โครงการวิจัยย่อยลำดับที่ 10

เรื่อง การประเมินช่องสัญญาณที่มีแหล่งจ่ายรวมในช่องการสื่อสารที่เกิดการเฟดดิง ปีที่ 4

1. ผู้รับผิดชอบโครงการ รศ.ดร. ประสิทธิ์ ทีฆพุฒิ

2. วัตถุประสงค์

- เพื่อออกแบบวิจัยและพัฒนาเครื่องรับชนิดเทอร์โบชนิดใหม่ซึ่งสามารถกำจัดผลการรบกวนของ MAI และสามารถถอดรหัสของผู้ใช้แต่ละรายได้ในตัวเดียวกันเพื่อใช้ในระบบ CDMA
- เพื่อวิจัยค้นหาแนวทางใหม่ๆในการกำจัดผลการรบกวนของผู้ใช้รายอื่นที่รบกวนต่อผู้ใช้ที่สนใจ (multiple access elimination) และทำการออกแบบเครื่องรับชนิดใหม่ที่สามารถทำงานร่วมกับรหัสเทอร์โบ
- เพื่อศึกษาและวิจัยระหว่างความซับซ้อนและประสิทธิภาพของเครื่องรับที่นำเสนอเปรียบเทียบกับเครื่องรับที่ถูกนำเสนอโดยนักวิจัยต่างประเทศมาก่อนหน้านี้ เพื่อศึกษาความเป็นไปได้ที่จะนำมาใช้จริง
- พัฒนาและปรับปรุงอัลกอริทึมในการเข้ารหัสและถอดรหัสสำหรับในเครื่องรับและส่ง
- เผยแพร่ผลงานการวิจัยในรูปของสื่อสิ่งพิมพ์และระบบอินเตอร์เน็ต แก่ผู้สนใจทั้งในประเทศและต่างประเทศ

3. ขอบเขตหรือเป้าหมายของโครงการ

- ทำการวิจัยและศึกษาบทความทางวิชาการที่เกี่ยวข้องกับอัลกอริทึมในระบบ CDMA
- พัฒนาและปรับปรุงอัลกอริทึมที่ใช้กับระบบ Multiuser Detection ในระบบ CDMA โทรศัพท์เคลื่อนที่ในยุคที่ 3และ 4ให้มีประสิทธิภาพสูงขึ้น
- ศึกษาและทำทดลองโดยใช้การเข้ารหัสแหล่งกำเนิดที่มีคุณสมบัติการแพร่กระจายของข้อผิดพลาด
- ค้นหาแนวทางใหม่ๆ ในการกำจัดผลการรบกวนของผู้ใช้รายอื่นที่รบกวนต่อผู้ใช้ที่สนใจ
- จัดทำบทความทางวิชาการ เพื่อเผยแพร่ความรู้และผลงานที่ได้จากการทำวิจัยทั้งในระดับชาติ และ ระดับนานาชาติ

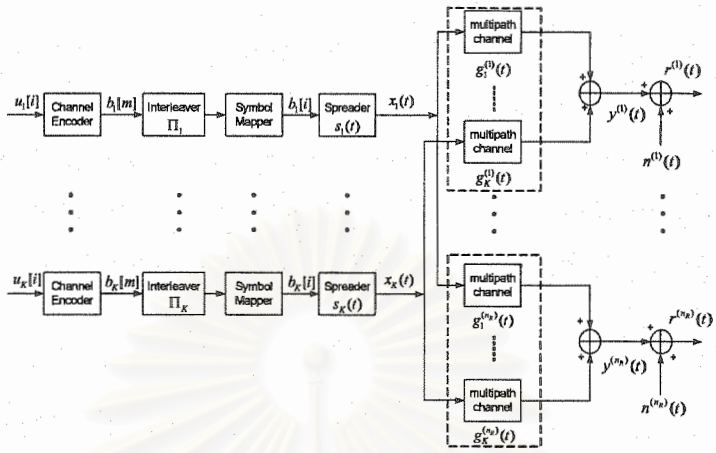
4. ส่วนงานที่ได้ดำเนินการไปแล้ว

- พัฒนาและปรับปรุงโครงสร้างของเครื่องรับที่สถานีฐานแบบดีเทกต์ผู้ใช้หลายคนในระบบ DS-CDMA
- พัฒนาและปรับปรุงอัลกอริทึมโดยใช้รหัส Turbo code ในระบบที่มีการประมาณ หาค่าช่อง สัญญาณ
- พัฒนาวิธีการ Turbo Multiuse detection ในระบบ CDMA เพื่อนำมาใช้ในโทรศัพท์เคลื่อนที่ในยุคที่ 3 และ 4
- ทำการพัฒนาและศึกษา EM-algorithm (Expectation Maximization Algorithm) เพื่อนำมาใช้ในการประมาณหาค่าช่องสัญญาณของระบบ CDMA
- ทดลองเพิ่มตำแหน่งที่เป็นไปได้ของสัญลักษณ์ต้องห้ามเพื่อวัดประสิทธิภาพในการทำงานของตัวเข้าและถอดรหัสและศึกษาหาผลกระทบที่เกิดจากวิธีการเข้ารหัสช่องสัญญาณรวมกับการเข้ารหัสแหล่งกำเนิด

