โครงการวิจัยย่อยลำดับที่ 11

เรื่อง การประเมินช่องสัญญาณที่มีแหล่งจ่ายรวมในช่องการสื่อสารที่เกิดการเฟดดิง ปีที่ 5

1. **ผู้รับผิดชอบโครงการ** รองศาสตราจารย์ ดร. ประสิทธิ์ ทีฆพุฒิ

2. วัตถุประสงค์

จุดประสงค์ของโครงการวิจัยนี้วิจัยเกี่ยวกับเทคโนโลยีโทรคมนาคมสื่อสารไร้สายในระบบ CDMA เนื่องมาจากในปัจจุบันแนวโน้มทางการสื่อสารในอนาคตไม่ได้จำกัดอยู่เพียง การส่งสัญญาณเสียงแต่เพียงอย่างเดียวเท่านั้นการส่งสัญญาณในลักษณะอื่น ๆ เช่น ภาพเคลื่อนไหว ข้อมูลภาพนิ่งค่อนข้างที่จะได้รับความนิยมมากขึ้นและมีปริมาณเพิ่มขึ้น ทำให้ทรัพยากรของระบบที่มีอยู่อย่างจำกัดก็ต้องถูกจัดสรรเพื่อให้เกิดประโยชน์สูงสุด หนึ่งในหัวข้อโครงการค้นคว้าวิจัยที่มีอยู่อย่างกว้างขวางในปัจจุบันคือระบบสื่อสาร ที่รองรับการส่งข้อมูลจากผู้ใช้บริการจำนวนหลายๆรายพร้อมกันในเวลาเดียวกันโดยผ่านช่องสัญญาณเพียงช่องเดียว (CDMA) โดยที่ผ่านมามีหลายวิธีที่ทำให้สามารถส่งข้อมูลจากผู้ใช้หลายรายผ่านช่องสัญญาณช่องเดียวได้ เทคนิคการเข้าถึงหลายทางแบบแบ่งรหัส (Code Division Multiple Access หรือ CDMA) ก็เป็นเทคนิคหนึ่งที่ได้รับการค้นคว้าวิจัยจนสามารถนำไปใช้งานได้จริงมาเป็นระยะเวลาหนึ่ง อีกทั้งในปัจจุบันเทคนิคนี้ยิ่งได้รับความสนใจเพิ่มมากขึ้นเนื่องจากเป็นที่คาดหมายว่าวิธีการเข้าถึงหลายทางแบบแบ่งรหัสนี้ (CDMA) จะถูกนำมาใช้ในระบบโทรศัพท์เคลื่อนที่รุ่นที่สาม (3 Generation หรือ 3G) ตามมาตรฐาน UMTS/IMT 2000

ในขณะเดียวกันรหัสเทอร์โบ (Turbo code) ถูกยอมรับแล้วว่าเป็นกระบวนการเข้ารหัสและถอดรหัสที่สามารถลดความผิดพลาดจากการส่งข้อมูล digital ในช่องสัญญาณไร้สายที่มีการรบกวนแบบเกาส์สีขาวแบบบวก (AWGN) ได้ดีที่สุดในขณะนี้เท่าที่มนุษย์เคยทำมา ทำให้ในช่วงเวลา 4-5 ปีที่ผ่านมา งานวิจัยเกี่ยวกับรหัสเทอร์โบได้รับความนิยมเป็นอย่างสูง แต่เนื่องจากอุปสรรค์สำคัญในการนำเอารหัสเทอร์โบมาใช้ในระบบ CDMA คือการรบกวนกันของผู้ใช้รายอื่นๆที่ใช้ช่องสัญญาณเดียวกัน (multiple access interference : MAI) ทำให้ช่องสัญญาณที่เกิดขึ้นไม่เป็นเกาส์สีขาวแบบบวก (AWGN) เป็นผลทำให้รหัสเทอร์โบ (Turbo code) ไม่สามารถทำงานได้ ดังนั้นจุดประสงค์หลักของโครงการวิจัยนี้คือเป็นไปได้ที่จะนำมาใช้จริง

3. ขอบเขตหรือเป้าหมายของโครงการ

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

4. ส่วนงานที่ได้ดำเนินการไปแล้ว

- พัฒนาและปรับปรุงโครงสร้างของเครื่องรับที่สถานีฐานแบบดีเทกต์ผู้ใช้หลายคนในระบบ DS-CDMA

- พัฒนาและปรับปรุงอัลกอริทึมโดยใช้รหัส Turbo code ในระบบที่มีการประมาณ หาค่าช่องสัญญาณ

- พัฒนาวิธีการ Turbo Multiuse detection ในระบบ CDMA เพื่อนำมาใช้ในโทรศัพท์เคลื่อนที่ในยุคที่ 3 และ 4

- ทำการพัฒนาและศึกษา EM-algorithm (Expectation Maximization Algorithm) เพื่อนำมาใช้ในการประมาณหาค่าช่องสัญญาณของระบบ CDMA

- ทดลองเพิ่มตำแหน่งที่เป็นไปได้ของสัญลักษณ์ต้องห้ามเพื่อวัดประสิทธิภาพในการทำงานของตัวเข้าและถอดรหัสและศึกษาหาผลกระทบที่เกิดจากวิธีการเข้ารหัสช่องสัญญาณรวมกับการเข้ารหัสแหล่งกำเนิด

