ความจุความลับของช่องสัญญาณไร้สาย

Secrecy Capacity of Wireless Channels

เกียรติศักดิ์ ใหม่เจริญนุกูล
วิทยาลัยเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยรังสิต

บทคัดย่อ

ตามที่การเชื่อมต่อแบบไร้สายมีการประยุกต์ใช้งานอย่างแพร่หลาย ความมั่นคงของการเชื่อมต่อดังกล่าวจึงเป็นประเด็นสำคัญ การเข้ารหัสลับแต่ดั้งเดิมเป็นวิธีหลักสำหรับการสื่อสารอย่างมั่นคง อย่างไรก็ตาม วิธีสร้างความมั่นคงนี้อาจนำไปปฏิบัติได้ยากในโครงข่ายไร้สายสมัยใหม่บางประเภท เช่น โครงข่ายเฉพาะกิจและโครงข่ายอาร์เอฟไอดีที่ต้องการการจัดการอย่างเป็นระบบขนาดใหญ่และความซับซ้อนในการคำนวณต่ำ ตามลำดับ วิธีทางเลือกหนึ่งคือความมั่นคงชั้นกายภาพ ซึ่งใช้ประโยชน์จากสมบัติทางกายภาพของช่องสัญญาณวิทยุเพื่อทำให้การส่งข้อมูลเชื่อถือได้โดยไม่ต้องอาศัยกุญแจถอดรหัสลับ เนื่องจากความมั่นคงชนิดนี้ปรากฏจากการแสดงความลับทางทฤษฎีสารสนเทศ จึงได้มีความสนใจอย่างมากในความจุความลับของช่องสัญญาณไร้สายประเภทต่าง ๆ บทความนี้จะอธิบายโดยย่อถึงความจุดังกล่าวสำหรับผู้ใช้เดียว

คำสำคัญ : ทฤษฎีสารสนเทศ, ความมั่นคงชั้นกายภาพ, ความจุความลับ, ช่องสัญญาณไร้สาย

Abstract

As wireless networking has a wide range of applications, its security is an issue of concern. Encryption is traditionally the main route to secure communications. Nevertheless, this security solution may be difficult to implement in some modern wireless networks, e.g., ad hoc and radio-frequency identification (RFID) networks which require large-scale organization and low computational complexity, respectively. An alternative approach is physical-layer security, which leverages the physical properties of radio channels to achieve reliable data transmission without the need of secret keys. Since this kind of security emerged from the information theoretical characterization of secrecy, there has been great interest in secrecy capacity of various wireless channels. This paper provides an overview of such capacity for a single user.

Keywords : Information theory, Physical-layer security, Secrecy capacity, Wireless channel

1. บทนำ

การสื่อสารไร้สายเป็นหนึ่งในเทคโนโลยีสมัยใหม่ที่มีอยู่ทุกหนทุกแห่ง อาทิ ระบบโทรศัพท์เคลื่อนที่แบบรังผึ้ง (Cellular Telephony) เนื่องจากโครงข่ายไร้สายถูกนำไปใช้ประโยชน์อย่างแพร่หลาย เช่น ธุรกรรมทางการเงิน การเข้าถึงเครือข่ายทางสังคม และการติดตามตรวจสอบสิ่งแวดล้อม ความมั่นคงของโครงข่ายดังกล่าวจึงเป็นประเด็นที่สำคัญ จากแบบจำลองโอเอสไอ (Open Systems Interconnection: OSI) ความมั่นคงนี้เดิมถูกทำให้เกิดผลที่ชั้น (Layer) สูง ๆ เช่น ชั้นแอพพลิเคชั่นที่สร้างความมั่นคงให้กับโครงข่ายวายฟาย (Wi-Fi) ด้วยโปรโตคอลดับเบิลยูอีพี (Wired Equivalent Privacy: WEP) และโปรโตคอลดับเบิลยูพีเอ (Wi-Fi Protected Access: WPA) [1]

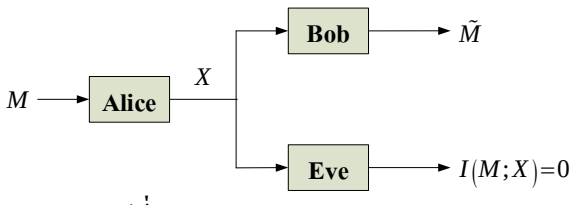
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การเข้ารหัสลับ (Encryption) เป็นวิธีการพื้นฐานอย่างหนึ่งสำหรับการรักษาความลับของข้อมูลและทำงานได้ดีในหลาย ๆ สถานการณ์ อย่างไรก็ตาม สำหรับสถาปัตยกรรมโครงข่ายสมัยใหม่ ประเด็นเกี่ยวกับการจัดการทรัพยากรหรือความซับซ้อนในการคำนวณอาจทำให้การเข้ารหัสลับข้อมูลทำได้ยาก ตัวอย่างเช่น โครงข่ายเฉพาะกิจ (Ad Hoc) ที่ซึ่งข้อความจากโหนดต้นทางอาจจะถูกส่งผ่านโหนดระหว่างทาง (Intermediate) เป็นจำนวนมากก่อนถึงโหนดปลายทาง และโครงข่ายอาร์เอฟไอดี (Radio-Frequency Identification: RFID) สำหรับอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things) ที่ซึ่งอุปกรณ์ปลายทาง (End Device) มีความซับซ้อนน้อยมาก [2] เมื่อไม่นานมานี้ การพัฒนาวิธีส่งผ่านข้อมูลอย่างมั่นคงโดยใช้คุณสมบัติทางกายภาพของช่องสัญญาณวิทยุได้รับความสนใจเป็นอย่างยิ่ง [3]-[11] ผลที่ได้เรียกว่าความมั่นคงชั้นกายภาพ (Physical-Layer Security) ซึ่งมีรากฐานมาจากการแสดงลักษณะของความลับในมุมมองของทฤษฎีสารสนเทศ (Information Theory)

