Detection with Binary Wireless Sensors

Sotaro Osanai ... *,
* Doshisha University, Kyoto,610-0321, Japan, (e-mail: jcheng@ieee.org)

***Abstract*—**

I. Introduction

II. System model

There are a total of K binary sensors. Each sensor detects its corresponding targets' status, active or inactive. The activity of users is time-variable. At time t, suppose that there are at most T ($T << K$) active targets. Denote by $\mathcal{T} \subset \{1, 2, \ldots, K\}$ the corresponding active sensor set. The k-th active node will transmit the its active status $b^{(k)} \in \{0, 1\}$ to the sink node.

In our communication scenario, we assign the k-th sensor a length-N signature sequence

$$\begin{aligned} \boldsymbol{s}^{(k)} &= (s_1^{(k)}, s_2^{(k)}, ..., s_N^{(k)})^{\mathtt{T}}, \\ & k = 1, 2, \ldots, K, \text{ and } s_n^{(k)} \in \{0, 1\}. \end{aligned}$$

For the status vector $\boldsymbol{b} = (b^1, b^2, \ldots, b^K)$, its (Hamming) weight satisfies

$$w(\boldsymbol{b}) \leq T$$

by assumption, where $w(\boldsymbol{b}) = \sum_{n=1}^{N} |b_n|$. Before each transmission, the active sensors estimate their channel state information (CSI) i.e., channel coefficients $\hat{h}^{(k)}$, from the pilot signals sent from the sink node. After channel estimation, the active sensors will transmit their statuses to the sink node. The active user's statuses are modulated to their signature sequences $\boldsymbol{s}^{(k)}$, while inactive users send $\mathbf{0}$, i.e., no-energy transmission. Then each modulated signature sequence will be pre-equalized by multiplying its estimated channel coefficients $\hat{h}^{(k)}$ and its transmit power $\sqrt{E_s}$. Let $h^{(k)}$ be the channel coefficient from the k-th user to sink node, which remains constant during N chips transmission. Over the multiple-access channel, each active user's transmission signal $\boldsymbol{s}^{(k)}$ is multiplied by the channel coefficient $h^{(k)}$.

In the receiver, the signals from active users are superposed. Gaussian noise $\boldsymbol{z}$ is added to the superposed signal, and received signal $\boldsymbol{y} = (y_1, y_2, ..., y_N)^{\mathtt{T}}$ is generated. Here we assume the block and chip synchronization between sensors. The received vector $\boldsymbol{y}$ from K users, including inactive users, can be written as

$$y_n = \sum_{k=1}^{K} b^{(k)} \sqrt{E_s} \bar{h}^{(k)} s_n^{(k)} + z_n, \quad n = 1, 2, ..., N \quad (1)$$

Here, $z_n \sim \mathcal{N}(0, \frac{N_0}{2})$, $n = 1, 2, \ldots, N$, are i.i.d zero-mean Gaussian variables with one-side power spectral density N_0.

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{bmatrix} = \begin{bmatrix} s_1^{(1)} & s_1^{(2)} & \ldots & s_1^{(K)} \\ s_2^{(1)} & s_2^{(2)} & \ldots & s_2^{(K)} \\ \vdots & \vdots & \ddots & \vdots \\ s_N^{(1)} & s_N^{(2)} & \ldots & s_N^{(K)} \end{bmatrix} \begin{bmatrix} b^{(1)}\sqrt{E_s}\bar{h}^{(1)} \\ b^{(2)}\sqrt{E_s}\bar{h}^{(2)} \\ \vdots \\ b^{(K)}\sqrt{E_s}\bar{h}^{(K)} \end{bmatrix} + \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_N \end{bmatrix}.$$

$$\boldsymbol{y} = \sqrt{E_s} S \bar{H} \boldsymbol{b} + \boldsymbol{z} \quad (2)$$

where $\bar{H} = \mathrm{diag}(\bar{h}^1, \bar{h}^2, \ldots, \bar{h}^K)$. Here $\bar{h}^{(k)} = h^{(k)}/\hat{h}^{(k)}$. We will detect of sensor statuses $b^{(k)}$, $k = 1, 2, \ldots, K$.

III. ML Detection

Base on $\boldsymbol{y}$, the receiver performs ML decoding (by full search) to recover the signature sequences

$$\hat{\boldsymbol{b}} = \underset{w(\boldsymbol{b}) \leq T}{\arg\max}\, \mathtt{Pr}(\boldsymbol{y}|\boldsymbol{b}) \quad (3)$$

$$= \underset{w(\boldsymbol{b}) \leq T}{\arg\min} \left(\sum_{n=1}^{N} \left(y_n - \sum_{k=1}^{K} b^{(k)} \sqrt{E_s} \bar{h}^{(k)} s_n^{(k)} \right)^2 \right) \quad (4)$$

IV. Multiuser Code Distance and Performance Bound

A. Multiuser Code Distance

We assume that each sensor node has perfect CSI, i.e., $\bar{h}(k) = 1$. We define the K-user code by

$$\mathcal{C} = \{\boldsymbol{c} = S\boldsymbol{b} | \boldsymbol{b} \in \{0, 1\}^K, w(\boldsymbol{b}) \neq T\}.$$

The node status vector $\boldsymbol{b}$ can be seen as the K-user message.

