A Feedback-Based Transmission for Wireless Networks with Energy and Secrecy Constraints

Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2011, Article ID 313269, 11 pages
doi:10.1155/2011/313269

Research Article

A Feedback-Based Transmission for Wireless Networks with Energy and Secrecy Constraints

Ioannis Krikidis,[1] John S. Thompson (EURASIP Member),[2] Steve McLaughlin (EURASIP Member),[2] and Peter M. Grant (EURASIP Member)[2]

[1] *Department of Computer Engineering & Informatics, University of Patras, Rio, 26500 Patras, Greece*
[2] *Institute for Digital Communications, The University of Edinburgh, Mayfield Road, Edinburgh EH9 3JL, UK*

Correspondence should be addressed to Ioannis Krikidis, krikidis@ucy.ac.cy

Received 10 July 2010; Revised 29 December 2010; Accepted 19 January 2011

Academic Editor: Lin Cai

This paper investigates new transmission techniques for clustered feedback-based wireless networks that are characterized by energy and secrecy constraints. The proposed schemes incorporate multiuser diversity gain with an appropriate power allocation (PA) in order to support a defined Quality-of-Service (QoS) and jointly achieve lifetime maximization and confidentiality. We show that an adaptive PA scheme that adjusts the transmitted power using instantaneous feedback and suspends the transmission when the required power is higher than a threshold significantly prolongs the network lifetime without affecting the QoS of the network. In addition, the adaptation of the transmitted power on the main link improves the secrecy of the network and efficiently protects the source message from eavesdropper attacks. The proposed scheme improves network's confidentiality without requiring any information about the eavesdropper channel and is suitable for practical applications. Another objective of the paper is the energy analysis of networks by taking into account processing and maintenance energy cost at the transmitters. We demonstrate that the combination of PA with an appropriate switch-off mechanism, that allows the source to transmit for an appropriate fraction of the time, significantly extends the network lifetime. All the proposed protocols are evaluated by theoretical and simulation results.

1. Introduction

Recent studies have shown that the Base Station (BS) and its associated operations are the main cause of power consumption in the modern wireless networks [1]. This result in combination with a continuing expansion of the current networks increases the demands on energy sources as well as some serious environmental issues like the increase of CO_2 emissions to the atmosphere [1, 2]. Therefore, a network design that efficiently uses its available energy resources is an urgent and important research topic. On the other hand, due to the broadcast nature of the transmission, the source message can be received from all the users that are within the transmission range, and therefore secure communication is also of importance. In this paper, we focus on wireless networks with energy and secrecy constraints and investigate some transmission techniques that improve network lifetime and confidentiality for users.

Several physical (PHY) layer techniques that decrease the network's energy requirements and extend the network lifetime have been proposed in the literature. In [3, 4] the authors introduce multihop transmission in order to reduce the energy consumption and they prove that short intermediate transmissions can result in significant energy savings. Accordingly, the channel capacity gain that arises from the cooperative diversity concept also yields a decrease in the required transmitted power. The energy efficiency of different relaying techniques is discussed in [5–8], and several relay selection metrics that incorporate instantaneous channelfeedback with residual energy in order to achieve lifetime improvements are presented in [9]. In addition, appropriate resource allocation strategies can minimize the energy consumption of a wireless network. The impact of scheduling on the network lifetime for different levels of channel knowledge is presented in [10], and several power allocation (PA) techniques which minimize the average

transmission power for different network configurations are discussed in [11–13]. On the other hand, in addition to the energy cost associated with the transmission process, data processing and system maintenance also contribute to the energy consumption at the transmitters [6]. In [14], the authors take into account the processing cost and they prove that dedicated relaying (fixed relaying) is more energy efficient than user cooperation (mobile relaying). Finally, a burst transmission system that switches off the transmitter for a fraction of time in order to reduce the processing cost and accumulate energy for future transmissions is analyzed in [15, 16] from an information theoretic standpoint. However, the quality of the instantaneous link is not taken into account, and PA as well as QoS issues are not discussed.

As for secure communication, various PHY layer techniques that increase the perfect secrecy capacity [17, 18] of a wireless network have recently been investigated. In [19], the authors propose a joint scheduling and PA scheme in order to maximize security for a downlink scenario with secrecy constraints. Another PHY layer approach that employs an appropriate distributed beamforming design, which forces the source signal to be orthogonal to the instantaneous eavesdropper channel, has been reported in [20, 21]. The application of the cooperative (relaying) concept at the PHY layer as a means to protect the source message from the eavesdropper was proposed in [22]. Finally, in [23], the authors introduce a jammer node that generates artificial interference in order to confuse the eavesdropper and maximize the secure rate. However, most of the existing works require a knowledge of the instantaneous eavesdropper links and therefore their practical application is limited. Furthermore, it is worth noting that in the current literature, network lifetime and PHY layer security are considered as two separate and independent problems, and therefore existing solutions may not deal with both issues in the most efficient way.

In this paper, we investigate some new transmission techniques that jointly achieve lifetime maximization and confidentiality improvements. Based on a clustered network topology with available channel feedback, we investigate two main transmission techniques that combine the multiuser diversity (MUD) concept [24], [25, Chapter 6] with an appropriate PA scheme under a target outage probability constraint. The first transmission approach employs a constant PA scheme and uses the MUD gain in order to save energy and protect the source message against potential attacks. The second approach uses more efficiently the available channel feedback and extracts the MUD gain by employing an adaptive PA scheme. This adaptive PA adjusts the transmitted power on the instantaneous quality of the link and suspends the transmission if the required power is higher than a selected threshold. We show that this scheme significantly increases the lifetime of the network and improves the PHY layer security for high target outage probabilities. It is worth noting that the proposed schemes are independent of the eavesdropper link (in contrast to previously reported work [19, 20, 23] which assumes that the instantaneous eavesdropper link can be estimated) and thus are suitable for practical applications where the knowledge of the instantaneous source-eavesdropper link is not available. Another contribution of the paper is the study of scenarios with high processing and maintenance cost. An appropriate burst transmission that switches off the transmitter for a fraction of time is integrated to the proposed PA schemes in order to minimize the total energy cost at the transmitters. We note that the bursty approach concerns scenarios with high processing and maintenance cost at the transmitter and is analyzed from a lifetime standpoint; an overall system optimization that employs bursty transmission in order to also establish a secure communication is beyond the scope of this paper. The lifetime and secrecy performance of the investigated schemes is analyzed theoretically, and simulation results validate the enhancements of the proposed schemes. This work is an extension of our previous work [26] where an adaptive PA and a routing scheme for a relaying configuration have been investigated in order to reduce energy consumption. However, in that work, MUD techniques, secrecy issues, and processing energy cost have not been discussed. To the best of our knowledge the combination of MUD with PA under a defined QoS constraint and towards a jointly optimization of network's lifetime and confidentiality is proposed in this paper for the first time.

