第二讲 向量空间

贺丽君
信息与通信工程学院
Email: lijunhe@mail.xjtu.edu.cn
2022-02

内容提要

- 向量空间与子空间
- 列空间与零空间
- 零空间在保密通信中的应用

内容提要

- 向量空间与子空间
- 列空间与零空间
- 零空间在保密通信中的应用

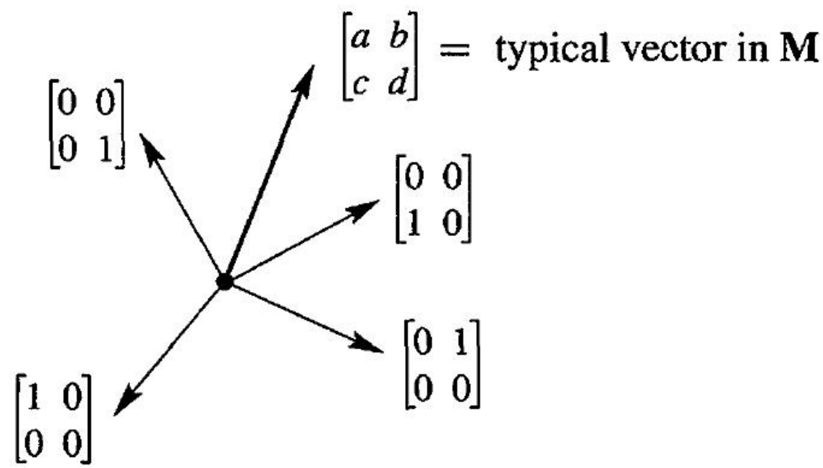
向量空间

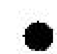
- 向量空间
  - 设V是若干向量的集合，V非空且对加法和数乘运算封闭，则集合V称为向量空间
  - 向量空间也称为线性空间
  - 任何向量空间必包含零向量
  - $\mathbf{R}^n$：具有n个实分量的列向量v的全体
  - $\mathbf{R}^2$：二维平面；$\mathbf{R}^3$：几何空间

向量空间

➢ 其他形式的向量空间

- M：所有2×2实矩阵的全体
- F：所有实函数$f(x)$的全体
- Z：仅由零向量构成的向量空间





smallest vector space
zero vector only

子空间 (Subspace)

➢ 子空间的定义

一个向量空间的子空间由该向量空间的一些向量组成(包含零向量)，且满足如下条件：如果v和w在该子空间内且c为任意标量，则

(1) v+w在该子空间内；

(2) cv在该子空间内。

子空间

- 子空间的例子
  - L：任何一条过(0,0,0)点的直线
  - P：任何一个过(0,0,0)点的平面
  - Z：零向量(0,0,0)构成的单点集
  - R^3：整个三维空间
  - Q：二维平面上的第一象限
  - U：所有2×2的上三角矩阵

张成子空间

不一定是子空间！

S ＝ 向量空间V中的一个向量集合

SS＝ S中向量的所有线性组合

＝ all $c_1\mathbf{v}_1+\ldots+c_N\mathbf{v}_N$

＝ 由S张成的V的子空间

SS是包含S的最小的子空间

内容提要

- 向量空间与子空间
- 列空间与零空间
- 零空间在保密通信中的应用

列空间 (Column Space)