- ปรับปรุงโปรแกรมให้สามารถรองรับความสามารถในการเพิ่มตำแหน่งของสัญลักษณ์ต้องห้าม

- ทำการทดลองเพื่อตรวจสอบว่าถ้าผ่านช่องสื่อสารที่มีสัญญาณรบกวนที่ก่อให้เกิดความผิดพลาดในปริมาณไม่มากนักจะสามารถทำการแก้ไขข้อผิดพลาดนั้นโดยใช้วิธีการเปลี่ยนสัญลักษณ์เป็นส่วนๆ ได้หรือไม่

- ทำการทดลองวัดความถูกต้องในการเปลี่ยนสัญลักษณ์เป็นส่วนๆ ว่ามีความถูกต้องเป็นปริมาณเท่าไหร่เมื่อเปรียบเทียบกับปริมาณของข้อผิดพลาดทั้งหมดที่เกิดขึ้นเนื่องจากสัญญาณรบกวนในช่องสัญญาณ

- ปรับปรุงและแก้ไขโปรแกรมเพื่อทำการทดสอบความถูกต้องในการเปลี่ยนสัญลักษณ์เป็นส่วนๆ

- วัดประสิทธิภาพวัดประสิทธิภาพในการเข้ารหัสลับของตัวเข้ารหัสและตัวถอดรหัสและศึกษาหาผลกระทบที่เกิดจากวิธีการทดลองเพิ่มตำแหน่งที่เป็นไปได้ของสัญลักษณ์ต้องห้าม

5. **ส่วนงานที่จะดำเนินการต่อไป**

- พัฒนาโครงสร้างของเครื่องรับที่สถานีฐานในระบบ Ds-CDMA ให้สามารถดีเทกต์ผู้ใช้หลายคนพร้อมๆ กันได้ในช่องสัญญาณข่ายเชื่อมโยงขาขึ้น

- พัฒนาซอฟแวร์ที่จำลองการทำงานของเครื่องรับแบบวนซ้ำโดยอาศัยตัวประมาณช่องสัญญาณ

- ทำการศึกษา EM algorithm เพื่อนำมาใช้ในระบบ ดีเทกต์ผู้ใช้หลายคนพร้อมๆกันและพัฒนาต่อไปในระบบที่สัญญาณ fading เป็นแบบ frequency selective และ time varying fading

6. ผลิตผลและหรือความสัมฤทธิผลของงานที่ได้ดำเนินการไปแล้ว

6.1 ผลงานนำเสนอในที่ประชุมวิชาการ

6.1.1 T. Ploysuwan and P. Teekaput ,“Blind Iterative Turbo Multiuser Detection For Uplink Cdma System With Uuknow Intercell Interferences,” Proc. EECON-28, pp 1033-1036, 20-21 Oct 2005

6.1.2T. Ploysuwan and P. Teekaput ,“Blind Turbo Multiuser Detector With Unknown Intercell Interferences” ” Proc. IEEE ISWPC, pp 620-626, 20-21 Jan 2006.

6.1.3 P. Teekaput and S. Chokchaitam, “Secure Embedded Error Detection Arithmetic Coding,” Proceedings of ICITA 2005, vol.2, pp. 568-571, Jul. 2005.

6.2 สิ่งประดิษฐ์

- โปรแกรมคอมพิวเตอร์จำลองการทำงานของภาครับ/ส่ง ข้อมูลในระบบ CDMA ที่พัฒนาโดยใช้โปรแกรม visual studio 7 และ MATLAB เวอร์ชัน 7

- โปรแกรมคอมพิวเตอร์จำลองการทำงานเครื่องรับในระบบ DS-CDMA และโปรแกรมตัวประมาณช่องสัญญาณโดยใช้วิธี EM Algorithm

- โปรแกรมคอมพิวเตอร์จำลองระบบ Asynchronous Uplink DS-CDMA พัฒนาโดยใช้โปรแกรม MATLAB เวอร์ชัน 7 และ visual studio 7

- โปรแกรมคอมพิวเตอร์จำลองการสร้างสัญญาณเฟดดิง

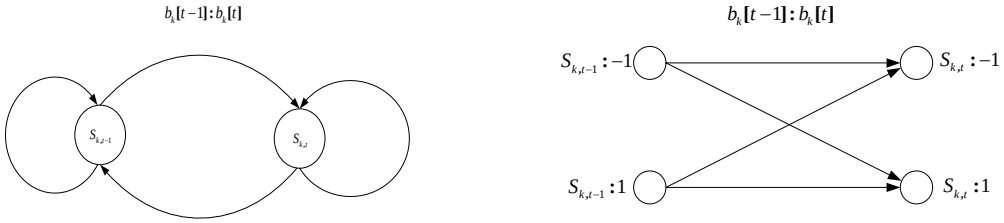
7. ทฤษฎีที่เกี่ยวข้อง

ภาคผนวก ก.

พิจารณาระบบขาขึ้นของ asynchronous CDMA โดยกำหนดให้มีผู้ใช้ K รายในระบบที่มีการรบกวนแบบ Addtive White Gaussain (AWGN) โดนสมมุติให้ที่สถานีฐานทราบเพียง spreading sequence ของแต่ผู้ใช้แต่ละรายภายในเซลล์ K รายโดยที่ spreading ดังนั้นสัญญาณที่ถูกส่งออกไปโดยผู้ใช้แต่ละรายจะมีลักษณะเป็น $x_k(t) = A_k \sum_{i=0}^{M-1} b_k[i] s_k(t - iT - d_k)$ โดยที่ค่า $d_k \quad (0 \le t < T)$ เป็นค่าหน่วงเวลาจากผู้ใช้แต่ละราย และค่าของสัญญาณ $s_k(t)$ สามารถเขียนได้เป็น $s_k(t) = \sum_{j=0}^{N-1} c_k[j] \psi(t - jT_c)$ ซึ่งจะมีค่าในช่วงเวลา $0 \le t \le T$ และ $T_c = T/N$. โดยที่ค่าสัญญาณของสัญญาณ $\psi(t)$ ถูกนอร์มอลไลซ์โดย $\int_0^{T_c} \psi(t)^2 dt = 1$ ในช่วงของ $\{c_k[j]\}_{j=0}^{N-1}$ เมื่อกำหนดให้สัญญาณ multi-path fading มีค่าเป็น $g_k(t) = \sum_{l=1}^{L} \alpha_{kl} \delta(t - \tau_{kl}^{(b)})$ โดยที่ค่า α_{kl} และ τ_{kl} อัตราขยายของช่องสัญญาณและค่าประวิงเวลาซึ่งคู่กับอัตราขยายโดยที่ $\tau_{k1} < \tau_{k2}, \ldots, < \tau_{kL}$ ในเสารับสัญญาณที่ b

