DEVICE-TO-DEVICE COMMUNICATIONS: THE PHYSICAL LAYER SECURITY ADVANTAGE

Daohua Zhu[⋆]*, A. Lee Swindlehurst*[†]*, S. Ali A. Fakoorian*[†]*, Wei Xu*[⋆]*, Chunming Zhao*[⋆]

[⋆] National Mobile Communications Research Lab, Southeast University, Nanjing, P. R. China
Email:{zhudaohua, wxu, cmzhao}@seu.edu.cn
[†] Center for Pervasive Communications and Computing, University of California, Irvine, CA, USA
Email:{afakoori, swindle}@uci.edu

ABSTRACT

In systems that allow device-to-device (D2D) communications, user pairs in close proximity communicate directly without using an access point (AP) as an intermediary. D2D communications leads to improved throughput, reduced power consumption and interference, and more flexible resource allocation. We show that the D2D paradigm also provides significantly improved security at the physical layer, by reducing exposure of the information to eavesdroppers from two relatively high-power transmissions to a single low-power hop. We derive the secrecy outage probability (SOP) for the D2D and cellular systems, and compare performance for D2D scenarios in the presence of a multi-antenna eavesdropper. The cellular approach is only seen to have an advantage in certain cases when the AP has a large number of antennas and perfect channel state information.

Index Terms— Device-to-device communications, physical layer security, secrecy outage probability

1. INTRODUCTION

The problem of improving wireless spectral efficiency to meet the growing demand for data services remains a challenging task. One effective solution is to divide network services into wide- and local-area applications and use Device-to-Device (D2D) communications as an alternative operational mode. In D2D communications, a direct connection between two local users is established, allowing them to directly exchange information instead of relaying the information through the cellular network, including the access point, gateway, core network, etc. The D2D approach has many advantages over standard cellular communications, such as higher local spectral efficiency, shorter delays, lower power consumption, etc. [1]. Most literature on D2D communications has focused on resource allocation and interference management issues [2, 3].

In this paper, we emphasize instead the enhanced security that D2D systems can achieve via the physical layer. Physical layer security generally refers to techniques that exploit wireless channel characteristics, modulation and coding, multiple antennas, and jamming to reduce the ability of eavesdroppers to detect and intercept sensitive communications. The interested reader can refer to [4–6] for an overview of recent information theoretic and signal processing advances in this area. D2D communications should naturally provide enhanced security due to the fact that the local communication can typically take place at lower power, and the fact that the information is exposed only during a single hop rather than by relaying through the AP. On the other hand, D2D links are often used by simple single-antenna devices, while the relayed message can take advantage of multiple antennas at the AP to improve directionality, which can increase gain toward desired users and away from potential eavesdroppers. In this paper we analytically quantify this trade-off and use several examples to illustrate when D2D links can offer a security advantage. The only prior work we are aware of on physical layer security and D2D systems is that of [7], which creatively considers the D2D pair as a helper that provides interference to mask the signal of a co-channel cellular user.

2. D2D WIRETAP CHANNEL MODEL

Figure 1 depicts the scenario considered in this paper, with a transmitting device, Alice, desiring to communicate a private message to a receiving device, Bob, in the presence of an eavesdropper, Eve. Normally, in a standard centralized cellular network, Alice would first transmit the message to an access point (AP), and then the message would be sent to Bob in a second hop. In the figure, we label the AP as a "relay" and use the subscript R to identify it, since in effect the AP is acting as a decode-and-forward (DF) relay. In the standard cellular approach, Eve can potentially wiretap both the uplink message from Alice as well as the downlink message from the AP. On the other hand, if a D2D link can be established between Alice and Bob, then Eve can only wiretap this single-hop link, which is likely to be at a lower power due to the need for avoiding interference to nearby cellular users. In either case, we assume that both Alice and Bob have a single antenna, while Eve has N_E and the AP has N_R antennas.

