Cross MAC/PHY Layer Security Design Using ARQ with MRC and Adaptive Modulation

Jehad M. Hamamreh*, Marwan Yusuf*, Tuncer Baykas*, Huseyin Arslan*
*School of Engineering and Natural Sciences, Istanbul Medipol University
Beykoz, Istanbul, 34810, Turkey

***Abstract*—In this work, Automatic-Repeat-Request (ARQ) and Maximal Ratio Combination (MRC), have been jointly exploited to enhance the confidentiality of wireless services requested by a legitimate user (Bob) against an eavesdropper (Eve). The obtained security performance is analyzed using Packet Error Rate (PER), where the exact PER gap between Bob and Eve is determined. PER is proposed as a new practical security metric in cross layers (Physical/MAC) security design since it reflects the influence of upper layers mechanisms, and it can be linked with Quality of Service (QoS) requirements for various digital services such as voice and video. Exact PER formulas for both Eve and Bob in i.i.d Rayleigh fading channel are derived. The simulation and theoretical results show that the employment of ARQ mechanism and MRC on a signal level basis before demodulation can significantly enhance data security for certain services at specific SNRs. However, to increase and ensure the security of a specific service at any SNR, adaptive modulation is proposed to be used along with the aforementioned scheme. Analytical and simulation studies demonstrate orders of magnitude difference in PER performance between eavesdroppers and intended receivers.**

I. Introduction

The increasing demand for wireless services, especially applications with sensitive personal and financial data contents, makes current wireless technologies encounter serious challenges regarding security between the trusted transceivers. In fact, security in wireless communication systems is becoming more demanding and is considered to be a substantial requirement in most modern standards, especially those related to health-care (IEEE 802.15.6) and public safety (TETRA). Traditionally, security has been addressed by using secret key-based methods as shown in Shannon's work [1]. The ultimate goal is to secure the mutual conveyed information among different communication parties. However, high layers cryptographic methods are not sufficient alone to ensure security. This is due to the recent unprecedented development in processing and computing devices which reveals the fact that if an eavesdropper is equipped with powerful processing tools, then it can eventually decode the transmitted data regardless of how much mathematically complex the used encryption algorithms are. Consequently, physical layer (PHY) security emerges as a promising concept to provide extra protection along with the conventional cryptography-based approaches. In Wyner's seminal paper [2], it was explained that confidential communication between legitimate users is possible without even sharing a secret key if the eavesdropper's channel is a degraded version of the intended receiver channel, this was achieved using random secrecy codes generated by channel dependent stochastic encoders. Motivated by the same paper [2], the achievable secrecy capacity from an information theoretic point of view was studied for several different communication scenarios, which are summarized in [3]. Moreover, various Wyner secrecy code designs along side adaptive rate transmission methods were proposed in the literature [4]-[7]. In particular, secrecy under joint channel coding, secrecy code and ARQ operation was studied in [8]-[10].

On the other hand, there has been an open research area for developing much more secure and robust methods based on the physical properties of the signal itself and the channel. Accordingly, exploiting some features in the waveforms and designing new methods based on the channel have been proposed for PHY security [11],[12]. Unfortunately, most of the proposed security techniques sacrifice some of the essential wireless system requirements such as energy, capacity, or even complexity. A good example of this is MIMO approaches and artificial noise-based methods [13],[14], whereas some other methods are computationally complex and hard to implement [13]. Additionally, there are methods dedicated only to specific waveforms such as OFDM [12]. In short, the majority of the developed security methods depend on exploiting a certain degree of freedom that might be existing in frequency, time, space, and code domains. Despite of all these constraints, still security can be provided by exploiting MAC layer features along with previously exploited physical layer properties. For instance, employing ARQ protocol, that takes advantage of the fact that only intended recipients can request retransmissions, can be used to enhance security.

In [15], HARQ was studied under quasi-static fading channel from an information theoretic point of view using outage probability metric. In fact, this metric does not take into account the impact of transmission parameters such as modulation, coding, packet length, and combination process [16]. As a result, it can not be linked with QoS requirements for different services as defined in [18]. Additionally, outage probability metric can not be practically measured by actual receiver in wireless networks since it is based on some predefined threshold values such as measuring the probability of the accumulated SNR or accumulated mutual information being less than a certain threshold. In fact, these values are associated with the actual transmitted information, which is practically unknown at the receiver. In [19], It was mentioned that the implementation of PHY security in a real system

978-1-4673-9814-5/16/$31.00 ©2016 IEEE

will be portion of a layered approach, and a key part of this research is the definition of relevant metrics that would make it possible to evaluate the performance of these hybrid schemes. Therefore, it would be very beneficial to use a metric that can assess the cross-layers performance, and at the same time, can be practically measured by wireless actual receivers. This is important since based on such metrics, some decisions including changing coding, modulation, power and even number of re-transmission rounds can be made. For instance, based on the requested service, modulation can be changed as it will be shown in this work. For more details about the current used security performance metrics, refer to Section II.A in [3]. On the other hand, quasi-static fading channel assumption may be impractical since the re-transmission delay in practical systems is mostly greater than the coherence time of the channel and hence the channel realizations become independent over different ARQ rounds [17]. Therefore, it would be interesting to show the exact security gap between Bob and Eve under practical channel scenarios. Moreover, deriving a practical PER formula for Eve will be very useful for ARQ security system designers. More importantly, a wise implementation of MRC on a signal level rather than bit level, along with adaptive modulation is shown to be a promising solution for practical security purposes.

