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
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 load condition of the channel, in a scheme called “demand”. The optimal frame size is selected dynamically depending on the load condition of the channel, in a scheme called “demand”. The optimal frame size is selected dynamically depending on the load condition of the channel, in a scheme called “demand”. The optimal frame size is selected dynamically depending on the load condition of the channel, in a scheme called “demand”. The optimal frame size is selected dynamically depending on the load condition of the channel, in a scheme called “demand”.

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 whole frame, the whole the A-MSDU frame ends up being retransmitted 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.

<table>
<thead>
<tr>
<th>Table I: Notations Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m$</td>
</tr>
<tr>
<td>$M$</td>
</tr>
<tr>
<td>$m'$</td>
</tr>
<tr>
<td>$r$</td>
</tr>
<tr>
<td>$\mu$</td>
</tr>
<tr>
<td>$T_{phy}$</td>
</tr>
<tr>
<td>$T_{mac}$</td>
</tr>
<tr>
<td>$TCW$</td>
</tr>
<tr>
<td>$T_{ack}$</td>
</tr>
<tr>
<td>$T_p$</td>
</tr>
<tr>
<td>$T_{mac}$</td>
</tr>
<tr>
<td>$T_f$</td>
</tr>
<tr>
<td>$F_E$</td>
</tr>
<tr>
<td>$D$</td>
</tr>
<tr>
<td>$T_{bound}$</td>
</tr>
<tr>
<td>$T_{shift}$</td>
</tr>
<tr>
<td>$T_j$</td>
</tr>
<tr>
<td>$T_s$</td>
</tr>
<tr>
<td>$T_C$</td>
</tr>
<tr>
<td>$T_{IFS}$</td>
</tr>
<tr>
<td>$T_{sym}$</td>
</tr>
<tr>
<td>$N_{bytes}$</td>
</tr>
<tr>
<td>$L_B$</td>
</tr>
<tr>
<td>$a$</td>
</tr>
<tr>
<td>$O_E$</td>
</tr>
<tr>
<td>$b$</td>
</tr>
<tr>
<td>$d$</td>
</tr>
<tr>
<td>$\eta_p$</td>
</tr>
<tr>
<td>$\eta_A$</td>
</tr>
<tr>
<td>$P_l$</td>
</tr>
<tr>
<td>$P_s$</td>
</tr>
<tr>
<td>$P_c$</td>
</tr>
<tr>
<td>$T_{frag}$</td>
</tr>
<tr>
<td>$P_{frame}$</td>
</tr>
<tr>
<td>$T_{ack}$</td>
</tr>
<tr>
<td>$L_{FCS}$</td>
</tr>
<tr>
<td>$\alpha$</td>
</tr>
<tr>
<td>$R$</td>
</tr>
</tbody>
</table>

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 define 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 $T_{phy}$ introduced by transmitting a packet, the authors in [5] derive an expression for the per packet MAC efficiency, $\eta_p$. Following the notation from [5], let $T_{mac}$ denote the time to transmit the PHY header, $T_{phy}$ the time to transmit the MAC header, $TCW$ the CSMA/CA backoff time, and $T_{ack}$ the time to transmit a MAC acknowledgement (ACK). Let $a = T_{phy} + T_{mac} + TCW + T_{ack}$ and $L_1$ be the

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

In addition, if we consider the time to transmit the payload of a frame to be $T_f = L_f/R$, then the per frame MAC 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 setting $r$ denote the average number of transmissions before all the fragments in a packet are transmitted successfully, the per frame MAC efficiency is given by:

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

Authorized licensed use limited to: UNIV OF ALABAMA-TUSCALOOSA. Downloaded on January 16, 2010 at 22:23 from IEEE Xplore. Restrictions apply.
efficiency is:
\[ \eta_f = \frac{T_f}{T_f + a + (r m'L_1/L_p) T_f}. \]  
(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:
\[ T_E = (8B T_{\text{and}} + 4B T_{\text{or}}) + (8B T_{\text{and}} + 7B T_{\text{or}} + 3B T_{\text{shift}}) + [46B T_{\text{and}} + (31B + 12) T_{\text{or}} + (64B + 96) T_{\text{shift}}] (\mu - 1), \]
where \( T_{\text{and}}, T_{\text{or}}, \) and \( T_{\text{shift}} \) represent the number of processing cycles for performing byte-wise AND, OR, and SHIFT operations, respectively, and \( \mu \) 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:
\[ O_E = \left[ \frac{L_f}{4B} \right] T_E. \]  
(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 \( \eta_f \) in (1). We obtain a new expression \( \eta_{p,AES} \) for the per packet MAC efficiency. For this subsection only, we denote by \( O_E = \lfloor L_p/(4B) \rfloor T_E \) the number of processing cycles for encrypting a frame.