ในการออกแบบโครงข่ายไร้สายให้มีความมั่งคงชั้นกายภาพนั้น ดัชนีสมรรถนะที่นำมาพิจารณาคือความจุความลับ (Secrecy Capacity) ของช่องสัญญาณไร้สาย บทความนี้จะนำเสนอพัฒนาการทางความจุดังกล่าว โดยเริ่มจากระบบความลับของ Shannon [3] ตามด้วยช่องสัญญาณดักฟังของ Wyner [4] และปิดท้ายด้วยการขยายผลไปสู่ช่องสัญญาณไร้สายประเภทต่าง ๆ [9]-[11]

2. ระบบความลับของ Shannon

Shannon เป็นคนแรกที่ศึกษาปัญหาการสื่อสารอย่างมั่นคงจากมุมมองของทฤษฎีสารสนเทศ [3] ระบบความลับที่ Shannon พิจารณาถูกแสดงในรูปที่ 1



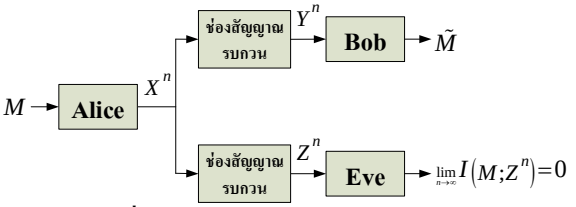
รูปที่ 1: ระบบความลับของ Shannon

จากรูปที่ 1 Alice Bob และ Eve ทำหน้าที่เป็นเครื่องส่ง เครื่องรับ และเครื่องดักฟัง ตามลำดับ Alice ต้องการส่งสาร M ไปยัง Bob โดยที่สารนี้ยังคงเป็นความลับต่อ Eve ทั้งนี้ Alice และ Bob มีกุญแจความลับร่วมกัน (แทนด้วย K) ซึ่ง Eve ไม่ทราบ เพื่อให้บรรลุวัตถุประสงค์ดังกล่าว Alice จะใช้ K เข้ารหัส M ไปเป็นอักษรรหัส (Codeword) X และ Bob จะใช้ K ถอดรหัส X เพื่อกู้คืน M

การสื่อสารในรูปที่ 1 จะมีความมั่นคงเมื่อสารสนเทศร่วม (Mutual Information) ระหว่างสาร M กับอักษรรหัส X ซึ่งเขียนแทนด้วย $I(M;X)$ มีค่าเท่ากับศูนย์ เนื่องจากสารสนเทศร่วมนี้สามารถเขียนอยู่ในรูปของเอนโทรปี (Entropy) ได้เป็น $I(M;X)=H(M)-H(M\mid X)$ โดยที่เอนโทรปี $H(M)=-\sum p(m)\log p(m)$ แสดงถึงความไม่แน่นอน (Uncertainty) เกี่ยวกับตัวแปรสุ่ม M, $p(m)$ คือความน่าจะเป็นที่ M มีค่าเท่ากับ m และเอนโทรปีแบบมีเงื่อนไข $H(M\mid X)$ คือความไม่แน่นอนในตัวแปรสุ่ม M หลังจากที่ได้สังเกตตัวแปรสุ่ม X ดังนั้น $I(M;X)=0$ หมายความว่าความไม่แน่นอนเกี่ยวกับสาร M มีค่าเท่ากับความไม่แน่นอนเกี่ยวกับสาร M หลังจากที่ได้สังเกตอักษรรหัส X หรือกล่าวอีกนัยหนึ่งสาร M และอักษรรหัส X นั้นเป็นอิสระต่อกันทางสถิติ เงื่อนไขดังกล่าวนำไปสู่ความลับสมบูรณ์ (Perfect Secrecy)

3. ช่องสัญญาณดักฟังของ Wyner

Wyner ได้นำเสนอช่องสัญญาณดักฟัง [4] ซึ่งมีรากฐานมาจากระบบความลับของ Shannon ความแตกต่างอยู่ตรงที่ไม่มีกุญแจความลับที่ Alice และ Bob แต่มีการรบกวนในช่องสัญญาณการสื่อสารดังแสดงในรูปที่ 2



รูปที่ 2: ช่องสัญญาณดักฟังของ Wyner

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 2 Alice ต้องการเข้ารหัสสาร M ไปสู่อักษรรหัส $X^n = (X_1,\ldots,X_n)$ เพื่อให้ Bob ผู้ซึ่งได้รับ $Y^n = (Y_1,\ldots,Y_n)$ สามารถกู้คืนสาร M ได้อย่างน่าเชื่อถือ (นั่นคือ $\lim_{n\to\infty} P\{\tilde{M} \neq M\} = 0$) ในขณะที่ M ยังคงเป็นความลับต่อ Eve ผู้ซึ่งได้รับ $Z^n = (Z_1,\ldots,Z_n)$