$$
\begin{aligned}
r(t) &= \sum_{k=1}^{K} \sum_{i=0}^{M-1} b_k[i] \, h_k(t - iT) + n(t) \\
&= \underbrace{\sum_{i=0}^{M-1} b_k[i] \, h_k(t - iT)}_{y_k^{(b)}(t)} + \sum_{\substack{k'=1 \\ k' \neq k}}^{K_{in}-1} \sum_{i=0}^{M-1} b_{k'}[i] h_{k'}(t - iT)
\end{aligned}
\tag{1}
$$

เมื่อกำหนดให้ $l_k^{(b)} = \left\lfloor \left(d_k + \tau_{kL}^{(b)} + T_c \right) / T \right\rfloor$ เป็นค่าประวิงเวลาสูงสุดในแต่ละสัญลักษณ์ข้อมูลที่ส่ง ดังนั้นเมื่อทำการสุ่มเก็บ ข้อมูลทุกๆ เวลา $t = iT + nT_c$ ในแต่ละเสารับสัญญาณดังนั้นสัญญาณที่ได้รับจะสามารถจัดรูปได้และ Vector ของสัญญาณที่รับในเครื่องรับสามารถเขียนได้เป็น



1.1 state diagram 1.2 trellis diagram

รูปที่ 1. แสดงค่าสถานะเสมือนของข้อมูล $b_k[t]$ และ $b_k[t-1]$

-11

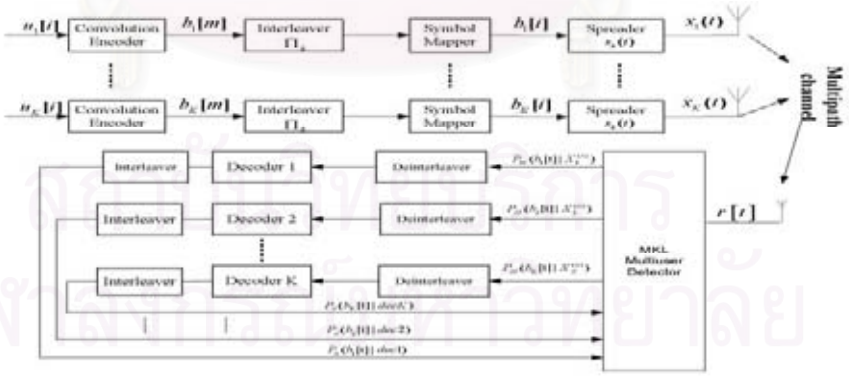
-1-1 11

$$r[t] = \sum_{k=1}^{K_{in}} \underbrace{\left(b_k[t]C_k^{(0)} + b_k[t-1]C_k^{(1)}\right)}_{D_k(\underline{b}_{k,t})} g_k + w[t]$$

$$= \sum_{k=1}^{K_{in}} \left(b_k[t]h_k^{(0)} + b_k[t-1]h_k^{(1)}\right) + w[t] \qquad (2)$$

$$= Hb[t] + w[t]$$

โดยอาศัยหลักการ maping โดยอาศัยหลักความเป็นไปได้ระหว่า $b_k[t]$ และ $b_k[t-1]$ ดังนั้น ในทุกๆคู่ของ $\underline{b}_{k,t} = (b_k[t], b_k[t-1])$ เราจะได้สามารถสร้างค่า state 1-1 ซึ่งคู่กับ state $\left(S_{k,t-1}, S_{k,t}\right) \rightarrow \left(b_k[t-1], b_k[t]\right) \rightarrow (s', s)$ เนื่องจากจุดประสงค์ของงานวิจัยนี้ต้องการประมาณค่าข้อมูลที่ถูกส่งและค่า parameter ของช่องสัญญาณดังนั้นกำหนดให้ $\theta = [\theta_1, \ldots, \theta_K]$ โดยที่ $\theta_k = \left\{g_k, B_k, \sigma_k^2\right\}$ และ $B_k = \left\{b_k[t]\right\}_{t=0}^{M}$ โดยที่ $B_{k/b_k[t]} = B_k \setminus b_k[i]$



รูป 2. รูปแบบของเครื่องส่งและรับในระบบ CDMA ที่นำเสนอ

2.1 **การประมาณค่า** Bayesian a posterior probability **ของค่า** θ_k

โดยการอาศัยวิธีการ kullblack-leibler ในกรณีที่เราสนใจผู้ใช้รายที่ k โดยให้ค่า parameter ของผู้ใช้รายอื่นคงที่คงที่ดังนั้น

$$KL(P(\theta_k^{(n-1)} \mid X_{k,M}^{(n)}) \| P(\theta_k \mid X_{k,M}^{(n)})) = \int P(\theta_k^{(n-1)} \mid X_{k,M}^{(n)}) \ln(\frac{P(\theta_k^{(n-1)} \mid X_{k,M}^{(n)})}{P(\theta_k \mid X_{k,M}^{(n)})}) d\theta_k$$
$$= E_{P(\theta_k^{(n-1)} \mid X_k^{(n)})} \left[\ln(\frac{P(\theta_k^{(n-1)} \mid X_{k,M}^{(n)})}{P(\theta_k \mid X_{k,M}^{(n)})}) \right] \quad (3)$$