- 列空间的定义

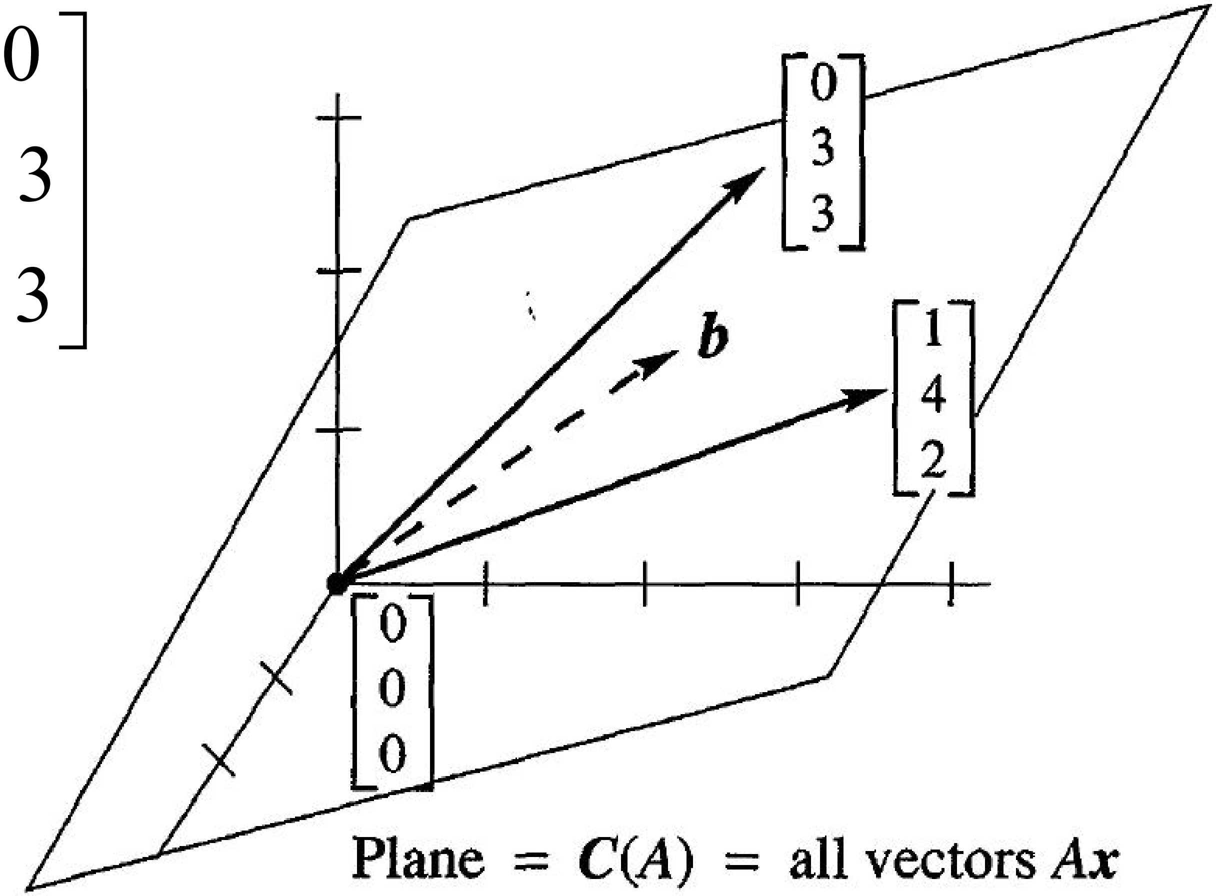
矩阵A的列空间 (记作$C(A)$)由该矩阵各列的**所有线性组合**组成，即所有可能的向量Ax

- 两点说明

  - Ax=b有解的充要条件是b在A的列空间内
  - 若A为$m \times n$矩阵，则$C(A)$是R^m的子空间

列空间

$$\mathbf{A}=\begin{bmatrix}1 & 0\\ 4 & 3\\ 2 & 3\end{bmatrix}$$



零空间 (Nullspace)

- 零空间的定义

  线性方程组Ax=0的全部解构成矩阵A的零空间，用$N(A)$表示。

- 几点说明

  - 如果b不为0，则Ax=b的解不构成子空间
  - 若A为$m \times n$矩阵，则$N(A)$是R^n的子空间
  - 若A为可逆矩阵，则$N(A)=Z$

零空间

例 1

$$\mathbf{A}=\begin{bmatrix}1 & 2\\ 3 & 6\end{bmatrix} \qquad N(\mathbf{A})=c\begin{bmatrix}-2\\ 1\end{bmatrix}$$

