Massive MIMO Physical Layer Cryptosystem through Inverse Precoding

Amin Sakzad
Clayton School of IT
Monash University
amin.sakzad@monash.edu

Joint work with
Ron Steinfeld

October 2015

MIMO Wiretap Channel 1

- We consider a slow-fading MIMO wiretap channel model as follows:

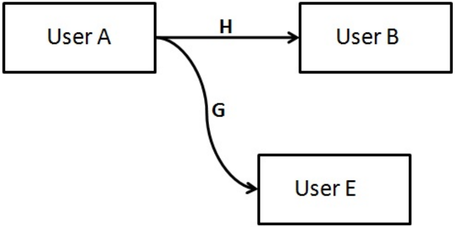

Figure: The block diagram of a MIMO wiretap channel.

MIMO Wiretap Channel 2

- The $n_r \times n_t$ real-valued MIMO channel from user A to user B is denoted by $\mathbf{H}$.

MIMO Wiretap Channel 2

- The $n_r \times n_t$ real-valued MIMO channel from user A to user B is denoted by $\mathbf{H}$.
- We also denote the channel from A to the adversary E by an $n_r' \times n_t$ matrix $\mathbf{G}$.

MIMO Wiretap Channel 2

- The $n_r \times n_t$ real-valued MIMO channel from user A to user B is denoted by $\mathbf{H}$.
- We also denote the channel from A to the adversary E by an $n_r' \times n_t$ matrix $\mathbf{G}$.
- The entries of $\mathbf{H}$ and $\mathbf{G}$ are identically and independently distributed (i.i.d.) based on a Gaussian distribution $\mathcal{N}_1$. This model can be written as:

$$\begin{cases} \mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{e}, \\ \mathbf{y}' = \mathbf{G}\mathbf{x} + \mathbf{e}'. \end{cases}$$

Dean-Goldsmith Model 1

- The entries x_i of $\mathbf{x} \in \mathbb{R}^{n_t}$, for $1 \leq i \leq n_t$, are drawn from a constellation $\mathcal{X} = \{0, 1, \ldots, m-1\}$ for an integer m.

Dean-Goldsmith Model 1

- The entries x_i of $\mathbf{x} \in \mathbb{R}^{n_t}$, for $1 \leq i \leq n_t$, are drawn from a constellation $\mathcal{X} = \{0, 1, \ldots, m-1\}$ for an integer m.
- The components of the noise vectors $\mathbf{e}$ and $\mathbf{e}'$ are i.i.d. based on Gaussian distributions $\mathcal{N}_{m^2\alpha^2}$ and $\mathcal{N}_{m^2\beta^2}$, respectively. We assume $\alpha = \beta$.

Dean-Goldsmith Model 1

- The entries x_i of $\mathbf{x} \in \mathbb{R}^{n_t}$, for $1 \leq i \leq n_t$, are drawn from a constellation $\mathcal{X} = \{0, 1, \ldots, m-1\}$ for an integer m.
- The components of the noise vectors $\mathbf{e}$ and $\mathbf{e}'$ are i.i.d. based on Gaussian distributions $\mathcal{N}_{m^2\alpha^2}$ and $\mathcal{N}_{m^2\beta^2}$, respectively. We assume $\alpha = \beta$.
- The channel state information (CSI) is available at all the transmitter and receivers.

Dean-Goldsmith Model 2

- To send a message $\mathbf{x}$ to B, user A performs a singular value decomposition (SVD) precoding.

Dean-Goldsmith Model 2

- To send a message $\mathbf{x}$ to B, user A performs a singular value decomposition (SVD) precoding.
- Let SVD of $\mathbf{H}$ be given as $\mathbf{H} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^t$. The user A transmits $\mathbf{V}\mathbf{x}$ instead of $\mathbf{x}$ and B applies a filter matrix $\mathbf{U}^t$ to the received vector $\mathbf{y}$.

Dean-Goldsmith Model 2

- To send a message $\mathbf{x}$ to B, user A performs a singular value decomposition (SVD) precoding.
- Let SVD of $\mathbf{H}$ be given as $\mathbf{H} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^t$. The user A transmits $\mathbf{V}\mathbf{x}$ instead of $\mathbf{x}$ and B applies a filter matrix $\mathbf{U}^t$ to the received vector $\mathbf{y}$.
- With this, the received vectors at B and E are as follows:

$$\begin{cases} \tilde{\mathbf{y}} = \mathbf{\Sigma}\mathbf{x} + \tilde{\mathbf{e}}, \\ \mathbf{y}' = \mathbf{G}\mathbf{V}\mathbf{x} + \mathbf{e}', \end{cases}$$

where $\tilde{\mathbf{e}} = \mathbf{U}^t\mathbf{e}$.