The squared distance of two K-user codewords:

$$d^2(\boldsymbol{c}, \boldsymbol{c}') = ||\boldsymbol{c} - \boldsymbol{c}'||_2^2 = \sum_{n=1}^{N} (c_n - c_n')^2 \quad (5)$$

or

$$d^2(S\boldsymbol{b}, S\boldsymbol{b}') = ||S(\boldsymbol{b} - \boldsymbol{b}')||_2^2 \quad (6)$$

$$= \sum_{n=1}^{N} \left(\sum_{k=1}^{K} s_n^{(k)} (b^{(k)} - b'^{(k)}) \right)^2 \quad (7)$$

where $||\boldsymbol{x}||_2 = \sqrt{x_1^2 + x_2^2 + \cdots + x_N^2}$ is Euclidean norm. Note that the squared distance is an integer in set $\{0, 1, \ldots, NT^2\}$.

The minimum squared distance of K-user code $\mathcal{C}$:

$$d^2_{\min} = \min_{\substack{\boldsymbol{b},\boldsymbol{b}'\in\{0,1\}^K \\ w(\boldsymbol{b})<T, w(\boldsymbol{b}')<T \\ \boldsymbol{b}\neq\boldsymbol{b}'}} d^2(S\boldsymbol{b}, S\boldsymbol{b}') \tag{8}$$

Distance enumerator $A_d(\boldsymbol{c})$, $d = 0, 1, \ldots, NT^2$, of codeword $\boldsymbol{c}$ in K-user code $\mathcal{C}$ is the number of codewords in $\mathcal{C}$ unequal to $\boldsymbol{c}$ and with distance d from $\boldsymbol{c}$.

Note that the distance enumerator here is defined for a specific K-user codeword. This is different from the definition for a single-user (linear) code, where all the codewords share the same distance enumerator.

The distance enumerating function is defined as

$$A(\boldsymbol{c}, D) = \sum_{i=0}^{NT^2} A_i(\boldsymbol{c}) D^i. \tag{9}$$

Example 1: Let $K = 4$, $N = 3$,and $T = 4$. Let the signature matrix be

$$S_4 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \tag{10}$$

which is in the transpose form of [1, Eq. (3)]. The 4-user code is

$$\mathcal{C} = \{(0,0,0)^{\mathrm{T}}, (1,0,1)^{\mathrm{T}}, \ldots, (2,2,3)^{\mathrm{T}}\}.$$

We give the distance enumerating functions of all the 16 codewords.

$A(\boldsymbol{c}_1, D) =?$
$A(\boldsymbol{c}_2, D) =?$
$\vdots$
$A(\boldsymbol{c}_{16}, D) =?$

□

Example 2: $K = N = T = 4$, Hadamard matrix of order 4.

$$S_{\mathrm{H4}} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \tag{11}$$

$A(\boldsymbol{c}_1, D) =?$

□

Example 3: $K = 12$, $N = 7$, $T = 12$. The signature matrix S_{12} is

$$S_{12} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{12}$$

which is in the transpose form of [1, Ex. 3].

$A(\boldsymbol{c}_1, D) =?$

□

B. Union Bound

Let $\boldsymbol{c} = S\boldsymbol{b}$, $\boldsymbol{e} = S\boldsymbol{b}'$.

$$\begin{aligned} \mathrm{P_W} &\triangleq \Pr(\hat{\boldsymbol{c}} \neq \boldsymbol{c}) \\ &\leq \sum_{\boldsymbol{c},\boldsymbol{e}\in\mathcal{C},\boldsymbol{c}\neq\boldsymbol{e}} \Pr(\boldsymbol{c} \to \boldsymbol{e}) \\ &= \sum_{\boldsymbol{c},\boldsymbol{e}\in\mathcal{C},\boldsymbol{c}\neq\boldsymbol{e}} \Pr\left(\sum_{n=1}^{N}(y_n - \sqrt{E_s}c_n)^2 \geq \sum_{n=1}^{N}(y_n - \sqrt{E_s}e_n)^2\right) \\ &= \sum_{\boldsymbol{c},\boldsymbol{e}\in\mathcal{C},\boldsymbol{c}\neq\boldsymbol{e}} \Pr\left(\sum_{n=1}^{N}(e_n - c_n)z_n \geq \frac{\sqrt{E_s}}{2}\sum_{n=1}^{N}(c_n - e_n)^2\right) \end{aligned}$$