例 2

$$\mathbf{A}=\begin{bmatrix}1 & 2 & 3\end{bmatrix} \qquad N(\mathbf{A})=c_1\begin{bmatrix}-2\\ 1\\ 0\end{bmatrix}+c_2\begin{bmatrix}-3\\ 0\\ 1\end{bmatrix}$$

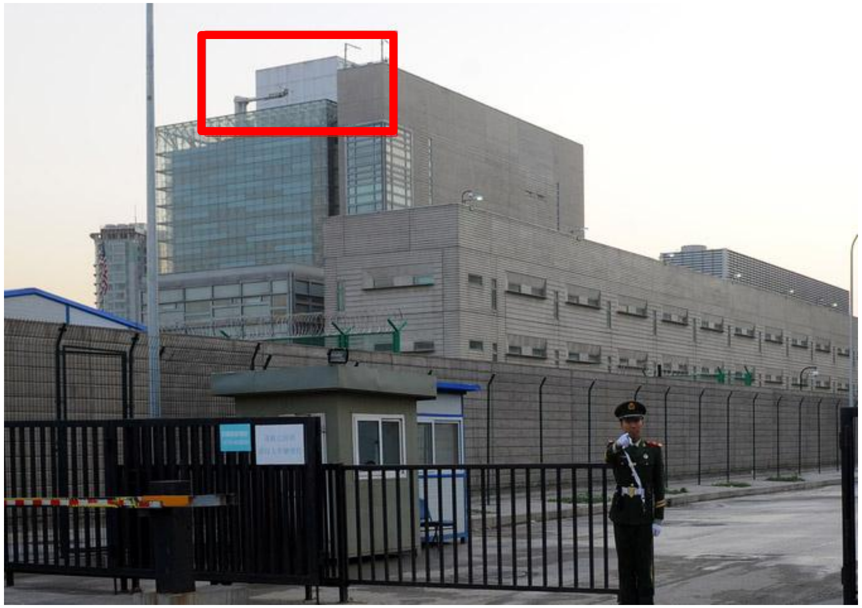
例 3

$$\mathbf{A}=\begin{bmatrix}1 & 2\\ 3 & 8\end{bmatrix} \qquad N(\mathbf{A})=\mathbf{Z}$$