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

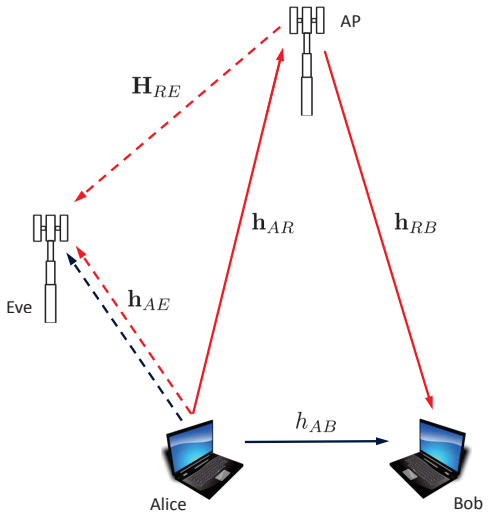

Fig. 1. D2D Communication Scenario with Eavesdropper.

As shown in the figure, we let h_{ij} (SISO), $\mathbf{h}_{ij}$ (MISO) or $\mathbf{H}_{ij}$ (MIMO) represent the channel between a transmitter $i \in \{A, R\}$ and receiver $j \in \{B, E, R\}$. We model all scalar channels as $h_{ij} = \tilde{h}_{ij}/d_{ij}^{\alpha}$, where $\tilde{h}_{ij}$ is a zero-mean unit variance circular complex Gaussian random variable (denoted as $\mathcal{CN}(0,1)$), d_{ij} is the distance between transmitter i and receiver j, and α is the path-loss exponent (assumed here to be the same for all links). This model is assumed to hold whether h_{ij} is the scalar channel h_{AB}, or an element of the MISO or MIMO channels, and we write $\tilde{\mathbf{H}}_{RE} = d_{RE}^{\alpha}\mathbf{H}_{RE}$ and $\tilde{\mathbf{h}}_{ij} = d_{ij}^{\alpha}\mathbf{h}_{ij}$. We assume that the AP has channel state information (CSI) for the instantaneous channels $\{\mathbf{h}_{AR}, \mathbf{h}_{RB}\}$ to Alice and Bob, Alice has CSI for the channels to the AP and Bob $\{\mathbf{h}_{AR}, h_{AB}\}$, and Eve has CSI for all channels. However, we assume that only the distribution of the eavesdropper's channels $\{\mathbf{h}_{AE}, \mathbf{H}_{RE}\}$ are known to Alice and the AP.

Letting x represent the single-stream message that Alice wishes to transmit to Bob, we first describe the data model for the signal received at Bob (y_B), Eve (y_E) and the access point (y_R) under the standard cellular setting. In the first hop, Alice transmits x to the AP and it is wiretapped by the eavesdropper:

$$y_R = \sqrt{P_A}\mathbf{w}_R^H\mathbf{h}_{AR}x + \mathbf{w}_R^H\mathbf{n}_R \quad (1)$$

$$y_E(1) = \sqrt{P_A}\mathbf{w}_E^H(1)\mathbf{h}_{AE}x + \mathbf{w}_E^H(1)\mathbf{n}_E(1), \quad (2)$$

where P_A is Alice's transmit power, $\{\mathbf{n}_R, \mathbf{n}_E\}$ represent noise at the AP and eavesdropper, and $\{\mathbf{w}_R, \mathbf{w}_E\}$ represent the receive beamformers used at the AP and eavesdropper, respectively. The noise at the AP and Eve is assumed to be spatially white with variance σ_R^2 and σ_E^2, respectively, so the optimal beamformers in terms of signal-to-noise ratio (SNR) are given by the maximal ratio combiner (MRC): $\mathbf{w}_R = \mathbf{h}_{AR}$ and $\mathbf{w}_E(1) = \mathbf{h}_{AE}$. We also write $y_E(1)$ to indicate the first hop. In the second hop, the AP transmits the message x to Bob and it is wiretapped by the eavesdropper:

$$y_B = \sqrt{P_R}\mathbf{h}_{RB}^H\mathbf{t}x + n_B \quad (3)$$

$$y_E(2) = \sqrt{P_R}\mathbf{w}_E^H(2)\mathbf{H}_{RE}\mathbf{t}x + \mathbf{w}_E^H(2)\mathbf{n}_E(2), \quad (4)$$