- ปรับปรุงโปรแกรมให้สามารถรองรับความาสามารถในการเพิ่มตำแหน่งของสัญลักษณ์ต้องห้าม
- ทำการทดลองเพื่อตรวจสอบว่าถ้าผ่านช่องสื่อสารที่มีสัญญาณรบกวนที่ก่อให้เกิดความผิดพลาดในปริมาณไม่มากนักจะสามารถทำการแก้ไขข้อผิดพลาดนั้นโดยใช้วิธีการเปลี่ยนสัญลักษณ์เป็นส่วนๆได้หรือไม่
- ทำการทดลองวัดความถูกต้องในการเปลี่ยนสัญลักษณ์เป็นส่วนๆ ว่ามีความถูกต้องเป็นปริมาณเท่าไหร่เมื่อเปรียบเทียบกับปริมาณของข้อผิดพลาดทั้งหมดที่เกิดขึ้นเนื่องจากสัญญาณรบกวนในช่องสัญญาณ
- ปรับปรุงและแก้ไขโปรแกรมเพื่อทำการทดสอบความถูกต้องในการเปลี่ยนสัญลักษณ์เป็นส่วนๆ
- วัดประสิทธิภาพวัดประสิทธิภาพในการเข้ารหัสลับของตัวเข้ารหัสและตัวถอดรหัสและศึกษาหาผลกระทบที่เกิดจากวิธีการทดลองเพิ่มตำแหน่งที่เป็นไปได้ของสัญลักษณ์ต้องห้าม

5. ส่วนงานที่จะดำเนินการต่อไป

- พัฒนาโครงสร้างของเครื่องรับที่สถานีฐานในระบบ Ds-CDMA ให้สามารถดีเทกต์ผู้ใช้หลายคนพร้อมๆกันได้ในช่องสัญญาณข่ายเชื่อมโยงขาขึ้น
- พัฒนาซอฟแวร์ที่จำลองการทำงานของเครื่องรับแบบวนซ้ำโดยอาศัยตัวประมาณช่องสัญญาณ
- ทำการศึกษา EM algorithm เพื่อนำมาใช้ในระบบ ดีเทกต์ผู้ใช้หลายคนพร้อมๆกันและพัฒนาต่อไปในระบบที่สัญญาณ fading เป็นแบบ frequency selective และ time varying fading
- ทดลองสร้างรหัสที่สามารถตรวจจับความผิดพลาดได้ถูกต้องมากเท่าที่ต้องการได้โดยการเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดซ้ำ
- พัฒนาซอฟแวร์ที่ทำการเข้ารหัสและถอดรหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดที่ผ่านการเข้ารหัสซ้ำได้



รูป 1. แสดงระบบ MIMO ของระบบ CDMA ขาขึ้น

พิจารณาระบบขาขึ้นของ asynchronous CDMA โดยกำหนดให้มีผู้ใช้ K รายและมีจำนวนเสารับจำนวน n_R เสารับโดนสมมุติให้ที่สถานีฐานทราบเพียง spreading sequence ของแต่ผู้ใช้แต่ละรายภายในเซลล์ $K_{in}(K_{in} \le K)$ โดยที่ spreading sequence ของผู้ใช้ภายนอกเซลล์รายที่$(K-K_{in})$ ไม่ทราบจากสถานีฐานจากรูปที่ 1 จะเห็นได้ว่าสัญญาณที่ถูกส่งออกมาจากเครื่องส่งแต่ละราย (mobile to base station) มีลักษณะเป็น $x_k(t)=A_k\sum_{i=0}^{M-1}b_k[i]s_k(t-iT-d_k)$ โดยที่ค่า d_k $(0\le t<T)$ เป็นค่าหน่วงเวลาจากผู้ใช้แต่ละรายและค่าของสัญญาณ $s_k(t)$ สามารถเขียนได้เป็น $s_k(t)=\sum_{j=0}^{N-1}c_k[j]\psi(t-jT_c)$ ในช่วงเวลา $0\le t\le T$ และ $T_c=T/N$. โดยที่ค่าสัญญาณของสัญญาณ $\psi(t)$ ถูกนอร์มอลไลซ์โดย $\int_0^{T_c}\psi(t)^2dt=1$ ในช่วงของ $\{c_k[j]\}_{j=0}^{N-1}$ เมื่อกำหนดให้สัญญาณ multi-path fading ในผู้ใช้แต่ละรายที่เสารับลำดับที่ b = 1,2,.., n_R มีค่าเป็น $g_k^{(b)}(t)=\sum_{l=1}^{L}\alpha_{kl}^{(b)}\delta(t-\tau_{kl}^{(b)})$ โดยที่ค่า $\alpha_{kl}^{(b)}$ และ $\tau_{kl}^{(b)}$ อัตราขยายของช่องสัญญาณและค่าประวิงเวลาซึ่งคู่กับอัตราขยาย โดยที่ $\tau_{k1}^{(b)}<\tau_{k2}^{(b)},\ldots,<\tau_{kL}^{(b)}$ ในเสารับสัญญาณที่ b

$$r^{(b)}(t)=\sum_{k=1}^{K}\sum_{i=0}^{M-1}b_k[i]\,h_k^{(b)}(t-iT)+n^{(b)}(t)$$

$$=\underbrace{\sum_{i=0}^{M-1}b_k[i]\,h_k^{(b)}(t-iT)}_{y_k^{(b)}(t)}+\underbrace{\sum_{\substack{k'=1\\k'\neq k}}^{K_{in}-1}\sum_{i=0}^{M-1}b_{k'}[i]h_{k'}^{(b)}(t-iT)}_{\text{intracell Interference}}$$

$$+\underbrace{\sum_{k''=K_{in}+1}^{K}\sum_{i=0}^{M-1}b_{k''}[i]h_{k''}^{(b)}(t-iT)}_{\text{intercell Interference}}+n^{(b)}(t)$$

$$r^{(b)}(t) = \underbrace{y_k^{(b)}(t) + \sum_{\substack{k'=1 \\ k' \neq k}}^{K_{in}-1} y_{k'}^{(b)}(t) + \sum_{k''=K_{in}+1}^{K} y_{k''}^{(b)}(t)}_{y^{(b)}(t)} + n^{(b)}(t) \qquad (1)$$