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

By replacing \( L_p \) in the expression of \( O_E \), we obtain:
\[ O_E = \left[ x + \frac{y_p}{4B} \right] T_E = (x + 1) T_E. \]  
(4)

The last equality is due to the fact that \( 0 \leq \frac{y_p}{4B} < 1 \). By further replacing \( x \) with \( \frac{L_p - y_p}{4B} \), we have:
\[ O_E = \left( \frac{L_p - y_p}{4B} + 1 \right) T_E. \]  
(5)

Then the MAC efficiency incorporating AES overhead is given by:
\[ \eta_{p,AES} = \frac{L_p}{L_p + \tau (\frac{1}{8} + m'L_1 + r T_E (L_p - y_p)/(4B) + 1)} = \eta_{p,AES} (L_p, y_p). \]  
(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:
\[ \text{sign} \frac{\partial \eta_{p,AES}}{\partial L_p} = \text{sign} \left( \frac{L_p}{8} + m'L_1 + r T_E \left( 1 - \frac{y_p}{4B} \right) \right) = 1. \]

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, \( y_p < 4B \), \( \text{sign} \frac{\partial \eta_{p,AES}}{\partial y_p} = \text{sign} \left( \frac{r}{8} + m'L_1 \right) = 1 \) 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:
\[ \lim_{L_p \to \infty} \eta_{p,AES} = \frac{1}{1 + \frac{r T_E}{4B}}. \]  
(7)

Since we need a finite value for \( L_p \) which will render a near optimal throughput, we define a real valued factor \( \alpha \) s.t. \( 0 < \alpha < 1 \) to help solve the following problem. Given \( \alpha \), find \( L_p, \alpha \) such that for any \( L_p > L_p, \alpha \) we have:
\[ \max \eta_{p,AES} > \eta_{p,AES} > \alpha \max \eta_{p,AES}. \]  
(8)

A small \( \alpha \) value stands for a light load, while a large value signifies an increased load.

By combining relations (6) - (8) we obtain:
\[ \left( 1 + \frac{r T_E}{4B} \right) L_p > \alpha \left( L_p + \frac{r T_E}{4B} \right) + r \left( \frac{1}{8} + m'L_1 \right) - \frac{y_p}{4B} r T_E. \]

Further manipulating and isolating \( L_p \), gives us:
\[ L_p > \alpha \left( \frac{1}{1 - \alpha} \right) \frac{r \left( \frac{1}{8} + m'L_1 + T_E \left( 1 - \frac{y_p}{4B} \right) \right)}{1 + \frac{r T_E}{4B}}. \]

Since \( 0 < \alpha < 1 \), we can write \( \alpha = 1 - \frac{1}{n} \Rightarrow \frac{1}{1 - \alpha} = n - 1 \).

We have:
\[ L_p \geq (n-1) \frac{r \left( \frac{1}{8} + m'L_1 + T_E \left( 1 - \frac{y_p}{4B} \right) \right)}{1 + \frac{r T_E}{4B}}. \]

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 \( d = (r m'L_1)/(L_p) \) 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, see [5].

In this section, we characterize the maximum efficiency \( \eta_{\text{max}} \), and the maximum throughput \( S_{\text{max}} \) that any MAC aggregation scheme can support. We first show that \( \eta_{\text{max}} = 1/(1 + d) \) and \( S_{\text{max}} = R/(1 + d) \), 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:
\[ \frac{d\eta_{f,AES}}{dT_f} \approx (2 + d)O_E + (1 + d)T_f + a - (O_E + T_f)(1 + d) = O_E + a > 0. \]

We then have:
\[ \frac{O_E}{(2 + d)O_E + a} < \eta_{f,AES} \leq \frac{1}{1 + d}. \tag{10} \]

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

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: \( \nu = \alpha S_{\text{max}} = \alpha R/(1 + d) \) bits per second, where \( \alpha \leq 1 \). 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:
\[ E[q(k + 1)] = \nu[(1 + d)(T_f + O_E) + a + O_E] = \nu(1 + d)E[q(k)]/R + a + O_E \]
\[ = \nu(E[q(k)] + \alpha E[q(k)] + \alpha E[q(k)]/R + a + O_E). \]

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

Asymptotically, when \( t \to \infty \) and \( \alpha < 1 \),
\[ E[L_f] = E[q(k)] = \frac{\alpha R}{1 + d} \frac{1}{1 - \alpha} [a + O_E]. \tag{11} \]

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 \( \eta_{f, AES} \):
\[ \eta_{f, AES} = \frac{E[q]/R}{1 + d} \frac{E[q]/R + a + O_E}{1 + d + (1 + d)(1/\alpha - 1)} = \frac{\alpha}{1 + d} \eta_{\text{max}}. \]

Hence for \( \alpha \) 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 \( E[L_f] \) over the expected time slot duration \( E[T] \): \( S = E[L_f]/E[T] \).

