Robust CDMA Receiver Design under Disguised Jamming

Kai Zhou Tianlong Song Jian Ren Tongtong Li
Department of Electrical & Computer Engineering
Michigan State University

March, 2016

Outline

- Introduction
- Problem Formulation
- Robust Receiver Design
- Secure Scrambling
- Conclusions

Introduction (1/2)

- **Code Division Multiple Access (CDMA) [1]**
  - Signal is spread over a bandwidth N times larger by using a specific PN code
  - Robust under narrow band jamming, low SNR levels and malicious detection/attacks
- **Security of Existing CDMA Systems [2, 3]**
  - The security of CDMA relies on the randomness in PN sequences
  - A sequence generated from an n-stage LFSR can be reconstructed with a 2n-bit sequence segment

Introduction (2/2)

- **Disguised Jamming [4, 5]**
  - Disguised jamming can be launched if the PN code is known to the jammer
  - Highly correlated with the signal, and has a power level close or equal to the signal power.
- **Threats of Disguised Jamming [6]**
  - Due to the symmetricity between the jamming and authorized signal, the receiver is fully confused and cannot really distinguish the authorized signal from jamming.
  - A stronger result shows that *the capacity of the system is zero!*
  - The result cannot be changed by bit-level error control coding.

Problem Formulation (1/3)

- **Transmitted Signal**
  - The transmitted signal can be written as

$$s(t) = uc(t), \tag{1}$$

where u is the symbol to be transmitted, and $c(t)$ the general baseband signal of the spreading sequence.

- **Disguised Jamming**
  - Mimicking the transmission pattern of the authorized user, the disguised jamming can be written as

$$j(t) = v\gamma c(t - \tau). \tag{2}$$

Problem Formulation (2/3)

- **Received Signal**
  - The received signal can be written as

$$r(t) = s(t) + j(t) + n(t) = uc(t) + v\gamma c(t-\tau) + n(t), \qquad (3)$$

where $n(t)$ is the noise.

- **Symbol Estimation**
  - A conventional CDMA receiver estimates the transmitted symbol as

$$\hat{u} = \frac{1}{T}\int_0^T r(t)c(t)dt. \qquad (4)$$

Problem Formulation (3/3)

- **Symbol Estimation**
  - Replacing the received signal $r(t)$ in (4) with (3), we have

$$\hat{u} = u + v\gamma\frac{1}{T}\int_0^T c(t-\tau)c(t)dt + \frac{1}{T}\int_0^T n(t)c(t)dt. \qquad (5)$$

- **Worst Case**
  - In the worst case, when $\tau = 0$ and $\gamma = 1$, (5) can be simplified as

$$\hat{u} = u + v + \frac{1}{T}\int_0^T n(t)c(t)dt. \qquad (6)$$

  - Probability of symbol error: $\mathcal{P}_s \geq \frac{M-1}{2M}$. LOWER BOUNDED!!!

Robust Receiver Design (1/4)

- **MSE Minimization**
  - The MSE between the received signal and the jammed signal can be calculated as

$$J(u, v, \tau, \gamma) = \frac{1}{T} \int_0^T |r(t) - uc(t) - v\gamma c(t - \tau)|^2 dt. \tag{7}$$

  - Our goal is

$$\{\hat{u}, \hat{v}, \hat{\tau}, \hat{\gamma}\} = \arg \min_{u,v,\tau,\gamma} J(u, v, \tau, \gamma). \tag{8}$$

  - Difficult task. Too many parameters!

Robust Receiver Design (2/4)