The contribution of the paper is three-fold.

(1) The combination of a constant PA scheme with the MUD under a predefined QoS constraint. The extraction of the MUD gain improves both *network lifetime* and *confidentiality* (joint optimization).

(2) The investigation of an adaptive PA scheme that adjusts the transmitted power to the instantaneous quality of the channel. MUD gain and adaptive PA further improve the *network lifetime* and the *confidentiality* of the network (joint optimization).

(3) The development of a bursty transmission mechanism that takes into account the processing and the maintenance cost at the transmitters. Bursty transmission is combined with the proposed PA techniques in order to minimize the total energy cost. It is introduced as an efficient technique to increase the *lifetime of a network* with a high "offline" energy cost and is analyzed from an energy point of view (energy optimization).

The remainder of the paper is organized as follows. Section 2 introduces the system model and presents the basic assumptions required for the analysis. Section 3 focuses on the transmission process and analyzes two main PA schemes in terms of lifetime and secrecy. In Section 4, we focus on scenarios with high processing and maintenance cost and we introduce bursty transmission for further energy savings. Numerical results are presented and discussed in Section 5, followed by concluding remarks in Section 6.

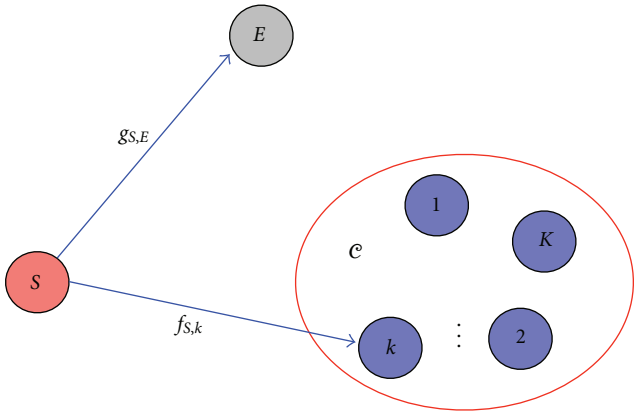

Figure 1: The system model.

2. System Model

In this section, we introduce the network topology and we present the main assumptions that are used for our analysis.

2.1. Network Topology. We assume a simple configuration consisting of one source S (i.e., a base station), a cluster $\mathcal{C} = \{1, \ldots, K\}$ of K destinations, and one eavesdropper node E. The time is considered slotted with each slot having a unit duration, and, at each time slot, the source transmits a message to a single destination $k^* \in \mathcal{C}$ based on a time-division multiaccess (TDMA) scheme. The source has an infinite number of messages for each destination, and each message is transmitted with a rate R bits per channel use (BPCU) and considered to be confidential (should be decoded only by the corresponding destination). Although the cluster's nodes are trusted, the E node, which is within the transmission coverage of the source node, tries to overhear (decode) the source message and thus threatens the confidentiality of the cluster. Figure 1 schematically presents the system configuration.

2.2. Channel Model. All wireless links exhibit fading and additive white Gaussian noise (AWGN). The fading is assumed to be stationary, with frequency nonselective Rayleigh block fading. This means that the fading coefficients $f_{S,k}$ (for the $S \rightarrow k$ link where $k \in \mathcal{C}$) and $g_{S,E}$ (for the $S \rightarrow E$ link) remain constant during one slot but change independently from one slot to another according to a circularly symmetric complex Gaussian distribution with zero mean and variance σ_f^2 and σ_g^2, respectively. Furthermore, the variance of the AWGN is assumed normalized with zero mean and unit variance, and the channel power of the selected link is defined as $f^* \triangleq |f_{S,k^*}|^2$. It is worth noting that the K destinations are clustered relatively close together (location-based clustering) and have the same average statistics but fade independently in each time slot; an appropriate clustering algorithm that organizes the nodes based on average SNR can support this assumption in practice [27, 28]. The instantaneous channel coefficients $f_{S,k}$ are known at the transmitter node and are estimated via a continuous training sequence (a feedback channel) that is transmitted by each node of the cluster. (The base station transmits a pilot signal which the cluster uses to estimate SNRs and then feeds back this information to the base station.) The tracking of the instantaneous channel quality at the source node via a feedback channel has been implemented in several modern wireless systems such as HSDPA and LTE [29].

2.3. Energy Assumptions. An initial energy $\mathcal{E}_0[0]$ is provided to the source in order to perform communication, and $\mathcal{E}_0[n] \geq 0$ denotes the residual energy that remains at the source node after the nth transmission. If $P[n]$ denotes the energy cost associated with the nth transmission, the residual energy is defined as $\mathcal{E}_0[n] = \mathcal{E}_0[n-1] - P[n]$. Due to the normalized slot duration, the measures of *energy* and *power* associated with one slot transmission become identical and therefore are used equivalently throughout the paper. The energy cost associated with the channel feedback (for the tracking of the channel coefficients $f_{S,k}$ at the transmitter) is considered as a default and fixed cost for the network and is therefore neglected in the analysis. It is worth noting that practical systems (e.g., LTE [29], IEEE 802.11 RTS/CTS [30]) use instantaneous signalling in order to perform communication, and therefore providing feedback is not an additional complexity for the system. A similar assumption is considered in [31], where the energy consumption related to the RTS/CTS signalling is considered fixed and neglected in the analysis.

2.4. Network Lifetime—Metric Definition. A main question that is discussed in this paper is how to maximize the lifetime of the clustered network considered given a predefined quality of service (QoS) performance criterion [32, 33]. If we assume that the QoS constraint refers to the maximum tolerable outage probability η, the optimization problem can be written as [9]

$$\mathcal{L}(\mathcal{E}_0[0]) = \max_n \{n : P_{\text{out}} \leq \eta\}, \tag{1}$$

where $\mathcal{L}(\mathcal{E}_0[0])$ denotes the lifetime of the network by using an initial energy budget $\mathcal{E}_0[0]$, $P_{\text{out}}(\cdot)$ is the outage probability of the system, and n denotes the nth transmission. Therefore, the lifetime is the time (in terms of time slots) until the source depletes its available energy, subject to a QoS constraint (in terms of outage probability).

2.5. Secrecy Definition. According to the principles of the PHY secrecy channel [17], the source node transmits a confidential message to the destination node while the eavesdropper node, which is within the transmission coverage of the source node, tries to overhear (decode) the source message. If we use as a secrecy performance criterion the secrecy outage probability, defined as the probability that the instantaneous secure rate is lower than a target secrecy rate

R_S (where $R_S \leq R$), the secrecy performance of the system is given as [17, 18]

$$P_{\text{s-out}} = \mathbb{P}\left\{\log(1+p_t f^*) - \log\left(1+p_t\left|g_{S,E}\right|^2\right) < R_S\right\}, \tag{2}$$

where $\log(\cdot)$ denotes the base-2 logarithm and p_t is the transmitted power. In contrast to the existing literature where the minimization of the secrecy outage probability assumes knowledge of the instantaneous eavesdropper link ($|g_{S,E}|^2$), here, we are interested in PHY layer techniques that are independent of the eavesdropper link and therefore are suitable for practical applications. The secrecy outage probability is an appropriate design metric when a fixed (Wyner) code chosen in advance is used for all channel conditions. However, the practical suitability of this metric is beyond the scope of this paper and can be found in [34] (code construction based on secrecy outage probability).