Correctness Condition for Dean-Goldsmith Cryptosystem

- Since $\mathbf{\Sigma} = \text{diag}(\sigma_1(\mathbf{H}), \ldots, \sigma_{n_t}(\mathbf{H}))$ is diagonal, user B recovers an estimate $\tilde{x}_i$ of x_i as follows:

$$\tilde{x}_i = \lceil \tilde{y}_i / \sigma_i(\mathbf{H}) \rfloor = x_i + \lceil \tilde{e}_i / \sigma_i(\mathbf{H}) \rfloor .$$

Correctness Condition for Dean-Goldsmith Cryptosystem

- Since $\mathbf{\Sigma} = \text{diag}(\sigma_1(\mathbf{H}), \ldots, \sigma_{n_t}(\mathbf{H}))$ is diagonal, user B recovers an estimate $\tilde{x}_i$ of x_i as follows:

$$\tilde{x}_i = \lceil \tilde{y}_i / \sigma_i(\mathbf{H}) \rfloor = x_i + \lceil \tilde{e}_i / \sigma_i(\mathbf{H}) \rfloor .$$

- The decoding process succeeds if $|\tilde{e}_i| < |\sigma_i(\mathbf{H})|/2$ for all $1 \leq i \leq n_t$.

Correctness Condition for Dean-Goldsmith Cryptosystem

- Since $\mathbf{\Sigma} = \text{diag}(\sigma_1(\mathbf{H}), \ldots, \sigma_{n_t}(\mathbf{H}))$ is diagonal, user B recovers an estimate $\tilde{x}_i$ of x_i as follows:

$$\tilde{x}_i = \lceil \tilde{y}_i / \sigma_i(\mathbf{H}) \rfloor = x_i + \lceil \tilde{e}_i / \sigma_i(\mathbf{H}) \rfloor .$$

- The decoding process succeeds if $|\tilde{e}_i| < |\sigma_i(\mathbf{H})|/2$ for all $1 \leq i \leq n_t$.
- Let $\mathbb{P}\left[\text{B}|\mathbf{H}\right]$ be the probability that B incorrectly decodes $\mathbf{x}$:

$$\begin{aligned} \mathbb{P}\left[\text{B}|\mathbf{H}\right] &\leq n_t \mathbb{P}_{w \hookleftarrow \mathcal{N}_{m^2\alpha^2}}\left[|w| < |\sigma_{n_t}(\mathbf{H})|/2\right] \\ &= n_t \mathbb{P}_{w \hookleftarrow \mathcal{N}_1}\left[|w| < |\sigma_{n_t}(\mathbf{H})|/(2m\alpha)\right] \\ &\leq n_t \exp\left((-|\sigma_{n_t}(\mathbf{H})|^2)/(8m^2\alpha^2)\right), \end{aligned}$$

Correctness Condition for Dean-Goldsmith Cryptosystem

- Since $\mathbf{\Sigma} = \text{diag}(\sigma_1(\mathbf{H}), \ldots, \sigma_{n_t}(\mathbf{H}))$ is diagonal, user B recovers an estimate $\tilde{x}_i$ of x_i as follows:

$$\tilde{x}_i = \lceil \tilde{y}_i/\sigma_i(\mathbf{H}) \rfloor = x_i + \lceil \tilde{e}_i/\sigma_i(\mathbf{H}) \rfloor .$$

- The decoding process succeeds if $|\tilde{e}_i| < |\sigma_i(\mathbf{H})|/2$ for all $1 \leq i \leq n_t$.
- Let $\mathbb{P}\left[\mathrm{B}|\mathbf{H}\right]$ be the probability that B incorrectly decodes $\mathbf{x}$:

$$\begin{aligned} \mathbb{P}\left[\mathrm{B}|\mathbf{H}\right] &\leq n_t \mathbb{P}_{w \hookleftarrow \mathcal{N}_{m^2\alpha^2}}\left[|w| < |\sigma_{n_t}(\mathbf{H})|/2\right] \\ &= n_t \mathbb{P}_{w \hookleftarrow \mathcal{N}_1}\left[|w| < |\sigma_{n_t}(\mathbf{H})|/(2m\alpha)\right] \\ &\leq n_t \exp\left((-|\sigma_{n_t}(\mathbf{H})|^2)/(8m^2\alpha^2)\right), \end{aligned}$$

- By choosing parameters like $m^2\alpha^2 \leq |\sigma_{n_t}(\mathbf{H})|^2/8\log(n_t/\varepsilon)$, one can ensure that B is less than any $\varepsilon > 0$.