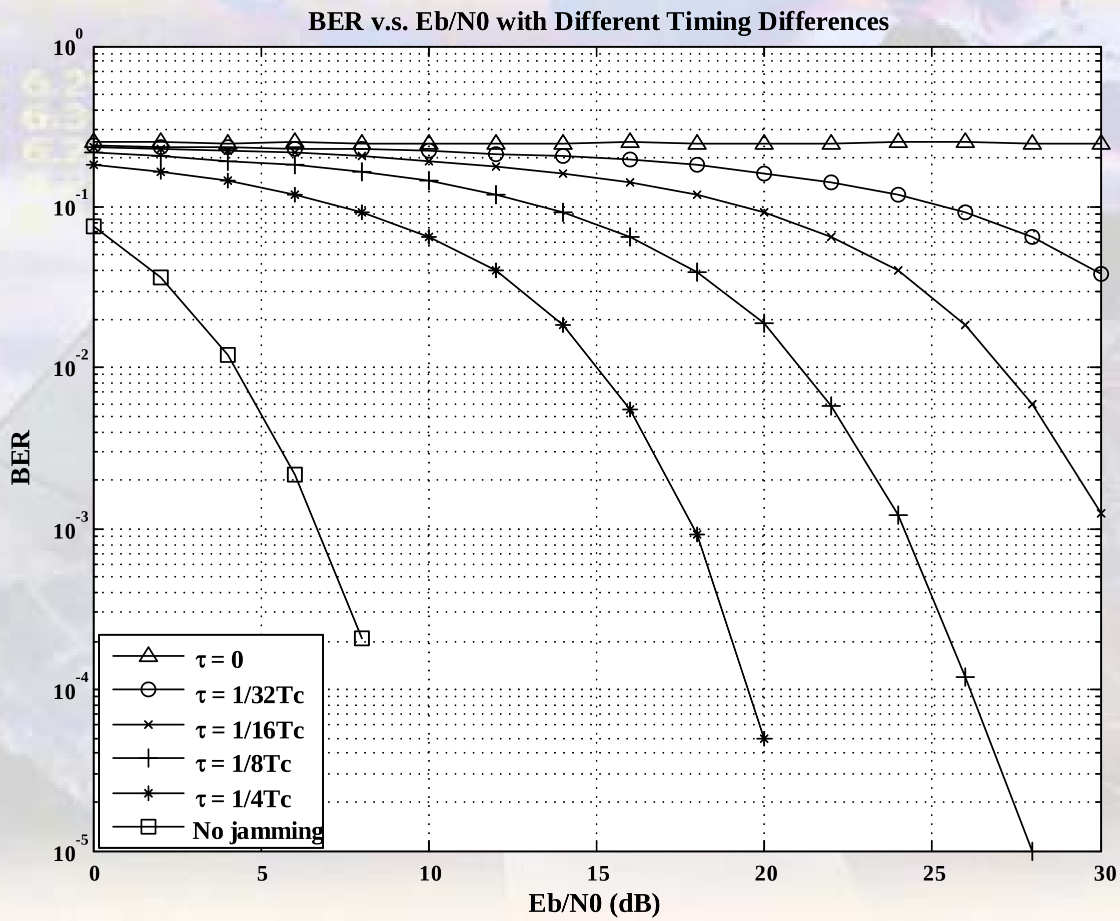
- **Problem Reduction**
  - To minimize (7), one necessary condition is that its partial derivatives regarding v and γ are zero, applying which (7) can be reduced to

$$J = \frac{1}{T}\int_0^T |r(t) - uc(t)|^2 dt - |A(u,\tau)|^2, \tag{9}$$

    which is a function depending only on u and τ.
  - In digital implementation, limited by the time resolution, τ becomes discrete and thus has only a few possible values with $|\tau| < T_c$.
  - Search on all (u, τ) pairs to find the minimum value.