3. MUD and PA towards Lifetime Maximization and Security

The MUD concept is related to an opportunistic scheduler (OS) that, at each time, selects as a destination the node with the strongest channel to the source. According to [24] and [25, Chapter 6] when channel side information (CSI) is available at the transmitter, the above scheduling policy uses more efficiently the common channel resources and maximizes the total and the individual throughput. The opportunistic scheduling decision can be written as

$$k^* = \arg\max_{k\in\mathcal{C}}\left\{\left|f_{S,k}\right|^2\right\}, \tag{3}$$

where k^* denotes the selected destination. Due to the cluster configuration considered, where nodes fade independently but with the same statistics, each node is selected with the same probability, (due to the symmetric channel model considered, each node is selected with a probability $1/K$ [30]) and therefore fairness as well as latency issues are not discussed further in this paper. In the following subsections, we investigate two combinations of the MUD concept with PA and we discuss the associated lifetime and secrecy performance.

3.1. A Constant PA Policy. The first approach incorporates the above MUD concept with a constant PA policy and is used as a *conventional* protocol; it is the scheme against which all the proposed schemes are compared. The source transmits its message to the selected destination, which has the strongest link with the source, by using a constant transmitted power for each transmission. This constant PA policy is related to the required QoS and corresponds to the minimum power level that must be transmitted by the source in order to support the target outage probability. More specifically, the transmitted power that supports a target outage probability η is calculated by solving the outage probability expression with respect to the transmitted power as follows:

$$\begin{aligned}
&\mathbb{P}\{\log(1+P_0 f^*) < R\} = \eta \\
&\Longrightarrow \mathbb{P}\left\{f^* < \frac{2^R-1}{P_0}\right\} = \eta \\
&\Longrightarrow Y\left(\frac{2^R-1}{P_0}\right) = \eta \\
&\Longrightarrow \left[1-\exp\left(-\lambda_f\frac{2^R-1}{P_0}\right)\right]^K = \eta \\
&\Longrightarrow P_0 = \frac{\lambda_f(1-2^R)}{\ln\left(1-\sqrt[K]{\eta}\right)},
\end{aligned} \tag{4}$$

where $Y(y) \triangleq [1-\exp(-\lambda_f y)]^K$ denotes the CDF of the random variable f^* (by applying order statistics), $\lambda_f \triangleq 1/\sigma_f^2$, and P_0 is the transmitted power.

3.1.1. Lifetime Performance. In each transmission slot, the source selects the node with the best link as a destination and transmits its message with a constant power P_0. This means that after each transmission, the residual energy is decreased by P_0 and therefore the source is active until its residual power becomes less than P_0. Based on this discussion, the lifetime of the network is defined as

$$L_0 = \left\lfloor \frac{\mathcal{E}[0]}{P_0} \right\rfloor, \tag{5}$$

where $\lfloor x \rfloor$ denotes the nearest integer to x towards zero.

3.1.2. Secrecy Performance. Due to the broadcast nature of the transmission, the source message is also received by the eavesdropper node E via the direct link $S \rightarrow E$. The secrecy performance of MUD with a constant PA is expressed as

$$\begin{aligned}
P_{\text{s-out0}} &= \mathbb{P}\{\log(1+P_0 f^*) - \log(1+P_0 g) < R_S\} \\
&= \mathbb{P}\left\{\log\left(\frac{1+P_0 f^*}{1+P_0 g}\right) < R_S\right\} \\
&\approx \mathbb{P}\left\{\log\left(\frac{f^*}{g}\right) < R_S\right\} \\
&= \mathbb{P}\left\{\frac{f^*}{g} < 2^{R_S}\right\} \\
&= V\left(2^{R_S}\right) = \sum_{m=0}^{K}\binom{K}{m}(-1)^m\frac{\lambda_g}{2^{R_S}\lambda_f m+\lambda_g},
\end{aligned} \tag{6}$$

where $V(\cdot)$ denotes the CDF of the random variable f^*/g which is given in Appendix A. As can be seen from (6), the secrecy outage probability of the system does not depend on the transmitted power P_0 and therefore is not a function of the parameter η (different QoS constraints correspond to the same secrecy performance). On the other hand, we can see that the OS affects the secrecy performance of the

system by decreasing the secrecy outage probability as the cardinality K of the cluster increases. Therefore diversity gain is introduced as an efficient mechanism to protect the source message without any explicit knowledge of the $S \to E$ link.

3.2. An Instantaneous Channel-Based PA. The second approach incorporates the MUD with an instantaneous channel-based PA in order to prolong the network lifetime and improve the secrecy performance of the system. This protocol uses channel feedback efficiently, which is available in the system for the implementation of the MUD, and adapts the PA policy to the instantaneous channel conditions without an extra overhead. More specifically, based on the instantaneous quality of the selected link, the source measures the minimum required transmitted power/energy in order to deliver its data correctly to the selected destination. The required transmitted power can be calculated by the expression of the instantaneous capacity as follows:

$$\log(1 + P_T f^*) = R \Longrightarrow P_T = \frac{2^R - 1}{f^*}, \tag{7}$$

where P_T denotes the required instantaneous transmitted power for successful decoding. The combination of the instantaneous transmitted power P_T with the required constant transmitted power P_0 in (4), which supports the outage probability constraint η, enables an adaptive PA policy to be used. This adaptive PA is described by two cases: (a) the source transmits with a power P_T if $P_T \leq P_0$, and (b) the source postpones the transmission if $P_T > P_0$. The basic motivation of this scheme is to avoid scenarios with wasted power consumption (i.e., the destination cannot decode the source message or the source transmits with a power higher than required) and thus to save energy without affecting the outage or the latency performance of the constant PA protocol. (The instantaneous channel-based PA postpones the source transmission when the channel is in outage therefore the data packet delay (measured in terms of time slots) is similar to the baseline constant PA scheme; an unused time slot in the adaptive PA scheme does not convey any information to the destination in the constant PA scheme and thus the delay performance is not affecting.) The adaptive PA policy is formulated as

$$P_1 = \begin{cases} P_T & \text{if } P_T \leq P_0, \\ 0 & \text{elsewhere,} \end{cases} \tag{8}$$

where P_1 denotes the transmitted power.

