which proves once again that its value is stable when L_p goes to infinity (Fig. 1(a)).

TABLE II: Parameters Used in Fig. 2 and Fig. 3

L_f(bytes)	2048
L_p(bytes)	256
L_{frag}(bytes)	256
L_{hdr}^{mac}(bytes)	37
L_{ack}(bytes)	46
$T_{hdr}^{phy}(\mu s)$	20
α	$0 \cdots 1$
Data rate (Mbps)	54

Equation (11) shows how the frame size adapts to the offered load. When the load is light, corresponding to small α, small frames will be used. As the traffic increases, larger frames will automatically be selected, shown in Fig. 2.

Also from (11) we can see that for a given degree of the load α, the frame size L_f scales with the PHY rate R (Fig. 3). Adapting the frame size to the PHY rate leads to maximizing

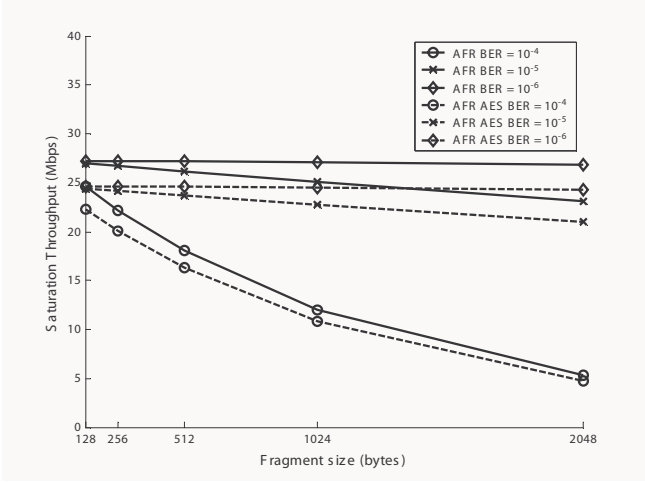


Fig. 4: AFR vs. AFR with AES encryption model. The parameters are listed in Table III.

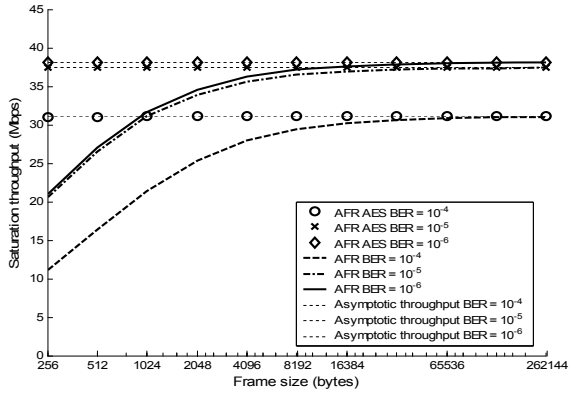
the MAC efficiency while minimizing the delay.

TABLE III: Parameters Used in Figures 4, 5 and 6

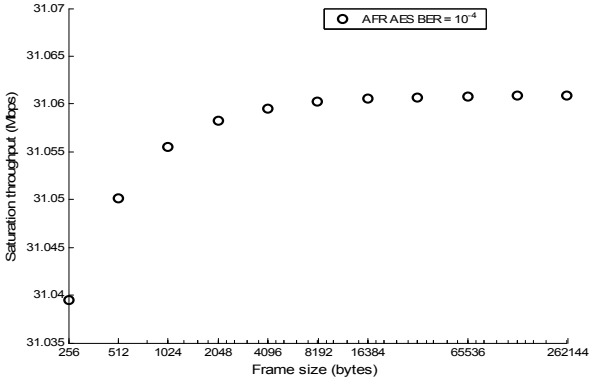
	Fig. 4	Fig. 5(a) and 5(b)	Fig. 6
L_f(bytes)	2048	$256 \cdots 262144$	65536
L_{frag}(bytes)	$128 \cdots 2048$	128	$64 \cdots 8192$
L_{hdr}^{frag}(bytes)			8
L_{FCS}(bytes)	2	2	2
L_{ack}(bytes)	46	46	
B(bytes)	4	4	4
N_{dbps}(bytes)			8
$T_{sym}(\mu s)$			1
$T_{SIFS}(\mu s)$	16	16	
$T_{EIFS}(\mu s)$	16	16	
$T_{hdr}^{phy}(\mu s)$	20	20	
$\sigma(\mu s)$	9	9	
Basic Rate (Mbps)	6	6	
Data rate (Mbps)	54	54	

