
# วิทยานิพนธ์

## การป้องกันการบุกรุกแบบไซบิลและการบุกรุกแบบอิคลิปส์ในเครือข่ายเพียร์ทูเพียร์

## DEFENDING SYBIL ATTACK AND ECLIPSE ATTACK ON PEER-TO-PEER NETWORK

นายณัฐวุฒิ กิจบุตราวัฒน์

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์

พ.ศ. ๒๕๕๑

# ใบรับรองวิทยานิพนธ์

**บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์**

วิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์)

**ปริญญา**

| วิศวกรรมคอมพิวเตอร์ | วิศวกรรมคอมพิวเตอร์ |
|---|---|
| **สาขา** | **ภาควิชา** |

**เรื่อง** การป้องกันการบุกรุกแบบไซบิลและการบุกรุกแบบอิคลิปส์ในเครือข่ายเพียร์ทูเพียร์

Defending Sybil Attack and Eclipse Attack on Peer-to-Peer Network

**นามผู้วิจัย** นายณัฐวุฒิ กิจบุตราวัฒน์

**ได้พิจารณาเห็นชอบโดย**

**อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก** .....

( ผู้ช่วยศาสตราจารย์จิตรทัศน์ ฝักเจริญผล, Ph.D. )

**อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม** .....

( อาจารย์ชัยพร ใจแก้ว, Ph.D. )

**หัวหน้าภาควิชา** .....

( ผู้ช่วยศาสตราจารย์เขมะฑัต วิภาตะวนิช, Ph.D. )

**บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์รับรองแล้ว**

.....

( รองศาสตราจารย์กัญจนา ธีระกุล, D.Agr. )

**คณบดีบัณฑิตวิทยาลัย**

วันที่ 5 เดือน มิถุนายน พ.ศ. 2551

วิทยานิพนธ์

เรื่อง

# การป้องกันการบุกรุกแบบไซบิลและการบุกรุกแบบอิคลิปส์ในเครือข่ายเพียร์ทูเพียร์

Defending Sybil Attack and Eclipse Attack on Peer-to-Peer Network


โดย

นายณัฐวุฒิ กิจบุตราวัฒน์


เสนอ

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์
เพื่อความสมบูรณ์แห่งปริญญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์)
พ.ศ. 2551

ณัฐวุฒิ กิจบุตราวัฒน์ 2551: การป้องกันการบุกรุกแบบไซบิลและการบุกรุกแบบอิคลิปส์ในเครือข่ายเพียร์ทูเพียร์ ปริญญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์) สาขาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก: ผู้ช่วยศาสตราจารย์จิตรทัศน์ ฝักเจริญผล, Ph.D. 37 หน้า

งานวิจัยนี้นำเสนอแนววิธีการป้องกันการบุกรุกในระบบเครือข่ายแบบเพียร์ทูเพียร์ที่ไม่มีโครงสร้างและไม่มีศูนย์กลางในการตรวจสอบ ได้แก่การบุกรุกในแบบไซบิลและการบุกรุกแบบอิคลิปส์

สำหรับปัญหาการบุกรุกแบบไซบิล งานวิจัยนี้ได้เสนอการปรับปรุงโปรโตคอลไซบิลการ์ด (SybilGuard) ที่ Yu et al. ได้นำเสนอในปี 2006 โดยได้เสนอวิธีการตรวจสอบแบบท้องถิ่นที่เมื่อนำไปใช้กับโปรโตคอลไซบิลการ์ดแล้ว สามารถรับประกันคุณภาพของการตรวจสอบได้กับทุก ๆ โหนดในเครื่องข่าย งานวิจัยนี้ได้พิสูจน์คุณภาพของวิธีการปรับปรุงดังกล่าวภายใต้โมเดลโลกใบเล็กบนพารามิเตอร์บางค่า และได้ใช้การจำลองสถานการณ์เพื่อวัดประสิทธิภาพในกรณีอื่น ๆ

สำหรับปัญหาการบุกรุกแบบอิคลิปส์ ที่ผู้บุกรุกต้องการควบคุมการสื่อสารของผู้ใช้ออกจากกลุ่มผู้ใช้อื่น ๆ เพื่อที่จะปิดกั้นหรือตรวจสอบการเข้าถึงเนื้อหานั้น งานวิจัยนี้ใช้อาศัยคุณสมบัติการขยายตัวที่ดีของเครือข่ายแบบเพียร์ทูเพียร์ เพื่อตรวจสอบว่าผู้ใช้กำลังอยู่ภายใต้การบุกรุกแบบอิคลิปส์ หรือไม่เช่นนั้นก็จะหาเพียร์อื่น ๆ ให้กับโหนดของผู้ใช้เพื่อหนีออกจากการปิดบังที่เกิดจากการบุกรุกแบบอิคลิปส์

ณัฐวุฒิ กิจบุตราวัฒน์ ศิรเทศัย ปานเจนดี 29 / 05 / 51

ลายมือชื่อนิสิต ลายมือชื่ออาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

Nathavuth Kitbutrawat 2008: Defending Sybil Attack and Eclipse Attack on Peer-to-Peer Network. Master of Engineering (Computer Engineering), Major Field: Computer Engineering, Department of Computer Engineering. Thesis Advisor: Assistant Professor Jittat Fakcheroenphol, Ph.D. 37 pages.

Peer-to-peer networks allow users to share information, thus performing, at the same time, as information producers and consumers. To increase the rate of information sharing, most networks have very open policies for joining. This makes the system venerable to various forms of attacks. More over, the lack of centralized control in peer-to-peer networks makes the traditional defensive methods not applicable to the peer-to-peer settings.

This thesis considers two types of attacks in peer-to-peer networks: Sybil attacks and Eclipse attack.

For Sybil attacks problem, we propose a local verification method that when using with SybilGuard gives a worst case performance guarantee. The method check if identities around an entity are honest. Under a small-world social network model with some parameter, this method is proven to give a guarantee for any honest user with high probability.

For Eclipse attacks where a group of malicious users try to control or block information from a target node to the other nodes, this thesis exploits the expansion property of peer-to-peer networks to design a protocol for handling Eclipse attacks. More specifically, the protocol can either ensure that either the user is under an eclipse attack, or provide a new peer that helps the user breaks the attack.

Nathavuth Kitbotrawat — Student's signature

Jittat Fakcheroenphol — Thesis Advisor's signature

3/06/08

# กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จลงได้ด้วยความช่วยเหลือจากผู้ช่วยศาสตราจารย์ จิตรทัศน์ ฝักเจริญผล ประธานกรรมการที่ปรึกษา ผู้ให้คำปรึกษาและแนวทางการทำวิจัย ตลอดจนข้อเสนอแนะที่มีประโยชน์ต่องานวิจัยนี้ อาจารย์ชัยพร ใจแก้ว กรรมการที่ปรึกษาวิชาเอก และ ผู้ช่วยศาสตราจารย์ อรรถสิทธิ์ สุรฤกษ์ อาจารย์ผู้ทรงคุณวุฒิจากภายนอก ที่ให้ข้อเสนอแนะที่มีคุณค่า เพื่อให้วิทยานิพนธ์นี้สมบูรณ์ยิ่งขึ้น

ข้าพเจ้าขอขอบคุณเพื่อนๆ นิสิตปริญญาโท, สมาชิกกลุ่มวิจัยเชิงทฤษฎี, เพื่อนๆ พี่ๆ ที่ศูนย์วิจัยเทคโนโลยีและคอมพิวเตอร์แห่งชาติ และบุคคลในครอบครัว ที่ช่วยเหลือข้าพเจ้าจนสามารถทำงานวิจัยชิ้นนี้สำเร็จได้ ขอขอบคุณเจ้าหน้าที่ธุรการ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาตร์ที่คอยอำนวยความสะดวกด้านประสานงาน และการดำเนินงานต่างๆ

ณัฐวุฒิ กิจบุตราวัฒน์

พฤษภาคม 2551

# สารบัญ

# สารบัญตาราง

# สารบัญภาพ

# สารบัญภาพ (ต่อ)

# การป้องกันการบุกรุกแบบไซบิลและการบุกรุกแบบอิคลิปส์ในเครือข่ายเพียร์ทูเพียร์

**Defending Sybil Attack and Eclipse Attack on Peer-to-Peer Network**

## คำนำ

ปัญหาการบุกรุกในระบบเครือข่ายเป็นปัญหาที่สำคัญปัญหาหนึ่งในปัจจุบันที่ระบบเครือข่ายถูกนำมาใช้มากขึ้น โดยในงานวิจัยนี้ได้สนใจระบบเครือข่ายแบบเพียร์ทูเพียร์ (peer-to-peer networks) ซึ่งเป็นระบบที่มีการทำงานในลักษณะของระบบแบบกระจาย (Distributed system) โดยจะมีการรับส่งข้อมูลระหว่างกันโดยไม่จำเป็นต้องผ่านตัวกลาง อย่างไรก็ตามระบบนี้ได้เป็นที่นิยมอย่างมากในปัจจุบัน

ระบบเครือข่ายแบบเพียร์ทูเพียร์มีปัญหาการโจมตีหลายรูปแบบ ไม่ต่างจากการโจมตีที่มีอยู่ในระบบเครือข่ายรูปแบบอื่นๆ แต่จะมีรูปแบบการโจมตีในบางรูปแบบที่กล่าวเฉพาะในเครือข่ายแบบเพียร์ทูเพียร์คือ การบุกรุกแบบไซบิล (Sybil Attack) และ การบุกรุกแบบอิคลิปส์ (Eclipse Attack) ซึ่งในงานวิจัยนี้จะสนใจในการแก้ปัญหาของการบุกรุกทั้ง 2 แบบนี้

การบุกรุกแบบไซบิล โดยปัญหานี้ถูกเสนอโดย Douceur (2002) ซึ่งเป็นปัญหาเกี่ยวกับการสร้างอัตลักษณ์ (Identity) จำนวนมากจากเอกลักษณ์ (Entity) เดียว ซึ่งในปกติในระบบเครือข่ายหนึ่งเอกลักษณ์จะมีเพียงหนึ่งอัตลักษณ์ใช้แสดงตน เพื่อทำให้เกิดความไม่เป็นธรรมและความผิดพลาดของระบบ

ส่วนการบุกรุกแบบอิคลิปส์นั้นถูกเสนอโดย Singh et al (2004) เป็นปัญหาการหลอกให้ผู้ใช้งานมาเชื่อมต่อกับกลุ่มผู้มุ่งร้าย ทำให้ผู้มุ่งร้ายสามารถควบคุมการสื่อสารของผู้ถูกโจมตีได้ และการโจมตีแบบอิคลิปส์สามารถนำการโจมตีแบบไซบิลเพื่อช่วยสร้างกลุ่มโหนดสำหรับโจมตีแบบอิคลิปส์ได้

# วัตถุประสงค์

1. ศึกษาและปรับปรุงวิธีการป้องกันการโจมตีแบบไซบิลในเครือข่ายแบบเพียร์ทูเพียร์
2. ศึกษาและพัฒนาวิธีการป้องกันการโจมตีแบบอิคลิปส์ในเครือข่ายแบบเพียร์ทูเพียร์

# การตรวจเอกสาร

## มาร์คอฟเชน (Markov Chain)

มาร์คอฟเชนเป็นกระบวนการแบบสุ่ม (Stochastic process) จะมีสถานะต่างๆ และมีคุณสมบัติมาร์คอฟ (Markov Property) คือความน่าจะเป็นที่จะอยู่ในสถานะใดๆ จะขึ้นกับสถานะที่เพิ่งผ่านมาเท่านั้น (Motwani และReghavan, 1995)

**นิยามที่ 1** *ตัวแปรสุ่ม $X_t$ เป็นสถานะที่อยู่ที่เวลา $t$ และ $P$ เป็นความน่าจะเป็นในการเดิน (Transition Probability) ให้ $P_{ij}$ เป็นความน่าจะเป็นที่จะเดินจากสถานะ $i$ ไปสถานะ $j$ จะได้ว่า*

$$P_{ij} = Pr[X_{t+1}=j \mid X_t=i, X_{t-1}=i_{t-1}, X_{t-2}=i_{t-2}, \ldots, X_0=i_0] = Pr[X_{t+1}=j \mid X_t=i]$$

ในกระบวนการสุ่มทำงานในระยะเวลานานมากพอจะเข้าสู่ค่าการกระจายตัวคงที่ (Stationary distribution) $\pi$ ที่ $\pi = \pi P$

## การเดินแบบสุ่มบนกราฟ (Random Walks on Graph)

การเดินสุ่มเป็นกระบวนการสุ่มสำหรับการเลือกสถานะตามลำดับ ในการเดินสุ่มบนกราฟสำหรับโหนด $u$ เลือกโหนด $v$ ที่ติดกันด้วยการสุ่ม จากนั้นเดินไปยังโหนด $v$ ที่เลือกนั้น และสุ่มเลือกเดินไปยังโหนดที่ติดกับโหนด $v$ (Motwani และReghavan, 1995)