เมื่อกำหนดให้ $l_k^{(b)} = \left\lceil \left(d_k + \tau_{kL}^{(b)} + T_c\right)/T \right\rceil$ เป็นค่าประวิงเวลาสูงสุดในแต่ละสัญลักษณ์ข้อมูลที่ส่ง ดังนั้นเมื่อทำการสุ่มเก็บข้มมูลทุกๆเวลา $t = iT + nT_c$ ในแต่ละเสารับสัญญาณดังนั้นสัญญาณที่ได้รับจะสามารถจัดรูปได้เป็น

$$y_k^{(b)}[i,n] = y_k^{(b)}(iT + nT_c) = \sum_{j=0}^{M-1} b_k[i] \underbrace{h_k^{(b)}(iT + nT_c - jT)}_{h_k^{(b)}[i-j,n]}$$

$$y_k^{(b)}[i,n] = \sum_{j=i-l_k^{(b)}}^{i} b_k[i] h_k^{(b)}[i-j,n] = \sum_{j=0}^{l_k^{(b)}} h_k^{(b)}[j,n] b_k[i-j] \qquad (2)$$

ทำการแทนสมการที่ 2 ลงในสมการที่ 1

$$r^{(b)}[i,n] = h_k^{(b)}[0,n] b_k[i] + \underbrace{\sum_{j=1}^{l_k^{(b)}} h_k^{(b)}[j,n] b_k[i-j]}_{ISI} + \sum_{k' \neq k} y_{k'}^{(b)}[i,n] + n^{(b)}[i,n] \qquad (3)$$

กำหนดให้ค่าประวิงเวลาสูงสุดของผู้ใช้ K ใน ทุกเสารับของสถานนีฐานเป็น $l^{(b)} = \max_{1 \le k \le K} \left\{ l_k^{(b)} \right\}$ และ $l = \max_{1 \le b \le nR} \left\{ l^{(b)} \right\}$ ดังนั้นเราจะพบว่า

$$\underbrace{\underline{r}^{(b)}[i]}_{N \times 1} = \left[r^{(b)}[i,0] \quad \cdots \quad r^{(b)}[i,N-1] \right]^T \qquad \underbrace{\underline{b}_{in}[i]}_{K_{in} \times 1} = \left[b_1[i] \quad \cdots \quad b_{K_{in}}[i] \right]^T$$

$$\underbrace{\underline{n}^{(b)}[i]}_{N \times 1} = \left[n^{(b)}[i,0] \quad \cdots \quad n^{(b)}[i,N-1] \right]^T \qquad \underbrace{\underline{b}_{out}[i]}_{(K-K_{in}) \times 1} = \left[b_{K_{in}+1}[i] \quad \cdots \quad b_K[i] \right]^T$$

$$\underbrace{\underline{H}_{in}^{(b)}[j]}_{N \times K_{in}} = \begin{bmatrix} h_1^{(b)}[j,0] & \cdots & h_{K_{in}}^{(b)}[j,0] \\ \vdots & \vdots & \vdots \\ h_1^{(b)}[j,N-1] & \cdots & h_{K_{in}}^{(b)}[j,N-1] \end{bmatrix}$$

$$\underbrace{\underline{H}_{out}^{(b)}[j]}_{N \times (K-K_{in})} = \begin{bmatrix} h_{K_{in}+1}^{(b)}[j,0] & \cdots & h_K^{(b)}[j,0] \\ \vdots & \vdots & \vdots \\ h_{K_{in}+1}^{(b)}[j,N-1] & \cdots & h_K^{(b)}[j,N-1] \end{bmatrix}$$

For $j = 0,1,\ldots,l$.

จากสมากรที่ 3 เราจะได้ว่า

$$\underline{r}^{(b)}[i] = \underline{H}_{in}^{(b)}[j] * \underline{b}_{in}[i] + \underline{H}_{out}^{(b)}[j] * \underline{b}_{out}[i] + \underline{n}^{(b)}[i]. \qquad (4)$$

ทำการรวมสัญญาณในแต่ละเสารับและเสาส่งจะได้ว่า

หรือเราสามาถเขียน 4 ในรูปของ

$$r[i]=\sum_{k=1}^{K_{in}}\underbrace{\left(b_k[i]C_k^{(0)}+b_k[i-1]C_k^{(1)}+\ldots+b_k[i-l]C_k^{(l)}\right)}_{s_k[i]}g_k[i]+v_{OMAI}[i]+n[i]$$
$$=\sum_{k=1}^{K_{in}}s_k[i]g_k[i]+v_{OMAI}[i]+n[i] \qquad (5)$$

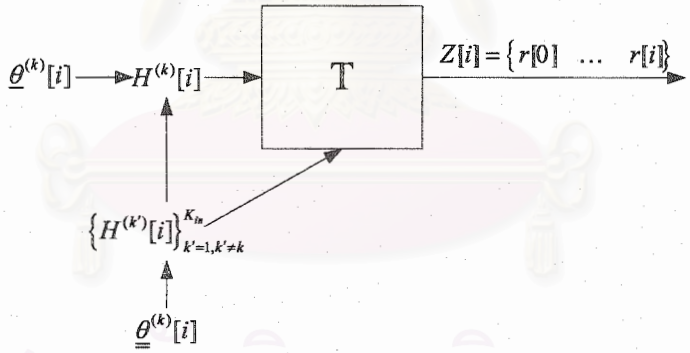
$r_k[i]=s_k[i]g_k[i]+n[i]$ for $k=1,\ldots,K_{in}$ and $r_{K_{in}+1}[i]=v_{OMAI}[i]+n[i]$

โดยการประมาณให้การเกิด fading มีลักษณะเป็น Markov process เราจะได้

$$g_k[i]=\psi_k[i]g_k[i-1]+w_k[i] \qquad k=1,\ldots,K_{in}$$
$$v_{OMAI}[i]=\psi_{K_{in}+1}[i]v_{OMAI}[i-1]+w_{K_{in}+1}[i]$$