Security Condition for Dean-Goldsmith Cryptosystem 1

- MIMO – Search problem: Recovering $\mathbf{x}$ from $\mathbf{y}' = \mathbf{G}_v\mathbf{x} + \mathbf{e}'$ and $\mathbf{G}_v$, with non-negligible probability, under certain parameter settings, upon using massive MIMO systems with large number of transmit antennas n_t.

Security Condition for Dean-Goldsmith Cryptosystem 1

- MIMO – Search problem: Recovering $\mathbf{x}$ from $\mathbf{y}' = \mathbf{G}_v\mathbf{x} + \mathbf{e}'$ and $\mathbf{G}_v$, with non-negligible probability, under certain parameter settings, upon using massive MIMO systems with large number of transmit antennas n_t.
- We say that the MIMO – Search problem is *hard* (secure) if any attack algorithm against MIMO – Search with run-time $\mathrm{poly}(n_t)$ has negligible success probability $n_t^{-\omega(1)}$.

Security Condition for Dean-Goldsmith Cryptosystem 2

- A polynomial-time complexity reduction is claimed from worst-case instances of the $\text{GapSVP}_{n_t/\alpha}$ in lattices of dimension n_t, to the $\text{MIMO} - \text{Search}$ problem with n_t transmit antennas, noise parameter α and constellation size m, assuming the following minimum noise level holds:

$$m\alpha > \sqrt{n_t}. \tag{1}$$

Security Condition for Dean-Goldsmith Cryptosystem 2

- A polynomial-time complexity reduction is claimed from worst-case instances of the $\text{GapSVP}_{n_t/\alpha}$ in lattices of dimension n_t, to the $\text{MIMO} - \text{Search}$ problem with n_t transmit antennas, noise parameter α and constellation size m, assuming the following minimum noise level holds:

$$m\alpha > \sqrt{n_t}. \tag{1}$$

- The above cryptosystem is called the *Massive* MIMO *Physical Layer Cryptosystem (*MM – PLC*)*.

Our Contributions

- We show that the eavesdropper can decrypt the information data under the same condition as the legitimate receiver.

Our Contributions

- We show that the eavesdropper can decrypt the information data under the same condition as the legitimate receiver.
- We study the signal-to-noise advantage ratio for a more generalized scheme with an arbitrary precoder and show that if $n'_r \gg n_t$, then there is no such an advantage.

Our Contributions

- We show that the eavesdropper can decrypt the information data under the same condition as the legitimate receiver.
- We study the signal-to-noise advantage ratio for a more generalized scheme with an arbitrary precoder and show that if $n'_r \gg n_t$, then there is no such an advantage.
- On the positive side, for the case $n'_r = n_t$, we give an $\mathcal{O}\left(n^2\right)$ upper bound on the advantage and show that this bound can be approached using an inverse precoder.

Our Contributions

- We show that the eavesdropper can decrypt the information data under the same condition as the legitimate receiver.
- We study the signal-to-noise advantage ratio for a more generalized scheme with an arbitrary precoder and show that if $n_r' \gg n_t$, then there is no such an advantage.
- On the positive side, for the case $n_r' = n_t$, we give an $\mathcal{O}\left(n^2\right)$ upper bound on the advantage and show that this bound can be approached using an inverse precoder.
- We give a lower bound on the decoding advantage ratio of the legitimate user over an eavesdropper who is equipped with a non-linear successive interference cancelation (SIC) stronger than linear receivers.