สำหรับกราฟไม่มีทิศทาง G=(V,E) ที่ $|V| = n$ และ $|E| = m$ และเมตริกซ์ของความน่าจะเป็นในการเดินทาง (transition matrix) $P$ จะเป็นเมตริกขนาด $n \times n$ ให้ $P_{ij}$ เป็นความน่าจะเป็นที่จะเดินทางจากโหนด i ไปโหนด j จะได้ว่า

$$P_{ij} = \frac{1}{d(i)} \text{ เมื่อมีเส้นเชื่อมระหว่าง i และ j}$$

*เมื่อ d(i) คือ จำนวนเส้นเชื่อมที่ติดกับสถานะ $i$* นอกจากนั้น $P_{ij} = 0$

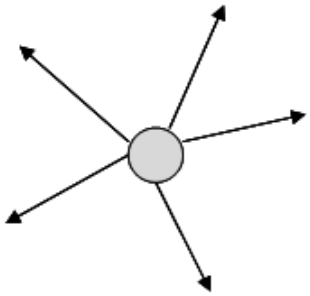
**นิยามที่ 2** (Motwani และReghavan, 1995) *กราฟ $G = (V, E)$ สำหรับ $v \in V$ จะได้ว่าการกระจายตัวคงที่สำหรับการเดินแบบสุ่มที่สถานะ v ใดๆเท่ากับ $\pi_v = d(v)/2m$ เมื่อ d(v) คือ จำนวนเส้นเชื่อมที่ติดกับสถานะ v*

จากนิยามกล่าวได้ว่าหากเดินสุ่มในกราฟนานพอ ความน่าจะเป็นที่จะเดินสุ่มไปที่โหนด $v$ จะเข้าสู่ค่าการกระจายตัวคงที่ $\pi_v = d(v)/2m$

**เครือข่ายสังคม (Social networks)**

เครือข่ายสังคมคือกราฟที่แสดงความสัมพันธ์เชิงสังคมระหว่างคู่ของโหนด ยกตัวอย่างเช่น กราฟแสดงการรู้จักกันของผู้ใช้บนโปรแกรมส่งรับข้อความ อาจมีเส้นเชื่อมระหว่างผู้ใช้สองคนถ้าทั้งคู่อยู่ในรายการติดต่อ (contact list) ของอีกฝ่าย (Yu et al., 2006)

เครือข่ายสังคมจะมีลักษณะเป็นกราฟไม่มีทิศทาง(Undirected Graph) และความน่าจะเป็นในการเลือกเส้นทางเดินของโหนดหนึ่งๆในกราฟจะกระจายตัวแบบสม่ำเสมอ (uniform distributed) โดยกราฟจะมีลักษณะเหมือนกราฟขยาย (Expander Graph) ดังนั้นจึงมีคุณสมบัติผสมอย่างรวดเร็ว (fast mixing) ซึ่งจะกล่าวในหัวข้อถัดไป



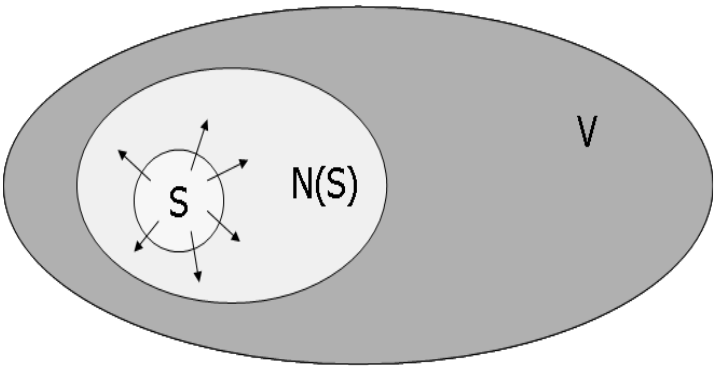
**ภาพที่ 1** โหนดที่มี 5 เส้นเชื่อมและความน่าจะเป็นที่จะเลือกเส้นทางแต่ละเส้นเท่ากับ 0.2

สำหรับเครือข่ายเชิงสังคมได้มีความพยายามที่จะสร้างแบบจำลองลักษณะการเชื่อมต่อโหนดในกราฟลักษณะนี้คือแบบจำลองโลกใบเล็ก โดยแบบจำลองดังกล่าวที่ได้รับการยอมรับคือแบบจำลอง “โลกใบเล็ก” ของ Kleinberg (2000)

**กราฟขยาย (Expander Graph)**

กราฟขยายคือกราฟเชื่อมต่อ (Connected Graph) ที่มีลักษณะกระจายตัวที่ดี เป็นกราฟที่มีสับเซต $S$ ของกราฟ จะมีเส้นเชื่อมออกไปเชื่อมต่อกับโหนดจำนวนมากที่อยู่ข้างนอกสับเซต $S$ (Motwani และReghavan, 1995)

**นิยามที่ 3** (Motwani และReghavan, 1995) *กราฟ $G=(V,E)$ เป็นกราฟขยาย สำหรับ $S \subseteq G$ และ $N(S)$ คือเซตของโหนดใกล้เคียงของ $S$ สำหรับ $|S| \le |V|/2$ จะมีจำนวนจริงคงที่ $\alpha$ ที่ $|N(S)| = \alpha * |S|$*




**ภาพที่ 2** การขยายของกราฟ

**นิยามที่ 4** (Motwani และReghavan, 1995) *ถ้ากราฟ $G=(V,E)$ เป็นกราฟขยายโหนดสองโหนดที่สุ่มเลือกมาจาก 2 ตำแหน่งใดๆบนกราฟ G ถ้าสร้างเส้นทางแบบสุ่มๆออกมาจากทั้ง 2 โหนดจะมีคุณสมบัติผสมเร็ว (fast mixing) กล่าวคือทั้งสองเส้นทางจะพบกันในเวลา $O(\log(n))$ เมื่อ n คือจำนวนโหนดทั้งหมด*

ดังนั้นการเดินทาง $O(\log(n))$ ครั้งก็เพียงพอที่จะเดินทั่วกราฟ โดยจะมีอัลกอริทึมสำหรับสร้างกราฟรูปแบบนี้คือ กราฟสุ่มแบบทั่วไป (Random Regular Graph) กับกราฟสุ่มดีกรีสม่ำเสมอ (Random d-Regular Graph)

**แบบจำลองกราฟสุ่มดีกรีสม่ำเสมอ (Random d-Regular Graph)**

เป็นแบบจำลองกราฟขยาย สำหรับกราฟ G=(V,E) โดยที่ V คือเซตของโหนดและ E คือเซตของเส้นเชื่อม สำหรับ $|V| = n$ และ $|E| = m$ และจำนวนเส้นเชื่อมที่ออกจากทุกๆโหนด $v \in V$ ใดๆจะเท่ากับ d เส้น สำหรับเซต $S \in V$ และ $N(S)$ คือเซตของโหนดที่เชื่อมต่อกับเซต S จะได้ว่า

อัตราการขยายตัว (expansion rate) $h(G)$ จะมีค่าเท่ากับ $|N(S)|/|S|$ สำหรับจำนวนโหนดในเซต S ที่ $|S| \le n/2$

สำหรับกราฟขยายที่มีการกำหนดขนาดดีกรี ให้ A คือ Adjacency Matrix คือ matrix ขนาด $n \times n$ ให้ $A_{ij} = 1$เมื่อโหนด i มีเส้นเชื่อมกับโหนด j นอกจากนั้น $A_{ij} = 0$ สำหรับค่าไอเกน $\lambda_1, \lambda_2, \lambda_3, ...\lambda_{n-1}$จะได้ $\lambda_1 = d$ และ $\lambda_1 \ge \lambda_2 \ge \lambda_3 \ge ... \ge \lambda_{n-1}$

**ทฤษฎีบทที่ 1** (Tanner, 1984; Alon และ Milman, 1985; Alon, 1986) *สำหรับกราฟสุ่มดีกรีสม่ำเสมอ* $G = (V, E)$ *ที่* $|V| = n$ *มีดีกรีเท่ากับ d สำหรับ Adjacency Matrix A มีค่าไอเกน* $\lambda_1, \lambda_2, \lambda_3, ...\lambda_{n-1}$ *ที่* $\lambda_1 = d$ *และ* $\lambda_1 \ge \lambda_2 \ge \lambda_3 \ge ... \ge \lambda_{n-1}$ *สำหรับสับเซต* $S \in V$ *ที่* $|S| \le |V|/2$ *จะมีอัตราการขยาย h(G) คือ*

$$\frac{d - \lambda_2}{2} \le h(G) \le \sqrt{2d(d - \lambda_2)}$$

**ทฤษฎีบทที่ 2** (Friedman, 2003) *ค่าไอเกน (eigenvalues) ลำดับที่ 2 สำหรับกราฟแบบสุ่มดีกรีสม่ำเสมอ (random d-regular)* $G = (V, E)$ *ที่* $|V| = n$ *มีดีกรี d และมีค่า* $\varepsilon > 0$ *จะได้ว่า*

$$\lambda_2 \le 2\sqrt{d-1} + \varepsilon$$

*ด้วยความน่าจะเป็น* $1 - n^{-\Omega(d)}$

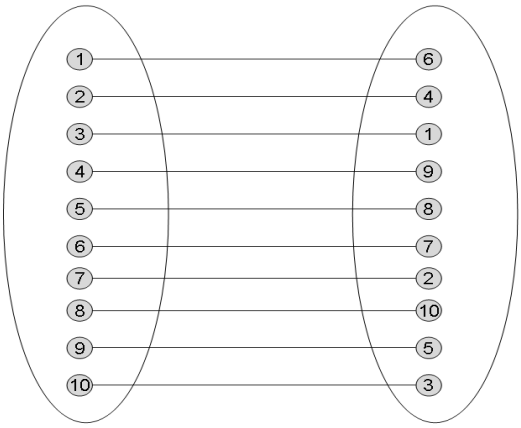
จากทฤษฎีบทที่ 1 และทฤษฎีบทที่ 2 เราจะได้ทฤษฎีบทที่ 3 ซึ่งจะได้ใช้ต่อไปเมื่อเราวิเคราะห์วิธีการแก้ปัญหาการบุกรุกแบบอีคลิปส์

**ทฤษฎีบทที่ 3** *สำหรับกราฟสุ่มดีกรีสม่ำเสมอ* $G = (V, E)$ *ที่* $|V| = n$ *มีดีกรีเท่ากับ d ถ้า* $\lambda_2 \le 2\sqrt{d-1} + o(1)$ *อัตราการขยายตัว* $h(G)$ *จะมีค่าไม่ต่ำกว่า* $d/2$ *ด้วยความน่าจะเป็นที่สูง*

**พิสูจน์** นำค่าไอเกนลำดับที่ 2 จากทฤษฎีบทที่ 2 ไปแทนในทฤษฎีบทที่ 1 จะได้ว่าอัตราการขยายตัวของกราฟสุ่มดีกรีสม่ำเสมอ $h(G)$ ที่มีดีกรีเท่ากับ $d$ จะมากกว่า $d/2$ เนื่องจากทฤษฎีบทที่ 2 เป็นจริงด้วยความน่าจะเป็นที่สูงดังนั้น $h(G) \ge d/2$ เป็นจริงด้วยความน่าจะเป็นที่สูง ■

สำหรับอัลกอริทึมที่ใช้สร้างกราฟสุ่มดีกรีสม่ำเสมอจะเป็นการทำ 2d-regular จะได้กราฟสุ่มดีสม่ำเสมอดีกรี 2d สำหรับการสร้างกราฟ $G$=($V$,$E$) ที่ $|V| = n$ โหนด สร้างเซต $V'$ ที่เหมือนกับเซต $V$ จากนั้นทำการเรียงลำดับเซต $V'$ แบบสุ่ม (random permutation) สำหรับเซต $V'$ แล้วให้จับคู่

ระหว่างโหนดในเซต *V* กับเซต *V'* ที่อยู่ตำแหน่งตรงกัน จากนั้นทำการสร้างเส้นเชื่อมระหว่างโหนดใน *G* ที่เป็นโหนดที่ถูกจับคู่กันระหว่างเซต *V* กับเซต *V'*




**ภาพที่ 3** วิธีการสร้างกราฟด้วยอัลกอริทึมกราฟสุ่มดีกรี 2d สม่ำเสมอ (Random 2d-regular Graph)

จากรูปจะเห็นว่าแต่ละโหลดจะได้เส้นเชื่อมเพิ่ม 2 เส้น เช่นในภาพที่ 3 โหนด 1 จะมีการสร้างเส้นเชื่อมกับโหนดที่ 6 และโหนดที่ 3 ก็มีเส้นเชื่อมไปโหนดที่ 1 เช่นกัน จากนั้นวน d รอบก็จะได้กราฟที่มีดีกรีเท่ากับ 2d