II. CONTRIBUTIONS

We summarize the main contributions of this paper as follows: **First**, we prove by analysis and simulation that without any knowledge on Eve's channel at the transmitter, the use of ARQ mechanism along with MRC that works on a signal level basis and before demodulation can provide a significant secrecy gain. The gain depends on the channel characteristics and maximum number of rounds set by the adapted protocol. More specifically, our simulation results show precisely the secure region represented by PER gap between Eve and Bob at various SNR values and L rounds. **Second**, we derive accurate PER formulas for both Bob and Eve in an i.i.d Rayleigh fading channel. **Third**, we introduce PER as a new and adequate security performance metric to measure the secrecy gap between Bob and Eve at MAC and upper layers. **Fourth**, we show through the relationship between PER and QoS that security methods should take into account the type of service that is targeted to be secured. **Finally**, to provide secure services at any distance (SNR) Eve may be located at, adaptive modulation is proposed to be used with ARQ. It is worth mentioning that ARQ-based security technique is not only suitable to be employed alongside PHY security solutions, but also can meet the constraints and requirements of energy efficiency demands for green radio applications.

III. SYSTEM MODEL AND PRELIMINARIES

As visualized in Fig. 1, we consider a communication system employing ARQ protocol in an i.i.d Rayleigh fading channel over the retransmitted packets. In particular, a transmitter (Alice) is communicating with a legitimate receiver (Bob) in the presence of an eavesdropper (Eve). The ARQ transmission mechanism works as follows: First, Alice transmits a data packet to Bob which is overheard by Eve, after receiving the transmitted packet, Bob decides success or failure by sending back an ACK or NACK messages to Alice through an error-free feedback channel, which is accessed by Eve as well. If a NACK is received by Alice and the current retransmission index is less than the maximum number of retransmissions (L), Alice resends the same data packet with same transmission parameters, i.e. the packet is encoded using the same channel code and modulated by the same modulation type during each retransmission. The receiver then uses MRC to combine the data packet with the previously received ones. If ACK is received by Alice or L is reached, Alice starts transmitting a new data packet. In each retransmission round, both Bob and Eve try to detect the transmitted packet by combining the received data from all preceding retransmissions of the same data packet via MRC as explained later. If Bob cannot extract the packet after L rounds, then Bob records a packet error for the data packet.

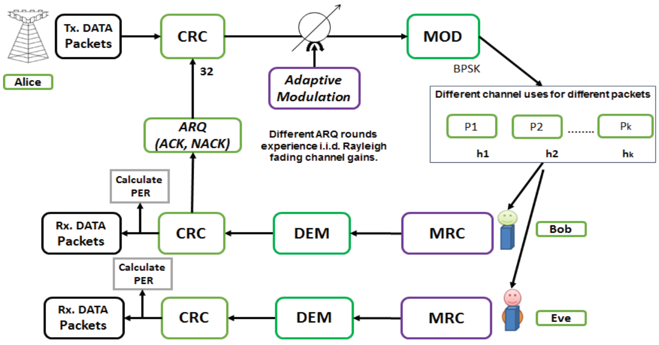


Fig. 1. System model for the ARQ scheme considered in this work.

The following assumptions are also taken into account: 1) The channel is constant within each ARQ round (N symbols), but it is independent across ARQ rounds [17]. 2) A maximum of L ARQ rounds are allowed which limits both complexity and delay. 3) Alice has no knowledge on Eve's channel since Eve is a passive node. 4) Alice has only the normal feedback information about Bob such as SNR and ACK/NACK. 5) The worst security scenario is considered, where Eve is aware of the retransmission process and can employ MRC. It should be emphasized that transmission slots in modern systems are roughly around one millisecond, during which the channel is approximately constant. In practice, an ARQ round corresponds to a single transmission slot, but subsequent ARQ rounds are separated in time by at least a few slots to allow for decoding and ACK/NACK feedback. Thus the assumption of independent channels across ARQ rounds is reasonable and more practical than the postulate of static gains over different rounds [15].

IV. MRC IMPLEMENTATION

The system is designed in such a way to keep retransmitting the same data packet as long as CRC detects an error in the received packet (i.e. CRC output is one) and the current retransmission round index is less than (L) set by ARQ protocol. This process allows for implicit rate adaptation to the instantaneous Bob's channel quality because Bob stops asking for retransmission once his channel conditions experienced by a packet are good enough to allow for successful decoding. In fact, there are different combination methods that can be performed at different signal processing levels such as before demodulation, or after demodulation and before decoding [17], or even after decoding. However, in our case, since we are using the same modulation, coding and power in each retransmission round, the combination process at the receiver is performed before demodulation. Each version of the received packet at each round is multiplied by the corresponding estimated channel conjugate. The output of this process is saved in a buffer so that it can be combined with the forthcoming retransmission versions of the same packet. The combined received packet is then jointly demodulated, and then CRC is used to detect if there is any bit errors in the received packet or not. According to the output of CRC, the receiver decides whether to ask for retransmission (i.e. send NACK message), or stop the process of retransmitting the same packet by sending an ACK message. The received signal $y^k_{b/e}$ at the k^{th} round for both Bob and Eve is modeled as