ดังนั้น

$$r_k[i]=A_k[i]x_k[i]+n[i]$$
$$x_k[i]=\psi_k[i]x_k[i-1]+w_k[i]$$
$$r_k[i]=r[i]-\sum_{k'=1:k'\neq k}^{K_{in}}A_{k'}[i]x_{k'}[i]$$
$$Z[i]=\{r[0]\quad\ldots\quad r[i]\}$$



โดยการอาศัย Em algorithmเราจะได้

For $k=1,\ldots,K_{in}$

E-Step

$$Q^{(k)}\left(\underline{\theta}^{(k)}[i]\,|\,\tilde{\theta}^{(k)}[i]\right)=E\left\{\log f\left(H^{(k)}[i]\,|\,\underline{\theta}^{(k)}[i]\right),Z[i],\tilde{\theta}^{(k)}[i]\right\}$$

$$Q^{(k)}\left(\underline{\theta}^{(k)}[i]\,|\,\tilde{\theta}^{(k)}[i]\right)=C-\log\|R_k[i]\|-\frac{1}{2}tr\left[R_k^{-1}[i]\left(x_k[i\,|\,i]-\psi_k[i]x_k[i-1\,|\,i]\right)\left(x_k[i\,|\,i]-\psi_k[i]x_k[i-1\,|\,i]\right)^H\right]$$

$$-\log\|\Sigma_k[i]\|-\frac{1}{2}tr\left[\Sigma_k^{-1}[i]\left(r_k[i]-A_k[i]x_k[i\,|\,i]\right)\left(r_k[i]-A_k[i]x_k[i\,|\,i]\right)^H\right]$$

Where $x_k[i\,|\,i]=\langle x_k[i]\rangle=E\left\{x_k[i]\,|,Z[i],\tilde{\theta}^{(k)}[i]\right\}$

$x_k[i-1\,|\,i]=\langle x_k[i-1]\rangle=E\left\{x_k[i-1]\,|,Z[i],\tilde{\theta}^{(k)}[i]\right\}$

CM-step

Matrix lemma $\frac{\partial}{\partial X^*} tr(AX^H) = \frac{\partial}{\partial X^*} tr(X^H A) = A$ $\frac{\partial}{\partial X} \log\|X\| = \left(X^{-1}\right)^T = \left(X^T\right)^{-1}$

$\frac{\partial}{\partial X} tr(X^{-1}A) = -\left(X^{-1}AX^{-1}\right)^T$

CM1-Step

Replacing $\psi_k[i] = \tilde{\psi}_k[i-1]$ $R_k[i] = \tilde{R}_k[i-1]$ $\Sigma_k[i] = \tilde{\Sigma}_{k-1}[i]$

$\tilde{\psi}_k[i] = \left\langle x_k[i]x_k[i-1]^H \right\rangle \left\langle x_k[i-1]x_k[i-1]^H \right\rangle^{-1} = M_{12}M_2^{-1}$

$\tilde{\psi}_k[i] = \left(x_k[i\,|\,i]x_k[i-1\,|\,i]^H + P_k[i,i-1\,|\,i]\right)\left(x_k[i-1\,|\,i]x_k[i-1\,|\,i]^H + P_k[i-1\,|\,i]\right)^{-1}$

CM2-Step

Replacing $\psi_k[i] = \tilde{\psi}_k[i]$ $R_k[i] = \tilde{R}_k[i-1]$ $\Sigma_k[i] = \tilde{\Sigma}_{k-1}[i]$

$R_k[i] = \frac{1}{2}\left\langle \left(x_k[i] - \psi_k[i]x_k[i-1]\right) \right\rangle \left\langle \left(x_k[i] - \psi_k[i]x_k[i-1]\right)^H \right\rangle$

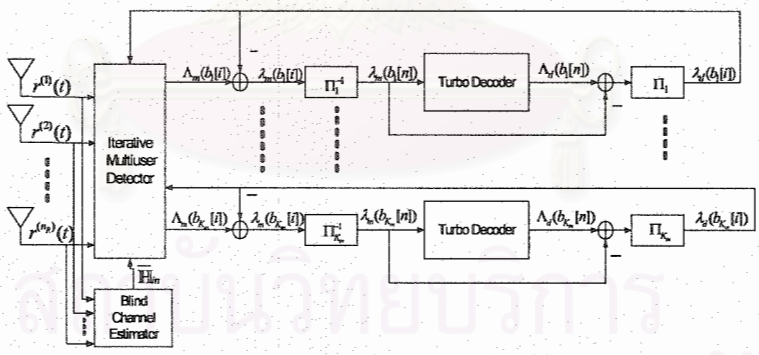
$= \frac{1}{2}\left(M_1 - \tilde{\psi}_k[i]M_{12}^H\right)$

CM3-Step

Replacing $\psi_k[i] = \tilde{\psi}_k[i]$ $R_k[i] = \tilde{R}_k[i]$ $\Sigma_k[i] = \tilde{\Sigma}_{k-1}[i]$

$\Sigma_k[i] = \frac{1}{2}\left\langle \left(r_k[i] - A_k[i]x_k[i]\right) \right\rangle \left\langle \left(r_k[i] - A_k[i]x_k[i]\right)^H \right\rangle$

ในส่วนนี้จะแสดงผลการทดลองและเครื่องรับที่นำเสนอโดยอาศัยตัวประมาณช่องสัญญาณโดยใช้วิธี EM มาใช้ในภาครับ