**แบบจำลองโลกใบเล็ก (Small world)**

Kleinberg (2000) ได้เสนอแบบจำลองโลกใบเล็กเป็นอัลกอริทึมที่ใช้สร้างแบบจำลองโดยกำหนดให้มีโหนดจำนวน $N^2$ โหนดจะวางตัวอยู่ในตารางขนาด $N \times N$ จากนั้นการเชื่อมต่อจะถูกระบุโดยพารามิเตอร์สามตัวคือ p , q และ r โหนดทุกโหนดจะมีเส้นเชื่อมไปยังทุก ๆ โหนดที่มีระยะบนตารางดังกล่าวไม่เกิน p จากนั้นแต่ละโหนด v จะมีเส้นเชื่อม q เส้น เชื่อมกับโหนดอื่นๆ ที่ถูกสุ่มมา โดยมีความน่าจะเป็นที่จะมีเส้นเชื่อมไปยังโหนด u ที่อยู่ห่างเป็นระยะ d(v,u) ด้วยความน่าจะเป็นที่แปรผันตรงกับ $d(v,u)^{-r}$

**แบบจำลองพรีเฟอร์เรนเชียล (Preferential Attachment Model)**

Barabasi และ Albert (1999) ได้เสนอแบบจำลองสำหรับระบบเครือข่ายเวิลด์ไวด์เว็บ มีคุณสมบัติกระจายตัวแบบขนาดอิสระและกฎกำลัง (scale-free power-law distribution) โดยคุณสมบัตินี้จะเกิดจาก เครือข่ายขยายตัว (expand) อย่างต่อเนื่องจากการเพิ่มโหนดใหม่ และโหนด

ใหม่จะเชื่อมต่อกับโหนดเก่าที่มีการเชื่อมต่อที่ดี ในการสร้างแบบจำลองจะคำนึงคุณสมบัติทั้งสองที่กล่าวมาดังนี้

1. เครือข่ายขยายตัวอย่างต่อเนื่อง (scale-free) เริ่มต้นด้วยโหนด $m_0$ โหนด ทุกๆ 1 ช่วงเวลาให้เพิ่มโหนดหนึ่งโหนดที่มีเส้นเชื่อม $m$ เส้น ที่ $m \le m_0$ ไปยังโหนดในระบบ $m$ โหนดที่ไม่ซ้ำกัน

2. โหนดใหม่จะเชื่อมต่อกับโหนดเก่าที่มีการเชื่อมต่อที่ดี (preferential attachment) การเลือกสร้างเส้นเชื่อมสำหรับโหนดใหม่ จะทำการเลือกโหนดในระบบด้วยความน่าจะเป็น $\prod$ สำหรับการเลือกโหนด i ที่มีเส้นเชื่อม $k_i$ เส้นจะได้ $\prod = k_i / \sum k$ กล่าวคือโหนดที่มีเส้นเชื่อมมากจะมีความน่าจะเป็นที่จะถูกเลือกสูง

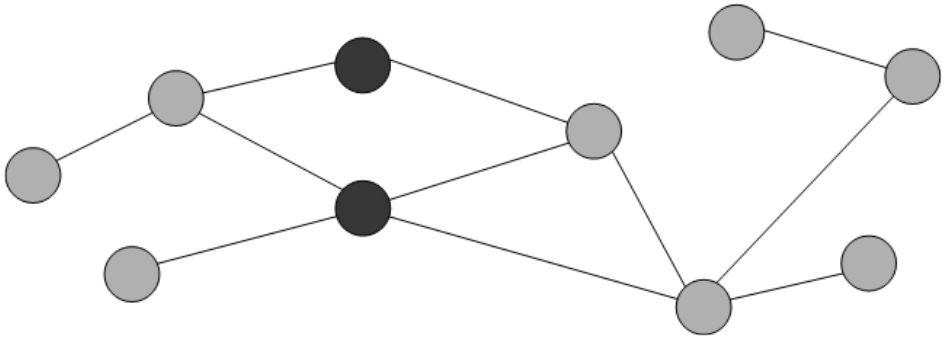
ในงานวิจัยนี้จะสร้างแบบจำลองโดยใช้ $m_0$ และ $m$ เป็น $d+1$ และ $d$ ตามลำดับ กล่าวคือในการเริ่มต้นจะเลือกโหนดมา $d+1$ โหนดจากนั้นสร้างเส้นเชื่อมถึงกันหมด จากนั้นค่อยๆเพิ่มโหนดใหม่ สุ่มโหนด m โหนดที่อยู่ในระบบมาเชื่อมต่อกับโหนดที่เพิ่มเข้ามาใหม่ โดยความน่าจะเป็นในการเลือกโหนดที่จะสร้างเส้นเชื่อมด้วยจะเป็นการกระจายตัวแบบสม่ำเสมอ (uniform distribution)

**การบุกรุกแบบไซบิล**

การบุกรุกแบบไซบิลถูกนำเสนอโดย Douceur (2002) เป็นการนำเสนอรูปแบบของการโจมตีรูปแบบใหม่ในระบบเครือข่ายเพียร์ทูเพียร์ มีลักษณะของการโจมตีเพื่อทำให้เกิดความไม่เท่าเทียมกันโดยอาศัยว่า ตามปกติสำหรับเอกลักษณ์ใดๆ จะมีอัตลักษณ์ใช้แทนเพียงแค่อัตลักษณ์เดียว ระบบจะทำการจัดสรรค์ทรัพยากรอย่างเท่าเทียม ซึ่งการโจมตีที่ว่านี้จะทำการสร้างอัตลักษณ์จำนวนมากจากเอกลักษณ์เดียวเพื่อให้ได้รับการจัดสรรค์ทรัพยากรมากกว่าที่ควรจะเป็น การแก้ปัญหาการบุกรุกแบบไซบิลจะถูกจัดเป็น 2 ประเภทใหญ่ๆคือการแก้ปัญหาแบบใช้ศูนย์กลางในการตรวจสอบกับแบบไม่ใช้ศูนย์กลางในการตรวจสอบ ในงานวิจัยนี้จะสนใจการแก้ปัญหาการบุกรุกแบบไซบิลที่ไม่ใช้ศูนย์กลางในการตรวจสอบ

**การโจมตีแบบอิคลิปส์**

การโจมตีแบบอิคลิปส์ถูกนำเสนอโดย Singh et al. (2004) สำหรับการโจมตีแบบอิคลิปส์ในเครือข่ายเพียร์ทูเพียร์ เป็นการโจมตีเพื่อต้องการควบคุมการสื่อสารของโหนดที่ถูกโจมตี โดยจะโจมตีในลักษณะของการจัดการเรื่องเส้นเชื่อมต่อเพื่อให้โหนดที่ถูกโจมตีถูกแบ่งแยกออกจากกลุ่มโหนดอื่นดังรูป



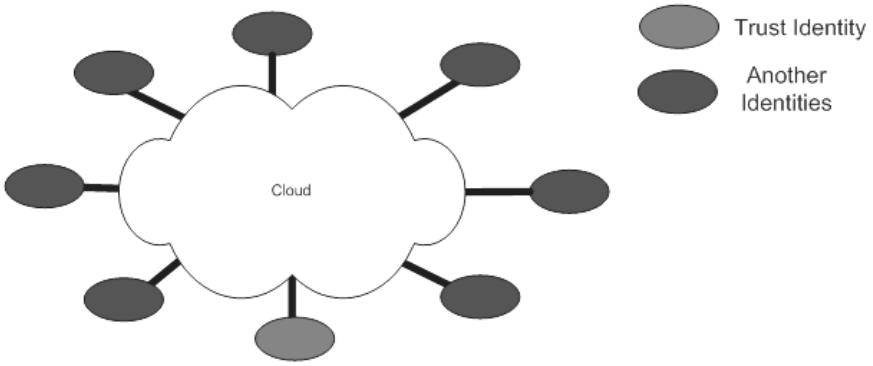
**ภาพที่ 4** ลักษณะการโจมตีแบบอิคลิปส์โดยผู้มุ่งร้าย

จากรูป จะเห็นได้ว่ากลุ่มโหนดทางซ้ายกับกลุ่มโหนดทางขวาถูกคั่นด้วยโหนดที่มุ่งร้าย แสดงด้วยโหนดสีดำ โดยหากมีการสื่อสารระหว่างโหนด 2 กลุ่ม ผู้มุ่งร้ายสามารถควบคุมข้อมูลที่ส่งกันได้ และการโจมตีแบบอิคลิปส์สามารถนำการโจมตีแบบไซบิลซึ่งสร้างโหนดปลอมจำนวนมากมาช่วยในการสร้างการโจมตีได้

## งานวิจัยในอดีตของปัญหาการบุกรุกแบบไซบิล

### การบุกรุกแบบไซบิล (The Sybil Attack)

Douceur (2002) ได้เสนอโมเดลในการศึกษาการบุกรุกแบบไซบิล โดยพิจารณาการเชื่อมต่อในระบบเครือข่ายเป็นแบบกลุ่มเมฆ ผู้ใช้แต่ละคนจะสื่อสารกับเครือข่ายนี้โดยรับส่งข้อความ (message) กับระบบเครือข่าย ในโมเดลนี้ผู้ใช้จะไม่ทราบว่าคนอื่น ๆ ที่ติดต่อด้วยเชื่อมต่อมาจากที่ใด




**ภาพที่ 5** แบบจำลองเครือข่ายเป็นแบบกลุ่มเมฆ

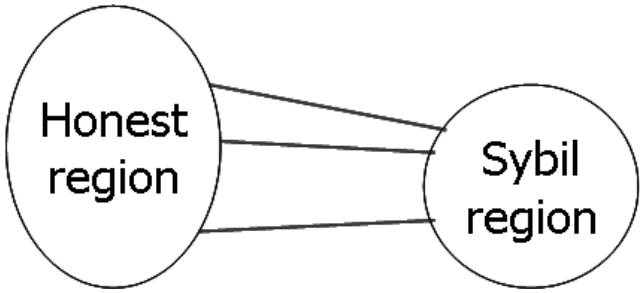
ในโมเดลดังกล่าว การตรวจสอบเดียวที่ทำได้คือการส่งการท้าทาย (challenge) ที่จะต้องตอบสนองโดยใช้ทรัพยากรบางอย่าง (เช่น เวลาการประมวลผล ความกว้างช่องสัญญาณ หรือ เนื้อที่หน่วยความจำสำรอง) ที่จะตอบสนองทันสำหรับเอกลักษณ์เดียวเท่านั้น ไม่สามารถตอบแทนหลายอัตลักษณ์ได้ เช่น ส่งจำนวนเต็มขนาดใหญ่ให้แยกตัวประกอบเป็นต้น ถ้าอัตลักษณ์ทั้งสองสามารถตอบสนองได้ทันทั้งคู่ ก็เป็นการยืนยันว่าอัตลักษณ์สองอัตลักษณ์เป็นอัตลักษณ์ที่ไม่ได้มาจากเอกลักษณ์เดียวกัน เนื่องจากในระบบแบบกระจายความแตกต่างเรื่องทรัพยากรจึงมีมาก ทำให้การส่งการท้าทายจะไม่ต้องการทรัพยากรที่มากเกินไป ไม่เช่นนั้นแล้วผู้ใช้ที่มีทรัพยากรต่ำจะไม่สามารถใช้งานระบบได้ ด้วยเหตุผลนี้ Douceur จึงกล่าวว่าหากเอกลักษณ์ที่มีทรัพยากรสูงกว่าทรัพยากรน้อยที่สุดที่ต้องการอย่างน้อย b เท่าจะสามารถสร้างอัตลักษณ์ได้ b อัตลักษณ์ นอกจากนี้ Douceur กล่าวอีกว่าจะไม่สามารถป้องกันการบุกรุกแบบไซบิลไม่ได้ถ้าการตรวจสอบอัตลักษณ์ที่เข้ามาพร้อมกันด้วยคนละเวลากัน หรือให้โหนดที่ยอมรับไปแล้วช่วยในการตัดสินใจ ดังนั้นแล้ว Douceur จึงสรุปว่าจะไม่สามารถป้องกันการบุกรุกแบบไซบิลได้ ถ้าไม่มีระบบกลางในการยืนยันตัว