内容提要

- 向量空间与子空间
- 列空间与零空间
- 零空间在保密通信中的应用

无线网络安全面临的挑战



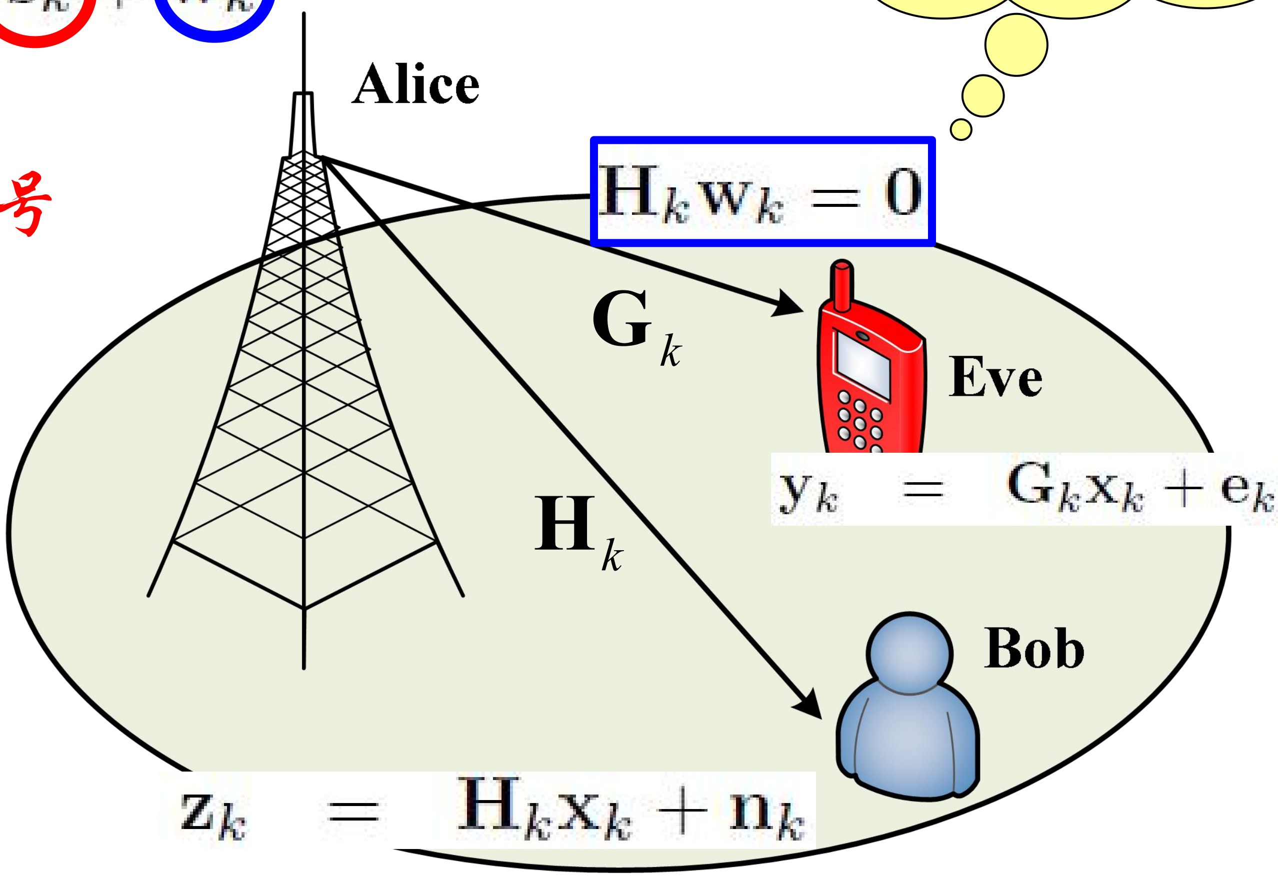
单纯依赖于加密的网络安全协议无法保障通信系统的传输安全性！

新型保密通信技术

$\mathbf{x}_k = \mathbf{s}_k + \mathbf{w}_k$ → 发送端人

信息信号

在合法用户信道的零空间注入人工噪声



注入人工噪声防窃听：1.窃听者在哪？2.如何不影响合法用户

新型保密通信技术

$\mathbf{x}_k = \mathbf{s}_k + \mathbf{w}_k$ → 发送端人工噪声

信息信号

$\mathbf{s}_k = \boxed{\mathbf{p}_k} u_k$

天线分配系数

$\boxed{\mathbf{H}_k \mathbf{p}_k \neq 0}$

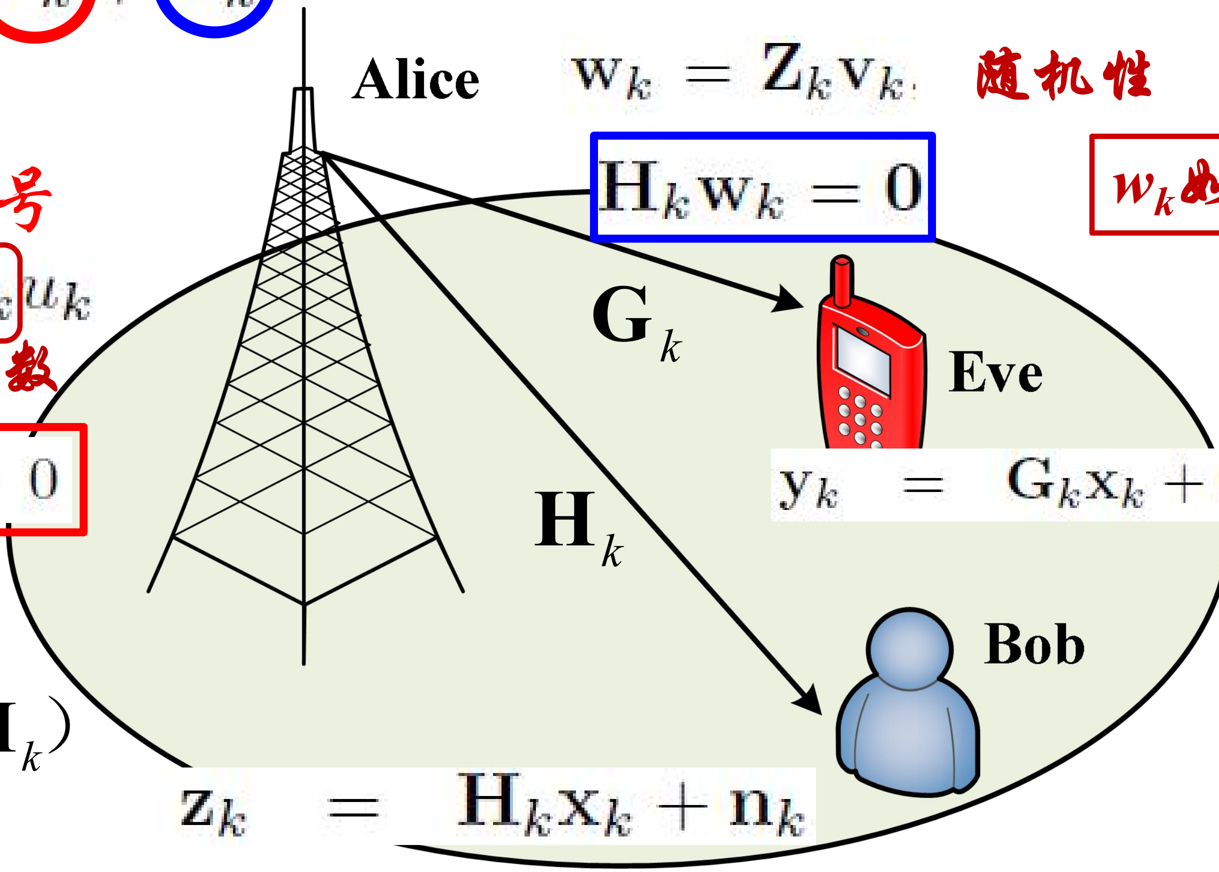
$\Downarrow$

$\mathbf{p}_k \perp N(\mathbf{H}_k)$