เนื่องจากมีการรบกวนในช่องสัญญาณสื่อสาร Wyner จึงแนะนำให้ผ่อนปรนหลักเกณฑ์ของความลับสมบูรณ์ที่เป็นจริงได้ยาก (นั่นคือ ความอิสระต่อกันทางสถิติระหว่างสาร M กับเอาต์พุตช่องสัญญาณ Z^n) ด้วยการพิจารณาความอิสระต่อกันเชิงเส้นกำกับ (Asymptotic) ตามความยาวของอักษรรหัส n แทน นั่นคือ $\lim_{n\to\infty} \frac{I(M;Z^n)}{n} = 0$ หลักเกณฑ์นี้มีชื่อว่าความลับแบบจาง (Weak Secrecy) ซึ่งแสดงถึงสารสนเทศเกี่ยวกับสาร M ที่รั่วไหลไปยัง Eve ในอัตรา (Rate) ที่ขึ้นอยู่กับความยาว n

เงื่อนไขข้างบนสามารถปรับให้เข้มงวดขึ้นด้วยการเอาพจน์ n ออก นั่นคือ $\lim_{n\to\infty} I(M;Z^n) = 0$ ซึ่งนำไปสู่ความลับแบบเข้มแข็ง (Strong Secrecy) [5] จะเห็นว่าจำนวนสารสนเทศที่รั่วไหลไปยัง Eve จะหายไปเมื่อ n มีค่ามากขึ้นโดยไม่มีที่สิ้นสุด ความลับแบบเข้มแข็งนี้ทำให้มั่นใจว่าอัตราความผิดพลาดของการถอดรหัสมีค่าเข้าใกล้ 1 แบบเอกซ์โพเนนเชียล ไม่ว่า Eve จะใช้แผนการถอดรหัสแผนใดก็ตาม [6]

Wyner ยังได้นิยามความจุความลับ (ซึ่งแสดงถึงอัตราสูงสุดที่ยังทำให้ความต้องการของ Alice บรรลุผล นั่นคือ Bob สามารถกู้คืนสารของ Alice ได้แต่ Eve ทำไม่ได้) สำหรับช่องสัญญาณดักฟังที่ไม่มีความจำเชิงวิยุต (Discrete Memoryless) ดังสมการที่ (1)

$$C_s = \max_{X\to Y\to Z} \left(I(X;Y) - I(X;Z)\right) \qquad (1)$$

โดยที่ $X \to Y \to Z$ แทนความสัมพันธ์แบบห่วงโซ่มาร์คอฟ (Markov Chain) ซึ่งนิยามดังนี้ กำหนดให้ $p(X,Z)$ เป็นการแจกแจงความน่าจะเป็นร่วม (Joint Probability Distribution) ของตัวแปรสุ่ม X และ Z, และ $p(X|Y)$ เป็นการแจกแจงความน่าจะเป็นแบบมีเงื่อนไขของตัวแปรสุ่ม X อันเนื่องจากตัวแปรสุ่ม Y (Conditional Probability Distribution of X Given Y) ดังนั้น X, Y และ Z จะมีความสัมพันธ์แบบห่วงโซ่มาร์คอฟ $X \to Y \to Z$ ก็ต่อเมื่อ $p(X,Z|Y) = p(X|Y)\,p(Z|Y)$ หรือกล่าวอีกนัยหนึ่ง X และ Z เป็นอิสระต่อกันแบบมีเงื่อนไข (Conditional Independent) อันเนื่องจาก Y [12] การทำให้มีค่าสูงสุดในสมการที่ (1) นั้นพิจารณาจากตัวแปรสุ่ม X, Y และ Z ทั้งหมดที่เป็นไปได้ตามความสัมพันธ์ดังกล่าว

ที่มาของความจุความลับในสมการที่ (1) สามารถอธิบายได้ดังนี้ Alice ไม่เพียงส่งสารลับไปยัง Bob แต่ต้องส่งสารดัมมี (ซึ่ง Bob และ Eve ไม่ทราบ) ด้วยโดยการสุ่มเลือกจากอักษรรหัสที่มีอยู่ด้วยอัตราเท่ากับ $I(X;Z)$ หรือตามคุณภาพช่องสัญญาณของ Eve ทำให้ Eve เต็มไปด้วยสารสนเทศที่ไร้ประโยชน์จากสารดัมมีและไม่เหลือทรัพยากรสำหรับการถอดรหัสสารลับ [7] เนื่องจาก $I(X;Y)$ เป็นอัตราที่ Alice สามารถส่งสารลับไปยัง Bob ได้อย่างน่าเชื่อถือ และ Bob ต้องถอดรหัสทั้งสารลับและสารดัมมีเพื่อให้กู้คืนได้อย่างถูกต้อง ดังนั้นอัตราที่เหลือสำหรับการส่งผ่านสารลับได้อย่างมั่นคงจึงมีค่าเท่ากับ $I(X;Y) - I(X;Z)$