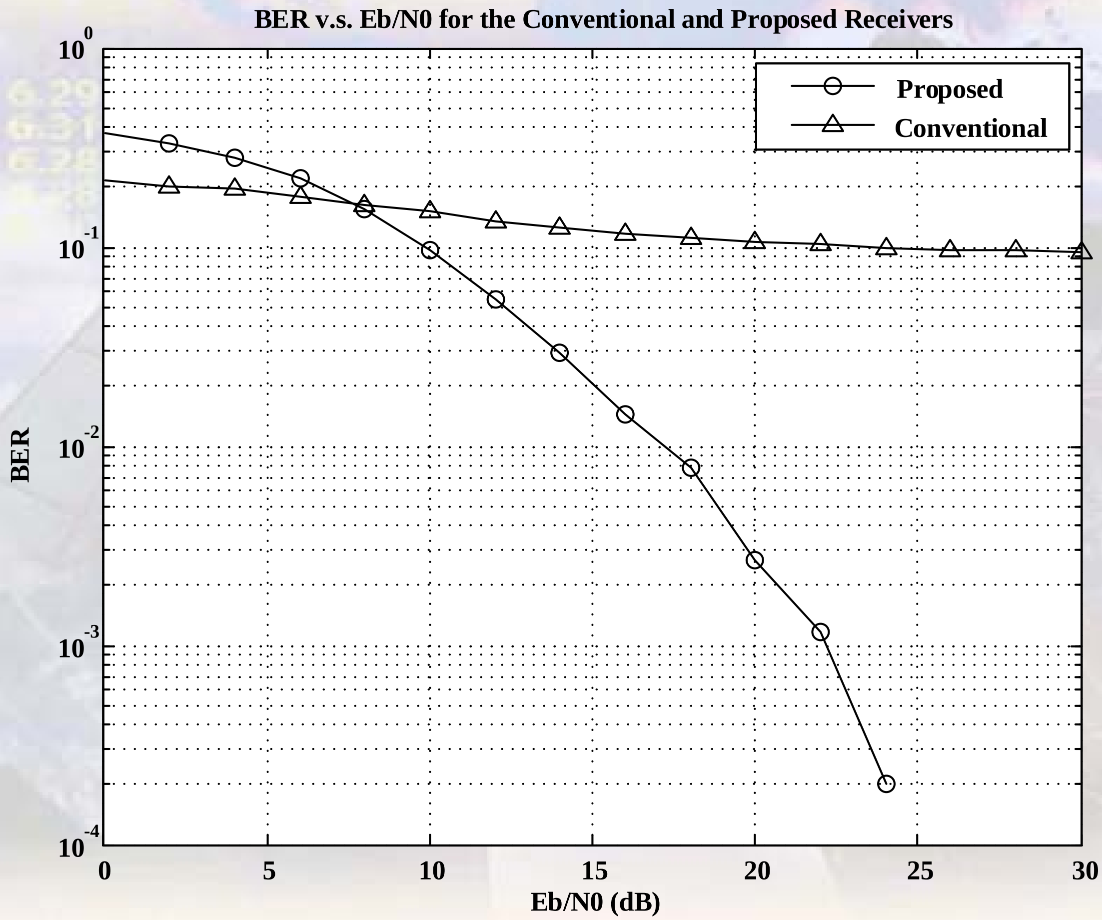
Robust Receiver Design (3/4)

- **Numerical Results: Threats of Disguised Jamming**



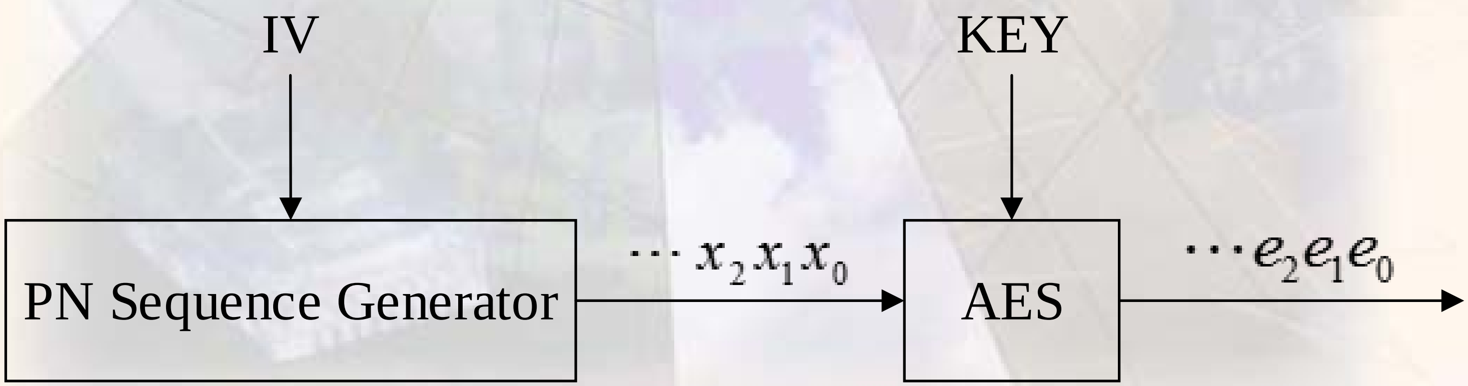
Robust Receiver Design (4/4)