$\mathbf{w}_k = \mathbf{Z}_k \mathbf{v}_k$ 随机性

$\boxed{\mathbf{H}_k \mathbf{w}_k = 0}$

$\boxed{w_k \text{如何取？}}$



$\mathbf{y}_k = \mathbf{G}_k \mathbf{x}_k + \mathbf{e}_k$

$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{n}_k$

注入人工噪声防窃听：1.窃听者在哪？2.如何不影响合法用户

新型保密通信技术

$$\mathbf{x}_k = \mathbf{s}_k + \mathbf{w}_k$$

→ 发送端人工噪声

$$\mathbf{w}_k = \mathbf{Z}_k \mathbf{v}_k$$

随机性

$$\boxed{\mathbf{H}_k \mathbf{w}_k = 0}$$

$\boxed{w_k\text{如何取？}}$

信息信号

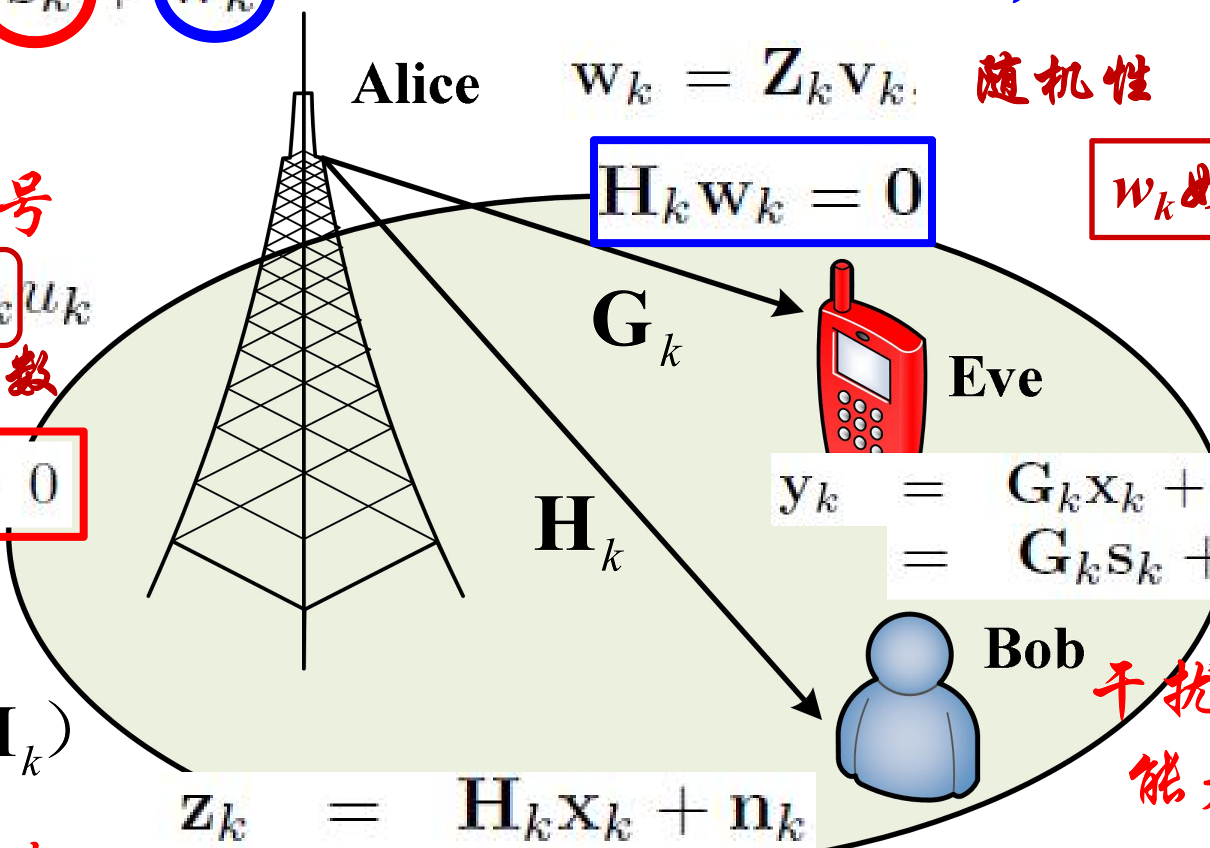
$$\mathbf{s}_k = \boxed{\mathbf{p}_k} u_k$$

天线分配系数

$$\boxed{\mathbf{H}_k \mathbf{p}_k \neq 0}$$

$$\Downarrow$$

$$\mathbf{p}_k \perp N(\mathbf{H}_k)$$



$$\begin{aligned} \mathbf{y}_k &= \mathbf{G}_k \mathbf{x}_k + \mathbf{e}_k \\ &= \mathbf{G}_k \mathbf{s}_k + \underline{\mathbf{G}_k \mathbf{w}_k} + e_k \end{aligned}$$

干扰受限，性能严重恶化

$$\begin{aligned} \mathbf{z}_k &= \mathbf{H}_k \mathbf{x}_k + \mathbf{n}_k \\ &= \mathbf{H}_k \mathbf{s}_k + n_k \end{aligned}$$

传输可靠性不受影响

谢谢大家！