assuming the AP has power P_R and uses the linear precoder $\mathbf{t}$, and the noise at Bob is $\mathcal{CN}(0, \sigma_B^2)$. Since the elements of $\mathbf{H}_{RE}$ are independent $\mathcal{CN}(0,1)$ variables, we assume the AP uses the maximum ratio transmit precoder $\mathbf{t} = \mathbf{h}_{RB}/\|\mathbf{h}_{RB}\|$. Eve again employs the MRC beamformer, now given by $\mathbf{w}_E(2) = \mathbf{H}_{RE}\mathbf{t} = \mathbf{H}_{RE}\mathbf{h}_{RB}/\|\mathbf{h}_{RB}\|$.

The D2D data model only involves a single hop in which Alice transmits directly to Bob, and it is wiretapped by Eve:

$$y_B = \sqrt{P_A'}h_{AB}x + n_B \quad (5)$$

$$y_E = \sqrt{P_A'}\mathbf{w}_E^H\mathbf{h}_{AE}x + \mathbf{w}_E^H\mathbf{n}_E. \quad (6)$$

Here, Alice's transmit power P_A' will in general be different than in the cellular case.

3. SECRECY ANALYSIS

We compare the secrecy outage probability (SOP) for the standard cellular and D2D networks assuming that the uplink and downlink cellular transmissions each constitute one-half a D2D channel use. As such, the AP essentially acts as a DF relay, and the mutual information for the cellular link is given by [8, 9]:

$$I_B = \frac{1}{2}\min(\log_2(1+\rho_{AR}), \log_2(1+\rho_{RB})) \,, \quad (7)$$

where $\rho_{AR} = P_A\|\mathbf{h}_{AR}\|^2/\sigma_R^2$ is the uplink SNR at the AP and $\rho_{RB} = P_R\|\mathbf{h}_{RB}\|^2/\sigma_B^2$ is the downlink SNR at Bob.

Unlike Bob, in the cellular scenario Eve sees the message over both the uplink and downlink channels:

$$\mathbf{y}_E = \begin{bmatrix} \sqrt{P_A}\|\mathbf{h}_{AE}\|^2 \\ \sqrt{P_R}\|\frac{\mathbf{H}_{RE}\mathbf{h}_{RB}}{\|\mathbf{h}_{RB}\|}\|^2 \end{bmatrix} x + \begin{bmatrix} \mathbf{h}_{AE}^H\mathbf{n}_E(1) \\ \frac{\mathbf{h}_{RB}^H\mathbf{H}_{RE}^H}{\|\mathbf{h}_{RB}\|}\mathbf{n}_E(2) \end{bmatrix}, \quad (8)$$

where $\mathbf{y}_E = [y_E(1) \;\; y_E(2)]^T$. The mutual information at the eavesdropper is thus

$$I_E = \frac{1}{2}\log_2\left(1 + \frac{P_A\|\mathbf{h}_{AE}\|^2}{\sigma_E^2} + \frac{P_R\|\frac{\mathbf{H}_{RE}\mathbf{h}_{RB}}{\|\mathbf{h}_{RB}\|}\|^2}{\sigma_E^2}\right) \quad (9)$$

$$= \frac{1}{2}\log_2(1+\rho_{AE}+\rho_{RE}) \,, \quad (10)$$

where $\rho_{AE} = \frac{P_A}{\sigma_E^2}\|\mathbf{h}_{AE}\|^2$ and $\rho_{RE} = \frac{P_R}{\sigma_E^2}\|\frac{\mathbf{H}_{RE}\mathbf{h}_{RB}}{\|\mathbf{h}_{RB}\|}\|^2$. Combining (7) and (10), the secrecy rate in the cellular case $R_{s,c}$ is given by

$$R_{s,c} = \frac{1}{2}\Big[\min(\log_2(1+\rho_{AR}), \log_2(1+\rho_{RB})) - \log_2(1+\rho_{AE}+\rho_{RE})\Big]^+ , \quad (11)$$

where $z^+ = \max\{z, 0\}$.