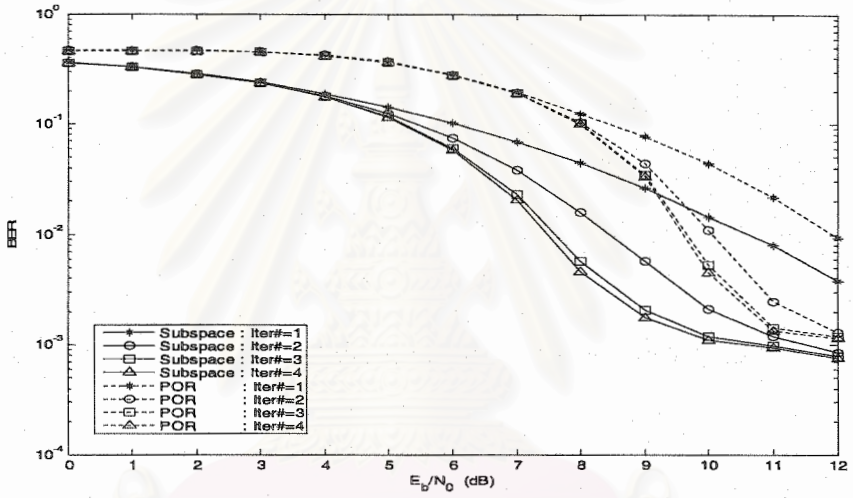
รูป 3. รูปแบบของเครื่องรับในระบบ CDMA ที่นำเสนอ

จากรูป 3 "Iterative multiuser detector" จะทำการสร้างสัญญาณ $\Lambda_m(b_k[i]) = \lambda_m(b_k[i]) + \lambda_d(b_k[i])$ a posterior likelihood ratio แลกเปลี่ยนกับตัวถอดรหัสช่องสัญญาณ Turbo decoder ในลักษณะที่เป็นรอบๆ (iteration) โดยถ้ากำหนดว่าสัญญาณที่ออกจาก "Iterative multiuser detector" ผ่านตัวกรอง filter มามีลักษณะสัญญาณเป็น

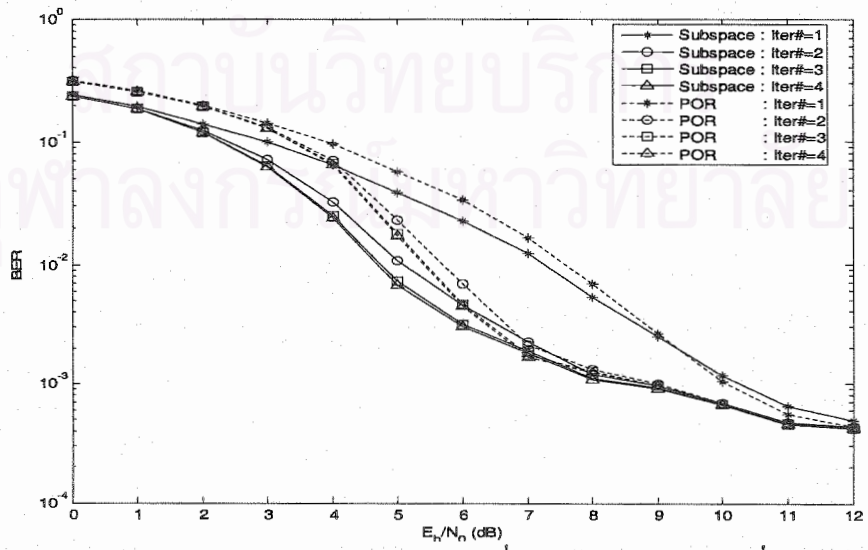
$$z_k[i] = \tilde{b}_k[i] + w_k^H \left[\mathbf{r}[i] - \overline{\mathbf{H}}_{in}^{(k)} \underline{\mathbf{A}}^{(k)} \tilde{\mathbf{b}}_{in}^{(k)}[i] \right] = \mu_k b_k[i] + \nu_k[i] \qquad (12)$$

โดยที่อัตรส่วน likelihood ratio มีค่าเป็น

$$\begin{aligned} \lambda_m(b_k[i]) &= \log \frac{P(z_k[i] \mid b_k[i] = +1)}{P(z_k[i] \mid b_k[i] = -1)} \\ &= \frac{-\left|z_k[i] - \mu_k\right|^2}{2\upsilon^2} + \frac{\left|z_k[i] + \mu_k\right|^2}{2\upsilon^2} \\ &= \Re\left(\frac{2\mu_k z_k[i]}{\upsilon^2} \right) \end{aligned} \qquad (13)$$



รูป 4. สมรรถนะของ maximum BER user ในเครื่องรับในระบบ CDMA ที่นำเสนอ



รูป 5. สมรรถนะของ minimum BER user ในเครื่องรับในระบบ CDMA ที่นำเสนอ

เอกสารอ้างอิง

[1] X. Wang and A. Host-Madsen, "Group-blind multiuser detection for uplink CDMA," *IEEE J.Select. Areas Commun.*, vol. 17, pp. 1971 – 1984, Nov. 1999

[2] H. Liu and G. Xu, "A subspace method for signature waveform estimation in synchronous CDMA systems," *IEEE Trans. Commun.*, vol. 44, pp. 1346–54, Oct. 1996.

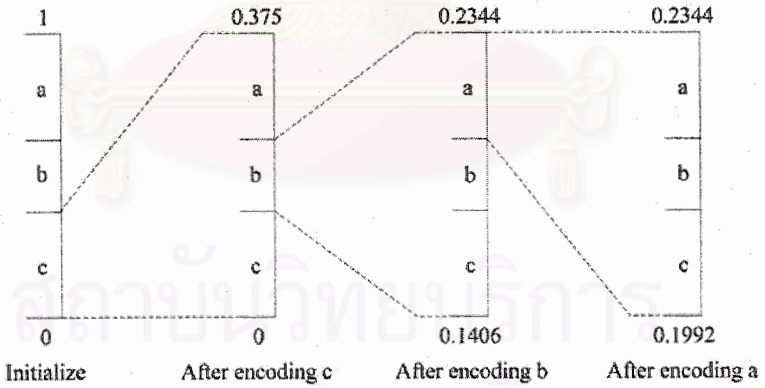
[3]Z. Xu, "Asymptotic performance of subspace methods for synchronous multirate CDMA systems," *IEEE Trans. on Signal Processing*, vol. 50, no. 8, pp. 2015-2026, August 2002.