Zero-Forcing (ZF) attack

- The eavesdropper E receives $\mathbf{y}' = \mathbf{G}_v\mathbf{x} + \mathbf{e}'$. Replacing the SVD, we get $\mathbf{y}' = \mathbf{U}'\mathbf{\Sigma}'(\mathbf{V}')^t\mathbf{x} + \mathbf{e}'$, where

$$\mathbf{\Sigma}' = \text{diag}\left(\sigma_1(\mathbf{G}_v), \ldots, \sigma_{n_t}(\mathbf{G}_v)\right) = \text{diag}\left(\sigma_1(\mathbf{G}), \ldots, \sigma_{n_t}(\mathbf{G})\right).$$

Zero-Forcing (ZF) attack

- The eavesdropper E receives $\mathbf{y}' = \mathbf{G}_v\mathbf{x} + \mathbf{e}'$. Replacing the SVD, we get $\mathbf{y}' = \mathbf{U}'\mathbf{\Sigma}'(\mathbf{V}')^t\mathbf{x} + \mathbf{e}'$, where

$$\mathbf{\Sigma}' = \text{diag}\left(\sigma_1(\mathbf{G}_v), \ldots, \sigma_{n_t}(\mathbf{G}_v)\right) = \text{diag}\left(\sigma_1(\mathbf{G}), \ldots, \sigma_{n_t}(\mathbf{G})\right).$$

- S(he) computes

$$\tilde{\mathbf{y}}' = (\mathbf{G}_v)^{-1}\mathbf{y}' = \mathbf{x} + \tilde{\mathbf{e}}', \tag{2}$$

where $\tilde{\mathbf{e}}' = \mathbf{V}'(\mathbf{\Sigma}')^{-1}(\mathbf{U}')^t\mathbf{e}'$. User E is now able to recover an estimate $\tilde{x}_i'$ of x_i by rounding:
$\tilde{x}_i' = \lceil \tilde{y}_i' \rfloor = \lceil x_i + \tilde{e}_i' \rfloor = x_i + \lceil \tilde{e}_i' \rfloor$.

Analysis of ZF attack

Lemma

The components of $\tilde{\mathrm{e}}'$ *in* (2) *are distributed as* $\mathcal{N}_{\sigma^2_{\mathrm{E}}}$ *with*

$$\sigma^2_{\mathrm{E}} \leq \frac{m^2\alpha^2}{\sigma^2_{n_t}(\mathbf{G})}.$$

The union bound

- The above explained ZF attack succeeds if $|\tilde{e}'_i| < 1/2$ for all $1 \leq i \leq n_t$.

The union bound

- The above explained ZF attack succeeds if $|\tilde{e}'_i| < 1/2$ for all $1 \leq i \leq n_t$.
- Let $\mathbb{P}_{\mathsf{ZF}}\left[\mathrm{E}|\mathbf{G}\right]$ denotes the decoding error probability that E incorrectly recovers $\mathbf{x}$ using ZF attack. Based on Lemma 1, we have

$$\begin{aligned}\mathbb{P}_{\mathsf{ZF}}\left[\mathrm{E}|\mathbf{G}\right] &\leq n_t \mathbb{P}_{w \hookleftarrow \mathcal{N}_{\sigma_{\mathrm{E}}^2}}\left[|w| < \frac{1}{2}\right] \\ &\leq n_t \mathbb{P}_{w \hookleftarrow \mathcal{N}_1}\left[|w| < \frac{|\sigma_{n_t}(\mathbf{G})|}{2m\alpha}\right]. \qquad (3)\end{aligned}$$

Distribution of the singular values

Theorem (Edelman89)

Let $\mathbf{M}$ *be an* $s \times t$ *matrix with i.i.d. entries distributed as* $\mathcal{N}_1$*. If* s *and* t *tend to infinity in such a way that* s/t *tends to a limit* $y \in [1, \infty]$*, then*

$$\frac{\sigma_t^2(\mathbf{M})}{s} \to \left(1 - \frac{1}{\sqrt{y}}\right)^2 \tag{4}$$

and

$$\frac{\sigma_1^2(\mathbf{M})}{s} \to \left(1 + \frac{1}{\sqrt{y}}\right)^2, \tag{5}$$

almost surely.

Asymptotic probability of error

Theorem

Fix any real $\varepsilon, \varepsilon' > 0$, *and* $y' \in [1, \infty]$, *and suppose that* $n_r'/n_t \to y'$ *as* $n_t \to \infty$. *Then, for all sufficiently large* n_t, *the probability* $\mathbb{P}_{\mathsf{ZF}}[\mathrm{E}]$ *that* E *incorrectly decodes the message* $\mathbf{x}$ *using a* ZF *decoder is upper bounded by* ε, *if*

$$m^2\alpha^2 \leq \frac{n_r'\left(\left(1 - \frac{1}{\sqrt{y'}}\right)^2 - \varepsilon'\right)}{8\log\left(\frac{2n_t}{\varepsilon}\right)}. \tag{6}$$

Advantage ratio

To analytically investigate the advantage of decoding at B over E, we define the following advantage ratio.