4. ความจุความลับของช่องสัญญาณไร้สายประเภทต่าง ๆ

หัวข้อนี้จะขยายความจุความลับข้างบนไปสู่กรณีช่องสัญญาณไร้สายประเภทต่าง ๆ ได้แก่ ช่องสัญญาณเกาส์เซียน (Gaussian) ช่องสัญญาณหลายทางเข้าหลายทางออก (Multiple-Input Multiple-Output: MIMO) และช่องสัญญาณเฟดดิง (Fading)

4.1 ช่องสัญญาณเกาส์เซียน

ในช่องสัญญาณเกาส์เซียน สัญญาณที่ Bob และ Eve ได้รับจาก Alice สามารถเขียนได้เป็น

$$Y_i = hX_i + N_i \qquad (2)$$

$$Z_i = gX_i + W_i \qquad (3)$$

ตามลำดับ โดยที่ h และ g คืออัตราการขยาย (Gain) ของช่องสัญญาณระหว่าง Alice กับ Bob และช่องสัญญาณ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระหว่าง Alice กับ Eve ตามลำดับ, N_i และ W_i คือ สัญญาณรบกวนเกาส์เซียนขาวแบบบวก (Additive White Gaussian Noise) ที่มีค่าเฉลี่ยเป็นศูนย์และความแปรปรวนเท่ากับ σ_N^2 และ σ_W^2 ตามลำดับ และ i คือดรรชนีการใช้ช่องสัญญาณ ความจุความลับของช่องสัญญาณประเภทนี้สามารถคำนวณได้เป็น [8]

$$C_S = \frac{1}{2}\log\left(1+\frac{P|h|^2}{\sigma_N^2}\right) - \frac{1}{2}\log\left(1+\frac{P|g|^2}{\sigma_W^2}\right) \quad (4)$$

โดยที่ P คือขีดจำกัด (Limit) สำหรับค่าเฉลี่ยกำลังส่งของอักษรรหัส X_i (นั่นคือ $\frac{\sum_{i=1}^{n}\mathrm{E}\left[X_i^2\right]}{n} \le P$ โดยที่ $\mathrm{E}[\cdot]$ คือค่าคาดหมาย)

กลยุทธ์ที่ทำให้บรรลุความจุความลับในสมการที่ (4) คือการกำหนดให้ X_i มีการแจกแจงทางสถิติแบบเกาส์เซียนและค่ากำลังส่งเท่ากับ P สมการนี้ทำให้ทราบว่าการสื่อสารในช่องสัญญาณเกาส์เซียนจะมีความมั่นคงก็ต่อเมื่อ Bob มีคุณภาพช่องสัญญาณดีกว่า Eve ในแง่ที่ว่าอัตราส่วนสัญญาณต่อสัญญาณรบกวน (Signal-to-Noise Ratio) ของช่องสัญญาณระหว่าง Alice กับ Bob มีค่ามากกว่าอัตราส่วนสัญญาณต่อสัญญาณรบกวนของช่องสัญญาณระหว่าง Alice กับ Eve (นั่นคือ $|h|^2/\sigma_N^2 > |g|^2/\sigma_W^2$)

4.2 ช่องสัญญาณหลายทางเข้าหลายทางออก

เนื่องจากการใช้สายอากาศส่งและสายอากาศรับหลายเสาสามารถปรับปรุงสมรรถนะของการสื่อสารไร้สายได้อย่างมีประสิทธิภาพ [13] ช่องสัญญาณหลายทางเข้าหลายทางออกจึงได้รับความสนใจอย่างมาก สมมติให้ Alice Bob และ Eve มีสายอากาศจำนวน l, m และ k เสา ตามลำดับ สัญญาณที่ Bob และ Eve ได้รับจาก Alice สามารถเขียนอยู่ในรูปของเวกเตอร์ที่มีมิติ $m\times 1$ และ $k\times 1$ ดังสมการที่ (5) และ (6) ตามลำดับ

$$\vec{Y}_i = \mathbf{H}\vec{X}_i + \vec{N}_i \quad (5)$$

$$\vec{Z}_i = \mathbf{G}\vec{X}_i + \vec{W}_i \quad (6)$$

โดยที่ $\vec{X}_i$ คือเวกเตอร์อักษรรหัสของ Alice ที่มีมิติ $l\times 1$ และมีเงื่อนไขบังคับเป็น $\mathrm{Tr}[\mathbf{Q}] \le P$ เมื่อ $\mathbf{Q} = \mathrm{E}\left[\vec{X}_i\vec{X}_i^{\dagger}\right]$, $\mathrm{Tr}[\cdot]$ คือผลบวกของสมาชิกในแนวทแยงมุม (Trace) ของเมทริกซ์, $\mathbf{H}$ และ $\mathbf{G}$ คือเมทริกซ์ที่ประกอบด้วยอัตราการขยายของช่องสัญญาณระหว่าง Alice กับ Bob และช่องสัญญาณระหว่าง Alice กับ Eve ตามลำดับ และมีมิติ $m\times l$ และ $k\times l$ ตามลำดับ และ $\vec{N}_i$ และ $\vec{W}_i$ คือเวกเตอร์สัญญาณรบกวนเกาส์เซียนขาวแบบบวกที่มีค่าเฉลี่ยเป็นศูนย์และเมทริกซ์ความแปรปรวนเท่ากับเมทริกซ์เอกลักษณ์ (Identity Matrix) ความจุความลับของช่องสัญญาณประเภทนี้สามารถคำนวณได้เป็น [9]

$$C_S = \max_{\mathrm{Tr}(\mathbf{Q})\le P}\left(\frac{1}{2}\log\det\left(\mathbf{I}_m + \mathbf{HQH}^{\dagger}\right) - \frac{1}{2}\log\det\left(\mathbf{I}_k + \mathbf{GQG}^{\dagger}\right)\right) \quad (7)$$