[4] Z. Xu, "On the second-order statistics of the weighted sample covariance matrix," *IEEE Trans. on Signal Processing*, vol. 51, no. 2, pp. 527-534, February 2003.

ภาคผนวก ข

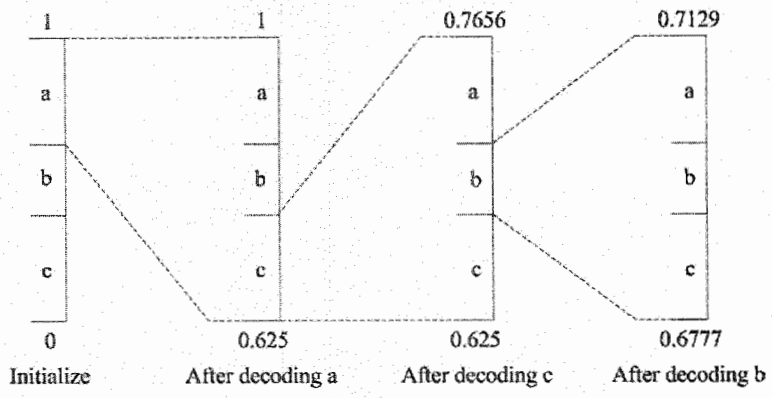
การเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดนั้นสามารถทำได้โดยการเพิ่มสัญลักษณ์ต้องห้ามลงไปในตารางความน่าจะเป็นที่ใช้ในการเข้ารหัสเชิงเลขคณิต โดยจะต้องมีการกำหนดตำแหน่งของสัญลักษณ์ต้องห้ามไว้ล่วงหน้าเนื่องจากการเข้ารหัสและถอดรหัสจำเป็นที่จะต้องสามารถสร้างตารางความน่าจะเป็นที่ใช้ในการเข้ารหัสและถอดรหัสที่ตรงกันทั้งด้านตัวเข้ารหัสและตัวถอดรหัส เนื่องจากหากไม่สามารถที่จะสร้างตารางความน่าจะเป็นที่ตรงกันได้ข้อมูลที่ถอดรหัสออกมาจากรหัสที่รับมานั้นจะเป็นข้อมูลที่ไม่ถูกต้องโดยข้อมูลที่ถอดออกมานั้นจะเกิดความผิดพลาดแบบต่อเนื่อง เนื่องจากการเข้ารหัสเชิงเลขคณิตมีคุณสมบัติการแพร่กระจายของความผิดพลาด (Error Propagation) คือ หากเกิดความผิดพลาดขึ้นครั้งหนึ่งจากการถอดรหัสเนื่องรหัสที่ได้รับไม่ถูกต้องหรือตารางที่ใช้ในการถอดรหัสไม่ตรงกันจะทำให้การถอดรหัสข้อมูลหลังจากจุดที่เกิดความผิดพลาดขึ้นจะเกิดความผิดพลาดตามไปด้วย

คุณสมบัติการแพร่กระจายของความผิดพลาดของการเข้ารหัสเชิงเลขคณิต สามารถอธิบายได้ด้วยตัวอย่างง่ายๆ ดังนี้ สมมติให้มีการเข้ารหัสข้อมูล *cba* โดยสัญลักษณ์ *c* มีค่าอยู่ในช่วง [0, 0.375) สัญลักษณ์ *b* มีค่าอยู่ในช่วง [0.375, 0.625) และสัญลักษณ์ *a* มีค่าอยู่ในช่วง [0.625, 1) โดยหลังจากการเข้ารหัสดังในรูปที่ 1 แล้วเราจะได้ว่า รหัส *cba* สามารถแทนได้โดยใช้ค่าในช่วง [0.1992, 0.2344) ในที่นี้ใช้ 001101 ซึ่งมีค่าเท่ากับ 0.203125



รูปที่ 1 การเข้ารหัสเชิงเลขคณิตของ *cba*

หลังจากที่ทำการส่งข้อมูลที่ผ่านการเข้ารหัสเรียบร้อยแล้วหากรหัสที่ตัวถอดรหัสได้รับไม่ถูกต้อง เช่นแทนที่จะได้รับรหัส 001101 กลับได้รับรหัส 101101 แทนทำให้การถอดรหัสแทนที่จะได้ข้อมูลที่ถูกต้องคือ *cba* กลับได้ข้อมูล *acb* แทนโดยการถอดรหัสของรหัส 101101 จะเป็นไปดังรูปที่ 2

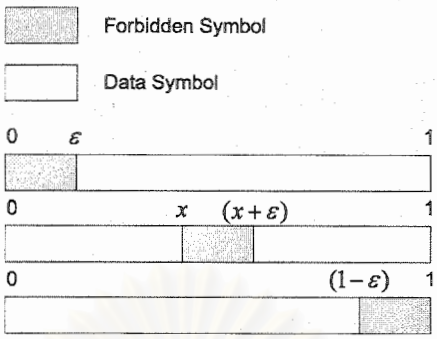


รูปที่ 2 การถอดรหัสของรหัส 101101

การที่บิตข้อมูลแรกที่ได้รับเปลี่ยนจาก 0 เป็น 1 ส่งผลให้ข้อมูลที่ถอดรหัสจากรหัสชุดนี้ผิดพลาดทั้งหมดถึงแม้ว่าข้อมูลที่เหลือจะถูกต้องทั้งหมดก็ไม่สามารถที่จะทำการถอดรหัสข้อมูลที่ถูกต้องได้ เช่นเดียวกันหากมีตารางความน่าจะเป็นที่ใช้ในการถอดรหัสครั้งใดไม่ตรงกับตารางความน่าจะเป็นที่ใช้ในการเข้ารหัสเพียงครั้งเดียวก็จะส่งผลให้การถอดรหัสที่เหลือทั้งหมดไม่ถูกต้องไปด้วย