$$y^k_{b/e} \quad = \quad h^k_{b/e} x + w^k_{b/e} \quad k = 1, 2, ..L \tag{1}$$

where x is a unit-power transmitted data packet, $h^k_{b/e}$ are the Rayleigh fading channel realizations between Alice and Bob/Eve over k^{th} round, and $w^k_{b/e}$ is the additive white Gaussian noise with power spectral density $N_{b/e}$ at Bob/Eve. According to the previous equation, $\gamma_{b/e}$ and $\bar{\gamma}_{b/e}$ are considered to be the instantaneous and average received SNR for both Bob and Eve at k^{th} round. Particularly, $\gamma_{b/e} = \frac{P_k |h^k_{b/e}|^2}{N_{b/e}}$ and $\bar{\gamma}_{b/e} = \frac{P_k}{N_{b/e}}$, where P_k is the transmitted power at k^{th} round, which is assumed to be fixed and normalized to unity during multi-packet transmission process. The received signals in the first and second retransmission rounds of the same packet are

$$y^1_{b/e} \quad = \quad h^1_{b/e} x + w^1_{b/e} \tag{2}$$

$$y^2_{b/e} \quad = \quad h^2_{b/e} x + w^2_{b/e} \tag{3}$$

hence, MRC process at the receiver side is as follows:

$$\hat{y}_{b/e} \quad = \quad y^1_{b/e} h^{1*}_{b/e} + y^2_{b/e} h^{2*}_{b/e} \tag{4}$$

$$\hat{y}_{b/e} \quad = \quad x \left(|h^1_{b/e}|^2 + |h^2_{b/e}|^2 \right) + \hat{w}_{b/e} \tag{5}$$

$$\hat{x} \quad = \quad x + \frac{\hat{w}_{b/e}}{\left(|h^1_{b/e}|^2 + |h^2_{b/e}|^2 \right)} \tag{6}$$

where $\hat{w}_{b/e} = w^1_{b/e} h^{1*}_{b/e} + w^2_{b/e} h^{2*}_{b/e}$. It is clear from (5) that the combination process depends on the channel gains of the receivers. Now, since Bob's channel is independent from Eve's one, the implicit adaptation process, resulted from ARQ mechanism and controlled by Bob will be in favor of him, but not Eve. This is because only Bob can ask for retransmission as per his channel conditions that affect his success in decoding the packet correctly. As a result, Eve will be in error in two cases: 1) if retransmission process is stopped by Bob before her success in packet decoding or 2) maximum number of retransmission rounds is reached, while she is still not able to decode the packet correctly. In other words, Eve's failure not only depends on her channel (γ_e), but also on Bob's success (γ_b). Simulation and analytical results prove that the use of ARQ in the proposed way can provide a significant PER difference between Bob and Eve in a real fading scenario.

V. Analytical Analysis of PER

As we stated in Sec. I, traditional secrecy metrics will not be suitable to practically reflect the security performance of ARQ-based schemes because of the existing decoding dependency between Bob and Eve. Thus, we resort to use PER as a new security metric. In the literature, the average PER of CC-HARQ after L^{th} round was discussed from reliability and optimal power allocation perspectives in [16]. However, from security point of view, Eve's performance comes into the picture. Therefore, finding exact PER for both Bob and Eve under the proposed ARQ scheme would be interesting and helpful for security designers. PER[1] can be expressed for both Bob and Eve as follows:

$$PER^{Bob}_L = \int_0^\infty .. \int_0^\infty f(\gamma^1_b)..f(\gamma^L_b) g_\gamma(\gamma^1_b)..g_\gamma(\gamma^L_b) d\gamma^1_b..d\gamma^L_b \tag{7}$$

$$PER^{Eve}_L = \int_0^\infty .. \int_0^\infty f(\gamma^1_e)..f(\gamma^L_e) g_\gamma(\gamma^1_e)..g_\gamma(\gamma^L_e) d\gamma^1_e..d\gamma^L_e \tag{8}$$

where $\gamma^L_{b/e} = \sum_{k=1}^L (\gamma^k_{b/e})$ is the total accumulated received SNR with the PDF given by $g_\gamma(\gamma^L_{b/e})$ for both Bob and Eve, respectively. $f(\gamma^k_{b/e})$ is considered to be the error probability relating function associated with Bob and Eve. According to [16], PER can be simplified as follows:

$$PER^{Bob}_L = \int_0^{\alpha_b} g_\gamma(\gamma^L_b)\, d\gamma^L_b, \quad \alpha_b = \int_0^\infty f(\gamma^L_b)\, d\gamma^L_b. \tag{9}$$

$$PER^{Eve}_L = \int_0^{\alpha_e} g_\gamma(\gamma^L_e)\, d\gamma^L_e, \quad \alpha_e = \int_0^\infty f(\gamma^L_e)\, d\gamma^L_e. \tag{10}$$

The complexity of finding exact PER is simplified when the effects of retransmission parameters, such as modulation, coding and combination are taken into consideration. That is because $\alpha_{b/e}$, which is called in the literature the waterfall threshold, can be taken from the simulation results of both Bob's and Eve's PER. Furthermore, $\alpha_{b/e}$ is related to a certain well defined system model design, which should be as comprehensive and close as possible to what happens in reality. Based on proposition (1) in [16], $PER^{Bob/Eve}_L$ can be

[1] For simplicity, we start our analysis by assuming that PER^{Eve}_L depends only on γ_e, but later in the final expression, we take its dependence on γ_b as well by doing simple intuitive probability analysis for the actual PER^{Eve}_L.