3.2.1. Lifetime Performance. According to (8), the transmitted power/energy is a random variable with an average value that can be calculated as

$$\begin{aligned} \mathbb{E}[P_1] &= \int_0^{P_0} t y\left(2^R - 1, t\right) dt \\ &= K\lambda_f \left(2^R - 1\right) \\ &\quad \times \sum_{m=0}^{K-1} \binom{K-1}{m} (-1)^m E_i\left(\frac{\lambda_f (2^R - 1)(m+1)}{P_0}\right), \end{aligned} \tag{9}$$

where $E_i(x) \triangleq \int_x^\infty \exp(-t)/t\, dt$ denotes the exponential integral and $y(\cdot)$ is the probability density function (PDF) of the random variable P_T, whose derivation is given in Appendix B. Therefore the lifetime of the network becomes equal to

$$L_1 = \left\lfloor \frac{\mathcal{E}[0]}{\mathbb{E}[P_1]} \right\rfloor. \tag{10}$$

3.2.2. Secrecy Performance. The secrecy outage probability of the system can be written as

$$\begin{aligned} P_{\text{s-out1}} &= \mathbb{P}\{\log(1 + P_1 f^*) - \log(1 + P_1 g) < R_S\} \\ &\quad \left(\text{where } P_1 < P_0 \Longrightarrow f^* > \underbrace{\frac{1}{\lambda_f} \log\left(\frac{1}{1 - \sqrt[K]{\eta}}\right)}_{\triangleq f_0} \right) \\ &= \mathbb{P}\left\{ R - \log\left(1 + \left(2^R - 1\right)\frac{g}{f^*}\right) < R_S \right\} \\ &= \mathbb{P}\left\{ \frac{f^*}{g} < \frac{2^{R-R_S} - 1}{2^R - 1} \right\} \\ &= U\left(\frac{1}{\lambda_f} \log\left(\frac{1}{1 - \sqrt[K]{\eta}}\right), \frac{2^R - 1}{2^{R-R_S} - 1}\right), \end{aligned} \tag{11}$$

where $U(\cdot)$ denotes the cumulative density function (CDF) of the random variable f^*/g with $f^* > f_0$ and its analytical expression is given in Appendix A. The above expression shows that in contrast to the constant PA scheme, here, the secrecy outage probability also depends on the parameter P_0 and therefore on the target outage probability η. Furthermore, a direct comparison of (6) and (11) reveals that $P_{\text{s-out1}} < P_{\text{s-out0}}$ for moderate values (η is much greater than zero.) of η and the secrecy gain of the instantaneous scheme becomes larger as the cardinality of the cluster K increases (the function $\Psi(f_0)$ in (A.1) of Appendix A is an increasing function with respect to the parameters η and K). This observation demonstrates that the combination of the MUD concept with an instantaneous PA policy jointly improves the lifetime and the secrecy performance (for moderate values of η) of the network. Furthermore, the improvement in the secrecy performance is achieved without any interaction with the eavesdropper link (i.e., estimation of the instantaneous $S \to E$ link), and therefore the instantaneous PA policy is introduced as an efficient practical PHY layer technique for systems with secrecy limitations (in practical systems the location of the eavesdropper node is unknown).

For extremely small values of η ($\eta \to 0$), the threshold f_0 tends to zero ($f_0 \to 0$) and, according to Appendix A, $U(0, x) = V(x)$. For this special case, we have that

$$\begin{aligned} P_{\text{s-out1}} &\approx V\left(\frac{2^R - 1}{2^{R-R_S} - 1}\right) \geq V\left(2^{R_S}\right) = P_{\text{s-out0}} \\ &\text{as } R_S \geq 0 \Longleftrightarrow \frac{2^R - 1}{2^{-R_S} \cdot 2^R - 1} \geq 2^{R_S}, \end{aligned} \tag{12}$$

and therefore the constant PA scheme outperforms the instantaneous PA scheme in terms of secrecy outage probability for small values of η. However, it is worth noting that for small secrecy target rates R_S (i.e., $R_S \to 0$), both schemes achieve the same secrecy performance.

4. Burst Transmission and PA towards Decreasing the Processing Cost

In practical systems the energy consumption at the transmitter consists of the energy associated with the transmission process and the energy associated with the data processing and the system maintenance. The maintenance energy represents the "offline" energy cost that is required in order to maintain the transmitter's infrastructure (i.e., cooling operations, control signalling, and network connectivity), and the processing energy cost corresponds to the required energy in order to form the source message (i.e., transmission operations like modulation, coding, etc.). In the previous section, the analysis has focused on the transmission process by assuming that the processing and the maintenance cost is negligible. In this section, we relax this assumption and we study energy efficient transmission techniques that take into account both types of energy consumption at the transmitter. We note that the bursty transmission is introduced here as an efficient technique in order to increase the lifetime of the network when the transmitter is characterized by high "offline" energy costs; the impact of the bursty transmission on the secrecy performance of the system is beyond the scope of this paper and can be considered for future work.

The Burst Transmission and Capacity Model. The total energy that is consumed at the transmitter depends on the fraction of time that the transmitter is "on." This observation motivates the investigation of sleeping (bursty) transmission techniques that switch off the transmitter for a fraction of time in order to reduce energy expenditure. If $p_t(\theta)$ denotes the total energy (including the transmission, processing, and maintenance cost) that is consumed at the transmitter and Γ is the processing and maintenance cost, the instantaneous channel capacity expression that integrates the switch-off operation is written as [15, 16]

$$C = \theta \log\left(1 + \left[\frac{p_t(\theta)}{\theta} - \Gamma\right] f\right), \tag{13}$$

where $\theta \in [0\ \ 1]$ is the fraction of time that the transmitter is active and f denotes the channel coefficient. In the following, we introduce some transmission techniques that minimize the total energy cost without affecting the outage performance of the system. For the sake of the simplicity and in order to focus on the impact of the bursty transmission on the lifetime of the network, the analysis here focuses on a single destination scheme ($K = 1$), but it can easily be extended to MUD applications (with $K > 1$); the combination of bursty transmission with MUD increases further the lifetime of the network. Furthermore, it is worth noting that although the energy model considered assumes a constant data processing and maintenance cost (for the time that the transmitter is "on") [15, 16], it is a guideline for more complicated cases and allows some interesting remarks about the impact of this type of energy cost on the lifetime of the network. A more sophisticated data processing energy model will be investigated in our future work.