โดยที่ $\mathbf{I}_m$ และ $\mathbf{I}_k$ คือเมทริกซ์เอกลักษณ์ที่มีมิติ $m\times m$ และ $k\times k$ ตามลำดับ

กลยุทธ์ที่ทำให้บรรลุความจุความลับในสมการที่ (7) จะเหมือนกับกลยุทธ์ที่ใช้ในหัวข้อ 4.1 แต่มีเงื่อนไขเพิ่มเติมคือเมทริกซ์ความแปรปรวน $\mathbf{Q}$ จะต้องถูกเลือกให้เหมาะที่สุดในแง่ที่ทำให้ผลต่างในวงเล็บมีค่าสูงที่สุด เนื่องจากโดยทั่วไปปัญหาการหาค่าเหมาะที่สุดนี้ไม่คอนเวกซ์ (Nonconvex) [14] รูปแบบแม่นตรง (Exact Form) ของ $\mathbf{Q}$ ที่เหมาะที่สุดจึงสามารถหาได้ในบางกรณีเท่านั้น ตัวอย่างเช่น กรณีที่ Alice มีสายอากาศหลายเสาและ Bob มีสายอากาศเพียงเสาเดียว ส่วน Eve อาจจะมีสายอากาศหลายเสา [10] ความจุความลับในกรณีนี้สามารถคำนวณได้เป็น

$$C_S = \frac{1}{2}\log\left(\lambda_{\max}\left(\mathbf{I}_l + P\mathbf{h}^{\dagger}\mathbf{h}, \mathbf{I}_l + P\mathbf{G}^{\dagger}\mathbf{G}\right)\right) \quad (8)$$

โดยที่ $\lambda_{\max}(\cdot,\cdot)$ เป็นค่าลักษณะเฉพาะทั่วไปสูงสุด (Maximum Generalized Eigenvalue) ของคู่ลำดับเมทริกซ์ [15] กลยุทธ์ที่ทำให้บรรลุความจุความลับในสมการที่ (8) คือการสร้างลำคลื่น (Beamforming) ในทิศทางของเวกเตอร์ลักษณะเฉพาะทั่วไป (Generalized Eigenvector) ที่สอดคล้องกับค่าลักษณะเฉพาะดังกล่าว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3 ช่องสัญญาณเฟดดิง

ในหัวข้อ 4.1 และ 4.2 ช่องสัญญาณที่พิจารณานั้นไม่มีการเปลี่ยนแปลงตลอดช่วงการสื่อสาร นั่นคือ อัตราการขยายของช่องสัญญาณระหว่าง Alice กับ Bob และช่องสัญญาณระหว่าง Alice กับ Eve เป็นค่าคงที่ อย่างไรก็ตาม สภาพนี้เกิดขึ้นจริงได้ยากในทางปฏิบัติเนื่องจากการแพร่กระจายของพหุวิถี (Multipath) และการแทรกสอดในการสื่อสารไร้สาย การเปลี่ยนแปลงที่เกิดขึ้นจากปัจจัยเหล่านี้เรียกว่าเฟดดิง

ในช่องสัญญาณเฟดดิง สัญญาณที่ Bob และ Eve ได้รับจาก Alice สามารถเขียนได้เป็น

$$Y_i = h_i X_i + N_i \tag{9}$$

$$Z_i = g_i X_i + W_i \tag{10}$$

โดยที่ตัวแปรต่าง ๆ มีนิยามตามสมการที่ (2) และ (3) ยกเว้น h_i และ g_i คือสัมประสิทธิ์การจางหายซึ่งแสดงถึงสภาพการสื่อสาร ณ ขณะเวลา i ในกรณีเฟดดิงแบบเออร์โกดิก (Ergodic) ที่ซึ่งสัมประสิทธิ์การจางหายเหล่านี้เป็นอิสระต่อกันและมีการแจกแจงเหมือนกัน (Independent and Identically Distributed) และเปลี่ยนแปลงตามเวลา ความจุความลับสามารถคำนวณได้เป็น [11]

$$C_S = \max_{\mathrm{E}_A[P(h,g)]\le P} \mathrm{E}_A\left[\frac{1}{2}\log\left(1+\frac{P(h,g)|h|^2}{\sigma_N^2}\right) - \frac{1}{2}\log\left(1+\frac{P(h,g)|g|^2}{\sigma_W^2}\right)\right] \tag{11}$$

โดยที่ $A=\left\{(h,g):\frac{|h|^2}{\sigma_N^2}>\frac{|g|^2}{\sigma_W^2}\right\}$, $\mathrm{E}_A[\cdot]$ คือค่าคาดหมายบนทุกคู่ลำดับ (h,g) ที่เป็นสมาชิกในเซต A,