Definition

For fixed channel matrices $\mathbf{H}$ and $\mathbf{G}$, the ratio

$$\mathsf{adv}_{\mathsf{ZF}} \triangleq \frac{\sigma^2_{n_t}(\mathbf{H})}{\sigma^2_{n_t}(\mathbf{G})}, \tag{7}$$

is called the advantage of B over E under ZF attack.

Advantage ratio of SVD precoder with ZF attack

Theorem

Let $\mathbf{H}_{n_r \times n_t}$ *be the channel between* A *and* B *and* $\mathbf{G}_{n'_r \times n_t}$ *be the channel between* A *and* E*, both with i.i.d. elements each with distribution* $\mathcal{N}_1$*. Fix real* $y, y' \in [1, \infty]$*, and suppose that* $n_r/n_t \to y$ *and* $n'_r/n_t \to y'$ *as* $n_t \to \infty$*. Then, using a* SVD *precoding technique in* $\mathsf{MM-PLC}$*, we have*

$$\mathit{adv}_{\mathsf{ZF}} \to \frac{\left(\sqrt{y}-1\right)^2}{\left(\sqrt{y'}-1\right)^2}$$

almost surely as $n_t \to \infty$*.*

General Precoder

- One may wonder whether a different precoding method (again, assumed known to E) than used above may provide a better advantage ratio for B over E.

General Precoder

- One may wonder whether a different precoding method (again, assumed known to E) than used above may provide a better advantage ratio for B over E.
- Suppose that instead of sending $\tilde{\mathbf{x}} = \mathbf{V}\mathbf{x}$, user A precodes $\tilde{\mathbf{x}} = \mathbf{P}(\mathbf{H})\mathbf{x}$, where $\mathbf{P} = \mathbf{P}(\mathbf{H})$ is some other precoding matrix that depends on the channel matrix $\mathbf{H}$.

General Precoder

- One may wonder whether a different precoding method (again, assumed known to E) than used above may provide a better advantage ratio for B over E.
- Suppose that instead of sending $\tilde{\mathbf{x}} = \mathbf{V}\mathbf{x}$, user A precodes $\tilde{\mathbf{x}} = \mathbf{P}(\mathbf{H})\mathbf{x}$, where $\mathbf{P} = \mathbf{P}(\mathbf{H})$ is some other precoding matrix that depends on the channel matrix $\mathbf{H}$.
- Therefore, in this general case, the advantage ratio of maximum noise power decodable by B to that decodable by E under a ZF attack at a given error probability generalizes from (7) to

$$\mathsf{adv}_{\mathsf{ZF}} \triangleq \frac{\sigma_{n_t}^2(\mathbf{HP})}{\sigma_{n_t}^2(\mathbf{GP})}. \tag{8}$$

Advantage ratio of general precoder with ZF attack

Theorem

Let $\mathbf{H}$ and $\mathbf{G}$ be as in Theorem 5. Then we have adv$_{\mathsf{ZF}} \leq$ *advup*$_{\mathsf{ZF}}$*. Furthermore, fix real $y, y' \in [1, \infty]$, and suppose that $n_r/n_t \to y$ and $n'_r/n_t \to y'$ as $n_t \to \infty$, so that $n'_r/n_r \to y'/y \triangleq \rho'$. Then, using a general precoding matrix $\mathbf{P}(\mathbf{H})$ in* MM − PLC*, we have*

$$\mathit{advup}_{\mathsf{ZF}} \to \frac{\left(\sqrt{y}+1\right)^2}{\left(\sqrt{y'}-1\right)^2}$$

almost surely as $n_t \to \infty$. Hence, in the case $n'_r = n_r$ and $y' = y \to \infty$, we have advup$_{\mathsf{ZF}} \to 1$*. Moreover, if advup*$_{\mathsf{ZF}} \to c$ *for some $c \geq 1$, then $\min(y', \rho') \leq 9$.*

Achievable Upper Bound on Advantage Ratio

Theorem (Edelman89)