The D2D case corresponds to a standard wiretap channel:

$$I_B = \log_2\left(1 + \frac{P'_A|h_{AB}|^2}{\sigma_B^2}\right) = \log_2(1+\rho_{AB}) \quad (12)$$

$$I_E = \log_2\left(1 + \frac{P'_A\|\mathbf{h}_{AE}\|^2}{\sigma_E^2}\right) = \log_2(1+\rho'_{AE}), \quad (13)$$

where $\rho_{AB} = P'_A|h_{AB}|^2/\sigma_B^2$ and $\rho'_{AE} = P'_A\|\mathbf{h}_{AE}\|^2/\sigma_E^2$. The secrecy rate for the D2D case is thus

$$R_{s,d} = \left[\log_2\left(\frac{1+\rho_{AB}}{1+\rho'_{AE}}\right)\right]^+. \quad (14)$$

It is well known that the SOP criterion is appropriate for fading channels, and is often used to determine the likelihood of achieving a certain secrecy rate, say R_t [10, 11]. The SOP for the cellular and D2D cases are respectively given by

$$\mathcal{P}^c_{out}(R_t) = \Pr\left\{\frac{\min(1+\rho_{AR}, 1+\rho_{RB})}{1+\rho_{AE}+\rho_{RE}} < 2^{2R_t}\right\} \quad (15)$$

$$\mathcal{P}^d_{out}(R_t) = \Pr\left\{\frac{1+\rho_{AB}}{1+\rho'_{AE}} < 2^{R_t}\right\}. \quad (16)$$

To derive analytical expressions for the SOP, we first define $\rho^r_{ij} = P_i d_{ij}^{-2\alpha}/\sigma_j^2$ to be the average SNR at receiver j for transmitter i. We will use the fact that $|\tilde{h}_{AB}|^2$ is exponentially distributed with unit hazard rate, while $\|\mathbf{h}_{AE}\|^2$, $\|\tilde{\mathbf{h}}_{AR}\|^2$, and $\|\tilde{\mathbf{h}}_{RB}\|^2$ have $\frac{1}{2}$-scaled central chi-square distributions with $2N_E, 2N_R$ and $2N_R$ degrees of freedom, respectively. For the term $\rho_{RE} = \rho^r_{RE}\|\frac{\tilde{\mathbf{H}}_{RE}\tilde{\mathbf{h}}_{RB}}{\|\tilde{\mathbf{h}}_{RB}\|}\|^2$, since the vector inside the squared norm is $\tilde{\mathbf{H}}_{RE}$ multiplied by normalized $\tilde{\mathbf{h}}_{RB}$, one can prove that the real and imaginary parts of these entries are i.i.d. zero-mean Gaussian distributed r.v.s with variance 1/2. We emphasize the fact that zero-mean Gaussian r.v.s are independent if and only if they are uncorrelated, and as a consequence, the squared norm in question is a 1/2-scaled chi-squared distributed r.v. with $2N_E$ degrees of freedom.

Denote random variables $\min(1+\rho_{AR}, 1+\rho_{RB})$ and $(\rho_{AE}+\rho_{RE})$ as X and Y, respectively. The CDF of a $\frac{1}{2}$-scaled central chi-square distribution can be written as [12] $F_S(s) = 1 - \sum_{c=0}^{N-1}\frac{s^c}{c!}e^{-s}$ where $s \geq 0$. Using simple order statistics, the CDF of X is given by

$$F_X(x) = 1 - e^{\rho}\sum_{p=0}^{N_R-1}\sum_{q=0}^{N_R-1}\frac{(x-1)^{p+q}}{p!q!(\rho^r_{AR})^p(\rho^r_{RB})^q}e^{-\rho x}, \quad (17)$$

where $x \geq 0$ and $\rho \triangleq 1/\rho^r_{AR} + 1/\rho^r_{RB}$. The variable Y is a weighted sum of chi-square r.v.s, with density [13]