โดยที่

$$x_k^{(n)}[t] = r[t] - \sum_{l=1}^{k-1} D_l(\hat{\underline{b}}_{l,t}^{(n)}) \hat{g}_l^{(n)} - \sum_{l=k+1}^{K} D_l(\hat{\underline{b}}_{l,t}^{(n-1)}) \hat{g}_l^{(n-1)} \quad (4)$$

และ

$$X_{k,M}^{(n)} = \left\{ x_k^{(n)}[1] \quad x_k^{(n)}[2] \quad ,\ldots, \quad x_k^{(n)}[M] \right\}$$

จากคุณสมบัติของ kullblack-leibler เราจะพบว่า

$$\theta_k^{(n-1)} = \left(B_k^{(n-1)}, g_k^{(n-1)}, \sigma_k^{2(n-1)} \right)$$

1. $KL(P(\theta_k^{(n-1)} \mid X_{k,M}^{(n)}) \| P(\theta_k \mid X_{k,M}^{(n)})) \geq 0$
2. ถ้า $KL(P(\theta_k^{(n-1)} \mid X_{k,M}^{(n)}) \| P(\theta_k \mid X_{k,M}^{(n)}))$=0 แสดงว่า $P(\theta_k \mid X_{k,M}^{(n)}) = P(\theta_k^{(n-1)} \mid X_{k,M}^{(n)})$ ใน ทุกกรณีของ θ_k

ดังนั้นเราสามารถหา θ_k

ดังนั้นโดยการหาค่าต่ำสุดของอัตราส่วน kullblack-leibler เพื่อที่จะทำให้ $P(\theta_k \mid X_{k,M}^{(n)}) = P(\theta_k^{(n-1)} \mid X_{k,M}^{(n)})$ ดังนั้นเราจะได้ว่า

$$P(\theta_k \mid X_{k,M}^{(n)}) = \arg\min_{\theta_k} KL(P(\theta_k^{(n-1)} \mid X_{k,M}^{(n)}) \,||\, P(\theta_k \mid X_{k,M}^{(n)})) \tag{5}$$

ดังนั้นเราจะสามารถหาค่าของ

$$P(b_k[t] \mid X_k^{(n)}) \propto \exp\left(E_{\theta^{(n-1)}_{k\backslash b_k[t]}} \left[\ln P\left(\theta_k, X_k^{(n)}\right) \right] \right) \tag{6}$$

$$\theta_k^{(n-1)} = \left(b_k^{(n)}[t] \quad , \theta^{(n-1)}_{k\backslash b_k[t]} \right)$$

$$P(g_k \mid X_k^{(n)}) \propto \exp\left(E_{\theta^{(n-1)}_{k\backslash g_k}} \left[\ln P\left(\theta_k, X_k^{(n)}\right) \right] \right) \tag{7}$$

$$\theta_k^{(n-1)} = \left(g_k^{(n)} \quad , \theta^{(n-1)}_{k\backslash g_k} \right)$$

$$P(\sigma_k^2 \mid X_k^{(n)}) \propto \exp\left(E_{\theta^{(n-1)}_{k\backslash \sigma_k^2}} \left[\ln P\left(\theta_k, X_k^{(n)}\right) \right] \right) \tag{8}$$

$$\theta_k^{(n-1)} = \left(\sigma_k^{2(n)} \quad , \theta^{(n-1)}_{k\backslash \sigma_k^{2(n)}} \right)$$

ในการหาค่าของ (6) เราสามารถคำนวณได้จาก

$$P(b_k[t] \mid X_k^{(n)}) \propto \exp\left(E_{\theta^{(n-1)}_{k\backslash b_k[t]}} \left[\ln P\left(\theta_k, X_k^{(n)}\right) \right] \right)$$

$$P(b_k[t] \mid X_k^{(n)}) \propto \exp\left(E_{\theta^{(n-1)}_{k\backslash b_k[t]}} \left[\ln P\left(b_k[t], \theta_{k/b_k[t]}, X_k^{(n)}\right) \right] \right)$$

$$\propto \exp\left(E_{\theta^{(n-1)}_{k\backslash b_k[t]}} \left[\ln P\left(b_k[t], X_k^{(n)} \mid \theta_{k/b_k[t]}\right) \right] \right) + \exp\left(E_{\theta^{(n-1)}_{k\backslash b_k[t]}} \left[\ln P\left(\theta_{k/b_k[t]}\right) \right] \right)$$

$$P\left(b_k[t], X_k^{(n)} \mid \theta_{k/b_k[t]}\right) = \sum_{S_{k,t-1}} \alpha_{t-1}(S_{k,t-1}) \gamma_t\left(\underline{b}_{k,t}\right) \beta_t(S_{k,t})$$

$$P\left(b_k[t], X_k^{(n)} \mid \theta_{k/b_k[t]}\right) = \underbrace{\sum_{S_{k,t-1}} \alpha_{t-1}(S_{k,t-1}) P\left(x_k^{(n)}[t] \mid \underline{b}_{k,t}, \theta_{k/b_k[t]}\right) \beta_t(S_{k,t})}_{P_{ext}(b_k[t])} \cdot P(b_k[t])$$