4.1. A Constant PA Policy. The first approach uses a constant PA policy at the transmitter and corresponds to a fixed total energy cost. More specifically, for the single destination configuration considered, we assume that an average knowledge of the source-destination link is available. In this case, the total energy cost that supports the target outage probability is given by solving the outage probability expression with respect to $P_0(\theta)$ as follows:

$$\begin{aligned}
&\mathbb{P}\left\{\theta \log\left(1 + \left[\frac{P_0(\theta)}{\theta} - \Gamma\right] f\right) < R\right\} = \eta \\
&\quad\Longrightarrow \mathbb{P}\left\{f < \frac{2^{R/\theta} - 1}{P_0(\theta)/\theta - \Gamma}\right\} = \eta \\
&\quad\Longrightarrow 1 - \exp\left(-\lambda_f \frac{\theta\left(2^{R/\theta - 1}\right)}{P_0(\theta)/\theta - \Gamma}\right) \qquad (14) \\
&\quad\Longrightarrow \lambda_f \frac{\theta\left(2^{R/\theta - 1}\right)}{P_0(\theta)/\theta - \Gamma} = \eta \quad (\text{with } 1 - \exp(-x) \approx x) \\
&\quad\Longrightarrow \lambda_f \frac{\theta\left(2^{R/\theta - 1}\right)}{P_0(\theta)/\theta - \Gamma} = \eta \\
&\quad\Longrightarrow P_0(\theta) = \frac{\lambda_f \theta\left(2^{R/\theta} - 1\right)}{\eta} + \theta\Gamma, \qquad (15)
\end{aligned}$$

where the approximation in (14) is tight when the SNR is high for the desired rate R and is used in order to simplify our derivations. As the total energy cost is a function of the parameter θ, an appropriate switch-off mechanism can result in significant energy savings. This switch-off mechanism corresponds to the solution of the following optimization problem:

$$\begin{aligned}
&\theta^* = \arg \min_{\theta \in [0\ \ 1]} \{P_0(\theta)\} \\
&\quad\Longrightarrow \frac{\partial P_0(\theta)}{\partial \theta} = 0 \\
&\quad\Longrightarrow \theta^* = \begin{cases} \dfrac{R\ln(2)}{W\left((\eta\Gamma - 1)/\exp(1)\right) + 1} \triangleq \Lambda & \text{if } \Lambda \in [0\ 1), \\ 1 & \text{elsewhere,} \end{cases} \qquad (16)
\end{aligned}$$

where $W(\cdot)$ denotes the Lambert W function defined as $z = W(z)\exp(W(z))$. For small values of η (as $\eta \to 0$), the optimal parameter θ^* becomes equal to one, and according to (15) the transmission energy cost (the first term in (15)) dominates the total energy cost $P_0(\theta) \approx (2^R - 1)/\eta \gg \Gamma$. For very low η, the required transmitted power/energy is significantly increased and becomes the main cause of energy consumption at the transmitter.

The lifetime of the network becomes equal to

$$L_0' = \left\lfloor \frac{\mathcal{E}[0]}{P_0(\theta^*)} \right\rfloor. \tag{17}$$

4.2. An Instantaneous Channel-Based PA Policy. In an equivalent way with the scheme proposed in Section 2.2, the second approach employs an instantaneous channel-based PA policy. Based on a continuous and instantaneous channel feedback (similar to this one that is used for the employment of the MUD concept), the transmitter measures the quality of the source-destination link and calculates the minimum required power in order to establish a successful communication with the destination. The combination of this calculated power amount with the constant PA policy proposed in the previous section enables the employment of an adaptive PA strategy that results in power savings. More specifically, for an instantaneous SNR equal to f, the required total energy cost equals to

$$P_T(\theta) = \frac{\theta\left(2^{R/\theta} - 1\right)}{f} + \theta\Gamma. \tag{18}$$

As the instantaneous total energy cost is a function of the parameter θ, an appropriate sleep mechanism enables a further energy reduction. The appropriate transmission fraction of the time is given as

$$\begin{aligned} \theta^{**} &= \arg \min_{\theta \in [0\ \ 1]} \{P_T(\theta)\} \\ &\Longrightarrow \theta^{**} \\ &= \begin{cases} \dfrac{R\ln(2)}{W((f\Gamma - 1)/\exp(1)) + 1} \triangleq \Lambda' & \text{if } \Lambda' \in [0\ 1), \\ 1 & \text{elsewhere.} \end{cases} \end{aligned} \tag{19}$$

The adaptive PA policy is formulated as

$$P_1' = \begin{cases} P_T(\theta^{**}) & \text{if } P_T(\theta^{**}) \le P_0(\theta^*), \\ 0 & \text{elsewhere,} \end{cases} \tag{20}$$

where the random variable P_1' denotes the transmitted power.

The lifetime of the network that is yielded from the application of the above instantaneous PA policy is given by

$$L_1' = \left\lfloor \frac{\mathcal{E}[0]}{\mathbb{E}[P_1']} \right\rfloor. \tag{21}$$

Due to the complexity of the PDF of the random variable $P_T(\theta^{**})$, the mean value of the random variable P_1 as well as the associated lifetime of the network is evaluated via numerical results in Section 5. However, in order to propose a theoretical estimate of the lifetime, in the following discussion, we investigate a useful lower bound.

A Lower Bound. The proposed lower bound assumes a constant transmission fraction of the time that is given as $\theta^{**} = \Theta \triangleq \mathbb{E}[\theta^{**}] = \mathbb{P}\{\Lambda' < 1\}\mathbb{E}[\Lambda'] + \mathbb{P}\{\Lambda' > 1\} \cdot 1$, where $\mathbb{E}[\cdot]$ denotes the expectation operation (i.e., for $R = 2$ BPCU and $\Gamma = 1000$ energy units, we have $\mathbb{P}\{\Lambda' < 1\} = 1$ and $\Theta = \int_0^\infty \Lambda' \lambda_f \exp(-\lambda_f f) df \approx 0.295$, where the integral is calculated numerically). In this case, the mean value of the random variable P_1' becomes equal to

$$\begin{aligned} \mathbb{E}[P_1''] &= \int_0^{P_0(\theta^*)} ty\left(\Theta\left[2^{R/\Theta} - 1\right], t\right) dt + \Theta\Gamma \\ &= K\lambda_f \Theta\left(2^{R/\Theta} - 1\right) \\ &\quad \times \sum_{m=0}^{K-1} \binom{K-1}{m} (-1)^m E_i\left(\frac{\lambda_f \Theta(2^{R/\Theta} - 1)(m+1)}{P_0'}\right) + \Theta\Gamma, \end{aligned} \tag{22}$$

where the above expression uses the proof in Appendix B. Therefore the lifetime of the network is approximated as

$$L_1'' = \frac{\mathcal{E}[0]}{\mathbb{E}[P_1'']}. \tag{23}$$

5. Numerical Results

Computer simulations have been carried out in order to validate the performance of the proposed schemes. The simulation environment follows the description in Section 2 with $\mathcal{E}[0] = 10^6$ energy units, $R = 2$ BPCU, $\lambda_f = 1$, and $\lambda_g = 10$ (the source-cluster link is much better than the source-eavesdropper link).