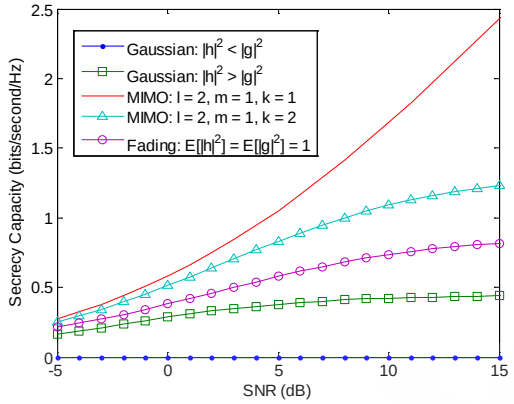
$$P(h,g)=\begin{cases}\dfrac{1}{\lambda\ln 2}-\dfrac{\sigma_N^2}{|h|^2}, \text{ if } |g|^2=0, \lambda<\dfrac{|h|^2}{\sigma_N^2\ln 2}\\ \dfrac{1}{2}\left[\sqrt{\left(\dfrac{\sigma_W^2}{|g|^2}-\dfrac{\sigma_N^2}{|h|^2}\right)\left(\dfrac{4}{\lambda\ln 2}-\dfrac{\sigma_N^2}{|h|^2}+\dfrac{\sigma_W^2}{|g|^2}\right)}-\dfrac{1}{2}\left(\dfrac{\sigma_N^2}{|h|^2}+\dfrac{\sigma_W^2}{|g|^2}\right)\right]^{1/2}, \text{ if } |g|^2>0,\\ \dfrac{|h|^2}{\sigma_N^2}>\dfrac{|g|^2}{\sigma_W^2}, \lambda<\dfrac{1}{\ln 2}\left(\dfrac{|h|^2}{\sigma_N^2}-\dfrac{|g|^2}{\sigma_W^2}\right)\\ 0, \text{ otherwise}\end{cases} \tag{12}$$

คือกำลังส่งที่เหมาะที่สุดโดยที่ λ ถูกเลือกให้สอดคล้องกับเงื่อนไขบังคับ $\mathrm{E}_A[P(h,g)]=P$ และดรรชนีการใช้ช่องสัญญาณ i ถูกละเว้นเพื่อความกระชับในการแสดงสมการ

กลยุทธ์ที่ทำให้บรรลุความจุความลับในสมการที่ (11) สามารถอธิบายได้ดังนี้ เริ่มจากการกำหนดให้ Alice และ Bob ทราบสารสนเทศของสถานะช่องสัญญาณอย่างสมบูรณ์ (Perfect Channel State Information) นั่นคือ ค่า h_i และ g_i สำหรับทุก i หรือที่เรียกว่าเรียวไลเซชัน (Realization) ของ h และ g ตามลำดับ เนื่องจากช่องสัญญาณการจางหายเหล่านี้สามารถจัดให้อยู่ในรูปเซตของช่องสัญญาณที่ขนานกันและไม่เปลี่ยนแปลงตามเวลา การจัดสรรกำลังส่งที่เหมาะที่สุดคือการให้กำลังส่งก็ต่อเมื่อเป็นไปตามเงื่อนไขที่ 1 และ 2 ในสมการที่ (12)

จากการเปรียบเทียบช่องสัญญาณเกาส์เซียนกับช่องสัญญาณเฟดดิง จะเห็นว่าการสื่อสารในช่องสัญญาณประเภทแรกจะมีความมั่นคงก็ต่อเมื่อเหตุการณ์ $|h|^2/\sigma_N^2>|g|^2/\sigma_W^2$ เกิดขึ้นแน่นอน นั่นคือ $\mathrm{P}\{|h|^2/\sigma_N^2>|g|^2/\sigma_W^2\}=1$ ส่วนสำหรับช่องสัญญาณประเภทหลังต้องการ $\mathrm{P}\{|h|^2/\sigma_N^2>|g|^2/\sigma_W^2\}>0$ (หรือกล่าวอีกนัยหนึ่ง มีอย่างน้อยหนึ่งเรียวไลเซชันของ h และ g ที่ซึ่ง $|h|^2/\sigma_N^2>|g|^2/\sigma_W^2$) และ λ ที่สอดคล้องกับเงื่อนไขที่ 1 หรือ 2 ในสมการที่ (12) เพื่อให้การสื่อสารมีความมั่นคง ดังนั้น เฟดดิงจึงเป็นประโยชน์ต่อการส่งผ่านสารลับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3: ความจุความลับของช่องสัญญาณเกาส์เซียน ช่องสัญญาณหลายทางเข้าหลายทางออก และช่องสัญญาณเฟดดิง ($\sigma_N^2 = \sigma_W^2$)

รูปที่ 3 แสดงผลการจำลองความจุความลับของช่องสัญญาณไร้สายประเภทต่าง ๆ ดังนี้

(1) ช่องสัญญาณหลายทางเข้าหลายทางออก โดยที่ Alice Bob และ Eve มีสายอากาศจำนวน 2, 1 และ 2 เสา ตามลำดับ ($l = 2, m = 1, k = 2$) และ $\mathbf{h} = \begin{bmatrix} 0.0991 - j0.8676 & 1.0814 + j1.1281 \end{bmatrix}$, $\mathbf{G} = \begin{bmatrix} 0.3880 + j1.2024 & -0.9825 + j0.5914 \\ 0.4709 - j0.3073 & 0.6815 - j0.2125 \end{bmatrix}$ ในสมการที่ (8) ซึ่งเหมือนกับที่กำหนดใน [10]