โดยที่

$$\alpha_{t-1}(S_{k,t-1}) = P\left(S_{k,t-1} = b_k[t\text{-}1], X_{k,1:t-1}^{(n)} \mid \theta^{(n-1)}_{k\backslash b_k[t]}\right)$$

$$\alpha_t(S_{k,t}) = \frac{\sum_{S_{k,t-1}} \alpha_{t-1}(S_{k,t-1}) \gamma_t\left(\underline{b}_{k,t}\right)}{\sum_{S_{k,t}} \sum_{S_{k,t-1}} \alpha_{t-1}(S_{k,t-1}) \gamma_t\left(\underline{b}_{k,t}\right)}$$

$$\beta_t(S_{k,t}) = P\left(X_{k,t+1:M}^{(n)} \mid S_{k,t} = b_k[t], \theta^{(n-1)}_{k\backslash b_k[t]}\right)$$

$$\beta_{t-1}(S_{k,t-1}) = \frac{\sum_{S_{k,t}} \beta_t(S_{k,t}) \gamma_t\left(\underline{b}_{k,t}\right)}{\sum_{S_{k,t}} \sum_{S_{k,t-1}} \alpha_{t-1}(S_{k,t-1}) \gamma_t\left(\underline{b}_{k,t}\right)}$$

$$\gamma_t\left(\underline{b}_{k,t}\right) = P\left(S_{k,t} = b_k[t], x_k^{(n)}[t] \mid S_{k,t-1} = b_k[t\text{-}1], \theta^{(n-1)}_{k\backslash b_k[t]}\right)$$

$$= P\left(x_k^{(n)}[t] \mid \underline{b}_{k,t}, \theta^{(n-1)}_{k\backslash b_k[t]}\right) P\left(\underline{b}_{k,t}\right)$$

$$P\left(x_k^{(n)}[t] \mid \underline{b}_{k,t}, \theta^{(n-1)}_{k\backslash b_k[t]}\right) \propto \left(\frac{1}{\sigma_k^{2(n-1)}}\right)^N \mathbf{exp}\left(-\frac{1}{\sigma_k^{2(n-1)}} \left\| x_k^{(n)}[t] - D_k(\underline{b}_{k,t}) g_k^{(n-1)} \right\|^2 \right)$$

ในการหาค่าช่องสัญญาณโดยอาศัยวิธีการค่าต่ำสุดของอัตราส่วน kullblack-leibler ทำให้เราได้ว่า

$$P(g_k \mid X_k^{(n)}) \propto \exp\left(E_{\theta^{(n-1)}_{k\backslash g_k}} \left[\ln P\left(\theta_k, X_k^{(n)}\right) \right] \right)$$

โดยเรากำหนดให้ค่าของ g_k มีค่า priori

เป็น $P(g_k) \propto \mathbf{exp}\left\{-\left(g_k - g_k^{(n-1)}\right)^H \Sigma_{g_k}^{-1(n-1)} \left(g_k - g_k^{(n-1)}\right)\right\}$

เมื่อเราใช้ (5) ในการาค่า g_k เราจะได้

$$P(g_k \mid X_k^{(n)}) \propto \mathbf{exp}\left(-g_k^H \left[\sum_{t=1}^{M}\sum_{\underline{b}_{k,t}} \lambda_k\left(\underline{b}_{k,t}\right)\left(\frac{1}{\sigma_k^{2(n-1)}} D_k(\underline{b}_{k,t})^H D_k(\underline{b}_{k,t}) + \Sigma_{g_k}^{-1(n-1)}\right)\right] g_k\right) \cdot$$

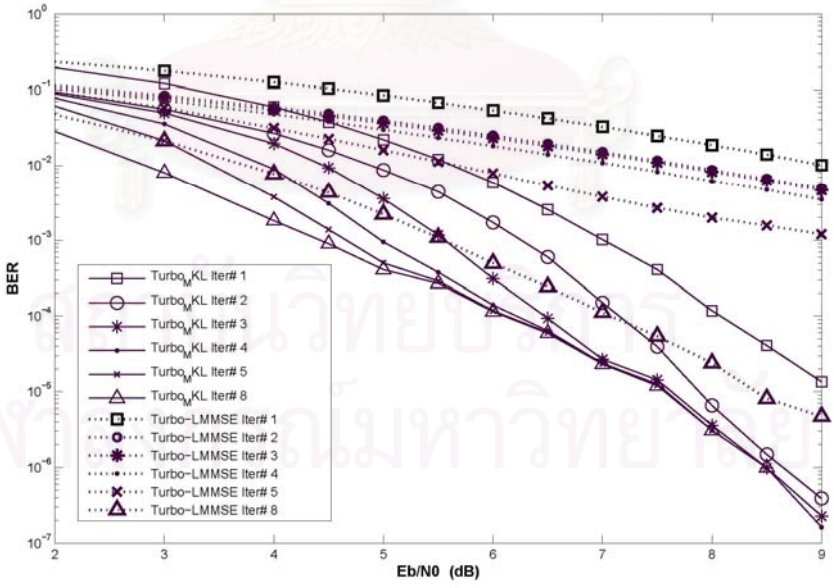
$$\mathbf{exp}\left(2\Re\left[g_k^H \left(\sum_{t=1}^{M}\sum_{\underline{b}_{k,t}} \lambda_k\left(\underline{b}_{k,t}\right)\left(\Sigma_{g_k}^{-1(n-1)} g_k^{(n-1)} + \frac{1}{\sigma_k^{2(n-1)}} D_k(\underline{b}_{k,t})^H x_k^{(n)}[t]\right)\right)\right]\right)$$