- **Numerical Results: Bit Error Rates**



Secure Scrambling

- **AES-based Secure Scrambling**
  - Generate the scrambling sequence using AES.
  - Cracking AES-based secure scrambling is equivalently breaking AES, which is secure under all known attacks.
- **Secure Scrambling Sequence Generation**



Capacity Analysis (1/3)

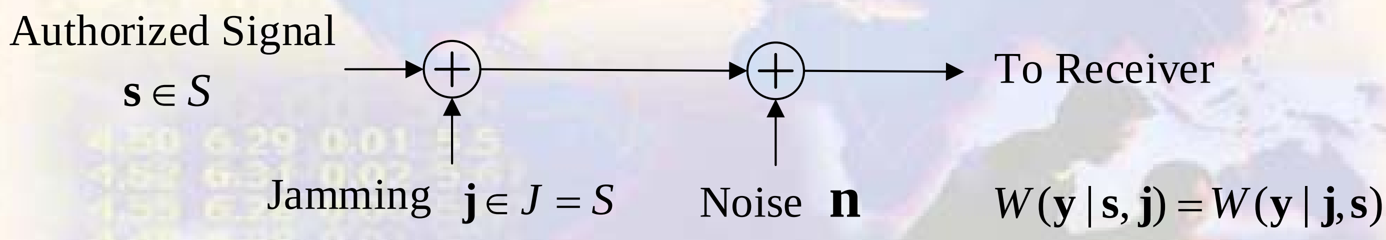
- **Arbitrarily Varying Channel (AVC) Model [6]**
  - An AVC channel model is generally characterized using a kernel $W : \mathcal{S} \times \mathcal{J} \rightarrow \mathcal{Y}$, where $\mathcal{S}$ is the transmitted signal space, $\mathcal{J}$ is the jamming space (i.e., the jamming is viewed as the arbitrarily varying channel states) and $\mathcal{Y}$ is the estimated signal space.
  - For any $\mathbf{s} \in \mathcal{S}$, $\mathbf{j} \in \mathcal{J}$ and $\mathbf{y} \in \mathcal{Y}$, $W(\mathbf{y}|\mathbf{s},\mathbf{j})$ denotes the conditional probability that $\mathbf{y}$ is detected at the receiver, given that $\mathbf{s}$ is the transmitted signal and $\mathbf{j}$ is the jamming.

Capacity Analysis: (2/3)