Let $\mathbf{M}$ *be a* $t \times t$ *matrix with i.i.d. entries distributed as* $\mathcal{N}_1$. *The least singular value of* $\mathbf{M}$ *satisfies*

$$\lim_{t \to \infty} \mathbb{P}\left[\sqrt{t}\sigma_t(\mathbf{M}) \geq x\right] = \exp\left(\frac{-x^2}{2} - x\right). \quad (9)$$

The upper bound

Theorem

Let $\varepsilon > 0$ be fixed, $\mathbf{H}$ and $\mathbf{G}$ be $n \times n$ matrices as in Proposition 5 with $n = n_t = n_r = n'_r$. Using a general precoder $\mathbf{P}(\mathbf{H})$ to send the plain text $\mathbf{x}$, the maximum possible adv$_{\mathsf{ZF}}$ that B can achieve over E, is of order $\mathcal{O}\left(n^2\right)$, except with probability $\leq \varepsilon$.

Inverse Precoder Model

- We have

$$\begin{cases} \tilde{\mathbf{y}} = \mathbf{I}_n \mathbf{x} + \tilde{\mathbf{e}}, \\ \mathbf{y}' = \mathbf{G}\mathbf{H}^{-1}\mathbf{x} + \mathbf{e}', \end{cases}$$

Inverse Precoder Model

- We have
$$\begin{cases} \tilde{\mathbf{y}} = \mathbf{I}_n \mathbf{x} + \tilde{\mathbf{e}}, \\ \mathbf{y}' = \mathbf{G}\mathbf{H}^{-1}\mathbf{x} + \mathbf{e}', \end{cases}$$
- Note that, for the inverse precoder the advantage ratio (7) under ZF decoding algorithm at user E can be written as $1/\sigma_n^2\left(\mathbf{G}\mathbf{H}^{-1}\right)$.

Inverse Precoder Model

- We have

$$\begin{cases} \tilde{\mathbf{y}} = \mathbf{I}_n \mathbf{x} + \tilde{\mathbf{e}}, \\ \mathbf{y}' = \mathbf{G}\mathbf{H}^{-1}\mathbf{x} + \mathbf{e}', \end{cases}$$

- Note that, for the inverse precoder the advantage ratio (7) under ZF decoding algorithm at user E can be written as $1/\sigma_n^2\left(\mathbf{G}\mathbf{H}^{-1}\right)$.

Distribution of quotient

Theorem

Let $\mathbf{Q} = \mathbf{G}\mathbf{H}^{-1}$, *where* $\mathbf{H}$ *and* $\mathbf{G}$ *are two* $n \times n$ *real Gaussian matrices. The distribution of* $\mathbf{Q}$ *is proportional to*

$$\frac{1}{\det\left(\mathbf{I}_n + \mathbf{Q}\mathbf{Q}^t\right)^n}. \tag{10}$$

Inverse Precoder achives maximum $\mathsf{adv}_{\mathsf{ZF}}$

Theorem

Let $\varepsilon > 0$ be fixed, $\mathbf{H}$ and $\mathbf{G}$ be $n \times n$ Gaussian matrices as in Proposition 5 with $n = n_t = n_r = n'_r$. Using an inverse precoder $\mathbf{P}(\mathbf{H}) = \mathbf{H}^{-1}$ to send the plain text $\mathbf{x}$, the decoding advantage with respect to zero-forcing attack $\mathsf{adv}_{\mathsf{ZF}}$, is at least $\frac{1}{4\log(1/\varepsilon)} \cdot \left(n^2 + n\right) = \Omega\left(n^2\right)$, except with probability $\leq \varepsilon$, for sufficiently large n.

The exact probability for different orders of n

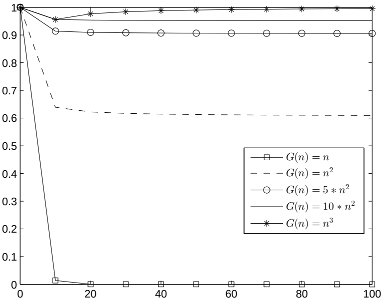

Figure: The amount of $\mathbb{P}\left[\mathsf{adv}_{\mathsf{ZF}} < G(n)\right]$ for different $G(n)$.

$\mathrm{adv}_{\mathrm{ZF}}$ for 1000 channel.