In Table 1, we focus on the transmission energy cost ($\Gamma = 0$) and we compare the constant and the instantaneous PA schemes in terms of lifetime for different values of K and target outage probabilities η. In the same table, we present the theoretical results (analytical values of the lifetime) that are provided by the proposed analytical methods; the analytical results are given in parentheses. The first important observation is that the target outage probability η has a significant impact on the network lifetime. As the outage probability η decreases, the required transmitted power is increased by significantly reducing the network's lifetime. On the other hand, the instantaneous PA policy outperforms the constant PA scheme and significantly extends the network's lifetime (i.e., for $K = 1$ and $\eta = 10^{-4}$, we have a gain factor $\mathcal{G}_{10^{-4}} \triangleq L_1/L_0 = 10187$). In addition, the performance gain is increased as the target outage probability η decreases (i.e., for $K = 1$, we have $\mathcal{G}_{10^{-1}} \triangleq L_1/L_0 = 4.8 \ll \mathcal{G}_{10^{-4}}$). The most important observation concerns the impact of the MUD concept on the network's lifetime. As the cardinality K of the cluster increases, the lifetime of the network is maximized; that is, for $\eta = 10^{-4}$, the gain for a constant PA policy for $K = 5$ in comparison to $K = 1$ is equal to $\mathcal{Q}_{10^{-4}} \triangleq L_0(K = 5)/L_0(K = 1) = 11707$. An increase of the cluster's cardinality improves the quality of the selected link and corresponds to a reduction on the required transmitted power. Furthermore, it can be seen that the combination of the MUD concept with the instantaneous PA policy is the

Table 1: The lifetime (in time slots) for the constant and the instantaneous PA MUD schemes; $R = 2$ BPCU, $\mathcal{E}_0[0] = 10^6$ energy units, and $\Gamma = 0$ energy units: simulation results (theoretical results).

η	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}
L_0 (constant PA with $K = 1$)	35120 (35120)	3350 (3350)	334 (333.5)	33 (33)	3 (3.3)
L_1 (inst. PA with $K = 1$)	169030 (187710)	81830 (82652)	52560 (52651)	38350 (38611)	30560 (30481)
L_0 (constant PA with $K = 3$)	207970 (207970)	80880 (80879)	35120 (35120)	15840 (15843)	7260 (7259.9)
L_1 (inst. PA with $K = 3$)	505510 (561630)	413250 (417410)	392400 (392830)	387590 (386540)	386480 (386540)
L_0 (constant PA with $K = 5$)	332280 (332280)	169230 (169230)	96420 (96423)	57520 (57519)	35120 (35120)
L_1 (inst. PA with $K = 5$)	679590 (755100)	592320 (598220)	575370 (575890)	572210 (572210)	571650 (571610)

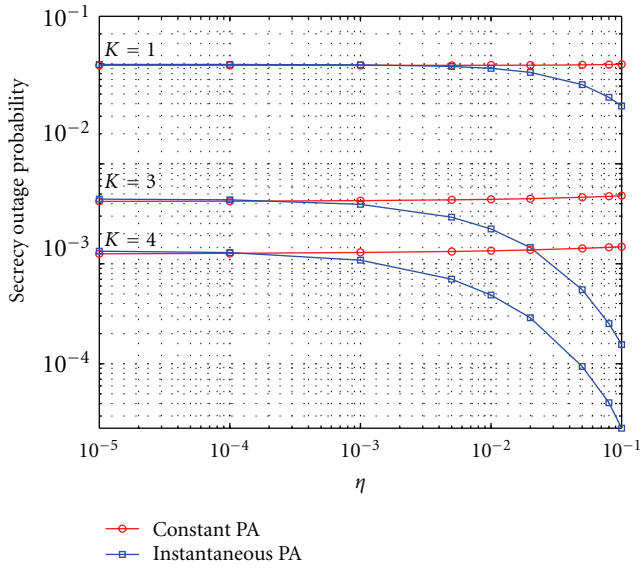

Figure 2: The secrecy outage probability versus the target outage probability η for a constant and an instantaneous PA policy; $R = 2$ BPCU, $R_S = 0.1$ BPCU, $K = 1, 3, 4$, $\sigma_f^2 = 1$, and $\sigma_g^2 = 0.1$; lines: simulation (Monte-Carlo) results, points: theoretical results.

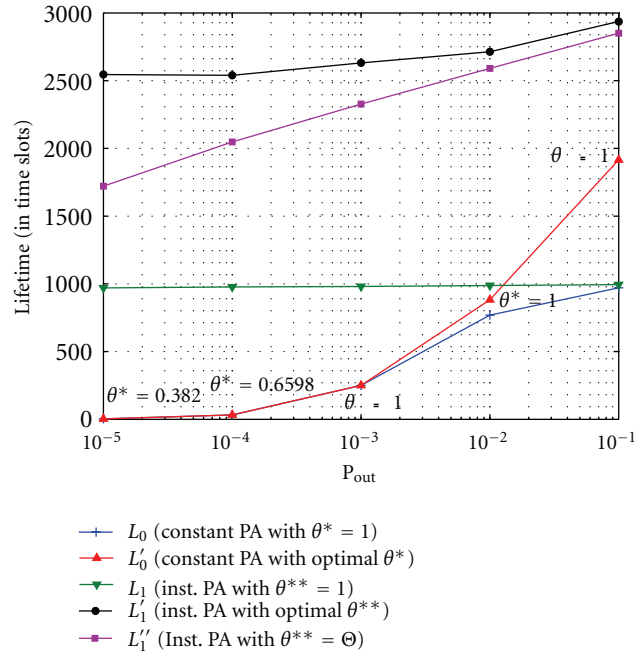

Figure 3: The lifetime (in time slots) for the constant and the instantaneous PA switch-off schemes versus the outage probability; $R = 2$ BPCU, $\mathcal{E}_0[0] = 10^6$ energy units, and $\Gamma = 1000$ energy units (θ^* is given for the constant PA with optimal θ^*).

optimal scheme and offers the maximal network lifetime. This combination uses more efficiently the MUD channel feedback and enjoys the benefits of both the adaptive PA and the MUD. As far as the theoretical results are concerned, it can be seen that the theoretical values that are provided by the proposed analysis efficiently approximate the true (simulated) values.

Figure 2 plots the secrecy outage probability achieved by the constant and instantaneous PA schemes versus the target outage probability η for $K = 1, 3, 4$, and a target secrecy rate equals $R_S = 0.1$ BPCU. The first observation is that the secrecy performance of the constant PA scheme is independent of the target outage probability η and therefore converges to a constant value. This result is in line with the analysis in (6) and reveals the constant PA scheme is not able to protect the confidentiality of the network. However, as the cardinality of the cluster increases, the secrecy performance is improved (converges to a lower floor). This result shows that the exploitation of MUD improves the capacity of the source-destination link and provides a mechanism for protection for the source message. On the other hand, the instantaneous PA scheme achieves a lower secrecy outage probability than the constant PA scheme for high η. This observation is justified by the analysis in (11) and shows that an instantaneous PA strategy not only extends the network lifetime but also achieves a higher confidentiality. However, as the target outage probability decreases, its secrecy gain decreases and converges to the secrecy performance of the constant PA scheme as η tends to zero (see (20)). In addition, it can be seen that the MUD significantly improves the secrecy gain of the instantaneous PA scheme (the gain becomes higher as K increases). The MUD provides a mechanism of message protection, which in combination with the instantaneous PA policy further boosts the secrecy of the network.