written in terms of cumulative distribution function (CDF):

$$PER_L^{Bob} = F_{\gamma_b}^L(\alpha_b) \quad = Pr\left(\sum_{k=0}^{L-1} \gamma_b^k < \alpha_b\right) \tag{11}$$

$$PER_L^{Eve} = F_{\gamma_e}^L(\alpha_e) \quad = Pr\left(\sum_{k=0}^{L-1} \gamma_e^k < \alpha_e\right) \tag{12}$$

where $Pr()$ is the probability function, $\alpha_{b/e}$ is a function of the transmission parameters, and is related to the instantaneous spectral efficiency (i.e. the accumulated information over total number of transmitted information [λ]). For equal power and modulation allocation during retransmission process and based on a result given in [21], the accurate PER_L^{Bob} formula can be expressed as in (13). The proof of how (11) is transformed into the form given in (13), is provided in the appendix.

$$PER_L^{Bob}(\gamma_b, \alpha_b) = 1 - \sum_{k=0}^{L-1} \frac{1}{k!}\left(\frac{\alpha_b}{\gamma_b}\right)^k * e^{\left(-\frac{\alpha_b}{\gamma_b}\right)} \tag{13}$$

where α_b is derived numerically from the extensive simulation results, that we performed at different PSK modulation orders (M) and different L. Next, we carried out fitting methods on the obtained simulation results to get a simple formula for $\alpha_{a/e}$ in i.i.d slowly Rayleigh fading channel as follows

$$\alpha_b = \alpha_e = 2^\lambda - 1, \quad \lambda = L \times \log_2(M) - 1, \quad \lambda \geq 2. \tag{14}$$

It should be emphasized that our derived PER_L^{Bob} is more accurate than the one given in [16], especially at low SNR as it will be seen in Sec. VI, Fig. 2. Additionally, α_L is simpler and directly written in terms of M and L. On the other hand, a generic PER expression for Eve when number of retransmission is greater than one ($L \geq 2$) is constructed as shown in (20). However, For the special case when $L = 2$ (related to voice service), Eve's PER can be written as

$$\begin{aligned} PER_L^{Eve}(\gamma_e, \gamma_b, \alpha_e, \alpha_b) \quad &= \quad \left(1 - e^{\left(-\frac{\alpha_e}{\gamma_e}\right)}\right)\left(e^{\left(-\frac{\alpha_b}{\gamma_b}\right)}\right) \\ &+ \quad \left(1 - \sum_{k=0}^{L-1} \frac{1}{k!}\left(\frac{\alpha_e}{\gamma_e}\right)^k * e^{\left(-\frac{\alpha_e}{\gamma_e}\right)}\right) \\ &* \quad \left(1 - e^{\left(-\frac{\alpha_b}{\gamma_b}\right)}\right), L = 2. \end{aligned} \tag{15}$$

As results from (15), PER_L^{Eve} is highly dependent on the success of Bob in decoding the retransmitted packet. In specific, Eve's packet decoding failure occurs if Bob was able to successfully decode the packet from the first or second round, while Eve was not able to successfully decode the packet neither from the first nor the second round, respectively. Additionally, both (16) and (17) exhibit the equal performance of both Bob and Eve at similar SNR values when $L = 1$.

$$PER_L^{Eve} = \left(1 - e^{\frac{-\alpha_e}{\gamma_e}}\right), L = 1 \tag{16}$$

$$PER_L^{Bob} = \left(1 - e^{\frac{-\alpha_b}{\gamma_b}}\right), L = 1 \tag{17}$$

VI. QoS-Based Adaptive Modulation

In addition to PER being a suitable metric in cross-layers security design as it reflects the influence of upper layers' functions such as ARQ, it can also be linked with QoS requirements for various digital wireless applications such as voice, video, web browsing and so forth [18]. In particular, a previous knowledge of the type of running application at user side is a very advantageous feedback that should be taken into account during the phase of security design process to ensure conveying a certain service confidentially. This can be used as a solution for some cases, where securing a certain service is extremely needed at any distance from the base station (BS). More accurately, if Eve is closer to the BS than Bob (i.e., SNR value at Eve is higher than Bob, where Eve can receive the requested service with a quality better than Bob), then secure service is hard to be achieved. This situation is clearly visualized in Fig. 2, where it is evident that secure voice communication for instance can not be achieved at (SNR$\geq$ 25) since Eve's PER is less than the minimum required QoS ($PER = 10^{-2}$) as indicated in [18]. This shows that the provided secrecy by the previous method (ARQ with MRC) is limited and might be insufficient in some cases where Eve may have better SNR than Bob. To