Fig. 4 plots the throughput versus fragment size in two cases: when encryption is not used, and when AES encryption is added to the AFR scheme for different error rates. The saturation throughput is diminished by encryption in each of the three cases.

Fig. 5(a) illustrates the saturation throughput with increasing frame size in the AFR and in the AFR with AES encryption scheme, under different error rates. Fig 5(b) offers a close-up of the throughput in the AFR scheme with encryption. We can see from the figure that $S_{AFR,AES}$ is concave as a function of L_f. In both schemes, the saturation throughput reaches the same asymptotic value. This maximum value is represented analytically in (15) and marked by horizontal lines, one for each BER in Fig. 5(a). Naturally, in practice, huge frame sizes are not feasible since arbitrarily large frames can affect fairness and scheduling [24]. As a remark, for IEEE802.11a, the maximum size of MAC frame is generally 2346 bytes [13], [23]. It can be seen from Fig. 5(a) that even frame sizes of $2048B$ render a near optimal throughput, as the gap between the maximum and actual throughput is significantly small as frame sizes increase. Note that in Fig. 5, we allow the frame size to be as large as 262144 bytes just for the purpose



(a) AFR and AFR with AES schemes



(b) Close-up of AFR with AES, BER = 10^{-4}

Fig. 5: (a) AFR vs AFR with AES with increasing frame sizes. (b) Close-up of the saturation throughput in the AFR with AES scheme, when BER = 10^{-4}. The parameter values are listed in Table III.

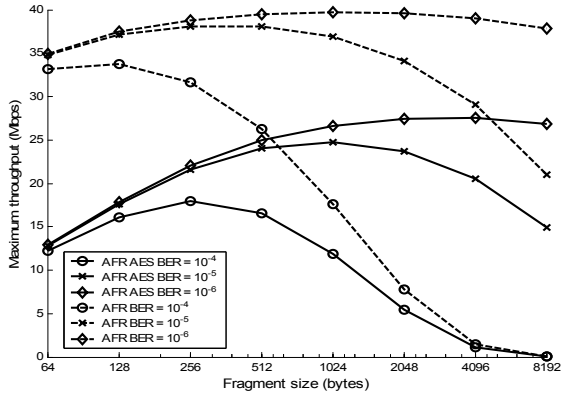


Fig. 6: Throughput vs. fragment size. The parameters are listed in Table III

of performance study, In a realistic network, the frame size should not be allow this large.

Fig. 6 plots the throughput versus fragment size in the AFR scheme and in the AFR with AES scheme. The existence of an optimal fragment size which maximizes throughput is evident from the figure. We can see that the optimal

fragment size depends on the BER, and its value is roughly doubled when encryption is added (from 128, 256 and 1024 in AFR to 256, 512 and 2048 bytes in AFR with encryption for $\mathrm{BER} = 10^{-4}, 10^{-5}, 10^{-6}$, respectively). The throughput however is significantly diminished by AES encryption.

VI. Conclusion

In this paper, we incorporated AES encryption overhead into the AFR scheme and expressed the MAC efficiency, queue dynamics, and MAC layer delay in this context. We derived an analytical expression of the saturation throughput under encryption and shown that it reaches is maximum as the frame size goes to infinity. We compared our results with the performance of AFR when encryption was not used.

The saturation throughput is diminished by encryption for all cases of different BERs. In both schemes, with and without encryption, the saturation throughput reaches the same asymptotic value.

We have also proven the existence of an optimal fragment size which maximizes throughput. This optimal fragment size depends on the BER, and its value is roughly doubled when encryption is added. The throughput however is significantly diminished by AES encryption.

