SCIENCE DILIMAN (JANUARY-JUNE 2018) 30:1, 5-23

Low-Complexity Physical Layer Security Scheme for Heterogeneous Cellular Networks based on Coordinated Precoding Design and Artificial Noise Generation

Neil Irwin M. Bernardo*
Electrical and Electronics Engineering Institute
University of the Philippines

Franz de Leon
Electrical and Electronics Engineering Institute
University of the Philippines

ABSTRACT

The undertaking for higher capacity and seamless wireless connectivity in next-generation mobile networks while maintaining an energy-efficient transmission requires a fundamental redesign of the existing cellular architecture. Heterogeneous network (HetNet) deployment is a promising architectural framework for meeting these design goals. However, an increase in cellular capacity and device connectivity would also result in an increase of sensitive data and classified information being exchanged over the network, thus making security another critical aspect in cellular network design. In this study, a convex optimization model was formulated that minimizes the total power consumption of the network while satisfying certain level of per-user data rate requirement and information secrecy at the physical layer. From this model, a low-complexity physical layer security scheme was developed that exploits coordinated precoding design, artificial noise generation, and a suboptimal sleep mode strategy in HetNets. Simulation results show that joint optimization of coordinated precoding scheme and artificial noise generation is an effective approach for increasing cellular capacity while simultaneously lowering the transmit power of the base stations and risk of eavesdropping attacks. Incorporating sleep mode mechanism in physical layer security transmission scheme of HetNets also reduced the total power consumption while maintaining a

*Corresponding Author

ISSN 0115-7809 Print / ISSN 2012-0818 Online

secured and reliable communication during low traffic periods. Furthermore, our proposed physical layer security scheme exhibited significant reduction in computational complexity, but at the expense of slight performance degradation in terms of energy efficiency.

Keywords: Physical Layer Security, Heterogeneous Networks, Small Cells, 5G

INTRODUCTION

The rapid growth of the number of mobile devices and data traffic created a demand for cellular technologies that can provide extremely high data throughput and seamless wireless coverage. One approach to meet this demand is through the dense deployment of multiple low-power small cell access nodes (SCAs) in order to complement the performance of high-power base stations (BS), thus forming a heterogeneous network (HetNet) (Nigam et al. 2014). SCAs can be deployed on hot spots with high throughput demand to offload the traffic from the macro-cell BS or on coverage holes to ensure uninterrupted connectivity. This results in large cellular capacity improvement. Several studies have also shown that, with proper coordinated transmission and interference mitigation schemes, heterogeneous network deployment is an energy-efficient alternative to traditional macro-cell-only cellular architecture in meeting the data rate requirement of future wireless applications (Bjornson et al. 2013; Tang et al. 2015; Nguyen et al. 2016; Vu et al. 2016). Due to these advantages, several regulatory bodies, as well as some major players in telecommunication industry, have acknowledged heterogeneous network deployment as an enabler for fifth generation mobile networks or 5G (International Telecommunication Union 2014; Samsung Electronics Co. 2015).

Aside from improvements in energy and spectral efficiency, cellular network security has also become a significant concern in mobile networks. The increase in data traffic and number of connected device had increased the risk of data theft and eavesdropping as more and more confidential data are being exchanged over the network (Yang et al. 2015). Furthermore, the growth of Internet-of-Things (IoT) would also require a sufficient security scheme that is both computationally-efficient and energy-efficient for low-power IoT devices (Trappe 2015). Security solutions for wireless devices are traditionally implemented at the application layer in the form of cryptography. However, the performance of these cryptographic protocols is highly dependent on the assumption of limited computational power of the eavesdropper, thus introducing potential vulnerabilities to network's data confidentiality (Mukherjee et al. 2014).

An alternative approach to encryption strategies is to implement security at the physical layer (PHY) of the network. PHY security can provide a quantifiable and information-theoretic security to the network by exploiting the random characteristics of wireless channel. HetNets are able to provide reliable security at the physical layer using coordinated precoding design (Lv et al. 2015; Bernardo and De Leon 2016), resource allocation strategy (Shiqi et al. 2016), and artificial noise (AN) generation (Deng et al. 2015; Wang et al. 2016) in fending off eavesdropping attacks. However, most studies on PHY security performance of HetNets assume that SCAs are always in active mode. In an energy efficiency perspective, time periods with low user density and low traffic would leave multiple SCAs idle, thus resulting in wasted energy. In practice, SCAs have sleep mode mechanism to adapt with high spatiotemporal variations in user density and mobile data traffic (Hoydis et al. 2011). Furthermore, PHY security approaches presented in the work of Lv et al. (2015) and Bernardo and De Leon (2016) have very high computational complexity, making them infeasible to implement in multi-tier cellular networks with dense layer of SCAs. As such, there is a need to implement computationally-efficient PHY security solutions for HetNets that consider sleep mode capabilities of SCAs.

This study presents a low-complexity PHY security scheme for heterogeneous cellular networks. We formulate an optimization model that solves for the optimal precoding vectors and AN signals which minimize the total power consumption of a heterogeneous network, while satisfying the Quality-of-Service (QoS) requirement of every user, the transmit power limitations of macro-cell BS and SCAs, and a certain degree of secrecy against eavesdropping attacks. Moreover, an algorithm that incorporates the sleep mode capability of SCAs in precoding and an AN design to further reduce the total power consumption is proposed. To the best of our knowledge, no prior study has been done with regards to the development of fast and low-power PHY security techniques for HetNets that consider their sleep mode capability.