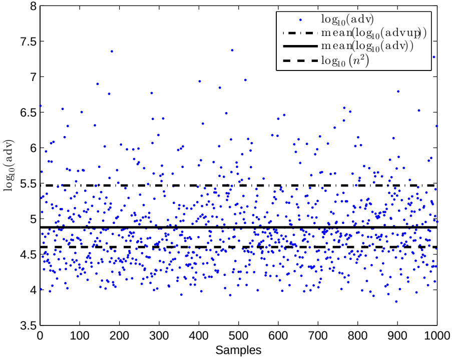

Figure: The advantage ratio (7) for 1000 square channels of size $n = 200$ using inverse precoder.

$\mathbb{P}\left[n^2\sigma_n^2 > x\right]$ for various n

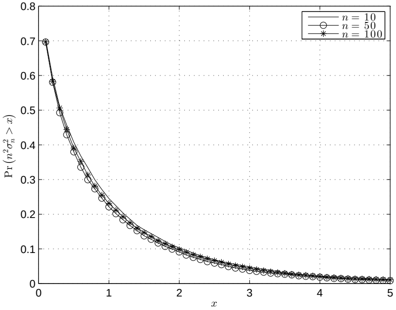

Figure: The numerical values of $\mathbb{P}\left[n^2\sigma_n^2 > x\right]$ for different dimensions $n = 10$, 50, and 100 for 10000 square channels of size $n = 100$ using inverse precoder.

Successive Interference Cancellation (SIC) 1

- A lattice reduction algorithm is conducted first, and then a nearest plane algorithm is applied.

Successive Interference Cancellation (SIC) 1

- A lattice reduction algorithm is conducted first, and then a nearest plane algorithm is applied.
- Let $\mathbf{G}\mathbf{H}^{-1} = \mathbf{Q} = \mathbf{O}\mathbf{R}$ be the QR decomposition of the equivalent channel. Then the received vector by user E equals $\mathbf{y}' = \mathbf{O}\mathbf{R}\mathbf{x} + \mathbf{e}'$.

Successive Interference Cancellation (SIC) 1

- A lattice reduction algorithm is conducted first, and then a nearest plane algorithm is applied.
- Let $\mathbf{G}\mathbf{H}^{-1} = \mathbf{Q} = \mathbf{O}\mathbf{R}$ be the QR decomposition of the equivalent channel. Then the received vector by user E equals $\mathbf{y}' = \mathbf{O}\mathbf{R}\mathbf{x} + \mathbf{e}'$.
- Upon receiving $\mathbf{y}'$, this user multiplies it by $\mathbf{O}^t$. Hence, we get

$$\begin{cases} \tilde{\mathbf{y}} = \mathbf{I}_n\mathbf{x} + \tilde{\mathbf{e}}, \\ \mathbf{y}'' = \mathbf{R}\mathbf{x} + \mathbf{O}^t\mathbf{e}' = \mathbf{R}\mathbf{x} + \mathbf{e}'', \end{cases}$$

Successive Interference Cancellation (SIC) 2

- In SIC decoding framework, the last symbol is decoded first, *i.e.*

$$\tilde{x}'_n = \left\lfloor \frac{y''_n}{r_{nn}} \right\rceil = x_n + \left\lfloor \frac{e''_n}{r_{nn}} \right\rceil$$

is an estimate for x_n.

Successive Interference Cancellation (SIC) 2

- In SIC decoding framework, the last symbol is decoded first, *i.e.*
$$\tilde{x}'_n = \left\lfloor \frac{y''_n}{r_{nn}} \right\rceil = x_n + \left\lfloor \frac{e''_n}{r_{nn}} \right\rceil$$
is an estimate for x_n.
- The other symbols are approximated iteratively using
$$\tilde{x}'_j = \left\lfloor \frac{y''_j - \sum_{k=j+1}^{n} r_{jk}\tilde{x}'_k}{r_{jj}} \right\rceil,$$
for j from $n-1$ downward to 1.

Successive Interference Cancellation (SIC) 2

- In SIC decoding framework, the last symbol is decoded first, *i.e.*
$$\tilde{x}'_n = \left\lfloor \frac{y''_n}{r_{nn}} \right\rceil = x_n + \left\lfloor \frac{e''_n}{r_{nn}} \right\rceil$$
is an estimate for x_n.
- The other symbols are approximated iteratively using
$$\tilde{x}'_j = \left\lfloor \frac{y''_j - \sum_{k=j+1}^{n} r_{jk}\tilde{x}'_k}{r_{jj}} \right\rceil,$$
for j from $n-1$ downward to 1.
- The above mentioned SIC finds the closest vector if the distance from input vector to the lattice is less than half the length of the shortest r_{jj}^2, that is $\frac{r_{nn}^2}{2}$.