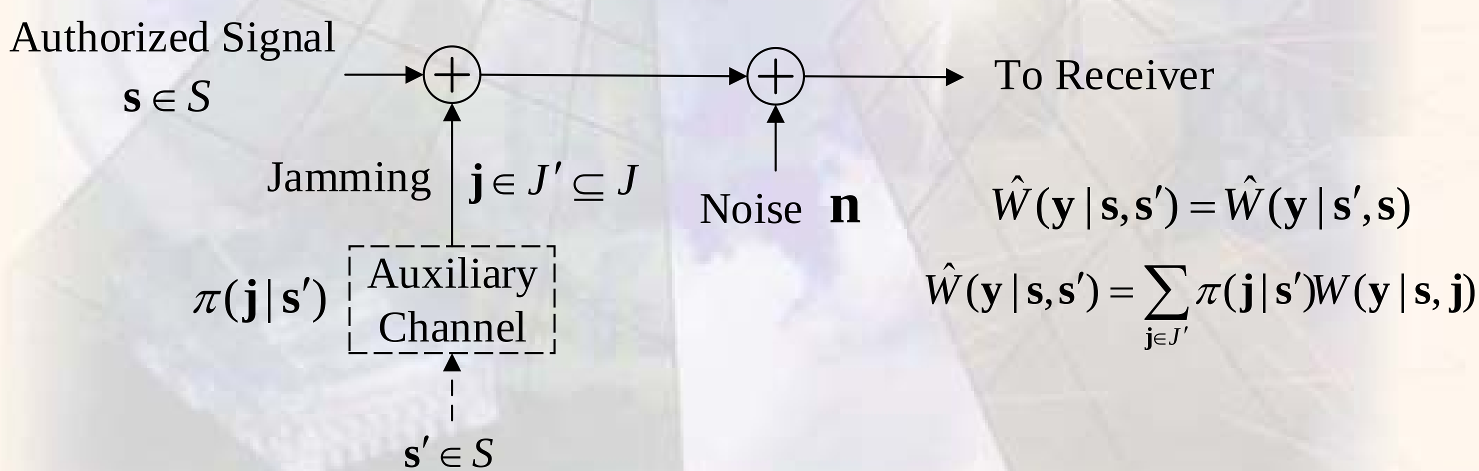
- **Definitions & Theorems**
  - **Definition 1**: The AVC is said to have a symmetric kernel, if $\mathcal{S} = \mathcal{J}$ and $W(\mathbf{y}|\mathbf{s},\mathbf{j}) = W(\mathbf{y}|\mathbf{j},\mathbf{s})$ for any $\mathbf{s},\mathbf{j} \in \mathcal{S}, \mathbf{y} \in \mathcal{Y}$.
  - **Definition 2**: Define $\hat{W} : \mathcal{S} \times \mathcal{S} \rightarrow \mathcal{Y}$ by $\hat{W}(\mathbf{y}|\mathbf{s},\mathbf{s}') \triangleq \sum_{\mathbf{j}\in\mathcal{J}'} \pi(\mathbf{j}|\mathbf{s}')W(\mathbf{y}|\mathbf{s},\mathbf{j})$, where $\pi : \mathcal{S} \rightarrow \mathcal{J}'$ is a probability matrix and $\mathcal{J}' \subseteq \mathcal{J}$. If there exists a $\pi : \mathcal{S} \rightarrow \mathcal{J}'$ such that $\hat{W}(\mathbf{y}|\mathbf{s},\mathbf{s}') = \hat{W}(\mathbf{y}|\mathbf{s}',\mathbf{s}), \forall \mathbf{s},\mathbf{s}' \in \mathcal{S}, \forall \mathbf{y} \in \mathcal{Y}$, then W is said to be symmetrizable.
  - **Existing Result [6]**: The deterministic code capacity of an AVC for the average probability of error is positive if and only if the AVC is neither symmetric nor symmetrizable.

Capacity Analysis (3/3)

- **Symmetric & Symmetrizable Kernels**



(a) Symmetric Kernel



(b) Symmetrizable Kernel

Secure Scrambling: Summary

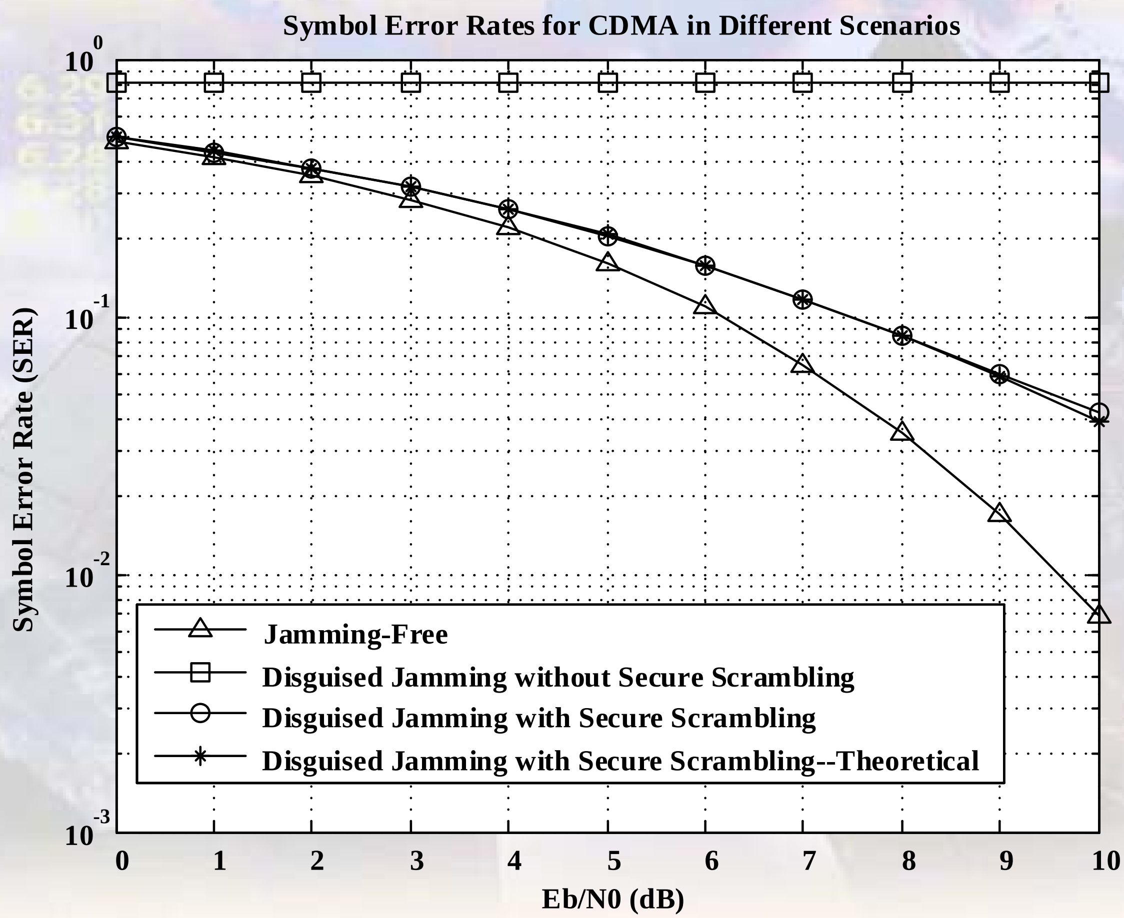
- **Comparison: without v.s. with Secure Scrambling**