และสามารถคำนวณค่า g_k ได้

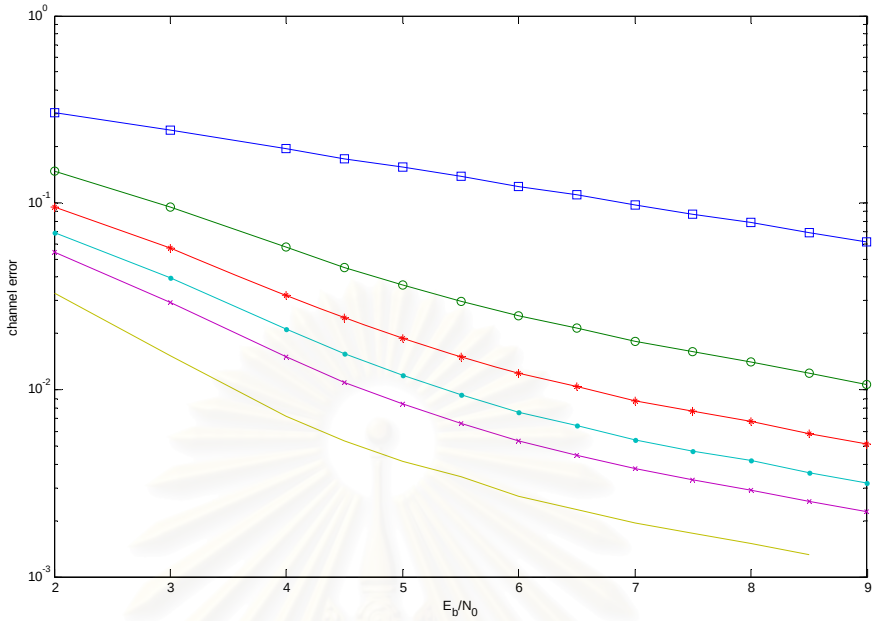
$$g_k^{(n)} = \left(I - \frac{\Sigma_{g_k}^{(n)}\Sigma_{k0}}{\sigma_k^{2(n-1)}}\right) g_k^{(n-1)} + \frac{\Sigma_{g_k}^{(n)}}{\sigma_k^{2(n-1)}} \sum_{t=1}^{M}\sum_{\underline{b}_{k,t}} \lambda_k\left(\underline{b}_{k,t}\right) D_k(\underline{b}_{k,t})^H x_k^{(n)}[t]$$

$$g_k^{(n)} = g_k^{(n-1)} + \frac{\Sigma_{g_k}^{(n)}}{\sigma_k^{2(n-1)}} \sum_{t=1}^{M}\sum_{\underline{b}_{k,t}} \lambda_k\left(\underline{b}_{k,t}\right) D_k(\underline{b}_{k,t})^H \left(x_k^{(n)}[t] - D_k(\underline{b}_{k,t}) g_k^{(n-1)}\right)$$

ผลการทดลอง



รูป 3. Performance BER Turbo-MKL และ turbo-LMMSE [7]

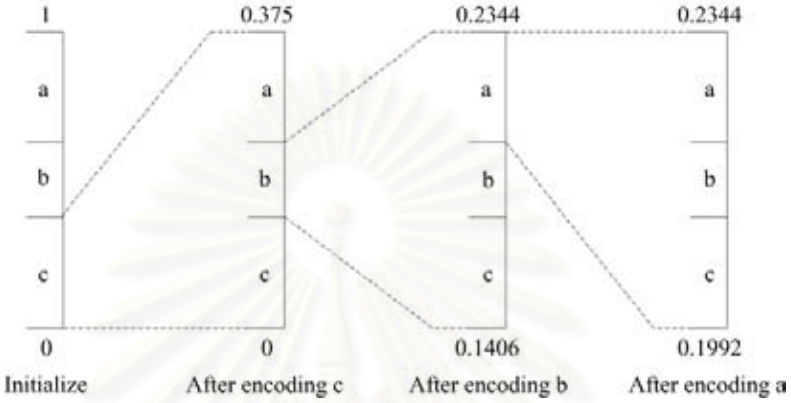


รูป 4. Performance of channel estimation error Turbo-MKL

การเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดนั้นสามารถทำได้โดยการเพิ่มสัญลักษณ์ต้องห้ามลงไปในตารางความน่าจะเป็นที่ใช้ในการเข้ารหัสเชิงเลขคณิต โดยจะต้องมีการกำหนดตำแหน่งของสัญลักษณ์ต้องห้ามไว้ล่วงหน้าเนื่องจากการเข้ารหัสและถอดรหัสจำเป็นที่จะต้องสามารถสร้างตารางความน่าจะเป็นที่ใช้ในการเข้ารหัสและถอดรหัสที่ตรงกันทั้งด้านตัวเข้ารหัสและตัวถอดรหัส เนื่องจากหากไม่สามารถที่จะสร้างตารางความน่าจะเป็นที่ตรงกันได้ข้อมูลที่ถอดรหัสออกมาจากรหัสที่รับมานั้นจะเป็นข้อมูลที่ไม่ถูกต้องโดยข้อมูลที่ถอดออกมานั้นจะเกิดความผิดพลาดแบบต่อเนื่อง เนื่องจากการเข้ารหัสเชิงเลขคณิตมีคุณสมบัติการแพร่กระจายของความผิดพลาด (Error Propagation) คือหากเกิดความผิดพลาดขึ้นครั้งหนึ่งจากการถอดรหัสเนื่องรหัสที่ได้รับไม่ถูกต้องหรือตารางที่ใช้ในการถอดรหัสไม่ตรงกันจะทำให้การถอดรหัสข้อมูลหลังจากจุดที่เกิดความผิดพลาดขึ้นจะเกิดความผิดพลาดตามไปด้วย