SYSTEM MODEL AND ALGORITHM FORMULATION

System Model for Heterogeneous Networks

We consider a single cell downlink scenario of a two-tier heterogeneous cellular network serving K authorized single-antenna user equipment (UE) (Figure 1). The macro-cell BS and SCAs are connected via a high capacity backhaul network which enables joint spatial soft-cell resource allocation (Parkvall et al. 2011; Bjornson et al. 2013). The backhaul network facilitates the information exchange and interference coordination of the network. Furthermore, the BS and SCAs allow spatial multi-flow transmission so that a UE can be served by multiple BS. In spatial multi-flow transmission, the BS and SCAs convey the same information symbol for *k*th UE, denoted by S_k, but independently apply precoding on the information symbol before transmission (Holma and Toskala 2012). In addition, the macro-cell BS also transmits an AN signal to degrade eavesdropper reception. AN signals do not carry any user information and are only emitted for the sole purpose of disrupting the eavesdroppers. The transmitted signals of the macro-cell BS and SCAs are given by:

$$\mathbf{x_0} = \sum_{k=1}^{K} \mathbf{w_{k,0}}\, s_{k,0} + \mathbf{v_0} \quad \text{and} \quad \mathbf{x_j} = \sum_{k=1}^{K} \mathbf{w_{k,j}}\, s_{k,j} \qquad (1)$$

where $w_{k,0} \in C^{N_{BS}X1}$ and $w_{k,0} \in C^{N_{SC}X1}$ are the precoding vectors of the BS and *j*th SCA, respectively. N_{BS} denotes the number of antennas at the macro-cell BS and N_{SC} denotes the number of antennas at each SCAs. $v_0 \in C^{N_{BS}X1}$ is the AN vector transmitted by the macro-cell BS.

K_{eve} single-antenna eavesdropping terminals are placed within the macro-cell and try to listen to the transmit signals x_0 and x_j. Furthermore, the eavesdroppers are assumed to be colluding; that is, an eavesdropper can share its observation of x_0 and x_j with other eavesdroppers. Collusion of eavesdroppers was modeled as a single eavesdropper with multiple antennas located at different locations in the cell

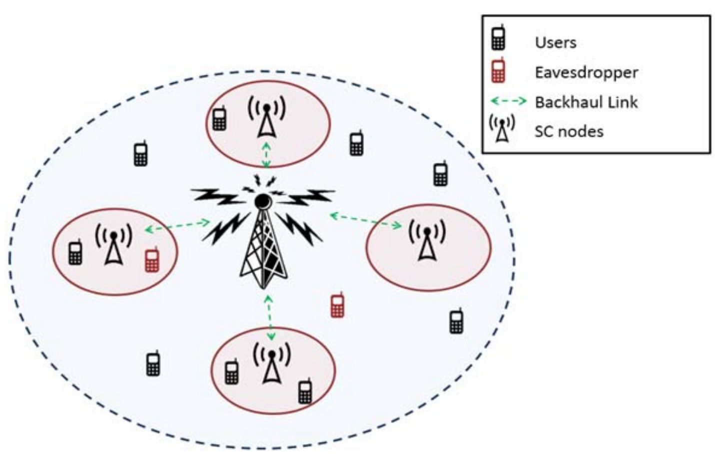

Figure 1. Illustration of a generic heterogeneous network: a macro-cell base station with NBS antennas and multiple small-cell access points communicate with *K* single-antenna UEs uniformly distributed over the macro-cell area.

(assuming that the received signals can be processed by a central node). This is similar to the colluding eavesdropper model presented in the work of Goel and Negi (2005).

The downlink transmission received by the *k*th UE can be expressed as:

$$y_k = \mathbf{h}^H_{k,0}\mathbf{x}_0 + \sum_{j=\text{all SC}} \mathbf{h}^H_{k,j}\mathbf{x}_j + n_k \quad (2)$$

where $h^H_{k,0} \in C^{1xN_{BS}}$ represents the channel from the macro-cell BS to *k*th UE and $h^H_{k,j} \in C^{1xN_{SC}}$ represents the channel from the *j*th SCA to *k*th UE. n_k is a zero mean circularly-symmetric complex Gaussian noise with variance σ_k^2. The signals received by the K_{eve} eavesdroppers are stored in a K_{eve}x1 vector y_{eve} given by:

$$\mathbf{y}_{eve} = \mathbf{H}^H_{eve,0}\mathbf{x}_0 + \sum_{j=\text{all SC}} \mathbf{H}^H_{eve,j}\mathbf{x}_j + \mathbf{n}_{eve} \quad (3)$$

The matrices $h^H_{eve,j} \in C^{K_{eve}xN_{BS}}$ and $h^H_{eve,j} \in C^{K_{eve}xN_{SC}}$ denote the channels from macro-cell BS to the eavesdroppers and from *j*th SCA to the eavesdroppers, respectively. n_{eve} is a K_{eve}x1 random vector that accounts for the noise at the eavesdroppers. The *kth*-element of vector y_{eve} denotes the received signal *kth* eavesdropper.

The Radio Frequency (RF) propagation model parameters are listed in Table 1, which mainly follow the works of Vu et al. (2016), Bernardo and De Leon (2016), and the RF propagation model presented in Small Cell Forum Release 7.0 document (Small Cell Forum 2012). The radio transmission from the BS and SCAs to the UE is a multi-carrier modulation scheme with a system bandwidth of 10 MHz and

Table 1. List of channel propagation parameters used to model the downlink transmission of Heterogenous Network

	Macro-cell	Small-cell
Cell Coverage	500m	40m
Distance-dependent Path Loss at distance d (in km) [NLOS]	151.1 + 42.8log(*d*) *dB*	145.4 + 37.5log(*d*) *dB*
Distance-dependent Path Loss at distance d (in km) [LOS]	123.4 + 24.2log(*d*) *dB*	103.8 + 20.9log(*d*) *dB*
LOS Probability	*Refer to Table 2-1 of Small Cell Forum Release 7.0 Document (2012)	
Std Dev for Log-normal Shadowing	4 dB (NLOS) , 3 dB (LOS)	
Carrier Frequency/Number of Subcarriers	2 GHz/600	
System Bandwidth/Subcarrier Bandwith	10 MHz/ 15 kHz	
Noise Power Density	-174 dBm/Hz (@ 5dB NF)	

subcarrier bandwidth of 15 kHz (similar to what is currently used in 4G cellular systems). Furthermore, it was also assumed that the separation between antenna elements is wide enough, such that users and eavesdroppers experience independent and identically distributed Rayleigh fading.