(2) ช่องสัญญาณหลายทางเข้าหลายทางออก โดยที่ Alice Bob และ Eve มีสายอากาศจำนวน 2, 1 และ 1 เสา ตามลำดับ ($l = 2, m = 1, k = 1$) และ $\mathbf{h} = \begin{bmatrix} 0.0991 - j0.8676 & 1.0814 + j1.1281 \end{bmatrix}$, $\mathbf{g} = \begin{bmatrix} 0.3880 + j1.2024 & -0.9825 + j0.5914 \end{bmatrix}$ ในสมการที่ (8) ซึ่งเหมือนกับที่กำหนดใน [10]

(3) ช่องสัญญาณเกาส์เซียน โดยที่ h และ g ในสมการที่ (4) มีขนาดเท่ากับของสมาชิกตัวแรกของ **h** และ **g** ข้างบน ตามลำดับ ดังนั้น $|h|^2 = 0.7626$ และ $|g|^2 = 1.5963$ ซึ่งเป็นตัวอย่างของกรณี $|h|^2 < |g|^2$

(4) ช่องสัญญาณเกาส์เซียน โดยที่ h และ g ในสมการที่ (4) มีขนาดเท่ากับของสมาชิกตัวหลังของ **h** และ **g** ข้างบน ตามลำดับ ดังนั้น $|h|^2 = 2.442$ และ $|g|^2 = 1.3151$ ซึ่งเป็นตัวอย่างของกรณี $|h|^2 > |g|^2$

(5) ช่องสัญญาณเฟดดิง โดยที่ h และ g ในสมการที่ (11) เป็นตัวแปรสุ่มเชิงซ้อนแบบเกาส์เซียน (Complex Gaussian Random Variable) ซึ่งเป็นอิสระต่อกัน และทั้งคู่มีค่าเฉลี่ยเท่ากับ 0 และความแปรปรวนเท่ากับ 1 (เหมือนกับที่กำหนดใน [11]) ดังนั้น $|h|^2$ และ $|g|^2$ มีการแจกแจงแบบเอกซ์โพเนนเชียลด้วยพารามิเตอร์เท่ากับ 1

ทั้งนี้ กำหนดให้ $\sigma_N^2 = \sigma_W^2$ สำหรับทุกช่องสัญญาณเพื่อความสะดวกในการจำลองผล และแกนนอนแสดงอัตราส่วนสัญญาณต่อสัญญาณรบกวน (Signal-to-Noise Ratio: SNR) ซึ่งก็คือ $\frac{P}{\sigma_N^2}$ [10]-[11]

ผลการจำลองในรูปที่ 3 แสดงให้เห็นว่าความจุความลับของช่องสัญญาณเกาส์เซียนจะมากกว่าศูนย์เมื่อ $\frac{|h|^2}{\sigma_N^2} > \frac{|g|^2}{\sigma_W^2}$ ตามที่ได้กล่าวไว้ข้างบน ส่วนสำหรับช่องสัญญาณหลายทางเข้าหลายทางออก ความจุความลับจะขึ้นอยู่กับจำนวนสายอากาศที่ใช้ด้วย เช่น ความจุนี้จะลดลงเมื่อ Eve มีสายอากาศมากขึ้น [10]

นอกจากช่องสัญญาณที่กล่าวมาทั้งหมดข้างต้น ซึ่งประกอบด้วยผู้ส่ง ผู้รับ และผู้ดักฟังอย่างละ 1 คน ยังมีงานอื่น ๆ ที่วิเคราะห์ความจุความลับในกรณีที่ซับซ้อนยิ่งขึ้น ตัวอย่างเช่น ช่องสัญญาณบรอดคาซท์ (Broadcast) ที่มีผู้รับหลายคน [16], ช่องสัญญาณเข้าถึงหลายทาง (Multiple Access) ที่มีผู้ส่งหลายคน [17] และช่องสัญญาณแทรกสอด (Interference) ที่มีทั้งผู้ส่งและผู้รับหลายคน [18] ผู้ที่สนใจกรณีเหล่านี้สามารถศึกษารายละเอียดได้จากเอกสารอ้างอิงดังกล่าว

5. สรุป

บทความนี้ได้นำเสนอพื้นฐานและสาระสำคัญเกี่ยวกับความจุความลับของช่องสัญญาณไร้สาย การวิเคราะห์ความจุนี้ด้วยทฤษฎีสารสนเทศได้แสดงให้เห็นว่าชั้นกายภาพสามารถทำให้เกิดความมั่นคงในการส่งผ่านข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในทางปฏิบัติการสร้างความมั่นคงชั้นกายภาพมีอยู่หลายวิธีด้วยกัน เช่น การสร้างกุญแจความลับจากสัมประสิทธิ์ช่องสัญญาณระหว่างผู้ส่งและผู้รับ [19]-[20], การสื่อสารแบบกลับทางเวลา (Time Reversal) ระหว่างผู้ส่งและผู้รับ [21] และการสร้างสัญญาณรบกวนเทียม (Artificial Noise) ที่ผู้ส่งหรือผู้รับ [22]-[23]