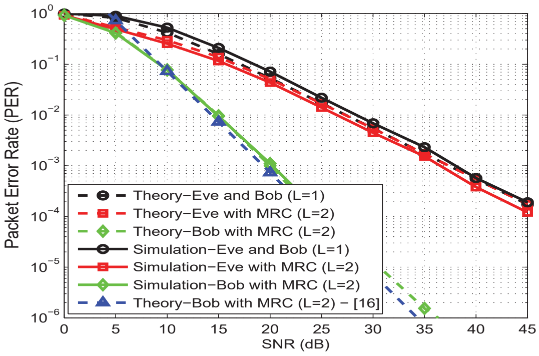
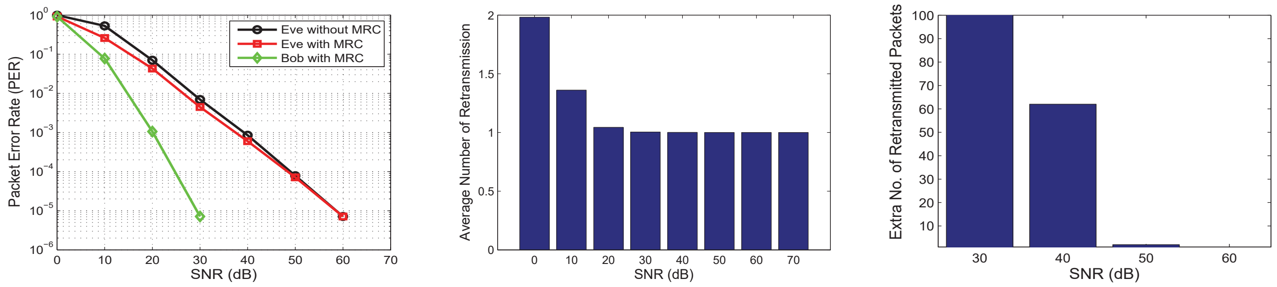


Fig. 2. Analytical and simulation results of ARQ (L=2) with BPSK.

$$\begin{aligned} PER_L^{Eve}(\gamma_e, \gamma_b, \alpha_e, \alpha_b) = \left(1 - e^{\left(-\frac{\alpha_e}{\gamma_e}\right)}\right)\left(e^{\left(-\frac{\alpha_b}{\gamma_b}\right)}\right) + \sum_{\dot{k}=1}^{L-2}\left(1 - \sum_{k=0}^{\dot{k}-1} \frac{1}{k!}\left(\frac{\alpha_e}{\gamma_e}\right)^k * e^{\left(-\frac{\alpha_e}{\gamma_e}\right)}\right) * \\ \left(\sum_{k=0}^{\dot{k}-1} \frac{1}{k!}\left(\frac{\alpha_b}{\gamma_b}\right)^k * e^{\left(-\frac{\alpha_b}{\gamma_b}\right)} - \sum_{k=0}^{\dot{k}-2} \frac{1}{k!}\left(\frac{\alpha_b}{\gamma_b}\right)^k * e^{\left(-\frac{\alpha_b}{\gamma_b}\right)}\right) + \left(1 - \sum_{k=0}^{L-1} \frac{1}{k!}\left(\frac{\alpha_e}{\gamma_e}\right)^k * e^{\left(-\frac{\alpha_e}{\gamma_e}\right)}\right)\left(1 - \sum_{k=0}^{L-2} \frac{1}{k!}\left(\frac{\alpha_b}{\gamma_b}\right)^k * e^{\left(-\frac{\alpha_b}{\gamma_b}\right)}\right) \end{aligned} \tag{20}$$

Generic PER formula for Eve over i.i.d. block Rayleigh fading channels when number of retransmission ($L > 2$)

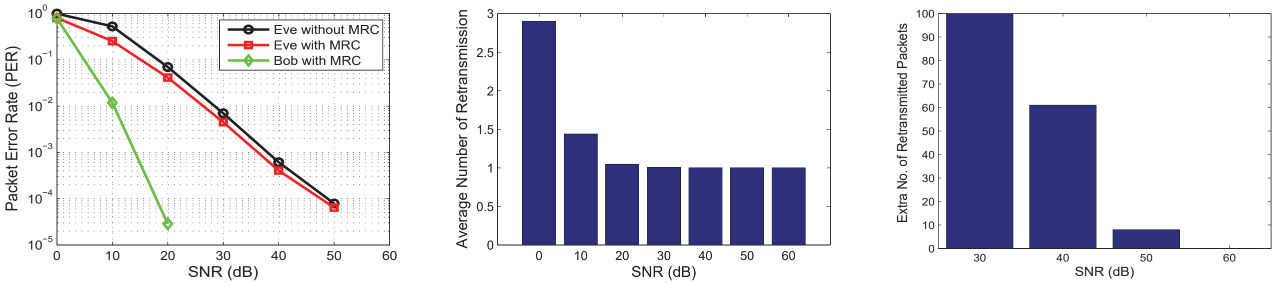


(a) ARQ

(b) ARQ

(c) ARQ, No. of Packets that are not successfully decoded from the first round

Fig. 3. PER security performance and average number of retransmissions for ARQ when $L = 2$.

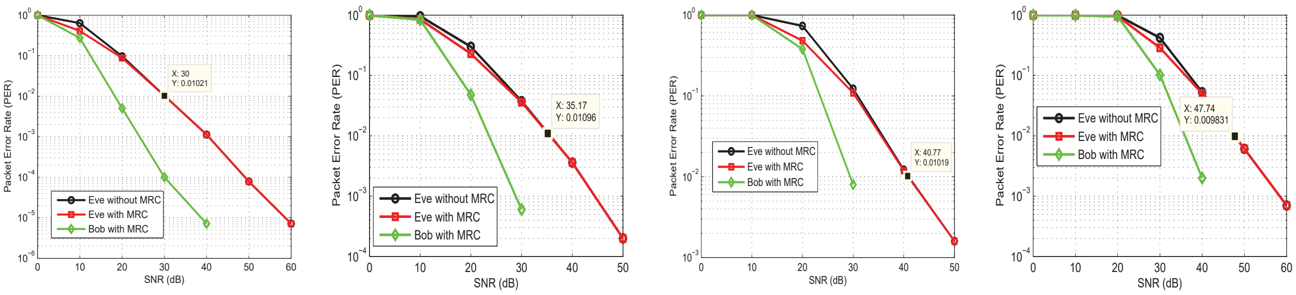


(a) ARQ

(b) ARQ

(c) ARQ, No. of Packets that are not successfully decoded from the first round

Fig. 4. PER security performance and average number of retransmissions for ARQ when $L = 3$.