FORMULATION OF THE OPTIMIZATION MODEL

As a starting point in the formulation of the optimization model, the objective function presented in our previous work (Bernardo and De Leon 2016) was modified. The objective is to optimize the power consumption of the network, while satisfying the QoS constraints and PHY security requirement of each UE. The objective function in the model is the total power consumption, denoted as $P_{TOTAL} = P_{dynamic} + P_{static}$, where

$$P_{static} = \sum_{j=0}^{M} \left(P_{cir,j} N_{SC} + P_{idle,j} \right) \tag{4}$$

$$P_{dynamic} = \sum_{j=0}^{M} \rho_j \sum_{k=1}^{K} \left\| \mathbf{w}_{\mathbf{k,j}} \right\|^2 + \rho_0 \left\| \mathbf{v}_{\mathbf{0}} \right\|^2 \tag{5}$$

ρ_j

P_{static} is the static power consumption which models the total power dissipation due to RF circuitry of the macro-cell BS and *M* SCAs. $P_{cir,j}$ and $P_{idle,j}$ denote the per-antenna circuit power consumption and non-transmission power consumption of the *j*th BS, respectively. The dynamic power consumption, denoted as $P_{dynamic}$, accounts for the aggregated emitted power of the macro-cell BS and M SCAs. The parameter $1/\rho_j \leq 1,\ j \in [0, M]$ models the power amplifier efficiency at *j*th transmitter. Higher value of means lower power amplifier efficiency, thus resulting in higher transmit power. Since the amplitude of signal transmission at each antenna element is controlled by the precoding vectors, the dynamic power consumption is proportional to the power allocated to each precoding vectors. Furthermore, the model for the dynamic power consumption presented in this work also accounts for the power allocated by the macro-cell BS in generating the AN signals.

To limit the maximum allowable transmission power of the macro-cell BS and SCAs, transmit power constraints should be imposed on the optimization model. These transmission power limits can be represented using the following inequality constraints:

$$\sum_{k=1}^{K} \mathbf{w}_{\mathbf{k,j}}^{\mathbf{H}} \mathbf{Q}_{\mathbf{j,l}} \mathbf{w}_{\mathbf{k,j}} \leq q_{j,l} \qquad \forall j \neq 0, \forall l = 1, \ldots, N_{SC} \tag{6}$$

$$\sum_{k=1}^{K}\left(\mathbf{w}_{k,0}^{\mathbf{H}}+\mathbf{v}_{0}^{\mathbf{H}}\right)\mathbf{Q}_{0,l}\left(\mathbf{w}_{k,0}+\mathbf{v}_{0}\right)\leq q_{0,l}\quad \forall l=1,\ldots,N_{BS} \tag{7}$$

where (6) denotes the transmit power limit for each SCAs and (7) denotes the transmit power limit for the macro-cell BS. The terms $q_{j,l}$ and $q_{0,l}$ denote the transmit power limit imposed on the *l*th antenna element at the *j*th SCA and macro-cell BS, respectively. The main difference between the (6) and (7) is the inclusion of the AN signal term in the inequality. $Q_{j,1}\in C^{N_{SC}\times N_{SC}}$ and $Q_{0,1}\in C^{N_{BS}\times N_{BS}}$ are weighting matrices for the constraints. Since per-antenna transmit power limits are desired, the weighting matrices are only non-zero at the *l*th diagonal element and zero elsewhere.

In addition to transmit power constraints, data rate requirement of each user should be defined. As such, Quality-of-Service constraints are included in the optimization model which specifies a minimum target for the information rate (in bits/s/Hz). These constraints can be defined as follows:

$$\log_2(1+\mathrm{SINR}_k)\geq\gamma_k,\quad \forall\, k=\{0,1,\ldots,K\} \tag{8}$$

where γ_k is the minimum information rate that the *k*th UE must satisfy; and SINR_k is the signal-to-interference and noise ratio at the kth UE, and can be expressed as:

$$\mathrm{SINR}_k=\frac{\sum_{j=0}^{M}\left|\mathbf{h}_{k,j}^{\mathbf{H}}\mathbf{w}_{k,j}\right|^2}{\sum_{i\neq k}^{K}\left(\sum_{j=0}^{M}\left|\mathbf{h}_{k,j}^{\mathbf{H}}\mathbf{w}_{i,j}\right|^2\right)+\left|\mathbf{h}_{k,0}^{\mathbf{H}}\mathbf{v}_0\right|^2+\sigma_k^2} \tag{9}$$

σ_k^2 denotes the noise power at the *k*th UE. Information symbols not intended to the *k*th UE, as well as non-information bearing AN signals, are treated as interference. The inequality constraint for the QoS is based from the well-known Shannon's capacity formula (Shannon 1948) which relates the theoretical limit for information rate to the received signal quality. This QoS constraint formulation has also been adopted in several research works (Bjornson et al. 2013; Lv et al. 2015; Bernardo and De Leon 2016; Nguyen et al. 2016).

Finally, a set of PHY security constraints that limits the signal quality at the eavesdroppers should be incorporated to the optimization model. This set of constraints can be expressed as:

$$\begin{aligned} &\mathrm{SNR}_{\mathrm{eve,k}} \le \delta_k \quad \forall\, \mathrm{k} \\ &where\ \ \mathrm{SNR}_{\mathrm{eve,k}} = \frac{\sum_{\mathrm{j=0}}^{\mathrm{M}} \left\| \mathbf{H}_{\mathbf{eve,j}}^{\mathbf{H}} \mathbf{w}_{\mathbf{k,j}} \right\|^2}{\left\| \mathbf{H}_{\mathbf{eve,0}}^{\mathbf{H}} \mathbf{v}_{\mathbf{0}} \right\|^2 + \sigma_{\mathrm{eve}}^2} \end{aligned} \tag{10}$$