**ไซบิลการ์ด (SybilGuard)**

Yu et al. (2006) ได้นำเสนอไซบิลการ์ด (SybilGuard) ที่เป็นวิธีที่ใช้จัดการกับการบุกรุกแบบไซบิลในระบบแบบกระจาย (Distributed System) ในระบบนี้สิ่งที่แตกต่างจากโมเดลของ Douceur (2002) คือการนำข้อมูลเกี่ยวกับความสัมพันธ์ทางสังคมระหว่างอัตลักษณ์ต่าง ๆ มาใช้ประโยชน์ ความสัมพันธ์นี้แสดงอยู่ในรูปของเครือข่ายสังคม (Social network) ข้อสมมติดังกล่าวทำให้ Yu et al. สามารถสร้างระบบที่ทำงานโดยไม่ใช้ระบบกลางในการยืนยันตัว และควบคุมความ

รุนแรงของการบุกรุกแบบไซบิลได้ สาเหตุที่ Yu et al. ไม่ใช้ระบบกลางในการตรวจสอบเนื่องจากมองว่าระบบกลางในการยืนยันตัวนั้นง่ายต่อการโจมตีและล้มเหลวได้ง่าย

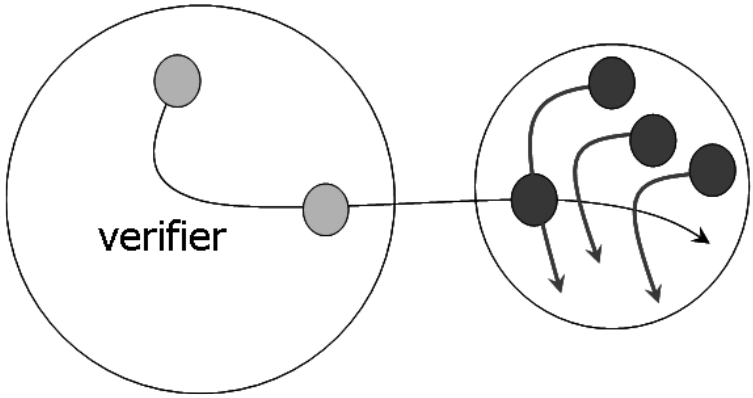
Yu et al. แบ่งโหนดในกราฟออกเป็น 2 กลุ่มเรียกว่ากลุ่มโหนดที่เชื่อถือได้ (Honest Region) กับกลุ่มไซบิลโหนด (Sybil Region) เส้นเชื่อมระหว่าง 2 กลุ่มจะเรียกว่าเส้นเชื่อมบุกรุก (Attack Edges)




**ภาพที่ 6** การแบ่งกราฟเครือข่ายสังคมออกเป็น 2 กลุ่ม

ไซบิลการ์ดใช้สมมติฐานที่ว่าเอกลักษณ์ไม่สามารถปลอมความสัมพันธ์กับเอกลักษณ์อื่นได้ ดังนั้นเอกลักษณ์ที่มุ่งร้ายสร้างอัตลักษณ์ปลอมจำนวนมากแต่ ความสัมพันธ์กับเอกลักษณ์อื่นจะมีไม่มากนัก การทำงานของอัลกอริทึมไซบิลการ์ดจะทำโดยการสร้างเส้นทางสุ่มด้วย “random route algorithm” เป็นการสร้งเส้นทางด้วยการเดินสุ่ม (random walk) ที่มีคุณสมบัติที่รับประกันว่าเส้นเชื่อมที่เส้นทางวิ่งออกจากโหนดใด ๆ จะขึ้นกับเส้นเชื่อมที่เส้นทางนั้นวิ่งเข้าไปยังโหนดนั้น ๆ ดังนั้นเส้นทางสุ่มใดๆ 2 เส้นเดินทางผ่านโหนดด้วยทางเข้าเดียวกันก็จะต้องวิ่งออกจากโหนดในเส้นทางเดียวกัน สังเกตว่าเส้นทางสุ่มจะไม่เหมือนกับการเดินแบบสุ่ม เนื่องจากการที่เอกลักษณ์ที่มุ่งร้ายรู้จักเอกลักษณ์ที่น่าเชื่อถือได้เพียงไม่กี่เอกลักษณ์ทำให้เส้นทางที่วิ่งผ่านอัตลักษ์ที่ถูกสร้างจะใช้เส้นทางทับซ้อนกัน Yu et al. จึงได้ทำการตัดกราฟระหว่างกลุ่มผู้มุ่งร้าย และกลุ่มที่เชื่อถือได้ โดยอัลกอริทึมของไซบิลการ์ดจะมีกระบวนการ ตรวจสอบอัตลักษณ์ B ที่ติดต่อเข้ามาจะกระทำดังนี้ สมมติว่ามีเส้นทางตรวจสอบที่สร้างด้วยกระบวนการสร้างทางสุ่ม (random route) $P_A$ ที่เริ่มจาก A มีระยะทาง w เป็นเส้นทางที่ใช้ตรวจสอบ B ให้สร้างเส้นทางสุ่ม $P_B$ ที่เริ่มจาก B ไปในกราฟเครือข่ายความสัมพันธ์ เป็นระยะ w ผู้ใช้ A จะยอมรับ B ถ้า (1) เส้นทาง $P_A$ และ $P_B$ ตัดกันและ A ยังไม่เคยรับอัตลักษณ์ใด ๆ ที่ตัดกับ $P_A$ โหนด u มาก่อน เมื่อโหนด u เป็นโหนดที่ $P_A$ และ $P_B$ ตัดกัน

ถ้าเส้นทางสุ่มที่ผู้ใช้สร้างขึ้นสำหรับการตรวจสอบ เดินผ่านเส้นเชื่อมบุกรุกจะทำให้เส้นทางการตรวจสอบจะล้มเหลวเนื่องจาก เส้นทางสุ่มเส้นนั้นยอมรับอัตลักษณ์ปลอมโดยไม่ได้เป็นไปตามวิธีการของอัลกอริทึม




**ภาพที่ 7** ความผิดพลาดของโปรโตคอลเมื่อเส้นทางสุ่มสำหรับตรวจสอบที่เดินผ่านเส้นเชื่อมบุกรุก

**ทฤษฎีบทที่ 4** (Yu et al., 2006) *สำหรับกราฟเครือข่ายสังคม $G = (V, E)$ เลือกผู้ใช้ $u$ ที่ซื่อสัตย์แบบสุ่มด้วยการกระจายแบบเอกรูปบนเซตของผู้ใช้ที่ซื่อสัตย์ทั้งหมด เส้นทางสุ่มความยาว $w$ ที่เริ่มจาก $u$ จะเดินผ่านเส้นเชื่อมบุกรุกขนาด $g$ เส้นด้วยความน่าจะเป็นไม่เกิน $gw/n$ เมื่อ $n$ แทนจำนวนโหนดในกราฟ ถ้าเส้นทางสุ่มมีความยาว $w = \Omega(\sqrt{n}\log n)$ และมีจำนวนเส้นเชื่อมบุกรุก $O(\sqrt{n}/\log n)$ อัลกอริทึมไซบิลการ์ดจะเดินผ่านเส้นเชื่อมบุกรุกด้วยความน่าจะเป็นไม่เกิน $O(1)$*

เพื่อป้องกันความล้มเหลว ความยาว w ที่ใช้จะต้องมีค่าน้อย อย่างไรก็ตามเส้นทางที่สร้างขึ้นจะต้องยาวพอที่จะทำให้เส้นทางสุ่มผู้ใช้ที่ซื่อสัตย์คนอื่น ๆ สร้างขึ้นมาตัดได้ ผู้พัฒนาไซบิลการ์ดได้พิสูจน์ว่าถ้า $w = \Omega(\sqrt{n}\log n)$ เส้นทางสุ่มของผู้ใช้ที่ซื่อสัตย์คนอื่น ๆ จะตัดเส้นทาง $P_A$ ด้วยความน่าจะเป็นที่สูง

ด้วยข้อจำกัดที่กล่าวมา ไซบิลการ์ดสามารถรองรับกรณีที่จำนวนเส้นเชื่อมบุกรุกไม่เกิน $O(\sqrt{n}/\log n)$ และระบบจะรับประกันว่า ผู้ใช้ใด ๆ จะรับอัตลักษณ์ที่มาจากผู้ใช้ที่มุ่งร้ายไม่เกิน $\Theta(g \cdot \sqrt{n}\log n)$ อัตลักษณ์

Yu et al. (2007) ได้นำเสนอโปรโตคอลไซบิลลิมิต (SybilLimit) ได้ปรับปรุงการสร้างเส้นทางสุ่ม โดยจะสร้างเส้นทางสุ่มที่ไม่ขึ้นต่อกันจำนวน $O(\sqrt{m})$ เส้นทาง เมื่อ m แทนจำนวนเส้นเชื่อมทั้งหมดระหว่างผู้ใช้ การกำหนดดังกล่าวทำให้ความยาว w ที่ต้องการนั้นสั้นลงเหลือ O (log n) ทำให้รองรับเส้นเชื่อมบุกรุกได้ถึง O (n / log n)

อย่างไรก็ตาม การรับประกันเชิงทฤษฎีของไซบิลการ์ดและไซบิลลิมิตเป็นแบบเฉลี่ย (average) กล่าวคือ ทั้งสองระบบจะรับประกันความสำเร็จสำหรับผู้ใช้ที่สุ่มมาแบบทั่วถึง แต่ไม่ได้

รับประกันความสำเร็จกับผู้ใช้ใด ๆ ยกตัวอย่างเช่น ผู้ใช้ที่มีเส้นเชื่อมติดกับผู้ใช้ที่มุ่งร้ายอาจไม่สามารถใช้งานได้ เป็นต้น

## งานวิจัยในอดีตของปัญหาการบุกรุกแบบอิคลิปส์

### การบุกรุกแบบอิคลิปส์บนเครือข่ายห่อหุ้ม (Eclipse Attacks on Overlay Networks)

Singh et al. (2004, 2006) ได้นำเสนอปัญหาการโจมตีแบบอิคลิปส์บนเครือข่ายซ้อนทับ ได้นำเสนอว่า เมื่อกำหนดดีกรีขาออกของแต่ละโหนดในตารางเส้นทาง (Routing Table) อัตราส่วนของโหนดที่ถูกโจมตีจะไม่เกิน $f/(1-f)$ เมื่อ $f$ คืออัตราส่วนของผู้มุ่งร้ายในระบบ

การกำหนดดีกรีคือการทำ Anonymous auditing สมมติ โหนด u ต้องการตรวจสอบโหนด v ที่เป็นกลุ่มโหนดใกล้เคียง (neighbor set) ของโหนด u ให้ทำการเลือกโหนด x ด้วยวิธีการสุ่ม เพื่อนำไปตรวจสอบโหนด v ว่ามีจำนวนดีกรีเกินหรือไม่ ถ้าจำนวนดีกรีเกินหรือไม่มีการตอบกลับให้ลบโหนด v ออกจากเซตของกลุ่มโหนดใกล้เคียง เนื่องจากการตรวจสอบไม่ได้ทราบว่าโหนด x ที่เลือกมานั้นเป็นผู้มุ่งร้ายหรือไม่ดังนั้นแล้วการตรวจสอบจะทำการตรวจสอบ n ครั้งและถ้าการตรวจสอบให้ผลว่าโหนด v เป็นผู้มุ่งร้ายมากกว่า k ครั้งถือโหนด v เป็นโหนดที่มุ่งร้าย และโหนดปกติจะถูกตรวจสอบว่าด้วยความน่าจะเป็น

$$\sum_{i=0}^{k-1}\binom{n}{i} f^{n-i}(1-f)^{i}$$

# วิธีการ

เป้าหมายของงานวิจัยนี้จะทำการป้องกันการบุกรุกแบบไซบิล และแบบอิคลิปส์ในระบบเครือข่ายแบบเพียร์ทูเพียร์ ดังนั้นในส่วนวิธีการที่จะกล่าว แบ่งเป็น 2 ส่วนคือการป้องกันการโจมตีแบบไซบิล และการป้องกันการโจมตีแบบอิคลิปส์

## 1. การป้องกันการโจมตีรูปแบบไซบิล

เป้าหมายของงานวิจัยสำหรับการป้องกันการบุกรุกแบบไซบิลคือปรับปรุงการรับประกันของระบบไซบิลการ์ดให้เป็นในกรณีที่แย่ที่สุด (worst case) กล่าวคือเรานำเสนอวิธีการตรวจสำหรับรับประกันผู้ใช้ทุกคน ในงานวิจัยนี้จะพิสูจน์หาระยะห่าง k ช่วงความสัมพันธ์ระหว่างผู้ใช้ที่ซื่อสัตย์และผู้ใช้ที่มุ่งร้าย ที่เพียงพอที่จะเปลี่ยนการรับประกันแบบเฉลี่ยของไซบิลการ์ดให้เป็นการรับประกันในกรณีที่แย่ที่สุด