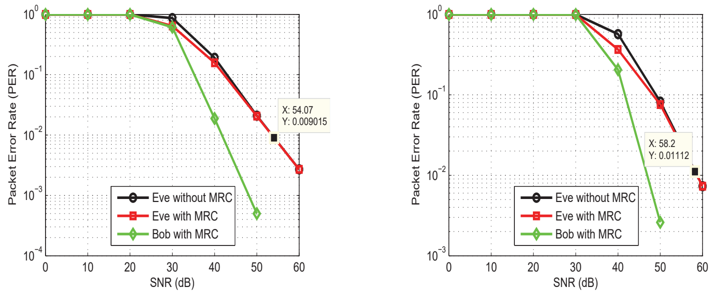
(a) ARQ ($4PSK$)

(b) ARQ ($8PSK$)

(c) ARQ ($16PSK$)

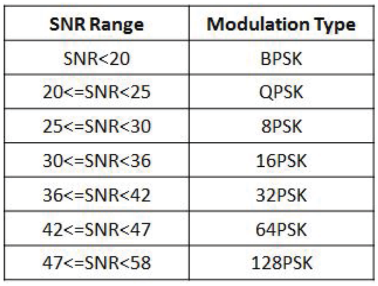
(d) ARQ ($32PSK$)

Fig. 5. PER security performance of ARQ when $L = 2$ with different PSK modulation orders.



(a) ARQ ($64PSK$)

(b) ARQ ($128PSK$)



SNR Range	Modulation Type
SNR<20	BPSK
20<=SNR<25	QPSK
25<=SNR<30	8PSK
30<=SNR<36	16PSK
36<=SNR<42	32PSK
42<=SNR<47	64PSK
47<=SNR<58	128PSK

(c) Adaptive switching modulation table based on Bob's PER $\leq 10^{-2}$ (voice service)

Fig. 6. Designed adaptive modulation tables and PER security performance of ARQ when $L = 2$ with different PSK modulation orders.

address this problem, we propose using adaptive modulation accompanied by ARQ to assure secure voice service against eavesdropping at any distance Eve may be located from the BS. In specific, an accurate adaptive modulation table (Fig. 6.c) is proposed to be used for providing guaranteed service-based security. More precisely, the modulation type is changed based on Bob's SNR in such a way that keeps Bob's PER less than a certain threshold related to the requested service, while Eve's PER is maintained to be greater than the that threshold. In this study, the proposed table is designed based on the QoS requirements associated with voice service as it will be shown in the next section. Keeping in mind that the same procedure can be used for securing other services such as video, which will have different adaptive tables. Although we have only targeted securing voice service in this paper, the same procedure followed in this context can be applied for securing other services such as video, messaging, web browsing and data streaming. However, these services will result in having different adaptive tables based on their QoS needs. Thus, further research has to be performed for finding security-based adaptive modulation tables for the rest of digital services that are defined in [18].

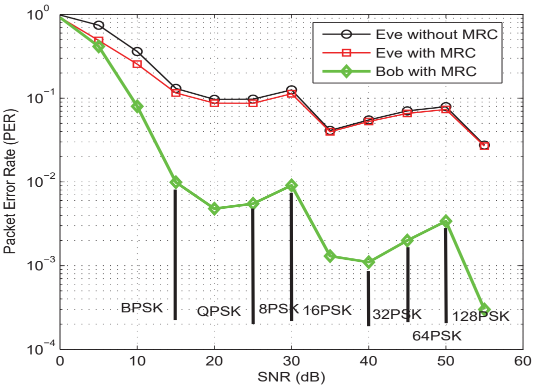


Fig. 7. Adaptive modulation process along with ARQ scheme ($L = 2$).