Table 1: Comparison of CDMA Systems with and without Secure Scrambling under Disguised Jamming.

	Without S.S.	With S.S.
Symmetric	Yes	No
Symmetrizable	N/A	No
SJNR	N/A	$\frac{N\sigma_s^2}{\lvert v\rvert^2+\sigma_n^2},\ v \in \Omega$
Error Probability	$\geq \frac{M-1}{2M}$	$\frac{1}{\lvert\Omega\rvert}\sum_{v\in\Omega}\mathcal{P}_\Omega\left(\frac{N\sigma_s^2}{\lvert v\rvert^2+\sigma_n^2}\right)$
Capacity	0	$\frac{B}{N}\frac{1}{\lvert\Omega\rvert}\sum_{v\in\Omega}\log_2\left(1+\frac{N\sigma_s^2}{\lvert v\rvert^2+\sigma_n^2}\right)$

Numerical Results

- **Comparison: Symbol Error Rates**



Conclusions

- We designed a novel CDMA receiver that is robust against disguised jamming;
- We developed a secure scrambling scheme to combat disguised jamming in CDMA systems;
- We proved that the capacity of the conventional CDMA systems without secure scrambling under disguised jamming is zero;
- The capacity can be significantly increased when CDMA systems are protected using secure scrambling.

Thank you!

Questions?

References

[1] C.-L. Wang and K.-M. Wu, "A new narrowband interference suppression scheme for spread-spectrum CDMA communications," vol. 49, no. 11, pp. 2832–2838, Nov 2001.

[2] J. Massey, "Shift-register synthesis and BCH decoding," vol. 15, no. 1, pp. 122–127, Jan 1969.

[3] T. Li, Q. Ling, and J. Ren, "Physical layer built-in security analysis and enhancement algorithms for CDMA systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, no. 1, p. 083589, 2007.

[4] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping-part i: System design," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 70 –79, Jan. 2013.

[5] M. Medard, "Capacity of correlated jamming channels," in *Allerton Conference on Communications, Computing and Control*, 1997.

[6] T. Ericson, "Exponential error bounds for random codes in the arbitrarily varying channel," vol. 31, no. 1, pp. 42–48, 1985.