Figure 3 deals with the efficiency of the proposed switch-off scheme in scenarios with a critical processing and maintenance cost. More specifically, Figure 3 compares (based on

simulation results) the constant and the instantaneous PA schemes in terms of lifetime for a processing cost $\Gamma = 1000$ energy units (a value that corresponds to a high energy processing cost) and different values of the target outage probability. The scenarios $\theta^* \equiv 1$ and $\theta^{**} \equiv 1$ are used as a reference for comparison. For the constant PA scheme, it can be seen that the parameter θ^* has an important impact on the network's lifetime. For high values of η, the optimal transmission fraction θ^* becomes less than one and results in significant energy savings. For example, for $\eta = 0.1$, the lifetime gain is equal to $\mathcal{G}_{10^{-1}} \triangleq L_1/L_0 \approx 2$ which corresponds to doubling the lifetime. A comparison of these results with the scenario of a negligible processing cost presented in Table 1 shows that the consideration of the processing cost significantly reduces the network lifetime (for $\eta = 10^{-2}$, the lifetime achieved by the constant PA scheme reduced from $L_0 = 3350$ timeslots to $L_0' = 882.5$ timeslots). On the other hand, as $\eta \to 0$, the optimal θ^* becomes equal to one and the processing cost dominates the total energy cost; in this case, the results presented in Table 1 and Figure 3 become equivalent (for $\eta = 10^{-4}$, we have $L_0 \approx L_0' = 3$).

On the other hand, in accordance with the scenario of a negligible processing cost, the instantaneous PA scheme significantly extends the network lifetime. The lifetime gain becomes higher as the target outage probability decreases (i.e., $\mathcal{G}'_{10^{-1}} \triangleq L_1'/L_0' \approx 3$ against $\mathcal{G}'_{10^{-4}} \triangleq L_1'/L_0' \approx 766$). In addition, the parameter θ^{**} has a significant impact on the lifetime performance. As can be seen, the optimal parameter θ^{**} extends the network lifetime in comparison with the case where $\theta^{**} \equiv 1$, while the energy cost seems to be constant for $\theta^{**} \equiv 1$. The main reason for this observation is that, for $\theta^{**} \equiv 1$, the processing cost is the main energy cost at the transmitter (the second term dominates the expression in (18)) and therefore the lifetime is almost independent of the target outage probability η. As far as the proposed estimation is concerned ($\Theta = \mathbb{E}[\theta^{**}]$), we can see that it efficiently approximates the true lifetime of the network (corresponding to the optimal θ^{**}) and provides a useful theoretical lower bound. It is worth noting that the quality of the estimation is improved as the target outage probability η increases.

6. Conclusion

This paper considered the transmission process in clustered wireless networks with energy and secrecy constraints. Two main techniques that incorporate the MUD gain with a PA have been investigated. The first approach employs a constant PA that is a function of the required QoS and uses the MUD gain as an efficient mechanism to protect the source message and prolong the network's lifetime. The second approach adapts the transmitted power on the instantaneous channel quality and switches off the transmission in outage conditions without affecting the QoS. The combination of this adaptive PA scheme with the MUD gain significantly extends the network lifetime and improves the confidentiality. In addition, scenarios with a high processing and maintenance energy cost have been investigated. We have shown that the application of an appropriate burst transmission to the proposed PA techniques significantly reduces the total energy cost at the transmitter. The enhancements of the proposed schemes have been validated by extended numerical and theoretical results.

Appendices

A. The CDF of the Random Variable f^*/g with $f^* > f_0$

Let f^* be a random variable which is equal to the maximum of K independent and identically distributed (i.i.d.) exponential random variables with parameter λ_f, and let the constraint $f^* > f_0$, where $f_0 > 0$ is a constant. If g is an exponential random variable with parameter λ_g, the CDF of the random variable $Z \triangleq f^*/g$ is given as

$$\begin{aligned}
U(f_0,x) &\triangleq \mathbb{P}\left\{\frac{f^*}{g} < x\right\} \\
&= \mathbb{P}\{f^* < xg\} \\
&= \int_{f_0/x}^{\infty} [Y(xt) - Y(f_0)]\, y_0(t)\, dt \\
&= \int_{f_0/x}^{\infty} \left[1 - \exp\left(-\lambda_f xt\right)\right]^K \lambda_g \exp\left(-\lambda_g t\right) dt \\
&\quad - \left[1 - \exp\left(-\lambda_f f_0\right)\right]^K \int_{f_0/x}^{\infty} \lambda_g \exp\left(-\lambda_g t\right) dt \\
&= \lambda_g \sum_{m=0}^{K} \binom{K}{m} (-1)^m \int_{f_0/x}^{\infty} \exp\left(-t\left[\lambda_f mx + \lambda_g\right]\right) dt \\
&\quad - \left[1 - \exp\left(-\lambda_f f_0\right)\right] \\
&= \underbrace{\sum_{m=0}^{K} \binom{K}{m} (-1)^m \frac{\lambda_g}{\lambda_f mx + \lambda_g}}_{\triangleq V(x)} \cdot \exp\left(-f_0\lambda_f m - \frac{\lambda_g f_0}{x}\right) \\
&\quad - \underbrace{\left[1 - \exp\left(-\lambda_f f_0\right)\right]^K \exp(-\lambda_g f_0)}_{\triangleq \Psi(f_0)}, \qquad \text{(A.1)} \\
&= V(x) \cdot \exp\left(-f_0\lambda_f m - \frac{\lambda_g f_0}{x}\right) - \Psi(f_0), \qquad \text{(A.2)}
\end{aligned}$$

where $Y(\cdot)$ denotes the CDF of the random variable f^* and $y_0(x) = \lambda_g \exp(-\lambda_g x)$ denotes the PDF of the random variable g, and, for the above expression, we have used the binomial theorem $(x+y)^n = \sum_{m=0}^{n} \binom{n}{m} x^{n-m} y^m$. From the above equation we can see that for $f_0 = 0$ we have $U(0,x) = V(x)$.