VII. SIMULATION SCENARIO AND RESULTS

Our simulations are divided into two parts: the first shows the security performance of ARQ with MRC, whereas the second shows the performance of ARQ with MRC and adaptive modulation. In the first part, multiple packets transmission system based on ARQ protocol with MRC when $L = 2$ rounds is adopted. Packet size of 432 symbols is used with additional 32 reliable CRC bits appended to the packet for the sake of error detection, BPSK is then used to modulate the data. Packets are then sent through slowly independent Rayleigh Fading channel, where retransmitted packets experience independent channel gains [17]. At the receiver, MRC method as described in Sec. IV is employed to combine the retransmitted packets, which are jointly demodulated and then passed through error detection process represented by CRC block. If a single bit error is detected in the packet then NACK is generated, otherwise, ACK is fed back. Finally, PER evaluation is performed as explained in [20], where packet size, number of packets to be tested and error count threshold are determined for different scenarios. Furthermore, The worst security scenario is assumed, where Eve is aware of the retransmission process and can employ MRC on a signal level to increase the probability of successful decoding. As exhibited in Fig. 2, good match is observed between our simulations and the analytically derived PER of both Bob and Eve. Furthermore, it is clear from Fig. 2 that our derived PER_L^{Bob} is more precise than the average one given in [16] since it is determined in terms of the instantaneous SNR, but not average SNR. On the other hand, ours is more general since it is applicable not only for high SNR regimes, but also for low SNR regimes. Moreover, it is also obvious that at SNR $= 5$ dB, PER values of Eve start dramatically diverging away from Bob's PER curve since the average number of required retransmission to achieve error-free packet reception at Bob begins to be less than 2 ($L \leq 2$) at SNR ≥ 5 dB as shown in Fig. 3.b. In fact, this happens due to the implicit adaptivity resulted from ARQ along with MRC. In Fig. 4, we test the effect of increasing (L) on enhancing the security gap region between Bob and Eve. It is clear that at SNR $= 0$ dB, PER values of Eve start deviating away from Bob's PER. This means that as L increases, security gap increases. Now when we look at Fig. 4.b by our abstract eyes, we see that the average number of retransmission at SNR $= 40$ dB is almost one, but Bob's PER is different than Eve's PER. To clarify why this happens, Fig. 3.c at $L = 2$ and Fig. 4.c at $L = 3$ are drawn to show that at SNR $= 40$ dB and even SNR $= 50$ dB still there are some extra packets retransmission, but because of the huge number of transmitted packets (around million) and the small percentage of the retransmitted packets, we see that the average number of retransmission is one as shown in Fig. 4.b, but it is not. The real situation is exhibited in Fig. 4.c, where the figure tells that the process of implicit adaptation due to ARQ is still active at even high SNR. As a result, a better performance for Bob's PER is expected. However, Fig. 4.c shows that at SNR $= 60$ dB, there is exactly zero packet retransmission, where all the packets are successfully decoded from the first round. This means that the performance of both Bob and Eve should be exactly the same, and this is indeed shown in Fig. 4.a, where PER goes to zero for all receiving parties (there is no lines or dots in Fig. 4.a at SNR $= 60$ dB). Notice that Bob's PER is zero at SNR > 20 dB, but the average number of retransmission equals one exactly at SNR $= 60$ dB. In the second part of our simulations, the adaptive modulation block shown in Fig. 1 is switched on. Now, modulation order is changing according to the QoS requirements for voice service, which is determined (as reported in LTE standard) in terms of PER being $\leq 10^{-2}$ and L being ≤ 2 since packet delay budget is determined to be less than 100 ms [18]. In fact, we obtain the exact SNR switching range by performing extensive simulations for different modulation orders as shown in Fig. 5.a-d and Fig. 6.a-b. At each one, we accurately determine at which SNR Bob's PER becomes less than 10^{-2}. Accordingly, an adaptive modulation table is specified. The table (Fig. 6.c) is designed based on the criteria of making sure that Bob's PER is less than or equal 10^{-2}, while Eve's PER is greater than 10^{-2}. Fig. 7 shows the exact obtained PER security performance using the proposed practical design (Bob's PER based-adaptive modulation table), where this method does not require any knowledge about Eve's channel. It is shown that Bob's PER is kept $< 10^{-2}$, while Eve's PER is kept $> 10^{-2}$, resulting in a secure voice service. It is also depicted that the Eve's PER behaviors with and without MRC at high SNR regime are almost the same, since only a few packets are retransmitted based on Bob's channel, but not Eve. As a result, Bob's PER enhances, whereas Eve's PER has insignificant improvements.

VIII. CONCLUSION

ARQ as a MAC layer mechanism with MRC on a signal level as a physical layer mechanism, have been utilized to provide confidential wireless services for legitimate users against eavesdropping. PER is suggested to be used as a new practical security metric in cross layers security design. The obtained results are analysed using PER, where the exact gap difference in PER between Bob and Eve is determined. Accurate PER formulas for both Eve and Bob in i.i.d Rayleigh fading channel are derived. The acquired simulation and theoretical results show that the employment of the proposed scheme can boost data security for certain services at specific SNR values, and it gets enhanced as number of allowable retransmissions (L) increases. Furthermore, QoS-based adaptive modulation is proposed to be used along with ARQ scheme to ensure security for specific services at any SNR Eve may encounter. Finally, this work has shown that taking QoS requirements for different services into account during the design phase is an efficient way for providing secure wireless systems.

APPENDIX

In (11), $\sum_{k=0}^{L-1} \gamma_b^k$ is a sum of L statistically independent and not identically distributed (i.n.i.d.) exponential random variables. Based on Theorem 2 (Sum Distribution) given in [21], the CDF of this sum can be written as

$$F_{\gamma_b}^{L}(\alpha_b) = 1 - \sum_{i=1}^{M_l} \sum_{j=1}^{\sigma_{i,l}} \sum_{k=0}^{j-1} \frac{\psi_{i,j}(\mu_l)}{k!} \left(\frac{\alpha_b}{\gamma_b}\right)^k * e^{\left(-\frac{\alpha_b}{\gamma_b}\right)} \quad (18)$$

where $\mu_l = diag(\gamma_{b,0}, \gamma_{b,2}, ..., \gamma_{b,L-1})$, and M_l is the number of distinct diagonal elements of μ_l. $\sigma_{i,l}$ indicates the multiplicity of μ_l. $\psi_{i,j}(\mu_l)$ is the (i,j)th characteristic coefficient of μ_l. For equal both modulation and power allocation during retransmission process, we have $M_l = 1$ and $\sigma_{i,l} = l$, thus (18) can be simplified as

$$F_{\gamma_b}^{L}(\alpha_b) = 1 - \sum_{k=0}^{L-1} \frac{1}{k!} \left(\frac{\alpha_b}{\gamma_b}\right)^k * e^{\left(-\frac{\alpha_b}{\gamma_b}\right)}. \quad (19)$$

By substituting (19) into (11), we get the accurate PER_L^{Bob} formula as expressed in (13). Note that the same procedure can be applied on Eve, but now we have to take into account the effect of Bob's packet decoding success on Eve.