Without Secure Scrambling (1/3)

- **Capacity Analysis: without Secure Scrambling**
  - The authorized signal

$$\mathbf{s} = u\mathbf{c} = [uc_0, uc_1, ..., uc_{N-1}]. \tag{10}$$

  - The disguised jamming

$$\mathbf{j} = v\mathbf{c} = [vc_0, vc_1, ..., vc_{N-1}]. \tag{11}$$

  - The received signal

$$\mathbf{r} = \mathbf{s} + \mathbf{j} + \mathbf{n}. \tag{12}$$

Without Secure Scrambling (2/3)

- **Capacity Analysis: without Secure Scrambling**
  - Define the authorized signal space as $\mathcal{S} = \{u\mathbf{c} | u \in \Omega\}$. It follows immediately that the disguised jamming space

$$\mathcal{J} = \{v\mathbf{c} | v \in \Omega\} = \mathcal{S}. \tag{13}$$

  - The CDMA system under disguised jamming can be modeled as an AVC channel characterized by the probability matrix

$$W_0 : \mathcal{S} \times \mathcal{S} \to \Omega, \tag{14}$$

    where $W_0(\hat{u}|\mathbf{s}, \mathbf{j})$ the conditional probability that $\hat{u}$ is estimated given that the authorized signal is $\mathbf{s} \in \mathcal{S}$, and the disguised jamming is $\mathbf{j} \in \mathcal{S}$.

Without Secure Scrambling (3/3)

- **Capacity Analysis: without Secure Scrambling**
  - The jamming and the authorized signal are fully symmetric as they are generated from exactly the same space $\mathcal{S}$.
  - Note that the recovery of the authorized symbol is fully based on **r** in (12), so we further have

$$W_0(\hat{u}|\mathbf{s}, \mathbf{j}) = W_0(\hat{u}|\mathbf{j}, \mathbf{s}). \tag{15}$$

- **Results for CDMA without Secure Scrambling**
  - Under disguised jamming, the kernel of the AVC corresponding to a CDMA system without secure scrambling, W_0, is symmetric.
  - Under disguised jamming, the deterministic capacity of a CDMA system without secure scrambling is zero!!!

With Secure Scrambling (1/6)

- **Capacity Analysis: with Secure Scrambling**
  - When the coding information of the authorized user is securely hidden from the jammer, the best the jammer can do would be using a randomly generated spreading sequence.
  - Define $\mathcal{D} = \{[d_0, d_1, ..., d_{N-1}] | d_n = \pm 1, \ \forall n\}$, and denote the randomly generated spreading sequence by $\mathbf{d} \in \mathcal{D}$, the chip-rate jamming can be represented as

$$\mathbf{j} = v\mathbf{d} = [vd_0, vd_1, ..., vd_{N-1}], \tag{16}$$

    where $v \in \Omega$ is the fake symbol.
  - The jamming space now becomes

$$\mathcal{J} = \{v\mathbf{d} | v \in \Omega, \mathbf{d} \in \mathcal{D}\}. \tag{17}$$

With Secure Scrambling (2/6)

- **Capacity Analysis: with Secure Scrambling**
  - Without the coding information $\mathbf{c}$, the jamming, $\mathbf{j}$, can only be generated from a space much larger than the authorized signal space. More specifically, $\mathcal{J} \supset \mathcal{S}$.
  - With the jamming space $\mathcal{J}$ as defined in (17), the AVC corresponding to the CDMA system with secure scrambling can be characterized by

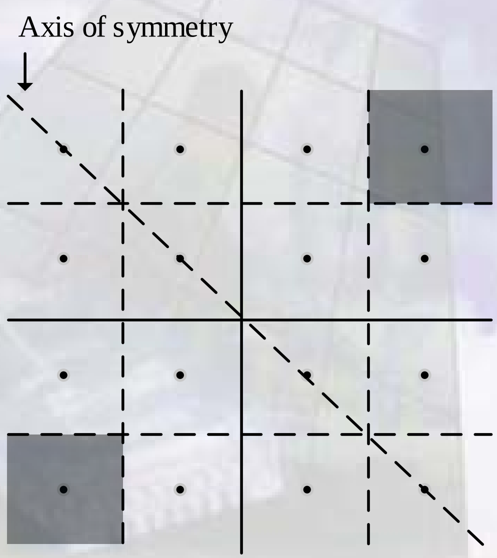
$$W : \mathcal{S} \times \mathcal{J} \to \Omega. \tag{18}$$

With Secure Scrambling (3/6)