ในส่วนหัวข้อที่จะกล่าวต่อไปจะเป็นเรื่อง การตรวจสอบแบบท้องถิ่นจะใช้วิธีการตรวจสอบแบบท้าทาย-ตอบสนอง ซึ่งการที่จะทำให้โหนดตรวจสอบว่าไม่มีผู้มุ่งร้ายในระยะ k ช่วงความสัมพันธ์ เนื่องงานวิจัยไม่ได้มุ่งเน้นวิธีการตรวจสอบด้วยเหตุนี้จึงเสนอแนวทางตรวจสอบ 2 แนวทาง ส่วนการพิสูจน์การรับประกันของการตรวจสอบแบบท้องถิ่นจะกล่าวในหัวข้อต่อไป

### 1.1. การตรวจสอบแบบท้องถิ่น (Local verification)

เนื่องจากไซบิลการ์ดการรับประกันจะเป็นแบบเฉลี่ย แต่ในความเป็นจริงในการเดินแบบสุ่มที่เริ่มจากโหนดที่ติดหรืออยู่ใกล้ผู้มุ่งร้ายระยะหนึ่ง โอกาสที่จะทำให้อัลกอริทึมไซบิลการ์ดทำงานผิดพลาดมีสูง ดังนั้นในส่วนนี้เราจะนำเสนอวิธีการเพื่อใช้รับประกันว่าสำหรับเอกลักษณ์ A ใด ๆ ที่ซื่อสัตย์จะไม่มีอัตลักษณ์สองอัตลักษณ์ใด ๆ ที่อยู่ในระยะไม่เกิน k ช่วงความสัมพันธ์จากอัตลักษณ์ของ A ที่เป็นของเอกลักษณ์เดียวกัน กระบวนการนี้ทำเพื่อเพิ่มความมั่นใจว่า A อยู่ห่างจากเส้นเชื่อมบุกรุกอย่างน้อย k ช่วงความสัมพันธ์ที่ทำอัลกอริทึมไซบิลการ์ดยังสามารถรับประกันความผิดพลาดได้

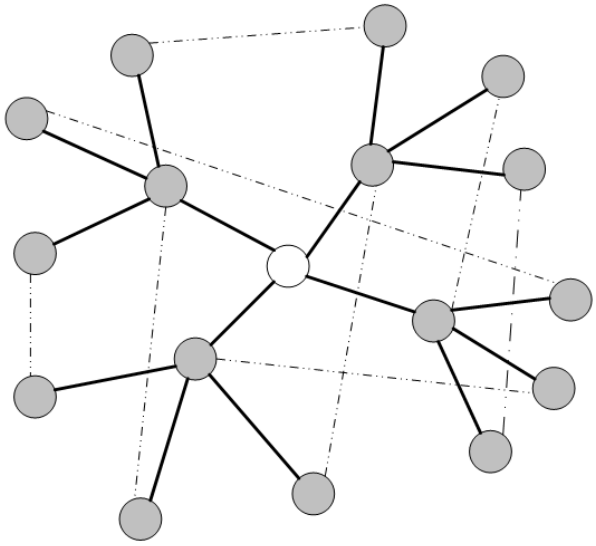
การตรวจสอบแบบท้องถิ่งจะใช้วิธีท้าทาย-ตอบสนอง (Challenge and Respond) ซึ่งเหมือนในแบบจำลองกลุ่มเมฆของ Douceur (2002) วิธีการทดสอบว่าอัตลักษณ์สองอัตลักษณ์มาจากผู้ใช้ที่แตกต่างกัน จะกระทำโดยการส่งการท้าทายไปยังอัตลักษณ์สองอัตลักษณ์ ถ้าทั้งสองอัตลักษณ์สามารถตอบสนองได้ทัน จะยอมรับว่ามาจากสองเอกลักษณ์ แต่จะมีวิธีการที่แตกต่างกัน โดย

วิธีการดังกล่าวจะทำการตรวจสอบทุกๆอัตลักษณ์ที่อยู่ในระยะ k ช่วงความสัมพันธ์ โดยการส่งการท้าทายที่แตกต่างกันไปยังทุก ๆ อัตลักษณ์ที่จะตรวจสอบ จากนั้นอัตลักษณ์ใดที่ไม่สามารถตอบสนองได้ทันเวลา จะถูกระบุว่าเป็นอัตลักษณ์ที่มาจากเอกลักษณ์ที่มุ่งร้าย

การตรวจสอบแบบท้องถิ่นแบบที่กล่าวมาข้างต้นสมมติว่าเอกลักษณ์ A ต้องการตรวจสอบทุก ๆ อัตลักษณ์ที่มีการเชื่อมต่อกับตนเองในระยะ k สังเกตว่า ถ้า k เป็นค่าคงที่ และดีกรีของโหนดมีค่าไม่มากกว่าค่าคงที่ c จำนวนอัตลักษณ์ที่อยู่ห่างไม่เกินระยะ k จะมีไม่เกิน $O(c^k)$ ซึ่งเป็นค่าคงที่เช่นเดียวกัน ให้เซต N แทนเซตของอัตลักษณ์ที่อยู่ต้องการทดสอบดังกล่าว เนื่องจากการตรวจสอบนี้ไม่ยากและไม่แตกต่างจากการตรวจสอบแบบรวมศูนย์มากนักจึงไม่ใช้ประเด็นของงานวิจัยนี้ อย่างไรก็ตามเพื่อแสดงว่าการตรวจสอบดังกล่าวเป็นไปได้เราแสดงวิธีการตรวจสอบสองแบบ

1.1.1. เอกลักษณ์ A จะเป็นผู้ส่งการร้องขอไปยังทุกอัตลักษณ์ในระยะ k ช่วงความสัมพันธ์จากเอกลักษณ์ A แล้วตรวจสอบว่าอัตลักษณ์ใดบ้างตอบสนองได้ทันเวลา

1.1.2. เอกลักษณ์ A จะจับคู่อัตลักษณ์ในระยะ k ช่วงความสัมพันธ์จาก A จากนั้น A จะเป็นผู้เลือกว่าอัตลักษณ์ใดจะตรวจสอบอีกอัตลักษณ์หนึ่งที่จับคู่ไว้ ในการจับคู่อัตลักษณ์ที่ตรวจสอบกันไม่ควรมีความสัมพันธ์กันในโลกความเป็นจริง ตัวอย่างการจับคู่ในวิธีนี้แสดงในภาพที่ 8



**ภาพที่ 8** วิธีการตรวจสอบแบบท้องถิ่นแบบที่ 2

ถ้าเราสมมติให้ไม่มีเอกลักษณ์ใดมีทรัพยากรมากกว่าทรัพยากรที่ต้องการในการตอบสนองการร้องขอ วิธีที่ 1 จะรับประกันว่า ไม่มีสองอัตลักษณ์ใน N ที่เป็นของเอกลักษณ์เดียว ข้อดีของการตรวจสอบด้วยวิธีที่ 1 คือ ในกรณีที่มีเอกลักษณ์ที่มุ่งร้ายที่มีทรัพยากรมากและมีหลายอัตลักษณ์อยู่ในเซต N วิธีดังกล่าวจะทำให้เอกลักษณ์นั้นได้รับการร้องขอเป็นจำนวนมากจะสามารถตรวจสอบพอได้ อย่างไรก็ตาม ภาระของ A ในการใช้การตรวจสอบวิธีที่ 1 ค่อนข้างมาก ส่วนวิธีที่ 2 จะใช้ทรัพยากรน้อยกว่าแต่ความยากจะอยู่ที่ปัญหาการจับคู่ตรวจสอบ ความถูกต้องในวิธีที่สองคือการที่อัตลักษณ์ที่จับคู่ต้องไม่ได้มาจากเครื่องเดียวกัน การแก้ปัญหานี้วิธีที่ง่ายสุดก็คือการจับคู่อัตลักษณ์ที่ไม่ได้มีความสัมพันธ์กัน หรือด้วยวิธีการจับคู่อัตลักษณ์ที่ไม่ได้มีพ่อแม่ร่วมกัน อย่างไรก็ตามอัตลักษณ์ที่มุ่งร้ายอาจเลือกเก็บอัตลักษณ์ที่อยู่ใกล้ A มาก ๆ เอาไว้ได้

หลังจากทำการตรวจสอบแบบท้องถิ่น แล้วพบโหนดที่มุ่งร้ายอยู่ใกล้การจัดการกับปัญหานี้อาจทำได้โดยการตัดอัตลักษณ์ที่เชื่อมต่อจาก A ไปยังทุก ๆ อัตลักษณ์ที่เชื่อมไปยังอัตลักษณ์ปลอมก็ได้

2. การป้องกันการโจมตีแบบอิคลิปส์ (defending eclipse attack)

ในงานวิจัยนี้จะแก้ปัญหาการบุกรุกแบบอิคลิปส์ในเครือข่ายแบบเพียร์ทูเพียร์ที่ไม่มีโครงสร้างและตัวกลางที่เชื่อถือได้ โดยระบบนี้การเชื่อมต่อของโหนดจะทำการร้องขอเพียร์จากโหนดที่เรารู้จักโดยส่วนใหญ่มักจะเป็นเพื่อน และการร้องขอโหนดเพิ่มจะทำการขอเพียร์จากโหนดที่เรารู้จักแล้ว การสร้างการโจมตีแบบอิคลิปส์ ผู้มุ่งร้ายจะอาศัยลักษณะการขอเพียร์แบบนี้มาสร้างการโจมตี โดยเมื่อมีการขอร้องเพียร์จากโหนดที่มุ่งร้าย โหนดที่มุ่งร้ายจะพยายามคืนเพียร์ที่อยู่ในกลุ่มผู้มุ่งร้ายที่มีความสัมพันธ์กัน ทำให้กลุ่มของโหนดดีที่ถูกโจมตีได้รับแต่เพียร์มุ่งร้าย

ในงานวิจัยนี้จะนำเสนออัลกอริทึมสำหรับการตรวจสอบและการหลีกเลี่ยงการถูกโจมตีแบบอิคลิปส์ โดยการร้องขอเพียร์อื่นที่ติดอยู่กับโหนดที่เรารู้จัก เพื่อขอรู้จักโหนดเพิ่มขึ้น สำหรับโหนด $u$ ที่ต้องการตรวจสอบว่าโดนโจมตีอยู่หรือไม่ ให้ทำการเดินแบบสุ่มความยาว $w$ เริ่มจากโหนด $u$ ทำการเลือกโหนด $v$ แบบสุ่ม จากโหนดที่ติดกับ $u$ จากนั้นก็เดินไปโหนด $v$ ที่เลือกมาแล้วทำการร้องขอโหนดที่ติดกับ $v$ จากนั้นก็สุ่มเลือกโหนดที่จะเดินต่อไปจากโหนดที่ได้รับมาจาก $v$ ทำเช่นนี้ $w$ รอบ สำหรับระบบเครือข่ายที่มีการขยายตัวดี ถ้าไม่ได้มีผู้มุ่งร้าย เราจะพบว่าจำนวนโหนดที่ได้รับคืนมาทั้งหมดจะมีจำนวนมาก ด้วยการวิเคราะห์โดยใช้กราฟสุ่มดีกรีสม่ำเสมอ (random d-regular) มาพิสูจน์เชิงทฤษฎี

สำหรับโหนดที่มุ่งร้ายที่ปิดบังโดยไม่อนุญาติให้โหนดที่ถูกโจมตีรับรู้โหนดที่น่าเชื่อถืออื่นๆ กล่าวคือในการร้องขอโหนดด้วยวิธีการเดินแบบสุ่มความยาว $w$ จะคืนแต่เฉพาะโหนดที่เป็นกลุ่มผู้มุ่งร้ายอื่นๆมาให้ทำให้โหนดที่ได้คืนกลับมารวมแล้วมีจำนวนน้อย เราจะตรวจพบได้ว่าถูกโจมตีอยู่ และเนื่องจากเราไม่ทราบถึงโหนดภายนอกอื่นๆ ดังนั้นวิธีที่จะหลุดจากการบุกรุกจึงมีวิธีเดียวคือการออกจากระบบ แต่ถ้าโหนดที่มุ่งร้ายพยายามปิดบังโหนดที่ถูกโจมตีโดย คืนโหนดอื่นมาบ้างเพื่อที่ป้องกันการตรวจพบการบุกรุกด้วยวิธีนี้ก็จะมีวิธีหนีจากการบุกรุกได้โดยการสุ่มเลือกโหนดที่ได้รับมา จากนั้นขอเชื่อมต่อกับโหนดนั้นแทนโหนดที่เชื่อมต่อเดิม สำหรับการตรวจสอบการบุกรุกแบบอิคลิปส์ สำหรับ $u$ เป็นโหนดที่ต้องการตรวจสอบว่าถูกโจมตีแบบอิคลิปส์ด้วยผู้มุ่งร้ายขนาด $k$ ด้วยการเดินแบบสุ่มความยาว $w$ และได้โหนดคืนกลับมาทั้งหมด $K_t$ โหนด จะเขียนเป็นอัลกอริทึมได้ดังภาพที่ 9

```
1. Procedure checkEclipse(Node u)
2. For i ← 1 to w
3.         v ← เลือกโหนดที่ติดกับ u ด้วยการสุ่ม
4.         เดินไปที่ v
5.         ร้องขอเพียร์จาก v
6. If จำนวนโหนดที่รู้จัก ≤ k then
7.         ออกจากระบบ
8. Else
9.         สุ่มเลือกโหนดที่ได้รับมาเชื่อมต่อแทนโหนดเดิม
```