δ_k is the maximum allowable signal-to-noise ratio (SNR) that the eavesdropper can detect from the downlink transmission of the *k*th UE. $\mathrm{SNR}_{\mathrm{eve},k}$ describes the combined signal quality of the signals intended to the *k*th UE at the colluding eavesdroppers' side. $\mathrm{SNR}_{\mathrm{eve},k}$ excludes the interference terms from signals intended to other UE, and is only degraded by the transmitted AN signal and eavesdropper noise power σ_{eve}^2. This was implemented to assume the worst-case scenario, wherein the eavesdropper can decouple the information for multiple UE. PHY security constraint in (10) is derived from the secrecy capacity formula given as:

$$C_s = \log_2(1+\mathrm{SINR}_{\mathrm{k}}) - \log_2(1+\mathrm{SNR}_{\mathrm{eve,k}}) \tag{11}$$

which follows the work of Lv et al. (2015). Secrecy capacity is the highest information rate at which the transmitter and the intended receiver can communicate while the eavesdroppers receive an arbitrarily small amount of information. Equation (11) also relates the secrecy capacity of the communication channel to the received signal quality of the eavesdroppers. Reduction of the signal quality at the eavesdroppers would increase the secrecy capacity. By setting a target secrecy capacity C_s and minimum QoS target γ_k, the lower bound value for δ_k can be obtained using the following expression:

$$\delta_k = 2\,\hat{}\,(\log_2(1+\gamma_k) - C_s) - 1 \tag{12}$$

Using the total power consumption in (4) and (5) as the objective function and inequalities (6), (7), (8), (10) as constraints, the optimization model can be formulated as:

$$\begin{aligned} &\min_{\mathbf{v_0},\,\mathbf{w_{k,j}} \forall \mathrm{k,j}} . \quad \mathrm{P_{dynamic}} + \mathrm{P_{static}} \\ &\mathrm{s.t.} \quad \log_2(1+\mathrm{SINR}_{\mathrm{k}}) \ge \gamma_{\mathrm{k}} \quad \forall\, \mathrm{k}, \\ &\qquad \sum_{\mathrm{k=1}}^{\mathrm{K}} \mathbf{w}_{\mathbf{k,j}}^{\mathbf{H}} \mathbf{Q}_{\mathbf{j,l}} \mathbf{w}_{\mathbf{k,j}} \le q_{j,l} \quad \forall j \ne 0, l, \\ &\qquad \sum_{\mathrm{k=1}}^{\mathrm{K}} \left(\mathbf{w}_{\mathbf{k,0}}^{\mathbf{H}} + \mathbf{v}_{\mathbf{0}}^{\mathbf{H}} \right) \mathbf{Q}_{\mathbf{0,l}} \left(\mathbf{w}_{\mathbf{k,0}} + \mathbf{v}_{\mathbf{0}} \right) \le q_{0,l} \quad \forall l, \\ &\qquad \quad \mathrm{SNR}_{\mathrm{eve,k}} \le \delta_k \quad \forall\, \mathrm{k} \end{aligned} \tag{13}$$

The above optimization model is not a convex optimization problem due to the QoS constraints and PHY security constraints. As such, the model must be reformulated in order to be computationally tractable. Semi-definite relaxation trick, similar to what was used in the work of Bjornson et al. (2016), was applied to the model. By letting $W_{k,j} \in S_{+}^{N} = W_{k,j} W_{k,j}^{H}$, $V_0 \in S^{N}_{+} = V_0 V_0^{H}$, and ignoring the requirement that $W_{k,j}$ and V_0 should be rank-1 matrices, the original optimization model is transformed to:

$$
\begin{aligned}
\min_{\mathbf{w}_{\mathbf{k,j}} \forall k,j} . \quad & \sum_{j=0}^{M} \rho_j \sum_{k=1}^{K} \mathrm{tr}(\mathbf{W}_{\mathbf{k,j}}) + \rho_0 \mathrm{tr}(\mathbf{V}_{\mathbf{0}}) + P_{\mathrm{static}} \\
\text{s.t.} \quad & \sum_{j=0}^{M} \mathbf{h}_{\mathbf{k,j}}^{\mathbf{H}} \left(\left(1 + \frac{1}{\tilde{\gamma}_k} \right) \mathbf{W}_{\mathbf{k,j}} - \sum_{i=1}^{K} \mathbf{W}_{\mathbf{i,j}} \right) \mathbf{h}_{\mathbf{k,j}} \geq \sigma_k^2 + \mathbf{h}_{\mathbf{k,0}}^{\mathbf{H}} \mathbf{V}_{\mathbf{0}} \mathbf{h}_{\mathbf{k,0}}, \forall k \\
& \sum_{k=1}^{K} \mathrm{tr}\left(\mathbf{Q}_{\mathbf{j,l}} \mathbf{W}_{\mathbf{k,j}} \right) \leq q_{j,l}, \quad \forall l, 1 \leq j \leq M \\
& \sum_{k=1}^{K} \mathrm{tr}\left(\mathbf{Q}_{\mathbf{0,l}} \left(\mathbf{W}_{\mathbf{0,j}} + \mathbf{V}_{\mathbf{0}} \right) \right) \leq q_{0,l}, \quad \forall l \\
& \sigma_{\mathrm{eve}}^2 + \mathrm{tr}\left(\mathbf{H}_{\mathbf{eve,0}}^{\mathbf{H}} \mathbf{V}_{\mathbf{0}} \mathbf{H}_{\mathbf{eve,0}} \right) \geq \sum_{j=0}^{M} \mathrm{tr}\left(\mathbf{H}_{\mathbf{eve,j}}^{\mathbf{H}} \left(\left(\frac{\mathbf{W}_{\mathbf{k,j}}}{\delta_k} \right) \right) \mathbf{H}_{\mathbf{eve,j}} \right), \forall k
\end{aligned}
\tag{14}
$$

where $\tilde{\gamma}_k = 2^{\gamma_k} - 1$. The removal of rank constraint implies that multiple transmitters can serve a UE, which is justified since spatial multi-flow transmission is allowed in our system model. Furthermore, the constraints were transformed into linear matrix inequalities (LMI) which inherently have a convex structure. Thus, the resulting optimization model is a convex semi-definite program (SDP) and the global optimum solution can be solved numerically using convex solvers.