Since

$$\sum_{n=1}^{N}(e_n - c_n)z_n \begin{cases} \sim \mathcal{N}(0, d^2(\boldsymbol{c},\boldsymbol{e})\frac{N_0}{2}), & \text{for } d(\boldsymbol{c},\boldsymbol{e}) \neq 0 \\ = 0, & \text{for } d(\boldsymbol{c},\boldsymbol{e}) = 0 \end{cases} \tag{13}$$

we have

$$\mathrm{P_W} \leq A_0(\boldsymbol{c}) + \sum_{d=1}^{NT^2} A_d(\boldsymbol{c}) Q\left(\sqrt{\frac{d^2 E_s}{2N_0}}\right) \tag{14}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-t^2/2}dt$ with $x \geq 0$. ($Q(x) = \frac{1}{2}\mathrm{erfc}(\frac{x}{\sqrt{2}})$, where erfc is the complementary error function.)

Let's consider the energy of one information bit (node status) E_b related to the energy E_s. An exact calculation of E_b will average over the various number of active nodes from 0 to T. In our analysis, for convenience, we only consider the case that number of active nodes are constant T, but at anytime different T nodes out of K are active.

Let $\dot{\boldsymbol{c}}_m$, $m = 1, 2, \ldots, M = \binom{K}{T}$, be the super codewords, which are formed from any T active nodes. Denote by $E_m = \sum_{n=1}^{N}|\dot{c}_{mn}|^2 E_s$ the energy that transmit the m-th codeword. The average energy of each codeword is thus

$$E_{\mathrm{A}} = \frac{1}{M}\sum_{m=1}^{M} E_m^T = \frac{1}{M}\sum_{m=1}^{M}\sum_{n=1}^{N}|\dot{c}_{mn}|^2 E_s.$$

Since $TE_b = E_{\mathrm{A}}$, we have

$$E_s = R' E_b$$

with

$$R' = T/\left(\frac{1}{M}\sum_{m=1}^{M}\sum_{n=1}^{N}|\dot{c}_{mn}|^2\right).$$

Let $R'_{\mathrm{sum}} = TR'$. It follows

$$\mathrm{P_W} \leq A_0(\boldsymbol{c}) + \sum_{d=1}^{NT^2} A_d(\boldsymbol{c}) Q\left(\sqrt{\frac{d^2 R'_{\mathrm{sum}} E_b}{2TN_0}}\right). \tag{15}$$

Note that true rate of each node is $R = 1/N$ and sum rate is $R_{\mathrm{sum}} = TR = T/N$.

Note that the term of 0-distance enumerator $A_0(\boldsymbol{c})$ does not exist if the multi-user code is uniquely decodable (UD). Using the smallest value of d for a K-user code $\mathcal{C}$, i.e., its

minimum distance $d_{\min}$, $\mathrm{P_W}$ for larger E_b/N_0 values can be approximated as

$$\mathrm{P_W} \approx A_{d_{\min}}(\boldsymbol{c}) Q\left(\sqrt{\frac{d_{\min}^2 R'_{\mathrm{sum}} E_b}{2TN_0}}\right). \tag{16}$$

Remark 1: In the case of $s_j \in \{-1, 1\}$, $E_s = RE_b$. Then we have

$$\mathrm{P_W} \le A_0(\boldsymbol{c}) + \sum_{d=1}^{NT^2} A_d(\boldsymbol{c}) Q\left(\sqrt{\frac{d^2 R_{\mathrm{sum}} E_b}{2TN_0}}\right). \tag{17}$$

$$\mathrm{P_W} \approx A_{d_{\min}}(\boldsymbol{c}) Q\left(\sqrt{\frac{d_{\min}^2 R_{\mathrm{sum}} E_b}{2TN_0}}\right). \tag{18}$$

□

V. Conclusion

Appendix A
Lindström's Binary Signature matrices [7] [8, pp. 196-198]

Let p be a prime, and $q = p^s$ be a prime power. Lindström gave a q-user signature code where at most T users are active. (We assume that $K = q$ here).

Let $\beta_i \in \mathrm{GF}(q)$, $i = 1, 2, \ldots, q$, and $\alpha \in \mathrm{GF}(q^T)$ be the prime element of extension field $\mathrm{GF}(q^T)$. Let v_i, $i = 1, 2, \ldots, q$, be integer such that

$$\alpha^{v_i} = \alpha + \beta_i, \quad i = 1, 2, \ldots, q.$$

Note that $\alpha + \beta_i \neq 0$, $\alpha + \beta_i \neq 1$, and $0 < v_i < q^T - 1$.