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

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: \( T_I = \sigma, T_3 = T_{phy} + T_f + T_{ack}, \) and \( T_C = T_{phy} + T_f + T_{EIFS}, \) where \( \sigma \) 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:
\[ E[T] = T_I T_1 + P_3 T_3 + P_C T_C, \tag{12} \]
event probabilities are defined as follows: \( P_I = (1 - \tau)^n \), \( P_3 = \left( \frac{n}{1} \right) \tau (1 - \tau)^{n-1} \), 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:

\[
S_{AFR,AES} = \frac{P_3 L_f (1 - p^f_{frag})}{P_3 R (T_f + m O_E + O_E,_{frag})} = \frac{P_3 L_f (1 - p^f_{frag})}{P_3 R (T_f + m O_E,_{frag})} \approx \frac{P_3 L_f (1 - p^f_{frag})}{c + O_E,_{frag}},
\]

where \( c = P_I T_I + P_3 T_3 + P_C T_C \) and \( p^f_{frag} \) 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 \( 0 \leq y_f < 4B \).

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

\[
S_{AFR} = \frac{P_3 (1 - p^f_{frag})}{(1 - P_I) T_f / L_f}.
\]

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

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

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

\[
\frac{dS_{AFR,AES}}{dL_f} = \frac{S_{AFR,AES}}{L_f} = \frac{\text{sign} \left\{ T_f + T_E (1 - y_f)/(4B) - L_f \frac{dT_f}{dT_E} \right\}}{\text{sign} \left\{ T_f + T_E (1 - y_f)/(4B) - L_f / R \right\}}
\]

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

\[
\frac{dS_{AFR,AES}}{dL_f} = \frac{\text{sign} \left\{ T_f (1 - y_f)/(4B) \right\}}{\text{sign} \left\{ T_f (1 - y_f)/(4B) - L_f / R \right\}} = +1.
\]

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

\[
\max S_{AFR,AES} = \lim_{L_f \rightarrow \infty} S_{AFR,AES} = \frac{P_3 (1 - p^f_{frag})}{(1 - P_I) (1/R + T_E/(4B))}.
\]

### C. Optimal Fragment Size

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

\[
S_{AFR,AES} = \frac{b' (1 - p^f_{frag}) L_{frag}}{(L_{frag} + c') (T_{sym} + O_E)}
\]

where \( b' = \frac{P_n N_{aps} S_{sym} + L_{frag}}{1 - P_I} \), \( c' = L_{FCS} + L_{hdr} \) are positive constants, \( T_{sym} \) and \( N_{aps} \) 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:

\[
S_{AFR,AES}(x) = \frac{x (1 - p_b)^x}{x + c'},
\]

where \( x \) stands for \( L_{frag} \).

We have:

\[
\text{sign} \frac{dS_{AFR,AES}}{dx} = \text{sign} \{ \ln (1 - p_b) x^2 + c'' \ln (1 - p_b) x + c' \}.
\]

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

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

The positive root is:

\[
x_2 = -\frac{c'}{2} \ln (1 - p_b) + \sqrt{\ln (1 - p_b)^2 + 4 \frac{c'}{2} \ln (1 - p_b)^{1/2}} < \frac{1}{\ln (1 - p_b)}.
\]

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:

\[
E[T] = E[\text{number of frames}] = \frac{P_T T_I + P_3 T_3 + P_C T_C}{P_3},
\]

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:

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

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

\[
p^f_{frag} = 1 - (1 - P_b) L_{frag} + L_{FCS}
\]

\[
\approx 1 - (1 - P_b) (L_{frag} + L_{FCS})
\]

\[
= P_b (L_{frag} + L_{FCS}).
\]
Combining the last two equations, we have:

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

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

\[
    D_{MAC}^{AFR} = r (P_I T_I + P_3 T_3 + P_C T_C + m'(L_{frag} - y_{frag} + 1) T_E).
\]

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. 1](image1.png)

Fig. 1: (a) Per frame MAC efficiency. (b) Parameters used.

![Fig. 2](image2.png)

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

![Fig. 3](image3.png)

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.

![Table II](image4.png)

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

Equation (11) shows how the frame size adapts to the offered load. When the load is light, corresponding to small \( \alpha \), 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 \( \alpha \), 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>
<thead>
<tr>
<th>TABLE III: Parameters Used in Figures 4, 5 and 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>(L_f) (bytes)</td>
</tr>
<tr>
<td>(L_{frag}) (bytes)</td>
</tr>
<tr>
<td>(L_{frag}) (bytes)</td>
</tr>
<tr>
<td>(L_{ack}) (bytes)</td>
</tr>
<tr>
<td>(N_{dbp}) (bytes)</td>
</tr>
<tr>
<td>(T_{sym}) ((\mu s))</td>
</tr>
<tr>
<td>(T_{EIFS}) ((\mu s))</td>
</tr>
<tr>
<td>(T_{DIFS}) ((\mu s))</td>
</tr>
<tr>
<td>(\sigma) ((\mu s))</td>
</tr>
<tr>
<td>Basic Rate (Mbps)</td>
</tr>
<tr>
<td>Data rate (Mbps)</td>
</tr>
</tbody>
</table>

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 2048 bytes 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 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 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 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 data rate, a simple solution considering the fairness is to integrate 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

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.

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.