$$f_{Y,1}(y) = M(-1)^{N_E-1}\sum_{l=1}^{N_E}\frac{A_l}{(N_E-l)!}\omega^{-(N_E+l-1)} \left[(-1)^{N_E-l}e^{-\frac{y}{\rho^r_{AE}}} - e^{-\frac{y}{\rho^r_{RE}}}\right]y^{N_E-l}, \quad (18)$$

in which $y \geq 0$, $M \triangleq 1/(\rho^r_{AE}\rho^r_{RE})^{N_E}$, $A_l \triangleq C^{l-1}_{N_E+l-2}$, $C^z_w = \frac{w!}{(w-z)!z!}$ and $\omega \triangleq (\rho^r_{AE} - \rho^r_{RE})/\rho^r_{AE}\rho^r_{RE}$. We note that a different expression is necessary for the special case when $\rho^r_{AE} = \rho^r_{RE}$ [13], but due to space limitations we do not include it here.

Based on the above, the cellular SOP can be computed as

$$\begin{aligned}
\mathcal{P}^c_{out}(R_t) &= \Pr\left\{\frac{\min(1+\rho_{AR}, 1+\rho_{RB})}{1+\rho_{AE}+\rho_{RE}} < 2^{2R_t}\right\} \\
&= \mathcal{E}_Y\{F_X(2^{2R_t} + 2^{2R_t}Y)\} \\
&= 1 - M(-1)^{N_E-1}e^{-\rho(2^{2R_t}-1)}\sum_{p=0}^{N_R-1}\frac{(2^{2R_t})^p}{p!(\rho^r_{AR})^p} \\
&\quad \sum_{q=0}^{N_R-1}\frac{(2^{2R_t})^q}{q!(\rho^r_{RB})^q}\sum_{m=0}^{p+q}C^m_{p+q}f^{p+q-m}\sum_{l=1}^{N_E}\frac{A_l\omega^{-(N_E+l-1)}}{(N_E-l)!} \\
&\quad \int_0^\infty y^{N_E+m-l}\left((-1)^{N_E-l}e^{-\mu_1 y} - e^{-\mu_2 y}\right)\mathrm{d}y \\
&= 1 - M(-1)^{N_E-1}e^{-\rho(2^{2R_t}-1)}\sum_{p=0}^{N_R-1}\frac{(2^{2R_t})^p}{p!(\rho^r_{AR})^p} \\
&\quad \sum_{q=0}^{N_R-1}\frac{(2^{2R_t})^q}{q!(\rho^r_{RB})^q}\sum_{m=0}^{p+q}C^m_{p+q}f^{p+q-m}\sum_{l=1}^{N_E}\frac{A_l\omega^{-(N_E+l-1)}}{(N_E-l)!} \\
&\quad (N_E+m-l)!\left[(-1)^{N_E-l}\mu_1^{-(N_E+m-l+1)} - \right. \\
&\quad \left.\mu_2^{-(N_E+m-l+1)}\right], \quad (19)
\end{aligned}$$

where $f = \frac{2^{2R_t}-1}{2^{2R_t}}$, $\mu_1 = \rho 2^{2R_t} + 1/\rho^r_{AE}$, and $\mu_2 = \rho 2^{2R_t} + 1/\rho^r_{RE}$. While (19) is cumbersome, we can observe that either increasing N_E or decreasing N_R will increase $\mathcal{P}^c_{out}(R_t)$, while clearly $\mathcal{P}^c_{out}(R_t) \to 1$ as $P_A \to 0$ or $P_R \to 0$. However, the behavior at high SNR is not immediately clear from (19).

For the D2D case, let U and V respectively represent the r.v.s $|h_{AB}|^2$ and $\|\mathbf{h}_{AE}\|^2$. As mentioned earlier, U is exponential with unity hazard rate: $f_U(u) = e^{-u}$, while V is a scaled central chi-square distribution with density $f_V(v) = \frac{v^{N_E-1}e^{-v}}{(N_E-1)!}$. The SOP of the D2D mode for a given target secrecy rate R_t is given by