Theorem 1 ([7]): Let $a_i, b_i \in \{1, 2, \ldots, q\}$ and $a_i \neq a_j$ if $i \neq j$ and $b_i \neq b_j$ if $i \neq j$. the following equation, for $0 \le t \le T$,

$$\begin{aligned}(\alpha + \beta_{a_1})(\alpha + \beta_{a_2}) \cdots (\alpha + \beta_{a_t}) \\ = \quad (\alpha + \beta_{b_1})(\alpha + \beta_{b_2}) \cdots (\alpha + \beta_{b_t})\end{aligned} \tag{19}$$

implies

$$(a_1, a_2, \ldots, a_t) = (b_1, b_2, \ldots, b_t). \tag{20}$$

□

Proof: We rewrite (19) as $f(\alpha) = 0$, which is a polynomial of α with degree at most $t-1$, ($0 \le t \le T$), and the coefficients over $\mathrm{GF}(q)$. Since α is the prime element of $\mathrm{GF}(q^T)$, i.e., the α is a root of an irreducible polynomial of degree T and thus can't satisfy such polynomial $f(\alpha)$. It implies that (20) satisfies. This proves the theorem. □

We rewrite (19) as

$$\alpha^{\sum_{i=1}^{t} v_{a_i}} = \alpha^{\sum_{i=1}^{t} v_{b_i}}. \tag{21}$$

By Theorem 1, for $\forall v_{a_i}, v_{b_i} \in \{v | \alpha^v = \alpha + \beta, \forall \beta \in \mathrm{GF}(q)\}$,

$$\sum_{i=1}^{t} v_{a_i} = \sum_{i=1}^{t} v_{b_i}, \quad 0 \le t \le T, \tag{22}$$

implies

$$(v_{a_1}, v_{a_2}, \ldots, v_{a_t}) = (v_{b_1}, v_{b_2}, \ldots, v_{b_t}).$$

Let $\boldsymbol{s}'_j$ be the binary representations of the numbers v_j. We prefix $\boldsymbol{s}'_j$ with additional digit 1, and obtain codewords $\boldsymbol{s}_j = (1, (\boldsymbol{s}'_j)^{\mathrm{T}})^{\mathrm{T}}$. The reason of prefixing the additional 1 is that in Theorem 1, the constant t is known. This means that in the decoding from the output of the channel, we must to know how many users are active. The sum of the first bits of signature codewords gives the number of active users t, $0 \le t \le Tt$.

The code length of the binary signature code is

$$\begin{aligned} n(q, T) &= \lceil \log(q^T - 1) \rceil + 1 \\ &\le T \log q + 2. \end{aligned}$$

Lindström's Binary Signature Codes (T-out-of-q)

The signature codewords (q: prime power)

$$\boldsymbol{s}_i, \quad i = 1, 2, \ldots q$$

are the binary representations of numbers

$$\forall v_i \in \{v | \alpha^v = \alpha + \beta, \forall \beta \in \mathrm{GF}(q)\}$$

with digital 1 prefixed, where $\alpha \in \mathrm{GF}(q^T)$ is prime element of $\mathrm{GF}(q^T)$.

Example 4: Lindström's binary signature matrix with $K = q = 2^3$, $T = 3$ is ....

□

REFERENCES

[1] J. Cheng, "Signature codes, coin-weighing problem, and user identification in communication systems," Doshisha ... vol. 60, pp. 1-6, March 2019.

[2] C. Schlegel, *Coordinated Multiuser Communications*, Springer, the Netherlands, 2010.

[3] S. J. Johnson, *Iterative Error Correction: Turbo, Low-Density Parity-Check and Repeat-Accumulate Codes*, Cambridge, U.K.: Cambridge Univ. Press, 2010.

[4] S. Verdu, *Multiuser Detection*, Cambridge, U.K.: Cambridge Univ. Press, 1998.

[5] G. Song, X. Wang, and J. Cheng, "Signature design of sparsely spread code division multiple access based on superposed constellation distance analysis," *IEEE Access*, vol. 5, pp. 23809-23821, Oct. 2017.

[6] J. Cheng, T. Ohira, K. Kamoi, and Y. Watanabe, "Spreading set with error correction for multiple-access adder channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5524-5529, Dec. 2006.

[7] B. Lindström, "Determining subsets by unramified experiments," in A Survey of statistical Design and Linear Models, J. N. Srivastava, ed. North-Holland, New York, 1975.

[8] L. Györfi, S. Győri, B. Laczay, M. Ruszinkó, *Lectures on Multiple Access Channels*, http://www.szit.bme.hu/~gyori/AFOSR_05/book.pdf.