**ภาพที่ 9** อัลกอริทึมสำหรับแก้ปัญหาการบุกรุกแบบอิคลิปส์

จากภาพที่ 9 พบว่าจำเป็นต้องมีการหาค่าตัวแปรที่เหมาะสมสำหรับอัลกอริทึม checkEclipse ดังนั้นการหาตัวแปรต่างๆที่เหมาะสมสำหรับอัลกอริทึมนี้ ในงานวิจัยนี้จะใช้การทดลองในการหาค่าที่เหมาะสมในแบบจำลองต่างๆ โดยจะกล่าวในส่วนของผลการวิจัย

# ผลการวิจัย

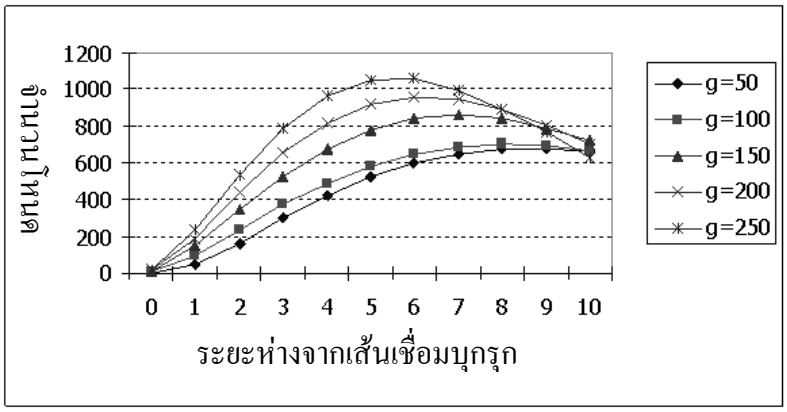
ในงานวิจัยนี้ได้สนใจในการแก้ปัญหาการบุกรุกแบบไซบิลและการบุกรุกแบบอิคลิปส์ในเครือข่ายเพียร์ทูเพียร์ ดังนั้นในส่วนของผลการวิจัยจะแบ่งการทดลองเป็นการทดลองสำหรับวิธีการป้องกันการบุกรุกแบบไซบิลและวิธีการป้องกันการบุกรุกแบบอิคลิปส์ โดยแต่ละแบบจะมีการทดลองเพื่อรับประกันแนวคิดด้วยการวิเคราะห์เชิงทฤษฎี และการวิเคราะห์ด้วยแบบจำลอง

## การทดลองสำหรับวิธีการป้องกันแบบไซบิล

ในส่วนของการทดลองสำหรับปัญหาการบุกรุกแบบไซบิลจะแบ่งเป็นสองส่วนคือ การทดลองเชิงทฤษฎี จะเป็นการทดลองเพื่อรับประกันแนวความคิดด้วยการคำนวนทางคณิตศาสตร์ และการทดลองด้วยแบบจำลองจะเป็นการทำการทดลอง โดยใช้แบบจำลองโลกใบเล็กของ Kleinberg (2000) ที่ใช้ค่าพารามิเตอร์คือ p=1, q=1 และ r=0 และหาระยะห่าง k จากอัตลักษณ์ที่มุ่งร้ายที่เพียงพอที่จะเปลี่ยนการรับประกันแบบเฉลี่ยของไซบิลการ์ดให้เป็นการรับประกันในกรณีที่แย่ที่สุด

### การกระจายตัวของโหนดในแบบจำลอง

ก่อนที่จะกล่าวถึงการรับประกันทางทฤษฎี ในงานวิจัยนี้จะแสดงถึงการกระจายของโหนดในแบบจำลองโลกใบเล็ก เราได้ทดลองสร้างเครือข่ายสังคมด้วยโมเดลของ Kleinberg (2000) แล้วนับจำนวนโหนดที่มีระยะไปยังเส้นเชื่อมบุกรุกไม่เกิน 10 ช่วง กราฟในภาพที่ 10 แสดงผลการทดลองบนกราฟขนาด 10,000 โหนด ที่สร้างด้วยพารามิเตอร์ $p = 2$, $q = 4$ และ $r = 1.9$ โดยทดลองในกรณีที่มีเส้นเชื่อมบุกรุกเท่ากับ 50, 100, 150, 200 และ 250 ตามลำดับ




**ภาพที่ 10** กราฟแสดงความสัมพันธ์ระหว่างจำนวนโหนดที่อยู่ห่างจากผู้มุ่งร้ายในแต่ละจำนวนของเส้น เชื่อมบุกรุก

จากภาพจะเห็นได้ว่าโดยปกติแล้วผู้ใช้ส่วนใหญ่จะอยู่ห่างจากเส้นเชื่อมบุกรุก (attack edges) ดังนั้นโปรโตคอลไซบิลการ์ดจึงทำงานสำเร็จด้วยความน่าจะเป็นที่สูง แต่สำหรับโหนดที่ติดกับเส้นเชื่อมบุกรุก ไซบิลการ์ดไม่ได้การันตีความถูกต้อง ในส่วนงานวิจัยนี้จะปรับปรุงไซบิลการ์ดให้สามารถรับประกันโหนดที่ติดกับเส้นเชื่อมบุกรุก เพื่อที่จะเปลี่ยนการรับประกันโดยเฉลี่ยของไซบิลการ์ดเป็นการรับประกันในกรณีที่แย่ที่สุด

**การวิเคราะห์เชิงทฤษฎี**

ในการวิเคราะห์แนวความคิดเชิงทฤษฎีจะพิจารณาในด้วยแบบจำลองโลกใบเล็กของ Kleinberg (2000) เนื่องจากการวิเคราะห์การกระจายตัวของกราฟในหัวข้อที่ผ่านมาพบว่าจำนวนโหนดที่อยู่ห่างจากผู้มุ่งร้ายมากกว่า 1 จะมีอยู่จำนวนมาก ดังนั้นโอกาสที่เราจะทำให้การตรวจสอบแบบท้องถิ่นสำเร็จก็จะมีอยู่สูงตามไปด้วย สำหรับแบบจำลองโลกใบเล็กของ Kleinberg (2000) ที่มีพารามิเตอร์ p=1, q=1 แล r=0 ในหัวข้อนี้จะพิสูจน์ว่าสามารถหาระยะที่เหมาะสม k ที่ยาวพอสำหรับการเดินแบบสุ่ม ที่จะเดินผ่านเส้นเชื่อมระยะไกลก่อนที่จะถึงผู้มุ่งร้าย เนื่องจากเมื่อเดินผ่านเส้นเชื่อมระยะไกลจะเหมือนการเลือกโหนดแบบสุ่มซึ่งสมมูลกับวิธีการของไซบิลการ์ด จึงสามารถใช้การรับประกันของไซบิลการ์ดได้ และจะทำให้สามารถเปลี่ยนการรับประกันแบบเฉลี่ยของไซบิลการ์ดให้เป็นการรับประกันในกรณีที่แย่ที่สุด

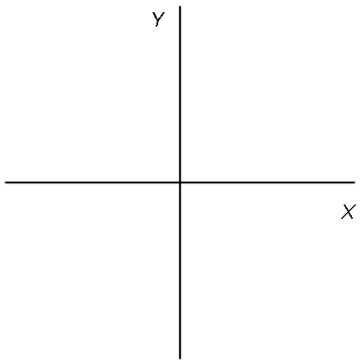
เนื่องจากในแบบจำลองโลกใบเล็กที่ใช้นี้ ที่ค่า q เท่ากับ 1 จะเป็นกรณีที่แย่ที่สุด เนื่องจากถ้าค่า q มากกว่านี้โอกาสที่การเดินสุ่มจะเลือกเส้นเชื่อมระยะไกลจะมีสูงขึ้นด้วย ส่วนค่า p ที่มากกว่า 1 จะคำนวนได้ยากดังนั้นในงานวิจัยนี้จะสนใจเฉพาะที่ค่า p=1 เท่านั้น

**ทฤษฎีบทที่ 5** *กราฟ G = (V, E) สร้างตามแบบจำลองโลกใบเล็กของ Kleinberg* (2000) *ที่สร้างด้วยพารามิเตอร์ p = 1, q = 1 และ r = 0 ความน่าจะเป็นที่จะเดินไปถึงผู้มุ่งร้ายที่อยู่ในพิกัด x,y ใดๆคือ*

$$\sum_{i=0}^{(w-l)/2} \binom{l+2i}{(l+2i+x+y)/2} \left(\frac{1}{2}\right)^{l+2i} \binom{l+2i}{(l+2i+x-y)/2} \left(\frac{1}{2}\right)^{l+2i} \left(\frac{4}{5}\right)^{l+2i}$$

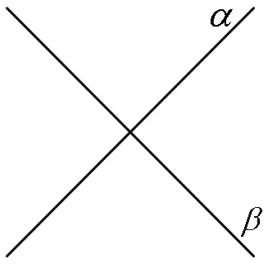
**พิสูจน์**

สังเกตว่าแบบจำลองโลกใบเล็กของ Kleinberg (2000) ที่สร้างด้วยพารามิเตอร์ p = 1, q = 1 และ r = 0 จากโหนด A ใดๆจะมีเส้นเชื่อมที่ติดอยู่ 5 เส้นการสุ่มทางเดินของ A ในแต่ละครั้งที่เดินเพื่อให้ไม่เดินผ่านเส้นเชื่อมระยะไกลจะมีทางเลือก 4 ทาง ซึ่งพิจารณาได้เป็นเวกเตอร์ของการเปลี่ยนตำแหน่งสี่แบบ คือ (1,0), (-1,0), (0,1), และ (0,-1) อย่างไรก็ตาม การวิเคราะห์โดยตรงกับทางเลือกดังกล่าวทำได้ลำบาก




**ภาพที่ 11** แกนเวคเตอร์สำหรับการเดินในแกนปกติ

เราจึงเปลี่ยนวิธีการสุ่มทิศทางในอีกรูปแบบซึ่งสมมูลกับการเลือกแบบเดิม ในการสุ่มแบบใหม่ เราจะโยนเหรียญที่ไม่เบี่ยงเบนสองเหรียญ ให้เวกเตอร์ที่สอดคล้องกับเหรียญทั้งสองเป็น $v_1 = (0.5, 0.5)$ และ $v_2 = (0.5, -0.5)$ สำหรับ $i \in \{1,2\}$ ดังภาพที่ 12




**ภาพที่ 12** แกนเวคเตอร์ในแนวแกนใหม่ที่การโยนเหรียญ 2 เหรียญจะเป็นอิสระต่อกัน

ให้ตัวแปรสุ่ม $D_i$ เท่ากับ $v_i$ ถ้าเหรียญที่ i ออกหัว และเท่ากับ $-v_i$ ถ้าเหรียญออกก้อย เวกเตอร์การเปลี่ยนทิศ D ที่ได้จากการโยนเหรียญทั้งสองจะมีค่าเท่ากับเวกเตอร์ $D_1+D_2$ สังเกตว่าความน่าจะเป็นที่จะได้การเปลี่ยนทิศผลลัพธ์แบบใด ๆ นั้นเท่ากับ 1/4 เช่นเดียวกับการสุ่มเลือกทิศทาง 4 แบบ การแปลงดังกล่าวถ้าจะพูดในเชิงคณิตศาสตร์ก็คือการเปลี่ยนฐานหลัก (basis) จาก (1,0) กับ (0,1) ไปเป็น $v_1 = (0.5, 0.5)$ กับ $v_2 = (0.5, -0.5)$ นั่นเอง

การเปลี่ยนฐานหลักดังกล่าวทำให้เราวิเคราะห์ความน่าจะเป็นที่ตำแหน่งที่เราอยู่ภายหลังการเดิน w ครั้งทำได้สะดวกขึ้น ถ้าพิกัดที่เราสนใจคือ (x, y) เราเขียนใหม่ได้เป็น $(x, y) = (x + y) v_1 + (x - y) v_2$ จากการพิจารณาดังกล่าว เราจะได้ว่า เราจะเดินไปอยู่ที่พิกัด (x, y) ก็ต่อเมื่อ เหรียญแรกออกหัวมากกว่าออกก้อยเป็นจำนวน x + y ครั้ง และเหรียญที่สองออกหัวมากกว่าออกก้อยเป็นจำนวนเท่ากับ x - y ครั้ง หรือในอีกทางหนึ่งก็คือ ในการโยนเหรียญแรก k ครั้ง เราได้หัวทั้งสิ้น $k/2 + (x + y)/2$ ครั้ง และในการโยนเหรียญที่สอง k ครั้ง เราได้หัวทั้งสิ้น $k/2 + (x - y)/2$ ครั้ง ซึ่งเกิดขึ้นด้วยความน่าจะเป็นเท่ากับ

$$\binom{k}{(k+x+y)/2}\left(\frac{1}{2}\right)^k\binom{k}{(k+x-y)/2}\left(\frac{1}{2}\right)^k$$