We realize that throughput is not the only objective of an 802.11 network. For example, fairness issue is another research goal, and had been well studied in the literature. Under the same date rate, a simple solution considering the fairness is to integrated a weighted fair scheduling with AFR together so that the optimal size of AFR is also can be limited by a weighted factor. Other well known fairness algorithms can be also integrated with AFR. These studies could be the future work as a different direction. However, this paper's focus is more on AES overhead on 802.11 performance, i.e., security overhead. We also realize that a huge aggregated frame could cause other problems besides fairness. One simple solution is to provide a limit/threshold on the maximum aggregated frame size as suggested in [26].

Our future work also includes applications of current 802.11n draft and similar proposals, such as A-MSDU and A-MPDU if the future IEEE 802.11n standard is published and available.

References

[1] Y. Xiao and J. Rosdahl, "Throughput limit for IEEE 802.11," IEEE 802 Interim Meeting, Wentworth Sydney, NSW, Australia, May 2002, document number: IEEE 802.11-02/291r0.

[2] Y. Xiao and J. Rosdahl, "Throughput and delay limits of IEEE 802.11," *IEEE Commun. Lett.*, vol. 6, no. 8, Aug. 2002, pp. 355-357.

[3] Y. Xiao and J. Rosdahl, "Performance analysis and enhancement for the current and future IEEE 802.11 MAC protocols," *ACM SIGMOBILE Mobile Computing Commun. Review*, vol. 7, no. 2, pp. 6-19, Apr. 2003.

[4] Q. Ni, T. Li, T. Turletti, and Y. Xiao, "AFR partial MAC proposal for IEEE 802.11n," IEEE 802.11-04-0950-00-000n, Aug. 2004.

[5] 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.

[6] J. Choi, J. Yoo, S. Choi, and C. Kim, "EBA: an enhancement of the IEEE 802.11 DCF via distributed reservation," *IEEE Trans. Mobile Comput.*, vol. 4, no. 4, pp. 378-390, July 2005.

[7] Q. Ni, I. Aad, C. Barakat, and T. Turletti, "Modeling and analysis of slow CW decrease for IEEE 802.11 WLAN," in *Proc. PIMRC*, 2003, pp. 1717-1721.

[8] X. Yang and N. Vaidya, "A wireless MAC protocol using implicit pipelining," *IEEE Trans. Mobile Comput.*, vol 5, no. 3, pp. 258-273, Mar. 2006.

[9] Y. Xiao, H. Li, K. Wu, K. K. Leung, and Q. Ni, "On optimizing backoff counter reservation and classifying stations for the IEEE 802.11 distributed wireless LANs," *IEEE Trans. Parallel Distributed Syst.*, vol. 17, no. 7, pp. 713-722, July 2006.

[10] B. Sadeghi, V. Kanodia, A. Sabharwal, and E. Knightly, "Opportunistic media access for multirate ad hoc networks," in *Proc. ACM MOBICOM*, 2002, pp. 24-35.

[11] J. Tourrilhes, "Packet frame grouping: improving IP multimedia performance over CSMA/CA," in *Proc. ICUPC*, 1998, pp. 1345-1349.

[12] V. Vitsas, *et al.*, "Enhancing performance of the IEEE 802.11 distributed coordination function via packet bursting," in *Proc. GLOBECOM*, 2004, pp. 245-252.

[13] IEEE std 802.11-1999, Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) quality of service (QoS) enhancements, IEEE 802.11e/D8.0, Feb. 2004.

[14] Y. Xiao, "IEEE 802.11n: enhancements for higher throughput in wireless LANs," *IEEE Wireless Commun.*, pp. 82-91, Dec. 2005.

[15] T. Li, Q. Ni, D. Malone, D. Leith, Y. Xiao, and T. Turletti, "A new MAC scheme for very high-speed WLANs," in *Proc. IEEE WOWMOM*, 2006, pp. 171-180.

[16] S. A. Mujtaba, *et al.*, "TGn sync proposal technical specification." [Online]. Available: www.tgnsync.org, IEEE 802.11-04/889r6, May 2005.