$$\begin{aligned}
\mathcal{P}^d_{out}(R_t) &= \Pr\left\{\frac{1+\rho_{AB}}{1+\rho_{AE'}} < 2^{R_t}\right\} \\
&= \int_0^\infty \int_0^{\frac{2^{R_t}-1}{\rho^r_{AB}} + \frac{\rho^r_{AE'}}{\rho^r_{AB}}2^{R_t}v} f_U(u)\mathrm{d}u\, f_V(v)\mathrm{d}v \\
&= 1 - e^{-\frac{2^{R_t}-1}{\rho^r_{AB}}}\int_0^\infty \frac{v^{N_E-1}}{(N_E-1)!}e^{-(1+\frac{\rho^r_{AE'}}{\rho^r_{AB}}2^{R_t})v}\mathrm{d}v \\
&= 1 - \left(\frac{1}{1+(\frac{d_{AB}}{d_{AE}})^{2\alpha}2^{R_t}}\right)^{N_E}e^{-\frac{2^{R_t}-1}{\rho^r_{AB}}}. \quad (20)
\end{aligned}$$

The behavior of the D2D SOP is more easily discerned

from (20), clearly showing how the SOP approaches 1 for increasing N_E, increasing d_{AB}/d_{AE}, and decreasing ρ^r_{AB}.

4. NUMERICAL EXAMPLES

Here we compare the D2D and cellular SOP for the type of scenario in which D2D communications would be considered, namely where the D2D distance is considerably less than the distance to the AP. In particular, we set $d_{AB} = 20$m and $d_{AR} = d_{RB} = 100.5$m, and we assume the average SNR of all desired links are identical: $\rho^r_{AB} = \rho^r_{AR} = \rho^r_{RB}$. The noise power is assumed to be the same at all nodes, the path-loss exponent is chosen as $2\alpha = 2.5$, $N_E = 4$, and the target secrecy rate is set to $R_t = 1$ bit per channel use. Four different eavesdropper locations are considered: Near Alice: $d_{AE} = 10$m, $d_{RE} = 102$m; Near AP: $d_{AE} = 100$m, $d_{RE} = 10$m; Semi-remote eavesdropper: $d_{AE} = d_{RE} = 158$m; Remote eavesdropper: $d_{AE} = d_{RE} = 304$m.

Fig. 2 shows SOP as a function of the desired link SNR when $N_R = 4$, and we observe excellent agreement between the simulated SOP (lines) and the analytical results (symbols). The cellular SOP is unity in all cases except for the remote eavesdropper (Case 4) indicated by the '+' symbol. On the other hand, the D2D SOP is only unity when the eavesdropper is near Alice; otherwise the D2D SOP is always strictly lower than in the cellular case, significantly so for high SNRs. The best D2D performance is obtained for the remote eavesdropper ('x'), next is the semi-remote case (triangles), followed by the near-AP case (squares).

Fig. 3 depicts the SOP as a function of N_R when $\rho^r_{AB} = \rho^r_{AR} = \rho^r_{RB} = 15$dB. The symbols correspond to the same eavesdropper locations as in the previous figure, with '*' representing the cellular SOP with a semi-remote eavesdropper. Here we see that the cellular approach can achieve an advantage provided there are sufficient antennas at the AP to provide beamforming gain that allows Alice to transmit with low power and the AP to precisely focus its transmissions on Bob. At least $N_R = 7$ is required for the remote eavesdropper, while $N_R > 20$ is necessary in the semi-remote case. Note that the ability of the cellular network to exploit N_R in this way depends on the assumption of accurate CSI, which can require a higher feedback or training overhead than in the D2D case. In addition, the performance degradation due to imperfect channel estimation would be greater in the multi-antenna cellular case. These two factors would in practice increase the number of AP antennas required to match the security offered by D2D communications.