จากคุณสมบัติการแพร่กระจายของความผิดพลาดของการเข้ารหัสเชิงเลขคณิตที่ได้กล่าวมาแล้วนี่เองที่ทำให้สามารถที่จะใช้คุณสมบัติดังกล่าวในการตรวจจับความผิดพลาดที่เกิดขึ้นในข้อมูลที่ได้รับได้ โดยการใส่สัญลักษณ์ต้องห้ามลงไปหรือที่เรียกว่า การตรวจจับความผิดพลาดแบบต่อเนื่อง (Continuous Error Detection: CED) [1], [2] โดยมีข้อกำหนดว่าในข้อมูลที่จะทำการเข้ารหัสนั้นจะไม่มีสัญลักษณ์ต้องห้ามอยู่ ทำให้สามารถบอกได้อย่างแน่นอนว่าหากมีการถอดรหัสได้สัญลักษณ์ต้องห้ามที่ฝั่งตัวถอดรหัสหมายความว่ามีการรับข้อมูลที่ผิดพลาดเกิดขึ้นแล้ว

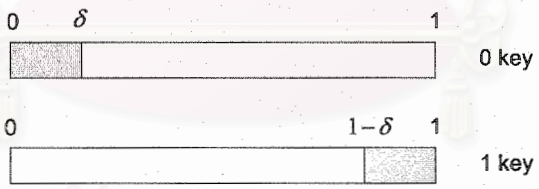
ตำแหน่งที่ใช้ในการวางสัญลักษณ์ต้องห้ามก็มีส่วนในการเข้ารหัสและถอดรหัส ดังที่ได้กล่าวไปแล้วว่าหากไม่สามารถที่จะสร้างตารางความน่าจะเป็นที่ใช้ในการเข้ารหัสและถอดรหัสที่ตรงกันได้ก็จะไม่สามารถถอดรหัสข้อมูลที่ถูกต้องได้ ดังนั้นในระบบที่มีการใช้การเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดจำเป็นที่จะต้องมีการตกลงตำแหน่งของสัญลักษณ์ต้องห้ามไว้ก่อนล่วงหน้า โดยตำแหน่งของสัญลักษณ์ต้องห้ามอาจเป็นไปตามรูปแบบใดรูปแบบหนึ่งในรูปที่ 3



รูปที่ 3 ตำแหน่งของสัญลักษณ์ต้องห้าม

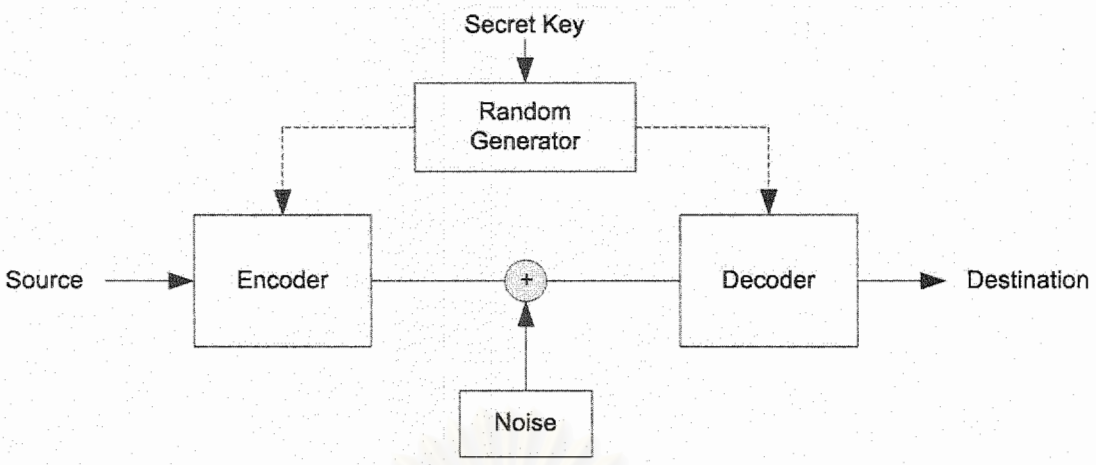
จะเห็นได้ว่าการวางสัญลักษณ์ต้องห้ามไว้ตรงกลางของตารางความน่าจะเป็นจะทำให้มีการคำนวณมากกว่าการวางสัญลักษณ์ต้องห้ามไว้ที่ปลายของตารางเนื่องจากมีการคำนวณเพียงฝั่งเดียว หากวางสัญลักษณ์ต้องห้ามไว้ตรงกลางของตารางความน่าจะเป็นจะต้องมีการคำนวณ 2 ฝั่งในกรณีที่เป็น การเข้ารหัสที่มีการใช้แบบจำลองแบบปรับได้ดังนั้นจึงควรเลือกใช้ตำแหน่งที่อยู่ที่ส่วนปลายของตาราง

ในระบบที่มีการใช้การเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดนั้นสามารถที่จะเพิ่มความสามารถในการเข้ารหัสลับได้โดยวิธีการดังต่อไปนี้ กำหนดให้ตำแหน่งของสัญลักษณ์ต้องห้ามมีการเปลี่ยนแปลงตำแหน่งทุกครั้งที่มีการเข้ารหัสสัญลักษณ์แต่ละสัญลักษณ์ โดยอาจกำหนดให้มีตำแหน่งของสัญลักษณ์สำหรับกุญแจแต่ละแบบดังรูปที่ 4