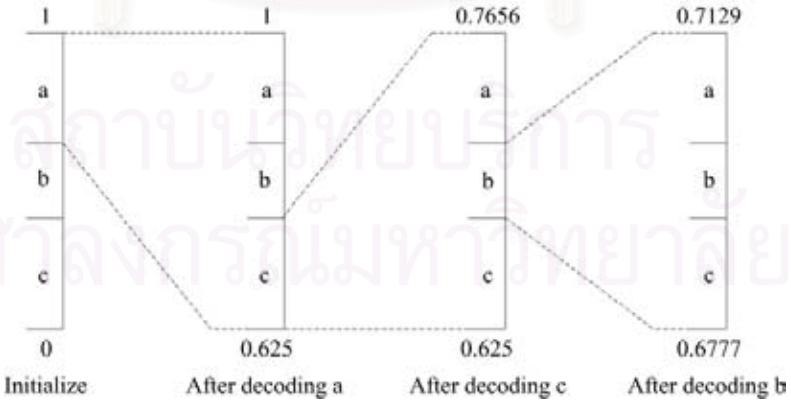
คุณสมบัติการแพร่กระจายของความผิดพลาดของการเข้ารหัสเชิงเลขคณิต สามารถอธิบายได้ด้วยตัวอย่างง่ายๆ ดังนี้ สมมติให้มีการเข้ารหัสข้อมูล *cba* โดยสัญลักษณ์ *c* มีค่าอยู่ในช่วง [0, 0.375) สัญลักษณ์ *b* มีค่าอยู่ในช่วง [0.375, 0.625) และสัญลักษณ์ *a* มีค่าอยู่ในช่วง [0.625, 1)

โดยหลังจากการเข้ารหัสดังในรูปที่ 1 แล้วเราจะได้ว่า รหัส *cba* สามารถแทนได้โดยใช้ค่าในช่วง [0.1992, 0.2344) ในที่นี้ใช้ 001101 ซึ่งมีค่าเท่ากับ 0.203125



รูปที่ 1 การเข้ารหัสเชิงเลขคณิตของ *cba*

หลังจากที่ทำการส่งข้อมูลที่ผ่านการเข้ารหัสเรียบร้อยแล้วหากรหัสที่ตัวถอดรหัสได้รับไม่ถูกต้องเช่นแทนที่จะได้รับรหัส 001101 กลับได้รับรหัส 101101 แทนทำให้การถอดรหัสแทนที่จะได้ข้อมูลที่ถูกต้องคือ *cba* กลับได้ข้อมูล *acb* แทนโดยการถอดรหัสของรหัส 101101 จะเป็นไปดังรูปที่ 2

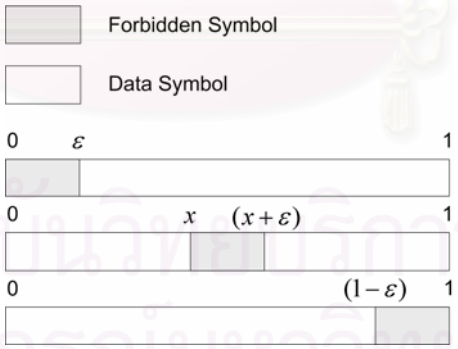


รูปที่ 2 การถอดรหัสของรหัส 101101

การที่บิตข้อมูลแรกที่ได้รับเปลี่ยนจาก 0 เป็น 1 ส่งผลให้ข้อมูลที่ถอดรหัสจากรหัสชุดนี้ผิดพลาดทั้งหมดถึงแม้ว่าข้อมูลที่เหลือจะถูกต้องทั้งหมดก็ไม่สามารถที่จะทำการถอดรหัสข้อมูลที่ถูกต้องได้ เช่นเดียวกันหากมีตารางความน่าจะเป็นที่ใช้ในการถอดรหัสครั้งใดไม่ตรงกับตารางความน่าจะเป็นที่ใช้ในการเข้ารหัสเพียงครั้งเดียวก็จะส่งผลให้การถอดรหัสที่เหลือทั้งหมดไม่ถูกต้องไปด้วย

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

ตำแหน่งที่ใช้ในการวางสัญลักษณ์ต้องห้ามก็มีส่วนในการเข้ารหัสและถอดรหัส ดังที่ได้กล่าวไปแล้วว่าหากไม่สามารถที่จะสร้างตารางความน่าจะเป็นที่ใช้ในการเข้ารหัสและถอดรหัสที่ตรงกันได้ก็จะไม่สามารถถอดรหัสข้อมูลที่ถูกต้องได้ ดังนั้นในระบบที่มีการใช้การเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดจำเป็นที่จะต้องมีการตกลงตำแหน่งของสัญลักษณ์ต้องห้ามไว้ก่อนล่วงหน้า โดยตำแหน่งของสัญลักษณ์ต้องห้ามอาจเป็นไปตามรูปแบบใดรูปแบบหนึ่งในรูปที่ 3