5. CONCLUSION

We have compared the physical layer security offered by a direct D2D connection between two network nodes with that achieved if the two nodes communicate indirectly via an AP. Expressions for the secrecy outage probability were derived

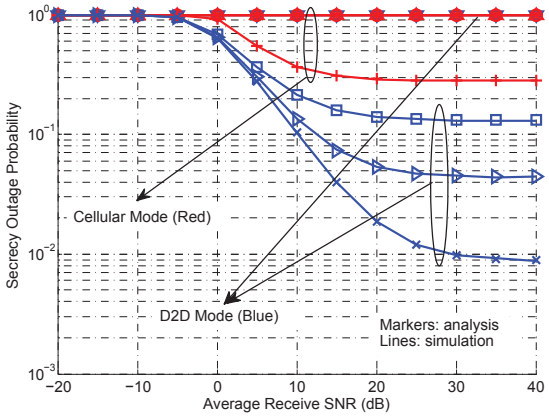

Fig. 2. SOP versus average SNR for both D2D and cellular modes, $N_E = N_R = 4$.

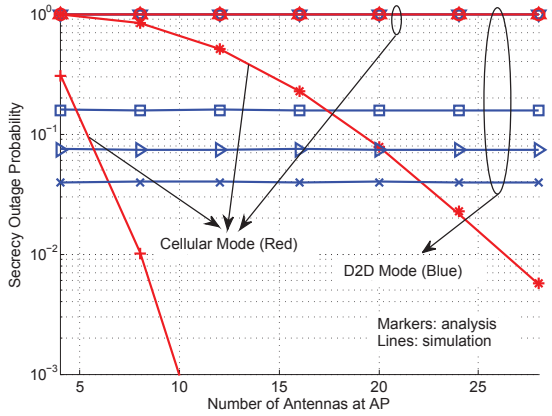

Fig. 3. SOP versus N_R for both D2D and cellular modes, $\rho^r_{AR} = \rho^r_{RB} = \rho^r_{AB} = 15$dB and $N_E = 4$.

for both cases assuming a multi-antenna AP, a multi-antenna eavesdropper, single-antenna devices and assuming that only statistical CSI is available for the eavesdropper channels. Results from numerical examples involving four different eavesdropper positions illustrated that in most scenarios, the D2D mode offers a security advantage over decode-and-forward messaging through the AP. However, it was observed that the cellular mode can outperform the D2D link when there are sufficiently many antennas at the AP. The array gain offered by the AP antennas allows Alice to significantly reduce her transmit power, and provides directional gain towards Bob. In practice, this gain would come at the cost of reduced spectral efficiency and sensitivity to imperfect CSI.

6. REFERENCES

[1] K. Doppler, M. Rinne, C. Wijting, C. Ribeiro, and K. Hugl, "Device-to-device communication as an underlay to LTE-advanced networks," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 42–49, Dec. 2009.

[2] C.-H. Yu, K. Doppler, C. B. Ribeiro, and O. Tirkkonen, "Resource sharing optimization for device-to-device communication underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2752–2763, Aug. 2011.

[3] D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, G. Feng, and S. Li, "Device-to-device communications underlaying cellular networks," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3541–3551, Aug. 2013.

[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge Univ. Press, 2011.

[5] *Physical Layer Security in Wireless Communications*, X. Zhou, L. Song and Y. Zhang, editors, CRC Press, Wireless Networks and Mobile Communications Series, Nov. 2013.

[6] Y.-W. Hong, P.-C. Lan, and C.-C. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Processing Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[7] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for device-to-device communication underlaying cellular networks," *IEEE Commun. Lett.*, accepted for publication, 2013.

[8] J. N. Laneman, D. Tse, and G. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Info. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[9] J. Huang and A. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[10] J. Huang, A. Mukherjee and A. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.

[11] N.-E. Wu and H.-J. Li, "Effect of feedback delay on secure cooperative networks with joint relay and jammer selection," *IEEE Wireless Commun. Lett.*, vol. 2, no. 4, pp. 415–418, Aug. 2013.

[12] F. Jiang, J. Wang, and A. Swindlehurst, "Interference-aware scheduling for connectivity in MIMO ad hoc multicast networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1762–1778, May 2012.

[13] E. Björnson, D. Hammarwall, and B. Ottersten, "Exploiting quantized channel norm feedback through conditional statistics in arbitrarily correlated MIMO systems," *IEEE Trans. Signal Process.*, vol. 57, no. 10, pp. 4027–4041, Oct. 2009.