[17] D. Skordoulis, Q. Ni, H. Chen, A. P. Stephens, C. Liu, and A. Jamalipour, "IEEE 802.11n MAC frame aggregation mechanisms for next-generation high-throughput WLANs," *IEEE Wireless Commun.*, vol. 15, no. 1, pp. 40-47, Feb. 2008.

[18] Y. Xiao, B. Sun, H. Chen, S. Guizani, and R. Wang, "Performance analysis of advanced encryption standard (AES)," *IEEE GLOBECOM*, 2006.

[19] 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. Netw.*, vol. 2006, Article ID 93830, 12 pages, 2006. doi:10.1155/WCN/2006/93830.

[20] FIPS Publication 197, "Advanced Encryption Standard," U.S. DoC/NIST, 2001.

[21] Remainder. (2008, 21 March) [Online]. Available: http://en.wikipedia.org/wiki/Remainder#The_case_of_general_integers.

[22] IEEE P802.11n, Draft 2.0, "Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Enhancements for higher throughput," Feb. 2007.

[23] IEEE 802.11a WG, Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specification: High-speed physical layer in the 5 GHz BAnd, IEEE, Sept. 1999.

[24] Y. Xiao, "Efficient MAC strategies for the IEEE 802.11n wireless LANs", *Wireless Commun. Mobile Comput.*, vol. 6, no. 4, pp. 453-466, 2006.

[25] P. Lettieri and M. B. Srivastava, "Adaptive frame length control for improving wireless link throughput, range, and energy efficiency," *Proc. IEEE INFOCOM*, 1998, pp. 564-571.

[26] Y. Xiao, "IEEE 802.11 performance enhancement via concatenation and piggyback mechanisms," *IEEE Trans. Wireless Commun.*, vol. 4, no. 5, pp. 2182-2192, Sept. 2005.

[27] G. Bianchi, L. Fratta, and M. Oliveri, "Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LANs," in *Proc. PIMRC 1996*, pp. 392-396.

[28] T. S. Ho and K. C. Chen, "Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LAN's," in *Proc. PIMRC 1996*, pp. 392-396.

[29] H. S. Chhaya and S. Gupta, "Performance modeling of asynchronous data transfer methods of IEEE 802.11 MAC protocol," *Wireless Netw.*, vol. 3, pp. 217-234, 1997.

[30] G. Bianchi, "IEEE 802.11-saturation throughput analysis," *IEEE Commun. Lett.*, vol. 2, no. 12, pp. 318-320, Dec. 1998.

[31] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535-547, Mar. 2000.

[32] E. Ziouva and T. Antonakopoulos, "CSMA/CA performance under high traffic conditions: throughput and delay analysis," *Computer Commun.*, vol. 25, pp. 313-321, 2002.

[33] C. H. Foh and J. W. Tantra, "Comments on IEEE 802.11 saturation throughput analysis with freezing of backoff counters," *IEEE Commun. Lett.*, vol. 9, no. 2, pp. 130-132, Feb. 2005.

[34] H. Wu, Y. Peng, K. long, S. Cheng, and J. Ma, "Performance of reliable transport protocol over IEEE 802.11 WLAN: analysis and enhancement," in *Proc. IEEE INFOCOM 2002*, vol. 2, pp. 599-607.

[35] Y. Xiao, "A simple and effective priority scheme for IEEE 802.11," *IEEE Commun. Lett.*, vol. 7, no. 2, pp. 70-72, Feb. 2003.

[36] Y. Xiao, "Performance analysis of priority schemes for IEEE 802.11 and IEEE 802.11e wireless LANs," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1506-1515, July 2005.

[37] I. Tinnirello, G. Bianchi, and Y. Xiao, "Refinements on IEEE 802.11 DCF modeling approaches," *IEEE Trans. Veh. Technol.*, accepted and to appear.

[38] F. Cal´i, M. Conti, and E. Gregori, "Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit," *IEEE/ACM Trans. Networking*, vol. 8, no. 6, pp. 785-790, Dec. 2000.