สังเกตว่าค่าความน่าจะเป็นข้างต้นยังไม่ได้คิดกรณีที่เราเลือกเส้นเชื่อมกระโดด ดังนั้น ความน่าจะเป็นที่ภายในการเดิน k ครั้ง เราเดินไปยังตำแหน่ง (x, y) ก่อนที่จะเลือกเส้นเชื่อมกระโดด คือ

$$\binom{k}{(k+x+y)/2}\left(\frac{1}{2}\right)^k\binom{k}{(k+x-y)/2}\left(\frac{1}{2}\right)^k\left(\frac{4}{5}\right)^k$$

ให้จำนวนครั้งที่โยนเหรียญที่น้อยที่สุดที่จะเดินจากเอนทิตี้ A แล้วไปตกที่โหนดที่มุ่งร้าย u เท่ากับ l ครั้งซึ่งมีค่าเท่ากับ $|x|+|y|$ ครั้ง พิจารณาจำนวนครั้งที่มีโอกาสเดินตกโหนดที่มุ่งร้าย u ภายในการเดินไม่เกิน w ครั้งจะเป็น l, l+2, l+4, l+6… w ครั้งเนื่องจากหากโยนเหรียญ l ครั้ง เหรียญแรกต้องออกหัว $(l+x+y)/2$ ครั้ง และเหรียญที่สองต้องออกหัว $(l+x-y)/2$ ครั้ง หากโยนเหรียญแรกหรือเหรียญที่สองได้หัวเกินจะต้องโดนออกก้อยเท่ากับจำนวนของการโยนได้หัวที่เกินมา ดังนั้นความน่าจะเป็นที่จะเดินจากเอนทิตี้ A แล้วไปตกที่โหนดที่มุ่งร้าย u ภายในการเดิน l, l+2, l+4… w ครั้งโดยไม่เลือกเส้นเชื่อมกระโดดจะเท่ากับ

$$\sum_{i=0}^{(w-l)/2} \binom{l+2i}{(l+2i+x+y)/2} \left(\frac{1}{2}\right)^{l+2i} \binom{l+2i}{(l+2i+x-y)/2} \left(\frac{1}{2}\right)^{l+2i} \left(\frac{4}{5}\right)^{l+2i} \quad \blacksquare$$

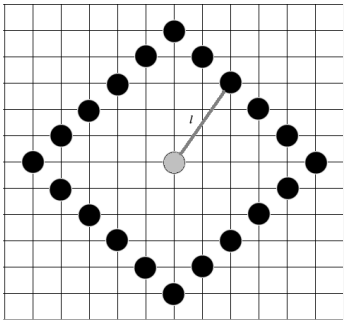
พิจารณาตารางกริดที่โมเดลเครือข่ายสังคมของ Kleinberg (2000) ที่พารามิเตอร์ p = 1, q = 1 และ r = 0 ให้โหนด A เป็นจุดกึ่งกลาง โดยให้เดินจาก A ไปยังโหนดบุกรุกที่อยู่รอบๆ โดยใช้การเดินไม่เกิน 20 รอบจะได้ผลดังตารางที่ 1

**ตารางที่ 1** ความน่าจะเป็นที่จะเดินตกไปยังโหนดที่มุ่งร้ายรอบๆเชิงทฤษฎี

| ระยะห่างในแนวแกนตั้ง | ระยะห่างในแนวแกนนอน | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | -5 | -4 | -3 | -2 | -1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 5 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| 4 | 0.00 | 0.00 | 0.00 | 0.00 | 0.01 | 0.01 | 0.01 | 0.00 | 0.00 | 0.00 | 0.00 |
| 3 | 0.00 | 0.00 | 0.01 | 0.01 | 0.02 | 0.03 | 0.02 | 0.01 | 0.01 | 0.00 | 0.00 |
| 2 | 0.00 | 0.00 | 0.01 | 0.03 | 0.06 | 0.10 | 0.06 | 0.03 | 0.01 | 0.00 | 0.00 |
| 1 | 0.00 | 0.01 | 0.02 | 0.06 | 0.16 | 0.34 | 0.16 | 0.06 | 0.02 | 0.01 | 0.00 |
| 0 | 0.00 | 0.01 | 0.03 | 0.10 | 0.34 | | 0.34 | 0.10 | 0.03 | 0.01 | 0.00 |
| -1 | 0.00 | 0.01 | 0.02 | 0.06 | 0.16 | 0.34 | 0.16 | 0.06 | 0.02 | 0.01 | 0.00 |
| -2 | 0.00 | 0.00 | 0.01 | 0.03 | 0.06 | 0.10 | 0.06 | 0.03 | 0.01 | 0.00 | 0.00 |
| -3 | 0.00 | 0.00 | 0.01 | 0.01 | 0.02 | 0.03 | 0.02 | 0.01 | 0.01 | 0.00 | 0.00 |
| -4 | 0.00 | 0.00 | 0.00 | 0.00 | 0.01 | 0.01 | 0.01 | 0.00 | 0.00 | 0.00 | 0.00 |
| -5 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |

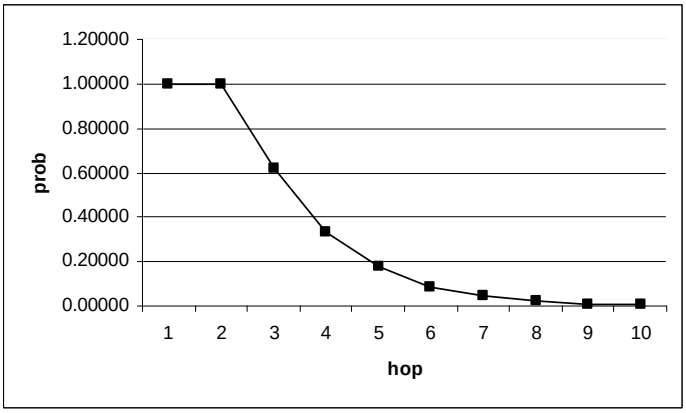
จากตารางที่ 1 พบว่ายิ่งอยู่ใกล้โอกาสที่จะเจอผู้มุ่งร้ายยิ่งสูงขึ้น จากนั้นพิจารณาโอกาสที่จะเดินกระโดดจากเส้นเชื่อมกระโดดแล้วตกที่โหนดที่มุ่งร้าย ให้ s เป็นจำนวนโหนดที่มุ่งร้ายทั้งหมด และ n เป็นจำนวนโหนดทั้งหมดคือ s/n

พิจารณาในสถานการณ์ที่แย่ที่สุด ที่มีผู้มุ่งร้ายอยู่รอบในระยะห่าง l ตามภาพที่ 13 จะมีความน่าจะเป็นของการเดินสุ่มเริ่มจากโหนดที่ซื่อสัตย์ A ใช้จำนวนการเดิน *w* ครั้งแล้วเดินตกโหนดที่มุ่งร้าย u โดยไม่กระโดดผ่านเส้นเชื่อมกระโดด




**ภาพที่ 13** โหนดที่มุ่งร้ายอยู่รอบโหนดที่ซื่อสัตย์ในระยะ $l = 5$

เนื่องจากโอกาสเดินตกโหนดที่มุ่งร้ายที่อยู่รอบในระยะ *l* คือผลรวมความน่าจะเป็นที่จะเดินตกโหนดที่มุ่งร้ายในระยะ *l* ทั้งหมด ผลที่ได้แสดงในกราฟตามภาพที่ 14




**ภาพที่ 14** ความน่าจะเป็นที่จะเดินตกเมื่อมีผู้มุ่งร้ายอยู่รอบในระยะต่างๆ

ข้อสังเกตถ้าโหนดที่มุ่งร้ายอยู่รอบในระยะตั้งแต่ 3 เป็นต้นไปจะยังมีโอกาสที่จะเดินหลุดจากกลุ่มผู้มุ่งร้ายที่อยู่รอบๆได้ ผ่านทางเส้นเชื่อมกระโดด

**การวิเคราะห์ด้วยการจำลอง**

ในส่วนนี้เรามีข้อสมมติพื้นฐานว่า ไม่มีเส้นเชื่อมบุกรุก ในระยะ k - 1 ช่วงความสัมพันธ์บนเครือข่ายสังคมจากA นั่นคือการตรวจสอบแบบท้องถิ่นที่เสนอตอนต้นทำได้สำเร็จ

เราจะพิจารณาเครือข่ายสังคมในโมเดลของ Kleinberg (2000) ที่พารามิเตอร์ p = 1, q = 1 และ r = 0 ในโมเดลดังกล่าวแต่ละโหนดจะมีเส้นเชื่อมติดกับโหนดรอบ ๆ บนตารางกริด และมีเส้นเชื่อมอีกหนึ่งเส้นที่กระโดดไปยังโหนดอื่นๆ ที่มีการกระจายแบบเอกรูป เรียกเส้นเชื่อมดังกล่าวว่าเส้นเชื่อมกระโดด สังเกตว่า ถ้าในการเดินแบบสุ่มออกจากโหนดใด เราเลือกเส้นเชื่อมกระโดดไปยังโหนดที่ซื่อสัตย์ เราจะเข้าสู่เงื่อนไขพื้นฐานของทฤษฎีบทที่ 1 นั่นคือ ด้วยการตรวจสอบแบบท้องถิ่นเราแปลงเงื่อนไขจากกรณีเฉลี่ย เป็นกรณีที่แย่ที่สุดได้

ในกรณีนี้ เนื่องจากเป็นการพิจารณาแบบท้องถิ่น เราจะพิจารณาเฉพาะกรณีที่เอกลักษณ์ A อยู่ที่จุด (0, 0) สมมติให้มีโหนด u ที่มุ่งร้ายที่อยู่ที่คู่อันดับ (x, y) ที่อยู่ห่างจากเป็นระยะ l หน่วยในตารางกริดที่โมเดลเครือข่ายสังคม เราจะคำนวณความน่าจะเป็นที่เอกลักษณ์ A จะสุ่มทางแล้วเดินเข้าไปยังโหนด u ภายในการเดิน w รอบ

เราได้ทดลองหาโอกาสที่จะวิธีของไซบิลการ์ดจะเดินเข้าไปในกลุ่มผู้มุ่งร้ายตามระยะห่างจากผู้มุ่งร้ายในโมเดลของเครือข่ายสังคมของ Kleinberg (2000) ที่มีพารามิเตอร์ p = 1, q = 1, และ r = 0 และจะเดินด้วยระยะทางไม่เกิน 20 ครั้งจะได้ค่าดังตารางที่ 2 ซึ่งมีค่าใกล้เคียงกับตารางที่ 1

**ตารางที่ 2** ความน่าจะเป็นที่จะเดินตกไปยังโหนดที่มุ่งร้ายรอบๆเชิงปฏิบัติ

| ระยะห่างในแนวแกนตั้ง | ระยะห่างในแนวแกนนอน | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 5 | 4 | 3 | 2 | 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| | 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 4 | 0 | 0 | 0 | 0 | 0.01 | 0.01 | 0.03 | 0 | 0 | 0 | 0 |
| | 3 | 0 | 0 | 0.01 | 0 | 0.01 | 0.04 | 0.02 | 0.02 | 0 | 0.02 | 0 |
| | 2 | 0 | 0 | 0.01 | 0.01 | 0.05 | 0.05 | 0.03 | 0.02 | 0 | 0 | 0 |
| | 1 | 0.01 | 0.01 | 0.02 | 0.03 | 0.13 | 0.29 | 0.11 | 0.05 | 0.02 | 0 | 0 |
| | 0 | 0.01 | 0.01 | 0.03 | 0.08 | 0.23 | | 0.32 | 0.06 | 0.02 | 0.01 | 0 |
| | 1 | 0 | 0.01 | 0.02 | 0.13 | 0.15 | 0.26 | 0.13 | 0.06 | 0.05 | 0 | 0 |
| | 2 | 0 | 0 | 0 | 0.03 | 0.06 | 0.11 | 0.04 | 0.02 | 0 | 0 | 0 |
| | 3 | 0 | 0 | 0 | 0.02 | 0.02 | 0.03 | 0.01 | 0 | 0 | 0.01 | 0 |
| | 4 | 0 | 0 | 0 | 0.01 | 0.01 | 0.03 | 0.02 | 0.01 | 0 | 0 | 0 |
| | 5 | 0 | 0 | 0.01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