Design of Low Computational Complexity Algorithm for PHY security

The solution obtained from the derived optimization model in the previous section is our benchmark for the achievable performance of heterogeneous network. The solution to the benchmark model can be calculated in polynomial time. However, the problem becomes infeasible to implement in real-time if N_{BS} and N_{SC} have large values. Thus, it is necessary to develop an alternative optimization model with complexity independent on N_{BS} and N_{SC}. This is achieved by assuming that the precoding vectors and AN vector can be expressed as:

$$
\mathbf{w}_{\mathbf{k,j}} = \sqrt{p_{k,j}}\,\mathbf{u}_{\mathbf{k,j}} \text{ and } \mathbf{v}_0 = \sum_{p=1}^{P} \sqrt{r_p}\,\mathbf{f}_p \tag{15}
$$

where $p_{k,j}$ is the power allocated to $w_{k,j}$, and $u_{k,j}$ is the unit vector that specifies the direction of the $w_{k,j}$. The expression for the regularized zero-forcing (RZF) precoding presented in the work of Bjornson et al. (2013) is used to compute $u_{k,j}$. The RZF precoding expression is given as:

$$\mathbf{u_{k,j}} = \frac{\left(\sum_{i=1}^{K} \frac{1}{\sigma_i^2}\mathbf{h_{i,j}}\mathbf{h_{i,j}^H} + \frac{K}{\gamma_k q_{j,l}}\mathbf{I}\right)^{-1}\mathbf{h_k}}{\left\|\left(\sum_{i=1}^{K} \frac{1}{\sigma_i^2}\mathbf{h_{i,j}}\mathbf{h_{i,j}^H} + \frac{K}{\gamma_k q_{j,l}}\mathbf{I}\right)^{-1}\mathbf{h_k}\right\|} \tag{16}$$

v_0 is expressed as a linear combination of the P column vectors $f_{0,} \dots, f_P$. The unit AN vector components f_p are chosen such that

$$\mathbf{H_0^H f_p} = \mathbf{0}\forall p, \text{ where } \mathbf{H_0} = \sum_{i=1}^{K}\mathbf{h_{i,0}}\mathbf{h_{i,0}^H} \tag{17}$$

i.e. the AN vector components should lie on the null space of H_0. This AN generation scheme is known as the null space method (Goel and Negi 2005; Zhou and McKay 2010). P denotes the nullity of matrix H_0. r_p is the power allocated to f_p. To ensure that the nullity is nonzero, N_{BS} is set to be greater than *K*.

Since the direction of the precoding vectors and AN vector components are known, the optimization model can be formulated as a power allocation strategy problem. The proposed low-complexity algorithm is implemented as follows:

1) Each transmitter j=0 to M computes the following quantities in parallel:

$$g_{k,i,j} = \left|\mathbf{h_{k,j}^H u_{i,j}}\right|^2 \quad g_{eve,k,j} = \left\|\mathbf{H_{eve,j}^H u_{k,j}}\right\|^2 \quad d_{eve,p} = \left\|\mathbf{H_{eve,0}^H f_p}\right\|^2 \tag{18}$$

2) The jth SCA sends the scalar values $g_{k,i,j}$ and $g_{evek,j}$ to the macro-cell BS. The macro-cell BS solves the convex optimization problem in (19) to obtain the optimal power allocation strategy, denoted by $p_{k,j}^*$ and r_p^*.

$$
\begin{aligned}
\min_{\substack{p_{k,j} \forall k,j \\ r_p \forall p}} . \quad & \sum_{j=0}^{M} \rho_j \sum_{k=1}^{K} p_{k,j} + \rho_0 \sum_{p=1}^{P} r_p + P_{static} \\
\text{s.t.} \quad & \sum_{j=0}^{M} \left(g_{k,k,j} p_{k,j} \left(1 + \frac{1}{\tilde{\gamma}_k} \right) - \sum_{i=1}^{K} g_{k,i,j} p_{i,j} \right) \geq \sigma_k^2, \forall k \\
& \sum_{k=1}^{K} p_{k,j} \left\| \mathbf{u}_{k,j} \right\|_\infty^2 \leq q_j, \quad \forall j \neq 0 \\
& \sum_{p=1}^{P} r_p \left\| \mathbf{f}_p \right\|_\infty^2 + \sum_{k=1}^{K} p_{k,0} \left\| \mathbf{u}_{k,0} \right\|_\infty^2 \leq q_0 \\
& \sigma_{eve}^2 + \sum_{p=1}^{P} r_p d_{eve,p} \geq \sum_{j=0}^{M} \frac{g_{eve,k,j} p_{k,j}}{\delta_k} \quad \forall k \\
& p_{k,j} \geq 0 \quad \forall k, j \\
& r_p \geq 0 \quad \forall p
\end{aligned}
$$

3) The optimal values $p_{k,j}^*$ that satisfy (19) are sent to the *j*th SCA. The precoding vectors and AN vector can now be computed by the macro-cell BS and SCAs using equation (15).

The optimization model presented in (19) is a linear problem (LP) which can be efficiently solved by convex solvers. Moreover, the unknown quantities are real-valued variables instead of complex-valued semi-definite matrices. The interference term caused by the AN signal to the UE is removed since AN signals are orthogonal to all UE channel vectors. The use of Chebyshev norm ($\|\cdot\|_\infty$) for the transmit power constraints provides an upper bound value on the per-antenna transmit power. This was done to remove the dependency of the optimization model on the total number of antenna elements.

Modifications to Incorporate Sleep Mode Capabilities in Proposed Algorithm

Sleep mode mechanism of HetNets is essential in order to reduce power consumption at low traffic periods. To include the sleep mode capability of SCAs in the optimization model given in (19), Boolean variables that determine the state of the *j*th small cell node, denoted as λ_j, were incorporated in the optimization model. A value of '1' indicates that the small cell is in active mode and a value of '0' indicates that the small cell is in sleep mode. With this, the optimization model can be stated as follows:

$$
\begin{aligned}
\min_{\substack{p_{k,j}\,\forall k,j \\ r_p\,\forall p \\ \lambda_j\,\forall j}} \quad & \sum_{j=0}^{M} \rho_j \sum_{k=1}^{K} p_{k,j} + \rho_0 \sum_{p=1}^{P} r_p + \mathrm{P}_{static,0} + \sum_{j=1}^{M} \left(\lambda_j \mathrm{P}_{static,j} + (1-\lambda_j)\, \mathrm{P}_{sleep,j} \right) \\
\text{s.t.} \quad & \sum_{j=0}^{M} \left(g_{k,k,j}\, p_{k,j} \left(1 + \frac{1}{\tilde{\gamma}_k} \right) - \sum_{i=1}^{K} g_{k,i,j}\, p_{i,j} \right) \geq \sigma_k^2, \ \forall k \\
& \sum_{k=1}^{K} p_{k,j} \left\| \mathbf{u}_{k,j} \right\|_\infty^2 \leq \lambda_j\, q_j, \quad \forall j \neq 0 \\
& \sum_{p=1}^{P} r_p \left\| \mathbf{f}_p \right\|_\infty^2 + \sum_{k=1}^{K} p_{k,0} \left\| \mathbf{u}_{k,0} \right\|_\infty^2 \leq q_0 \\
& \sigma_{eve}^2 + \sum_{p=1}^{P} r_p d_{eve,p} \geq \sum_{j=0}^{M} \frac{g_{eve,k,j}\, p_{k,j}}{\delta_k} \quad \forall k \\
& p_{k,j} \geq 0 \quad \forall k, j \\
& r_p \geq 0 \quad \forall p \\
& \lambda_j \in \{0,1\} \quad \forall j \neq 0
\end{aligned} \tag{20}
$$

where $P_{static,0}$ and $P_{static,j}$ are the static power consumption of the macro-cell BS and *j*th SCA, respectively. $P_{static,j}$ is the power consumption of the *j*th SCA when it is in sleep mode. The last term in the objective function indicates that an SCA can only be either in sleep mode or in active mode, and that its static power consumption will depend on its state. The introduction of the Boolean variable λ_j makes the problem intractable due to loss of convexity. LP relaxation can be applied in order to obtain an approximate solution to the problem. This is done by replacing the Boolean variables by continuous variables (i.e. $0 \leq \lambda_j \leq 1 \ \forall j$). Replacing the Boolean constraints in (20) provides a convex structure to the model. The resulting optimization model can be used to determine an approximate value of λ_j that lies within the interval [0, 1]. Decision on whether the *j*th SCA should be in sleep state or active state can be determined by comparing the approximate value of λ_j with some threshold τ. λ_j assumes a value of '1' if the approximate value is greater than τ and '0' if otherwise. Once a decision on the states of SCAs has been made after solving optimization model (20), the proposed low-complexity algorithm in (19) can be used to calculate the precoding and AN vectors, wherein SCAs in sleep mode are ignored in the power allocation strategy. Although the proposed PHY security algorithm which incorporates sleep mode mechanism of HetNets has a suboptimal power allocation strategy due to constraint relaxations, it is shown in the next section that it outperforms the achievable performance of HetNets without sleep mode mechanism when QoS requirement is low.

RESULTS AND DISCUSSION

The total power consumption of the proposed low-complexity algorithm is analyzed for varying per-user QoS requirement. The optimal solution of the model derived in (14) serves as a baseline for performance assessment. The HetNet consists of one macro-cell BS placed at the center and 18 SCAs strategically deployed as shown in Figure 2. The HetNet serves 10 UE, while 10 eavesdroppers uniformly distributed within the macro-cell coverage area try to intercept the data intended for each UE. The positions of UE and eavesdroppers are taken from a uniform distribution with lower and upper bound distances from the macro-cell BS of 35m and 500m, respectively. Furthermore, a constraint was added that the minimum distance between a mobile terminal and an SCA is 5m. These distance constraints are necessary to ensure the validity of the channel model parameters in Table 1. The value of δ_k is fixed at $2^{0.1}$-1 = 0.0717 for all users. Hardware parameters used in the simulation are listed in Table 2, which mainly follow those used in the works of Nguyen et al. (2016) and Tang et al. (2015).

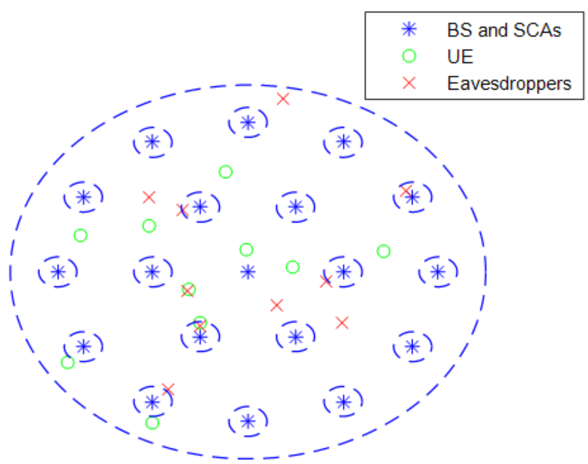

Figure 2. Illustration of a single-cell downlink scenario. BS and SCAs are fixed, while UE and eavesdroppers are uniformly distributed within the cell.

Table 2. List of hardware parameters used in simulation

	Macro-cell	**Small-cell**
Number of Antennas	16	4
Max Transmit Power	$P_{0,max}$ = 43 dBm $q_{0,l} = P_{0,max}/N_{BS}$	$P_{j,max}$ = 30 dBm $q_{j,l} = P_{j,max}/N_{SC}$
Per-antenna Circuit Power	189 mW	5.6 mW
Power Amplifier Efficiency	38.8%	5.2%
Non-transmission Power	30 dBm	20 dBm
Sleep Mode Power	-	5 dBm

Average total power consumption per 15 kHz subcarrier for different values of per-user QoS target is depicted in Figure 3. The optimization models presented in the previous section were implemented using a MATLAB-based modeling system for convex optimization called CVX (2010). The simulation results show that progression in average total power consumption is observed as per-user QoS target is increased. Although the proposed scheme enables fast precoding and AN vector design, deviation from the baseline performance is observed. The discrepancy in performance can be attributed to the heuristic structure of RZF precoding scheme, as discussed in the work of Bjornson et al. (2014). In the derivation of the RZF precoding structure, an assumption that the Lagrange multipliers for each user are of equal value was made, in order to reduce the complexity of the problem. However, this assumption causes a slight degradation in performance– a necessary trade-off to achieve practical implementation. RZF precoding is discussed in detail in the work of Bjornson et al. (2014). Nevertheless, the performance gap between the proposed algorithm and the optimal solution is small, with less than 1 dB (or 25%) difference in power consumption of the whole network at γ_k = 3.0 bits/s/Hz.