Advantage ratio under SIC

We define the following advantage ratio:

$$\mathsf{adv}_{\mathsf{SIC}} \triangleq \frac{r_{nn}^2(\mathbf{I})}{r_{nn}^2(\mathbf{Q})}, \tag{11}$$

is called the advantage of B over E under SIC attack. Since $r_{nn}^2(\mathbf{I}) = 1$, the $\mathsf{adv}_{\mathsf{SIC}} = 1/r_{nn}^2(\mathbf{Q})$.

Distribution of diagonal elements 1

Theorem

Let the matrices $\mathbf{Q}$, $\mathbf{O}$, and $\mathbf{R}$ be as above. Then r_{jj}^2 are independently distributed as $B^{II}\left(\frac{n-j+1}{2}, \frac{j}{2}\right)$, for $1 \leq j \leq n$.

A random variable v is said to have a beta distribution of the second type (beta prime distribution) $B^{II}(a,b)$ if it has the following probability density function

$$\frac{1}{\beta(a,b)} v^{a-1}(1+v)^{-(a+b)}, \quad v > 0,$$

where both a and b are non-negative and $\beta(a,b)$ is the beta function.

Distribution of diagonal elements 2

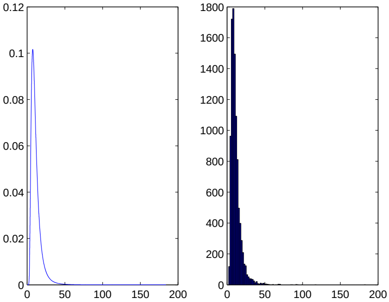

Figure: The numerical histogram and the theoretical p.d.f. of r_{jj}^2 for $j = 10$ and 10000 square channels of size $n = 100$ using inverse precoder.

Distribution of diagonal elements 3

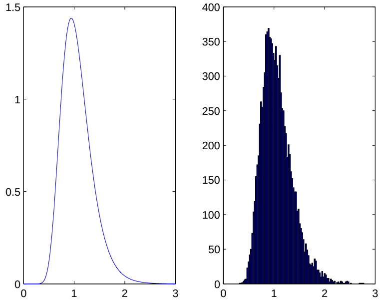

Figure: The numerical histogram and the theoretical p.d.f. of r_{jj}^2 for $j = 50$ and 10000 square channels of size $n = 100$ using inverse precoder.

Adversary with SIC

Theorem

Let $\mathbf{H}_{n\times n}$ *be the channel between* A *and* B *and* $\mathbf{G}_{n\times n}$ *be the channel between* A *and* E*, both with i.i.d. elements each with distribution* $\mathcal{N}_1$*. Then, using an inverse precoding technique in* $\mathsf{MM-PLC}$*, we have* $adv_{\mathsf{SIC}} = \mathcal{O}(n)$.

Numerical analysis of $\mathbb{P}\left[nr_{nn}^2(\mathbf{Q}) < x\right]$

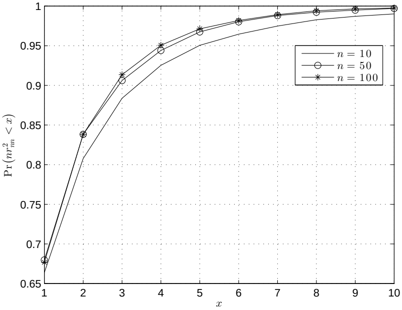

Figure: The numerical values of $\mathbb{P}\left[nr_{nn}^2(\mathbf{Q}) < x\right]$ for different dimensions $n = 10$, 50, and 100 for 10000 square channels of size $n = 100$ using inverse precoder.

Conclusions

- A Zero-Forcing (ZF) attack has been presented for the massive multiple-input multiple-output MIMO physical layer cryptosystem (MM – PLC).
- A decoding advantage ratio has been defined and studied for ZF linear receiver.
- It has been shown that this advantage tends to 1 employing a singular value decomposition (SVD) precoding approach at the legitimate transmitter and a ZF linear receiver at the adversary.
- An advantage ratio in the order of n^2 is achievable if the legitimate user applies an inverse precoder.
- If eavesdropper employs a stronger decoder algorithm such as a successive interference cancellation (SIC), then the advantage ratio will be reduced to a constant fraction of n.

Thank you!