การวิเคราะห์ข้างบนต้องการสารสนเทศของสถานะช่องสัญญาณอย่างสมบูรณ์ อย่างไรก็ตาม เงื่อนไขนี้อาจเป็นไปได้ยากในทางปฏิบัติ ตัวอย่างเช่น ถ้าผู้ดักฟังไม่ใช่ผู้ใช้งานจริงในโครงข่ายไร้สาย ก็ย่อมจะไม่เปิดเผยสารสนเทศใด ๆ เกี่ยวกับช่องสัญญาณของตน ความจุความลับของช่องสัญญาณไร้สายในกรณีดังกล่าวเป็นประเด็นที่จะศึกษาต่อไป

6. เอกสารอ้างอิง

[1] E. Tews and M. Beck, "Practical Attacks Against WEP and WPA," in Proceedings of the Second ACM Conference on Wireless Network Security, New York, NY, 2009, pp. 79-86.

[2] P. Guillemin and P. Friess, "Internet of Things—Strategic Research Roadmap," European Commission, Brussels, Belgium, Technical Report, September, 2009.

[3] C. E. Shannon, "Communication Theory of Secrecy Systems," The Bell System Technical Journal, Vol. 28, No. 4, pp. 656-715, October, 1949.

[4] A. D. Wyner, "The Wire-Tap Channel," The Bell System Technical Journal, Vol. 54, No. 8, pp. 1355-1387, October, 1975.

[5] U. Maurer and S. Wolf, "From Weak to Strong Information-Theoretic Key Agreement," in Proceedings of International Symposium on Information Theory, Sorrento, Italy, 2000, p. 18.

[6] I. Bjelakovic, H. Boche, and J. Sommerfeld, "Secrecy Results for Compound Wiretap Channels. Problems of Information Transmission, Vol. 49, No. 1, pp. 73-98, January, 2013.

[7] J. L. Massey, "A Simplified Treatment of Wyner's Wire-Tap Channel," in Proceedings of the 21st Allerton Conference on Communication, Control and Computing, Monticello, IL, October, 1983, pp. 268-276.

[8] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian Wire-Tap Channel," IEEE Transactions on Information Theory, Vol. 24, No. 4, pp. 451-456, July, 1978.

[9] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," IEEE Transactions on Information Theory, Vol. 57, No. 8, pp. 4961-4972, August, 2011.

[10] A. Khisti and G. W. Wornell, "Secure Transmission with Multiple Antennas—Part I: The MISOME Wiretap Channel," IEEE Transactions on Information Theory, Vol. 56, No. 7, pp. 3088-3104, July, 2010.

[11] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure Communication over Fading Channels," IEEE Transactions on Information Theory, Vol. 54, No. 6. pp. 2470-2492, June, 2008.

[12] T. M. Cover and J. A. Thomas, "Elements of Information Theory," Wiley, New York, NY, Second Edition, 2006.

[13] E. Biglieri, R. Calderbank, A. Constantinides, A. Goldsmith, A. Paulraj, and H. V. Poor, "MIMO Wireless Communications," Cambridge University Press, New York, NY, 2010.

[14] S. P. Boyd and L. Vandenberghe, "Convex Optimization," Cambridge University Press, New York, NY, 2004.

[15] G. Golub and C. F. V. Loan, "Matrix Computations," Johns Hopkins University Press, Baltimore, MD, Third Edition, 1996.

[16] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Message," IEEE Transactions on Information Theory, Vol. 24, No. 3, pp. 339-348, May, 1978.

[17] Y. Liang and H. V. Poor, "Multiple-Access Channels with Confidential Messages," IEEE Transactions on Information Theory, Vol. 54, No. 3, pp. 972-1002, March, 2008.

[18] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete Memoryless Interference and Broadcast Channels with Confidential Messages: Secrecy

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Rate Regions," IEEE Transactions on Information Theory, Vol. 54, No. 6, pp. 2493-2507, June, 2008.

[19] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-Telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel," in Proceedings of the 14th Annual International Conference on Mobile Computing and Networking, San Francisco, CA, 2008, pp. 128-139.

[20] A. Sayeed and A. Perrig, "Secure Wireless Communications: Secret Keys through Multipath," in Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, Las Vegas, NV, 2008, pp. 3013-3016.

[21] Y. Chen, F. Han, Y.-H. Yang, H. Ma, Y. Han, C. Jiang, H.-Q. Lai, D. Claffey, Z. Safar, and K. J. R. Liu, "Time-Reversal Wireless Paradigm for Green Internet of Things: An Overview," IEEE Internet of Things Journal, Vol. 1, No. 1, pp. 81-98, February, 2014.

[22] R. Negi and S. Goel, "Guaranteeing Secrecy Using Artificial Noise," IEEE Transactions on Wireless Communications, Vol. 7, No. 6, pp. 2180-2189, June, 2008.

[23] S. Gollakota and D. Katabi, "Physical Layer Wireless Security Made Fast and Channel Independent," in Proceedings of IEEE Conference on Computer Communications, Shanghai, China, 2011, pp. 1125-1133.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้