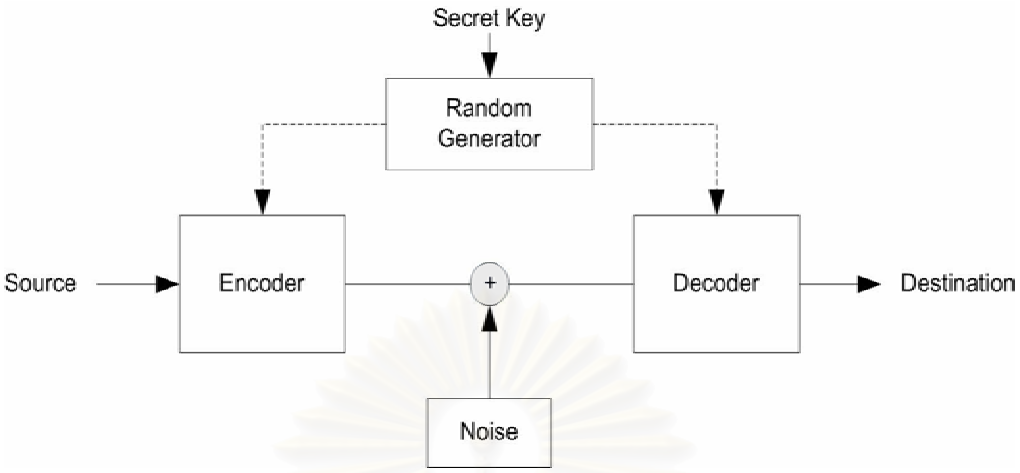
รูปที่ 3 ตำแหน่งของสัญลักษณ์ต้องห้าม

จะเห็นได้ว่าการวางสัญลักษณ์ต้องห้ามไว้ตรงกลางของตารางความน่าจะเป็นจะทำให้มีการคำนวณมากกว่าการวางสัญลักษณ์ต้องห้ามไว้ที่ปลายของตารางเนื่องจากมีการคำนวณเพียงฝั่งเดียว หากวางสัญลักษณ์ต้องห้ามไว้ตรงกลางของตารางความน่าจะเป็นจะต้องมีการคำนวณ 2 ฝั่ง ในกรณีที่เป็น การเข้ารหัสที่มีการใช้แบบจำลองแบบปรับได้ดังนั้นจึงควรเลือกใช้ตำแหน่งที่อยู่ที่ส่วนปลายของตาราง

ในระบบที่มีการใช้การเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดนั้นสามารถที่จะเพิ่มความสามารถในการเข้ารหัสลับได้โดยวิธีการดังต่อไปนี้ กำหนดให้ตำแหน่งของสัญลักษณ์ต้องห้ามมีการเปลี่ยนแปลงตำแหน่งทุกครั้งที่มีการเข้ารหัสสัญลักษณ์แต่ละสัญลักษณ์ โดยอาจกำหนดให้มีตำแหน่งของสัญลักษณ์สำหรับกุญแจแต่ละแบบดังรูปที่ 4

รูปที่ 4 ตำแหน่งของสัญลักษณ์ต้องห้ามและกุญแจ

การทำการเข้ารหัสลับในรูปแบบนี้จำเป็นที่จะต้องมีกุญแจที่มีจำนวนเท่ากับจำนวนของสัญลักษณ์ที่จะทำการเข้ารหัสโดยอาจสามารถสร้างได้โดยใช้ตัวกำเนิดสัญญาณไบนารีแบบสุ่มโดยใช้กุญแจลับ (Secret key) เป็นเมล็ด (Seed) ของกุญแจไบนารีที่มีความยาวเท่ากับสัญลักษณ์ที่จะทำการเข้ารหัส ทำให้สามารถเขียนระบบทั้งหมดที่ใช้ในการเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดและเข้ารหัสลับได้ดังรูปที่ 5



รูปที่ 5 ระบบเข้ารหัสเชิงเลขคณิตที่มีความสามารถในการตรวจจับความผิดพลาดและเข้ารหัสลับ

การเข้ารหัสในลักษณะดังกล่าวนั้นสามารถทำการขยายรูปแบบการใส่กุญแจได้โดยการเพิ่มตำแหน่งของกุญแจที่จะทำการใส่เพิ่มลงในข้อมูลโดยการเพิ่มจำนวนของตำแหน่งที่เป็นที่อยู่ของกุญแจนั้นจะไม่ส่งผลกับขนาดของข้อมูลที่ผ่านการเข้ารหัสแล้วเมื่อเทียบกับ

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.

[5]V. Smidl and A.Quinn, The Variational Bayes Method in Signal Processing Springer. Germany, 2006.

[6] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, Optimal decoding of linear codes for minimizing symbol error rate, IEEE Trans. Inform. Theory, vol. 20, pp. 284-287, Mar. 1974.

[7] X. Wang and H. Poor, “Iterative (turbo) soft interference cancellation and decoding for coded CDMA,” IEEE Trans. Commun., vol. 47, pp.1046-1061, 1999.

[8] M. Tuchler, A. Singer and R.Koetter, “Minimum mean squared error equalization using a priori information” IEEE Trans. Signal Processing,

vol. 50, pp. 673-683, March 2002.

[9] M. Tuchler, R. Koetter and A. Singer, “Turbo equalization : Principles and new results,” IEEE Trans. Commun., vol. 50, pp. 754-767, May 2002.

[10] R. Koetter, A.C. Singer, and M. Tuchler, “Turbo equalization,” IEEE Signal Processing Mag., vol. 21, no. 1, pp. 67-80, Jan. 2004.

[11] T. Abe and T.Matsumoto, “Space-time turbo equalization in frequencyselective MIMO channels,” IEEE Trans. Vehicular Technology, vol. 52, pp. 469 - 475, May 2003. V. Smidl and A.Quinn,

[12] S. Kullback and R. Leibler, On information and sufficiency, Annals of Mathematical Statistics, vol. 22, pp. 7987, 1951.