B. The PDF of the Random Variable A/f^*

Let f^* be a random variable that is equal to the maximum among K i.i.d. exponential random variables with a parameter λ_f. If A is a deterministic variable, the CDF of a random variable $Z \triangleq A/f^*$ is given as

$$\begin{aligned} Y_Z(A,x) &= \mathbb{P}\left\{\frac{A}{f^*} < x\right\} \\ &= 1 - \mathbb{P}\left\{f^* < \frac{A}{x}\right\} \\ &= 1 - \left[1 - \exp\left(-\lambda_f \frac{A}{x}\right)\right]^K, \end{aligned} \tag{B.1}$$

with a PDF equal to

$$\begin{aligned} y_Z(A,x) &= \frac{\partial Y_Z(x)}{\partial x} \\ &= K\lambda_f A \frac{1}{X^2}\left[1 - \exp\left(-\frac{\lambda_f A}{X}\right)\right]^{K-1} \exp\left(-\frac{\lambda_f A}{X}\right) \\ &= K\lambda_f A \sum_{m=0}^{K-1} \binom{K-1}{m} (-1)^m \exp\left(-\frac{\lambda_f A}{X}[m+1]\right). \end{aligned} \tag{B.2}$$

References

[1] S. Armour, T. O. Farrell, S. Fletcher et al., "Green Radio: Sustainable Wireless Networks," White Paper published on IET website, June 2009, http://kn.theiet.org/communications/Green_radio_file.cfm.

[2] T. Edler and S. Lundberg, "Energy efficiency enhancements in radio access networks," *Ericsson Review*, vol. 81, no. 1, pp. 42–2, 2004.

[3] A. Radwan and H. S. Hassanein, "Does multi-hop communication extend the battery life of mobile terminals?" in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '06)*, San Francisco, Calif, USA, December 2006.

[4] J. H. Chang and L. Tassiulas, "Energy conserving routing in wireless ad-hoc networks," in *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '00)*, pp. 22–31, March 2000.

[5] W. Wang, V. Srinivasan, and K. C. Chua, "Extending the lifetime of wireless sensor networks through mobile relays," *IEEE/ACM Transactions on Networking*, vol. 16, no. 5, pp. 1108–1120, 2008.

[6] S. Cui, A. J. Goldsmith, and A. Bahai, "Energy-efficiency of MIMO and cooperative MIMO techniques in sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 6, pp. 1089–1098, 2004.

[7] T. Himsoon, W. P. Siriwongpairat, Z. Han, and K. J. R. Liu, "Lifetime maximization via cooperative nodes and relay deployment in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 2, pp. 306–317, 2007.

[8] L. Simić, S. M. Berber, and K. W. Sowerby, "Partner choice and power allocation for energy efficient cooperation in wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications*, pp. 4255–4260, Beijing, China, June 2008.

[9] W. J. Huang, Y. W. Peter Hong, and C. C. Jay Kuo, "Lifetime maximization for amplify-and-forward cooperative networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 5, Article ID 4524272, pp. 1800–1805, 2008.

[10] Y. Chen, Q. Zhao, V. Krishnamurthy, and D. Djonin, "Transmission scheduling for optimizing sensor network lifetime: a stochastic shortest path approach," *IEEE Transactions on Signal Processing*, vol. 55, no. 5, pp. 2294–2309, 2007.

[11] Y. W. Hong, W. J. Huang, FU. H. Chiu, and C. C. J. Kuo, "Cooperative communications in resource-constrained wireless networks," *IEEE Signal Processing Magazine*, vol. 24, no. 3, pp. 47–57, 2007.

[12] F. Namin and A. Nosratinia, "Pragmatic lifetime maximization of cooperative sensor networks via a decomposition approach," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '08)*, pp. 3017–3020, Las Vegas, Nev, USA, April 2008.

[13] R. Jäntti and S. L. Kim, "Joint data rate and power allocation for lifetime maximization in interference limited ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 5, no. 5, pp. 1086–1094, 2006.

[14] L. Sankar, G. Kramer, and N. B. Mandayam, "Dedicated-relay vs. user cooperation in time-duplexed multiaccess networks," *IEEE Transactions on Wireless Communications*. In press.

[15] P. Youssef-Massaad, L. Zheng, and M. Medard, "Bursty transmission and glue pouring: on wireless channels with overhead costs," *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 5188–5194, 2008.

[16] V. Prabhakaran and P. R. Kumar, "Communication by sleeping: optimizing a relay channel under wake and transmit power costs," in *Proceedings of the IEEE International Symposium on Information Theory*, pp. 859–863, Seoul, Korea, June 2009.

[17] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[18] I. Csiszar and J. Korner, "BROADCAST CHANNELS WITH CONFIDENTIAL MESSAGES," *IEEE Transactions on Information Theory*, vol. IT-24, no. 3, pp. 339–348, 1978.

[19] Y. Liang, H. V. Poor, and L. Ying, "Wireless broadcast networks: reliability, security, and stability," in *Proceedings of the Information Theory and Applications Workshop (ITA '08)*, pp. 249–255, San Diego, Calif, USA, February 2008.

[20] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '09)*, pp. 2613–2616, Taipei, Taiwan, April 2009.

[21] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '07)*, pp. 2466–2470, Nice, France, June 2007.

[22] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[23] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[24] R. Knopp and P. A. Humblet, "Information capacity and power control in single-cell multiuser communications," in *Proceedings of the IEEE International Conference on Communications*, pp. 331–335, Seattle, Wash, USA, June 1995.

[25] D. Tse, *Fundamentals of Wireless Communication*, Cambridge University Press, New York, NY, USA, 2005.

[26] I. Krikidis, J. S. Thompson, and P. M. Grant, "Cooperative relaying with feedback for lifetime maximization," in *Proceedings of the IEEE International Conference on Communications Workshops (ICC '10)*, pp. 1–6, Cape Town, South Africa, May 2010.

[27] D. B. da Costa and S. Aissa, "Performance analysis of relay selection techniques with clustered fixed-gain relays," *IEEE Signal Processing Letters*, vol. 17, no. 2, pp. 201–204, 2010.

[28] S. Yang and J.-C. Belfiore, "Diversity of MIMO multihop relay channels," *IEEE Transactions on Information Theory*. In press, http://arxiv.org/abs/0708.0386.

[29] H. Holma and A. Toskala, *LTE for UMTS-OFDMA and SC-FDMA Based Radio Access*, John Wiley & Sons, New York, NY, USA, 2009.

[30] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 659–672, 2006.

[31] Z. Zhou, S. Zhou, J. H. Cui, and S. Cui, "Energy-efficient cooperative communication based on power control and selective single-relay in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 8, Article ID 4600219, pp. 3066–3078, 2008.

[32] J.-H. Chang and L. Tassiulas, "Routing for maximum system lifetime in wireless ad-hoc networks," in *Proceedings of the 37th Allerton Conference on Communications, Control, and Computing*, vol. 1, pp. 22–31, September 1999.

[33] Y. Chen and Q. Zhao, "An integrated approach to energy-aware medium access for wireless sensor networks," *IEEE Transactions on Signal Processing*, vol. 55, pp. 3429–3444, 2007.

[34] X. Tang, R. Liu, P. Spasojevíc, and V. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Transactions on Information Theory*, vol. 55, no. 4, pp. 1575–1591, 2009.