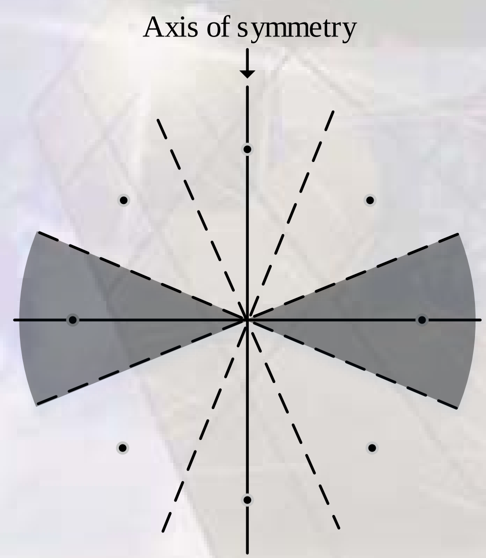
- **Capacity Analysis: with Secure Scrambling**
  - Since $\mathcal{J} \neq \mathcal{S}$, under disguised jamming, the kernel of the AVC corresponding to a CDMA system with secure scrambling, W, is nonsymmetric.
- **Stronger Result: Nonsymmetrizable**
  - According to Definition 2, we need to show that for any probability matrix $\pi : \mathcal{S} \to \mathcal{J}$, there exists some $\mathbf{s}_0, \mathbf{s}'_0 \in \mathcal{S}$ and $\hat{u}_0 \in \Omega$, such that
$$\hat{W}(\hat{u}_0|\mathbf{s}_0, \mathbf{s}'_0) \neq \hat{W}(\hat{u}_0|\mathbf{s}'_0, \mathbf{s}_0), \tag{19}$$
where $\hat{W}(\hat{u}|\mathbf{s}, \mathbf{s}') \triangleq \sum_{\mathbf{j}\in\mathcal{J}} \pi(\mathbf{j}|\mathbf{s}')W(\hat{u}|\mathbf{s}, \mathbf{j})$.

With Secure Scrambling (4/6)

- **Proof: Nonsymmetrizable**
  - We pick $\mathbf{s}_0 = u\mathbf{c}$, $\mathbf{s}'_0 = -u\mathbf{c}$, $\hat{u}_1 = u$ and $\hat{u}_2 = -u$. Note that "u" is picked such that $R(u)$ and $R(-u)$ are axial symmetric, and $|u| \geq |v|$, $\forall v \in \Omega$.



16QAM



8PSK

With Secure Scrambling (5/6)

- **Proof: Nonsymmetrizable**
  - The idea is to prove that $\hat{W}(\hat{u}_1|\mathbf{s}_0, \mathbf{s}_0') = \hat{W}(\hat{u}_1|\mathbf{s}_0', \mathbf{s}_0)$ and $\hat{W}(\hat{u}_2|\mathbf{s}_0, \mathbf{s}_0') = \hat{W}(\hat{u}_2|\mathbf{s}_0', \mathbf{s}_0)$ cannot hold simultaneously, by showing that

$$\hat{W}(\hat{u}_1|\mathbf{s}_0, \mathbf{s}_0') - \hat{W}(\hat{u}_2|\mathbf{s}_0, \mathbf{s}_0') > \hat{W}(\hat{u}_1|\mathbf{s}_0', \mathbf{s}_0) - \hat{W}(\hat{u}_2|\mathbf{s}_0', \mathbf{s}_0). \tag{20}$$

  - Following the definition of $\hat{W}$, we have

$$\begin{aligned} &\hat{W}(\hat{u}_1|\mathbf{s}_0, \mathbf{s}_0') - \hat{W}(\hat{u}_2|\mathbf{s}_0, \mathbf{s}_0') \\ &= \sum_{\mathbf{j}\in\mathcal{J}} \pi(\mathbf{j}|\mathbf{s}_0')[W(\hat{u}_1|\mathbf{s}_0, \mathbf{j}) - W(\hat{u}_2|\mathbf{s}_0, \mathbf{j})] > 0. \end{aligned} \tag{21}$$

With Secure Scrambling (6/6)

- **Proof: Nonsymmetrizable**
  - A complete proof that the kernel, W, is nonsymmetrizable can be found in our journal paper.
- **Results for CDMA with Secure Scrambling**
  - Under disguised jamming, the kernel of the AVC corresponding to a CDMA system with secure scrambling, W, is neither symmetric nor symmetrizable.
  - Under disguised jamming, the deterministic capacity of a CDMA system with secure scrambling is NOT zero.