ACKNOWLEDGMENT

This work has been supported by The Scientific Research Council of Turkey (TUBITAK) under grant No. 114E244.

REFERENCES

[1] C. E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J., vol. 28, no.4, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, The wire-tap channel, Bell Syst. Tech. J., vol. 54, no.8, pp. 1355–1387, 1975.

[3] Mukherjee, A.; Fakoorian, S.A.A.; Jing Huang; Swindlehurst, A.L., ”Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey,” in Communications Surveys and Tutorials, IEEE , vol.16, no.3, pp.1550-1573, Third Quarter 2014.

[4] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin, and J. M. Merolla, Applications of LDPC codes to the wiretap channel, IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[5] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, Secure nested codes for type II wiretap channels, in Proc. IEEE Information Theory Workshop on Frontiers in Coding Theory, Lake Tahoe, CA, Sep. 2-6, 2007.

[6] Mheich, Z.; Le Treust, M.; Alberge, F.; Duhamel, P.; Szczecinski, L., ”Rate-adaptive secure HARQ protocol for block-fading channels,” Signal Processing Conference (EUSIPCO), 2014 Proceedings of the 22nd European, pp.830–834, 1-5 Sept. 2014.

[7] Le Treust, M.; Szczecinski, L.; Labeau, F., ”Secrecy and Rate Adaptation for secure HARQ protocols,” Information Theory Workshop (ITW), 2013 IEEE, pp.1–5, 9-13 Sept. 2013.

[8] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels, IEEE Trans. Inf. Theory, vol. 55, no.4, pp. 1575–1591, Apr. 2009.

[9] M. Baldi, M. Bianchi, and F. Chiaraluce, Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: a security gap analysis, IEEE Trans. Inf. Forens. Security, vol. 7, pp. 883–894, June 2012.

[10] Tomasin, S.; Laurenti, N., ”Secure HARQ With Multiple Encoding Over Block Fading Channels: Channel Set Characterization and Outage Analysis, ”Information Forensics and Security, IEEE Transactions on ,vol.9, no.10, pp.1708–1719, Oct. 2014.

[11] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, Waveform design for secure SISO transmissions and multicasting, IEEE J. Sel. Areas Commun., Special Issue on Signal Proc. Techn. for Wireless Phys. Layer Security, vol. 31, no.1, pp. 1864–1874, Sept. 2013.

[12] Z. E. Ankarali, M. Karabacak, H. Arslan, ”Cyclic Feature Concealing CP Selection for Physical Layer Security”, IEEE Military Communications Conference (MILCOM), Baltimore, Maryland, pp. 485-481, Oct. 6-8, 2014.

[13] Jun Zhu; Schober, R.; Bhargava, V.K., ”Secure transmission in multicell massive MIMO systems,” Globecom Workshops (GC Wkshps), 2013 IEEE , vol., no., pp.1286–1291, 9-13 Dec. 2013.

[14] S. Goel and R. Negi, Guaranteeing secrecy using artificial noise, IEEE Trans. Wireless Commun., vol. 7, no.6, pp. 21802189, June 2008.

[15] Kundu, S.; Pados, D.A.; Batalama, S.N., ”Hybrid-ARQ as a communications security measure,” 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp.5681–5685, 4-9 May 2014.

[16] Songhu Ge; Yong Xi; Shengchun Huang; Jibo Wei, ”Packet Error Rate Analysis and Power Allocation for CC-HARQ Over Rayleigh Fading Channels,” Communications Letters, IEEE , vol.18, no.8, pp.1467,1470, Aug. 2014.

[17] Chaitanya, T.V.K.; Larsson, E.G., ”Optimal Power Allocation for Hybrid ARQ with Chase Combining in i.i.d. Rayleigh Fading Channels,” Communications, IEEE Transactions on , vol.61, no.5, pp.1835,1846, 2013.

[18] 3GPP TS 23.203 V11.6.0, ”Policy and charging control architecture”.

[19] Yi-Sheng Shiu; Shih Yu Chang; Hsiao-Chun Wu; Huang, S.C.-H.; Hsiao-Hwa Chen, ”Physical layer security in wireless networks: a tutorial,” in Wireless Communications, IEEE , vol.18, no.2, pp.66-74, April 2011.

[20] Approved Working Paper, International Civil Aviation Organization, Aeronautical Communications Panel (ACP), 5th-Meeting of the Working Group S (SURFACE), ”Packet Error Rate Evaluation Method”, introduced by Shoichi Hanatani, Toshiaki Akita, Ichiro Murata, 6 May 2014.

[21] Bletsas, A.; Hyundong Shin; Win, M.Z., ”Cooperative Communications with Outage-Optimal Opportunistic Relaying,” in Wireless Communications, IEEE Transactions on , vol.6, no.9, pp.3450-3460, September 2007.