[39] Y. C. Tay and K. C. Chua, "A capacity analysis for the IEEE 802.11 MAC protocol," *Wireless Netw.*, pp. 159-171, 2001.

[40] Y. Xiao, C. Bandela, X. Du, Y. Pan, and K. Dass, "Security mechanisms, attacks, and security enhancements for the IEEE 802.11 WLANs," *International J. Wireless Mobile Computing*, vol. 1, nos. 3/4, pp. 276-288, 2006.

[41] W. Stewart, Y. Xiao, B. Sun, and H. Chen, "Security mechanisms and vulnerabilities in the IEEE 802.15.3 wireless personal area networks," *International J. Wireless Mobile Computing*, vol. 2, no. 1, pp. 14-27, 2007.

[42] Y. Xiao, "Accountability for wireless LANs, ad hoc networks, and wireless mesh networks," *IEEE Commun. Mag.*, special issue on security mobile ad hoc sensor networks, vol. 46, no. 4, pp. 116-126, Apr. 2008.

[43] D. Takahashi and Y. Xiao, "Retrieving knowledge from auditing log files for computer and network forensics and accountability," *(Wiley J.) Security Commun. Netw.*, vol. 1, no. 2, pp. 147-160, Mar./Apr. 2008.

[44] K. Meng, Y. Xiao, and S. V. Vrbsky, "Building a wireless capturing tool for WiFi," *(Wiley J.) Security Commun. Netw.*, DOI: 10.1002/sec.107, accepted and to appear.

[45] Y. Xiao, "Flow-net methodology for accountability in wireless networks," *IEEE Netw.*, vol. 23, no. 5, pp. 30-37, Sept./Oct. 2009.

[46] A. Olteanu, Y. Xiao, and Y. Zhang, "Optimization between AES security and performance for IEEE 802.15.3 WPAN," *IEEE Trans. Wireless Commun.*, DOI: 10.1109/TWC.2009.090023, accepted.

[47] M. Zhao, Y. Yang, H. Zhu, W. Shao, and V. Li, "Priority-based opportunistic MAC protocol in IEEE 802.11 WLANs," *International J. Sensor Netw.*, vol. 3, no. 2, pp. 84-94, 2008.

[48] X. Lin, X. Ling, H. Zhu, P. Ho, and X. Shen, "A novel localised authentication scheme in IEEE 802.11 based wireless mesh networks," *International J. Security Netw.*, vol. 3, no. 2, pp. 122-132, 2008.

[49] R. A. Malaney, "Securing Wi-Fi networks with position verification: extended version," *International J. Security Netw.*, vol. 2, nos. 1/2, pp. 27-36, 2007.

[50] L. Watkins, R. Beyah, C. Corbett, "Using link RTT to passively detect unapproved wireless nodes," *International J. Security Netw.*, vol. 4, no. 3, pp. 153-163, 2009.

[51] J. B. Evans, W. Wang, and B. J. Ewy, "Wireless networking security: open issues in trust, management, interoperation and measurement," *International J. Security Netw.*, vol. 1, no.1/2, pp. 84-94, 2006.

[52] V. Karyotis, S. Papavassiliou, M. Grammatikou, and V. Maglaris, "A novel framework for mobile attack strategy modelling and vulnerability analysis in wireless ad hoc networks," *International J. Security Netw.*, vol. 1, nos. 3/4, pp. 255-265, 2006.

[53] F. Sun and M. A. Shayman, "On pairwise connectivity of wireless multihop networks," *International J. Security Netw.*, vol. 2, nos. 1/2, pp. 37-49, 2007.

[54] Q. Gu, P. Liu, C. Chu, and S. Zhu, "Defence against packet injection in ad hoc networks," *International J. Security Netw.*, vol. 2, nos. 1/2, pp. 154-169, 2007.

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) received the B.S. and M.S. degrees from Jilin University, Changchun, China, and the M.S. and Ph.D. degrees in computer science and engineering from Wright State University, Dayton, OH. He 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.