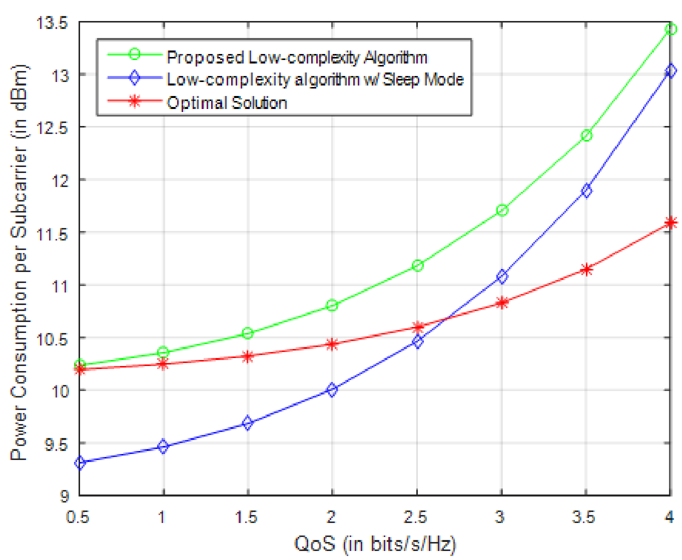

Figure 3. Average total power consumption of proposed low-complexity algorithm, low-complexity algorithm with sleep mode, and optimal solution for different QoS target.

The performance of the proposed algorithm allowing sleep mode in SCAs was also investigated. The total power consumption of the proposed algorithm allowing sleep mode is lower compared to the optimal performance of HetNets without sleep mode mechanism at $\gamma_k < 2.5$ bits/s/Hz. This shows that incorporating sleep mode capability to SCAs can reduce the power consumption at low traffic periods, while still maintaining a reliable and secure downlink transmission. At high per-user QoS requirement, the power consumption of the proposed algorithm allowing sleep mode approaches that of the proposed algorithm without sleep mode mechanism.

The impact of eavesdropper presence on the generated solution of the proposed algorithms was also analyzed and is depicted in Figure 4. Parameters used for this simulation experiment are similar to those used in Figure 3, but the per-user QoS targets γ_k are fixed at 2.0 bits/s/Hz and K_{eve} is varied instead of γ_k. The sudden jump on the average total power consumption in Figure 4 was caused by the AN signal.

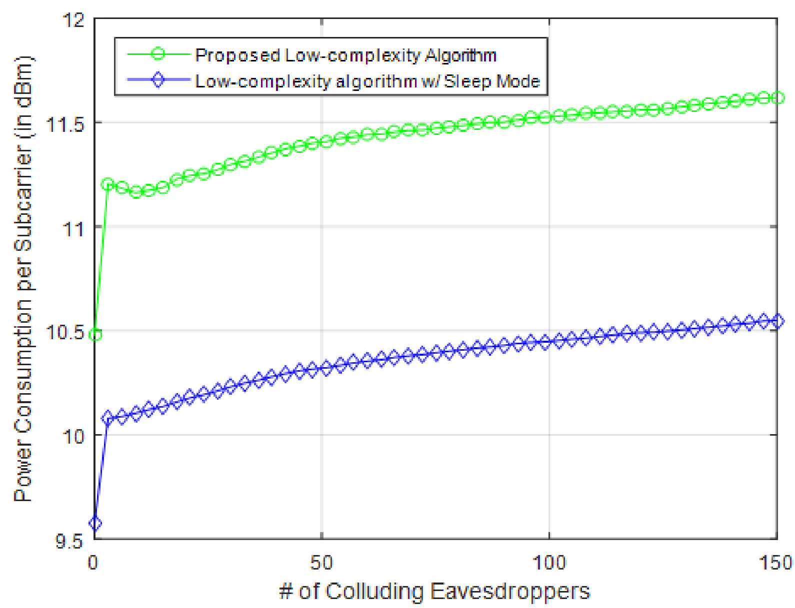

Figure 4. Average total power consumption of proposed low-complexity algorithm and low-complexity algorithm with sleep mode for varying eavesdropper count.

Since the purpose of the AN signal is to degrade the performance of the eavesdroppers, the AN signal will only have a non-zero power allocation if the eavesdroppers are present. In addition, the average total power consumption has a steadily increasing trend as the number of eavesdroppers grows. This result is not entirely unexpected due to the assumption that the eavesdroppers are colluding. Placement of additional eavesdroppers at random locations exploits receive spatial diversity which improves the quality of eavesdropped signals. As such, a more secured transmission strategy is required to degrade their signal reception. This is achieved by increasing the AN signal power or increasing the power allocation in RZF precoding.

The average runtimes of solving the benchmark performance and the proposed low-complexity schemes for different number of SCAs are listed in Table 3. The hardware used in conducting the simulation is an Intel Core i7-4770 with 3.40 GHz processing speed and 4 GB RAM. This hardware runs a Windows 7 64-bit Operating system with MATLAB 2015a installed. Runtime measurements were acquired using the built-in timeit function of MATLAB. Measured runtime in solving the benchmark performance exponentially increases as more SCAs are added to the simulation setup. This is expected since the matrix dimensions of the unknown semidefinite matrices $W_{k,j}$ scale up drastically with the addition of more SCAs. Meanwhile, runtime performances of the proposed PHY security schemes were not significantly affected by the addition of SCAs. However, the runtime of the proposed PHY security scheme doubled when sleep mode was considered. This is because the algorithm needs to solve two linear optimization problem: first is to determine whether the SCAs are in the active state or in sleep state using (20), and then solve the precoding vectors of all active SCAs using (19).