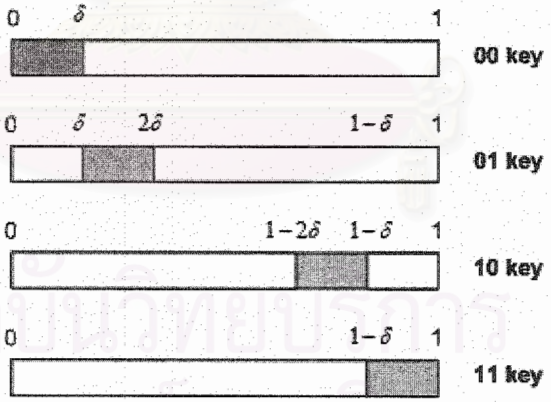
รูปที่ 4 ตำแหน่งของสัญลักษณ์ต้องห้ามและกุญแจ

การทำการเข้ารหัสลับในรูปแบบนี้จำเป็นที่จะต้องมีกุญแจที่มีจำนวนเท่ากับจำนวนของสัญลักษณ์ที่จะทำการเข้ารหัสโดยอาจสามารถสร้างได้โดยใช้ตัวกำเนิดสัญญาณไบนารีแบบสุ่ม โดยใช้กุญแจลับ (Secret key) เป็นเมล็ด (Seed) ของกุญแจไบนารีที่มีความยาวเท่ากับสัญลักษณ์ที่จะทำการเข้ารหัส ทำให้สามารถเขียนระบบทั้งหมดที่ใช้ในการเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดและเข้ารหัสลับได้ดังรูปที่ 5



รูปที่ 5 ระบบเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดและเข้ารหัสลับ

การเข้ารหัสในลักษณะดังกล่าวนั้นสามารถทำการขยายรูปแบบการใส่กุญแจได้โดยการเพิ่มตำแหน่งของกุญแจที่จะทำการใส่เพิ่มลงในข้อมูลโดยการเพิ่มจำนวนของตำแหน่งที่เป็นที่อยู่ของกุญแจนั้นจะไม่ส่งผลกับขนาดของข้อมูลที่ผ่านการเข้ารหัสแล้วเมื่อเทียบกับการเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดและเข้ารหัสลับแบบที่มีตำแหน่งที่เป็นไปได้ของกุญแจน้อยกว่า จะเห็นได้ว่าสิ่งที่ต้องการมากขึ้นในการเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดและเข้ารหัสลับที่มีตำแหน่งของกุญแจที่เป็นไปได้มากๆ นั้นจะมีความต้องการทรัพยากรมากขึ้นเพียงแต่ความสามารถในการคำนวณเท่านั้นจะไม่ส่งผลกระทบกับขนาดของข้อมูลที่ผ่านการเข้ารหัสแล้ว ตัวอย่างของตำแหน่งที่เป็นไปได้ของกุญแจที่มากขึ้นนั้นแสดงไว้ในรูปที่ 6



รูปที่ 6 ตัวอย่างตำแหน่งที่เป็นไปได้ของกุญแจ 4 ตำแหน่ง

การทดลองความสามารถในการบีบอัดข้อมูล

ทำโดยการเข้ารหัสข้อมูล book1 และ paper1 จาก ชุดทดสอบ Calgary Corpus โดยได้ผลการบีบอัดข้อมูลในรูปของบิตต่อไบต์ ดังต่อไปนี้

ตารางที่ 1 ผลการบีบอัดข้อมูล

แฟ้ม	SEEDAC 2	SEEDAC 4	SEEDAC 8
book1	4.612005	4.611996	4.61147
paper1	5.014654	5.014665	5.04671

จากตารางที่ 1 จะเห็นได้ว่าการเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดและเข้ารหัสลับที่มีจำนวนตำแหน่งของกุญแจที่เป็นไปได้ต่างๆ กันนั้นให้ผลการบีบอัดข้อมูลที่ไม่แตกต่างกัน

การเพิ่มจำนวนของตำแหน่งที่เป็นไปได้ของกุญแจนั้นจะส่งผลให้การเข้ารหัสลับของแต่ละสัญลักษณ์ที่ทำการเข้ารหัสนั้นจำเป็นจะต้องใช้เวลาในการเฟ้นหาตำแหน่งที่ถูกต้องนานยิ่งขึ้นทำให้ข้อมูลที่เป็นความลับที่ถูกลักลอบนำออกไปนั้นต้องใช้เวลาในการถอดรหัสลับให้ได้ข้อความที่ถูกต้องนั้นนานยิ่งขึ้นเนื่องจากต้องทำการตำรวจสอบหาตำแหน่งให้ครบทุกตำแหน่งในขณะที่ผู้ที่รู้ตำแหน่งของกุญแจนั้นจะไม่ได้ใช้เวลามากขึ้นในการถอดรหัสลับของข้อมูล อีกทั้งความสามารถในการตรวจจับความผิดพลาดของการเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดและเข้ารหัสลับก็มิได้สูญเสียไป การเพิ่มตำแหน่งของกุญแจในลักษณะนี้สามารถทำได้มากเท่ากับ 2^n ตำแหน่ง เมื่อ n เป็นจำนวนบิตที่ใช้ในการจัดเก็บค่าของขอบบนและขอบล่างในการเข้ารหัสเชิงเลขคณิต

เอกสารอ้างอิง

[1] C. Boyd, J.G. Cleary, S.A. Irvine, I. Rinsma-Melchert andI.H. Witten, "Integrating Error Detection into Arithmetic Coding", IEEE Trans. On Comm., vol.45, no.1, pp.1-3, Jan 1997.

[2] R. Anand, K. Ramchandran and I. V. Kozintsev. Continuous error detection (CED) for reliable communication. IEEE Trans. Commun., 49(9):1540–1549, September 2001.