Table 3. List of average runtimes in solving the original optimization model and the proposed low-complexity physical layer security schemes

Number of SCA	Runtime of Benchmark Performance (in seconds)	Runtime of Proposed Scheme (No Sleep mode) (in seconds)	Runtime of Proposed Scheme (No Sleep mode) (in seconds)
3 SCAs	2.534	0.165	0.337
6 SCAs	5.258	0.175	0.358
9 SCAs	10.227	0.187	0.382
12 SCAs	20.4917	0.198	0.404
15 SCAs	37.415	0.2083	0.425
18 SCAs	66.338	0.217	0.442

CONCLUSION

In this study, an optimization model which solves for the optimal values of the precoding vectors and an AN vector that minimizes the total power consumption, while satisfying certain level of data rate requirement and secrecy performance at the PHY layer, was developed. Using the formulated optimization model, a low-complexity algorithm which determines the optimal power allocation strategy for the precomputed AN vector and precoding vectors was designed. The performance of the proposed algorithm was analyzed by comparing it with the derived benchmark performance. Despite the decrease in computational complexity, deviation from the achievable performance was observed. However, the small increase in power consumption is an acceptable trade-off for the feasibility of real-time implementation. The algorithm was also extended to take into account the sleep mode capability of SCAs. Allowing SCAs to sleep during idle/low traffic periods could lessen the power consumption without sacrificing secrecy of communication—even outperforming the optimal solution for HetNets without sleep mode at low data rate requirement. Increase in eavesdropper also resulted in an increase in total power consumption. Finally, we note that, although perfect knowledge of UE and eavesdropper channel state information (CSI) was assumed in this study, modification of the proposed algorithm to be robust against imperfect CSI knowledge is considered for future work.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the UP Wireless Communications Engineering Laboratory for their support to the study.

REFERENCES

Bernardo NI, De Leon F. 2016. On the trade-off between physical layer security and energy efficiency of massive MIMO with small cells. In: International Conference on Advanced Technologies for Communications (ATC); Hanoi, Vietnam: IEEE Computer Society. p.135-140.

Bjornson E, Kountouris M, Debbah M. 2013. Massive MIMO and small cells: Improving energy efficiency by optimal soft-cell coordination. In: 20th International Conference on Telecommunications. p. 1-5.

Bjornson E, Bengtsson M, Ottersten B. 2014. Optimal multiuser transmit beamforming: A difficult problem with a simple solution structure [Lecture Notes]. IEEE Signal Processing Magazine. 31:142-148.

CVX Research Inc. 2010. CVX: MATLAB software for disciplined convex programming version 2.1.

Deng Y, Wang L, Wong K, Nallanathan A, Elkashlan M, Lambotharan S. 2015. Safeguarding massive MIMO aided HetNets using physical layer security. In: International Conference on Wireless Communications and Signal Processing (WCSP). IEEE Computer Society. p.1-5.

Goel S, Negi R. 2005. Secret communication in presence of colluding eavesdroppers. In: IEEE Military Communications Conference. 3:1501-1506.

Holma H, Toskala A. 2012. LTE Advanced: 3GPP Solution for IMT Advanced. 1st edition. New Jersy (US): John Wiley & Sons.

Hoydis J, Kobayashi M, Debbah M. 2011. Green small-cell networks. IEEE Vehicular Technology Magazine. 6:37-43.

[ITU] International Telecommunications Union. 2014. Future technology trends of terrestrial IMT systems. M-series.

Lv T, Gao H, Yang S. 2015. Secrecy transmit beamforming for heterogeneous networks. IEEE Journal on Selected Areas in Communications. 33:1154-1170.

Mukherjee A, Fakoorian SAA, Huang J, Swindlehurst AL. 2014. Principles of physical layer security in multiuser wireless networks: A survey. IEEE Communications Surveys and Tutorials. 16:1550-1573.

Nguyen LD, Tuan HD, Duong TQ. 2016. Energy-efficient signaling in QoS constrained heterogeneous networks. IEEE Access. 4:7958-7966.

Nigam G, Minero P, Haenggi M. 2014. Coordinated multipoint joint transmission in heterogeneous networks. IEEE Transactions on Communications. 62:4134-4146.

Parkvall S, Dahlam E, Jongren G, Landstrom S, Lindbom L. 2011. Heterogeneous network deployments in LTE – the soft-cell approach. Ericsson Review.

Samsung Electronics Co. 2015. White paper on 5G Vision [Internet]. [cited 2017 October 1]. Available from: http://www.samsung.com/global/business-images/insights/2015/Samsung-5G-Vision-0.pdf.

Shannon CE. 1948. A mathematical theory of communication. Bell Systems Technical Journal. 27:379-423.

Shiqi G, Chengwen X, Zesong F, Jingming K. 2016. Resource allocation for physical layer security in heterogeneous network with hidden eavesdropper. China Communications. 13:82-95.

Small Cell Forum. 2012. W-CDMA Open Access Small Cells: Architecture, Requirements, and Dependencies.

Tang J, So DKC, Alsusa E, Hamdi KA, Shojaeifard A. 2015. Resource allocation for energy efficiency optimization in heterogeneous networks. IEEE Journal on Selected Areas in Communications. 33:2104-2117.

Trappe W. 2015. The challenges facing physical layer security. IEEE Communications Magazine. 53:16-20.

Vu QD, Tran LN, Farrell R, Hong EK. 2016, Energy-efficient zero-forcing precoding design for small-cell networks. IEEE Transactions on Communications. 64:790-804.

Wang HM, Zheng TX, Yuan J, Towsley D, Lee MH. 2016. Physical layer security in heterogeneous cellular networks. IEEE Transactions on Communications. 64:1204-1219.

Yang N, Wang L, Geraci G, Elkashlan M, Yuan J, Di Renzo M. 2015. Safeguarding 5G Wireless communication networks using physical layer security. IEEE Communications Magazine. 53:20-27.

Zhou X, McKay MR. 2010. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation. IEEE Transactions on Vehicular Technology. 59:3831-3842.

Neil Irwin Bernardo <neil.bernardo@eee.upd.edu.ph> is an Assistant Professor of the Electrical and Electronics Engineering Institute, University of the Philippines Diliman. He received both his M.S. degree in Electrical Engineering and B.S. degree in Electronics and Communications Engineering from the same institute. His research interests include communication signal processing, software-defined radios, and MIMO.

Franz de Leon <franz.de.leon@eee.upd.edu.ph> received both his B.S. degree in Electronics and Communications Engineering in 2003 and M.S. degree in Electrical Engineering in 2005 from the University of the Philippines Diliman. He received his Ph.D. degree in Electrical and Electronic Engineering in 2014 from the University of Southampton, United Kingdom. He is an Assistant Professor in the Electrical and Electronics Engineering Institute, UP Diliman, whose interests include applications of digital signal processing in audio and communications.