จากตาราง ถ้าจะถอยโหนดเริ่มต้นให้ไกลจากผู้มุ่งร้ายได้ไกลประมาณ k = 3 โอกาสที่จะเดินไปยังกลุ่มผู้มุ่งร้ายจะมีค่าโดยเฉลี่ยน้อยมาก

## การทดลองสำหรับของวิธีการป้องกันแบบอิคลิปส์

จะเป็นการศึกษาแนวโน้มของระบบที่ไม่มีการถูกโจมตี เนื่องจากแนวความคิดที่ว่าถ้าถูกโจมตี เมื่อทำการร้องขอโหนดอื่นๆ โหนดที่มุ่งร้ายพยายามไม่คืนอื่นๆ ดังนั้นจำนวนโหนดที่ถามได้จะพบน้อย ถ้าผู้มุ่งร้ายยอมให้การรู้จักเปิดกว้างมากจะไม่สามารถควบคุมโหนดที่ถูกโจมตีได้ ดังนั้นเราจะพิจารณาหาว่าโดยปกติแล้วควรจะต้องเดินสุ่มถามกี่ครั้งและควรรู้จักอย่างน้อยกี่ตัว การทดลองจะใช้แบบจำลอง 2 ชนิดคือแบบจำลองกราฟสุ่มดีกรีสม่ำเสมอ (Random d-Regular Graph) กับแบบจำลองพรีเฟอร์เรนเชียล (Preferential Model) โดยจะมีการวิเคราะห์ความสำเร็จของอัลกอริทึม การทดลองในส่วนของ การทดสอบการเดินนับจำนวนโหนดที่รู้จักเพิ่มขึ้น เพื่อพิสูจน์แนวคิดเกี่ยวกับอัตราการขยายตัวของระบบเครือข่าย และการหาพารามิเตอร์ต่างๆที่เหมาะสมสำหรับอัลกอริทึม

### วิเคราะห์ความสำเร็จของอัลกอริทึม

จากอัลกอริทึมในรูปที่ 9 พิจารณา กราฟ $G = (V, E)$ พิจารณาโหนด $u$ ใดๆที่มีผู้มุ่งร้ายขนาด $k$ โหนดพยายามสร้างการบุกรุกแบบอิคลิปส์ สำหรับ $u$ เป็นโหนดที่ต้องการตรวจสอบว่าถูก

โจมตีแบบอิคลิปส์ด้วยผู้มุ่งร้ายขนาด $k$ ด้วยการเดินแบบสุ่มความยาว $w$ เพื่อร้องขอโหนดจากโหนด $v_1, v_2, \ldots v_w$ โดยที่ $v_i$ คือโหนดที่การเดินสุ่มครั้งที่ i เดินไป และได้โหนดคืนกลับมารวมทั้งหมด $K_t$ โหนด พิจารณา 2 กรณีคือ

**กรณีที่ 1** หลังการเดินสุ่มได้รับโหนดมารวมทั้งหมด $K_t$ ที่ไม่เกิน $k$ โหนดแสดงว่าถูกอิคลิปส์อย่างสมบูรณ์ ซึ่งหมายความว่าในการร้องขอด้วยวิธีการเดินแบบสุ่มความยาว w ไม่ได้รับโหนดที่เชื่อถือได้ อัลกอริทึมจะตรวจพบว่าโหนด $u$ ถูกโจมตีแบบอิคลิปส์และไม่มีสามารถหาโหนดที่น่าเชื่อถือมาเชื่อมต่อเพื่อหนีการบุกรุก ดังนั้นแนวทางแก้ไขที่ดีที่สุดคือการออกจากระบบ

**กรณีที่ 2** หลังการเดินสุ่มได้รับโหนดมารวมทั้งหมด $K_t$ ที่มากกว่า $k$ โหนด ไม่สามารถบอกได้ว่าถูกอิคลิปส์หรือไม่ อาจเป็นเพราะโหนดที่มุ่งร้ายพยายามคืนโหนดที่น่าเชื่อถือได้มาบ้าง อัลกอริทึมจะสุ่มเลือกโหนดอื่นมาสร้างเส้นทางเชื่อมต่อแทนโหนดที่เชื่อมต่อเดิม เพื่อหนีจากการถูกโจมตีได้

**ทฤษฎีบทที่ 6** *สำหรับกราฟสุ่มดีกรีสม่ำเสมอ $G = (V, E)$ ที่มีดีกรีของทุกโหนดเท่ากับ $d$ พิจารณาโหนด $u$ ใดๆ เป็นโหนดที่ต้องการตรวจสอบว่าถูกโจมตีแบบอิคลิปส์ด้วยผู้มุ่งร้ายขนาด $k$ ด้วยการเดินแบบสุ่มความยาว $w$ เพื่อร้องขอโหนดจากโหนด $v_1, v_2, \ldots v_w$ โดยที่ $v_i$ คือโหนดที่การเดินสุ่มครั้งที่ $i$ เดินไป และได้โหนดคืนกลับมาทั้งหมด $K_t$ โหนด สำหรับ $K_t$ ที่มากกว่า $k$ โหนด การเปลี่ยนการเชื่อมต่อจากโหนดที่เชื่อมต่ออยู่เดิม กับโหนดที่สุ่มจากโหนดที่ได้รับมา ความน่าจะเป็นที่จะหลุดจากการโจมตีแบบอิคลิปส์เท่ากับ $(K_t - k)/K_t$*

**พิสูจน์** พิจารณาเนื่องจากผู้มุ่งร้ายมีขนาด $k$ โหนด ดังนั้นโหนดที่ได้รับคืนกลับมา $K_t$ จะเป็นโหนดที่เชื่อถือได้เท่ากับ $K_t - k$ โหนด การสุ่มเลือกโหนดที่ได้รับมาหนึ่งโหนดมาเชื่อมต่อแทน โหนดที่เชื่อมต่อเดิมหนึ่งโหนด อัลกอริทึมจะสำเร็จด้วยความน่าจะเป็น $(K_t - k)/K_t$ ■

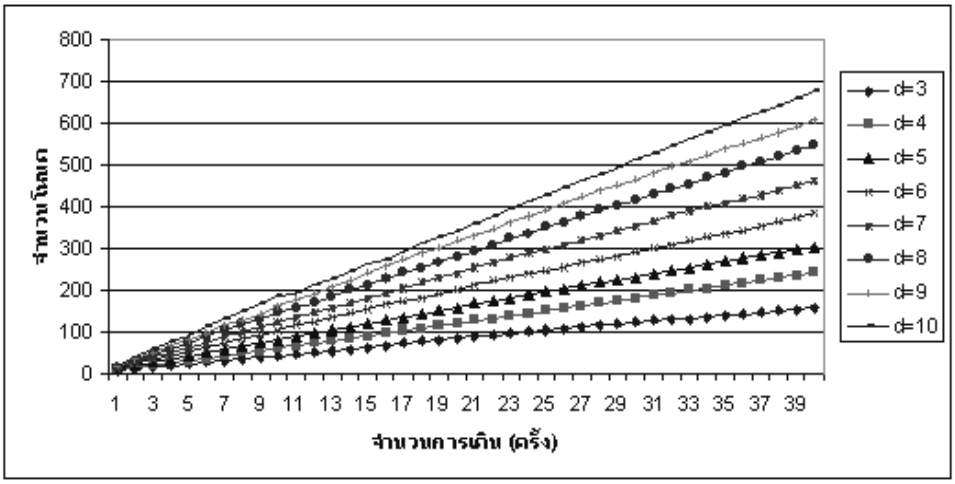
**ทดสอบจำนวนโหนดที่รู้จักเพิ่มขึ้นภายหลังจากการเดินสุ่ม**

เป็นการทดสอบเพื่อดูถึงอัตราการเพิ่มขึ้นของโหนดที่รู้จักเมื่อเดินโดยใช้การเดินแบบสุ่มแล้วร้องขอโหนดเพิ่ม เพื่อพิสูจน์ว่าโดยปกติการเดินแบบสุ่ม สำหรับระบบเครือข่ายที่ไม่ถูกโจมตีแบบอิคลิปส์ ถ้าการเดินแบบสุ่มไม่เกิดการเดินวนซ้ำ จำนวนโหนดที่รู้จักจะต้องเพิ่มมากขึ้น

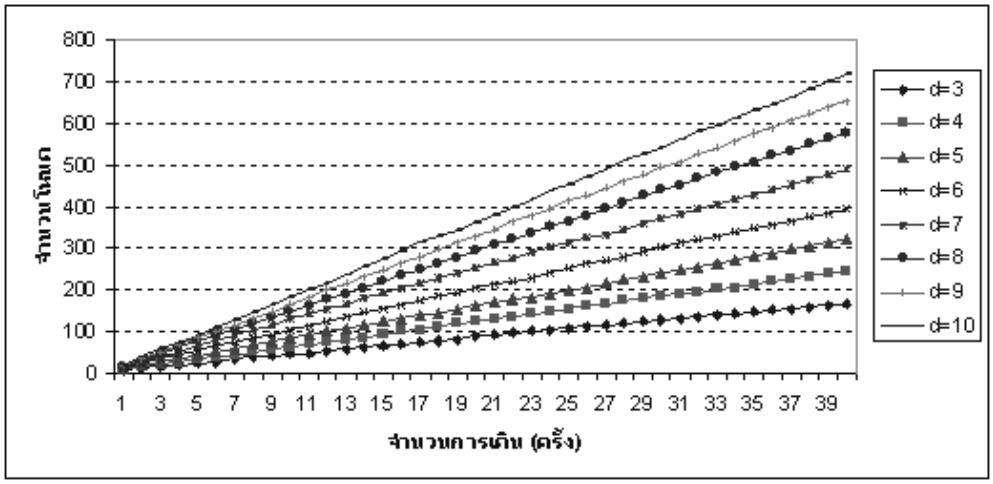
ในส่วนของวิธีการได้มีการพิสูจน์เกี่ยวกับอัตราการเพิ่มของเซตโหนดที่ได้รับคืนมา ถ้าเดินแบบสุ่มความยาว $w$ จะมีโหนดที่รู้จักเพิ่มขึ้นอย่างน้อย $(1+d/2)*w$ โหนด ดังนั้นในการทดลองเราจะทำการทดลองเพื่อพิสูจน์แนวคิดนี้ด้วยการวิเคราะห์ทางคณิตศาสตร์ด้วยกราฟสุ่มดีกรีสม่ำเสมอ และทำการทดลองด้วยการจำลองด้วยแบบจำลองพรีเฟอร์เรนเชียล (preferential model) เพื่อพิสูจน์ว่าสามารถนำอัลกอริทึม ไปใช้ในกราฟที่มีคุณสมบัติขยายตัวที่ดีแบบอื่นได้

1. ทดลองด้วยกราฟสุ่มดีกรีสม่ำเสมอ

พิจารณาผลที่ได้จากภาพที่15 และภาพที่16 เป็นการทดลองด้วยกราฟสุ่มดีกรีสม่ำเสมอที่ใช้พารามิเตอร์ d ต่างๆ และมีขนาดของกราฟคือ 5000 โหนดและ 50000 โหนดตามลำดับ ใช้การเดินแบบสุ่มความยาว 40



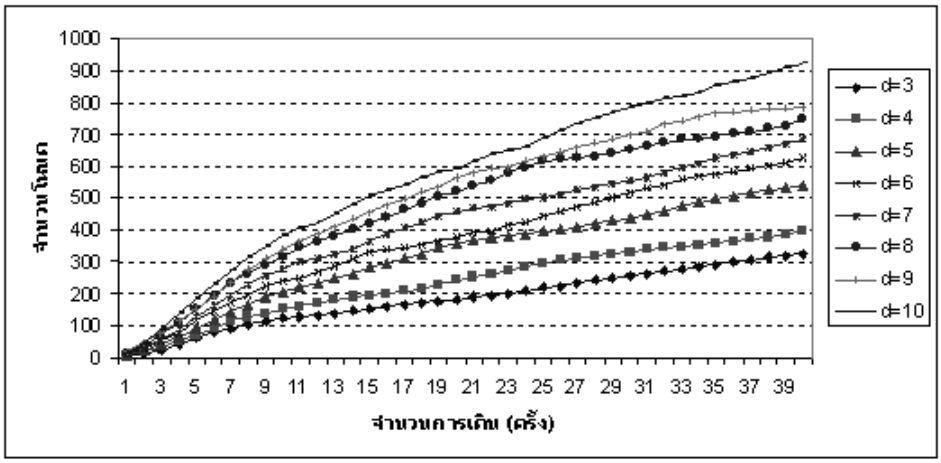

**ภาพที่15** จำนวนการเพิ่มของโหนดที่รู้จักตามจำนวนการเดินแบบสุ่มสำหรับกราฟสุ่มดีกรีสม่ำเสมอ (random d-regular graph) 5000 โหนด



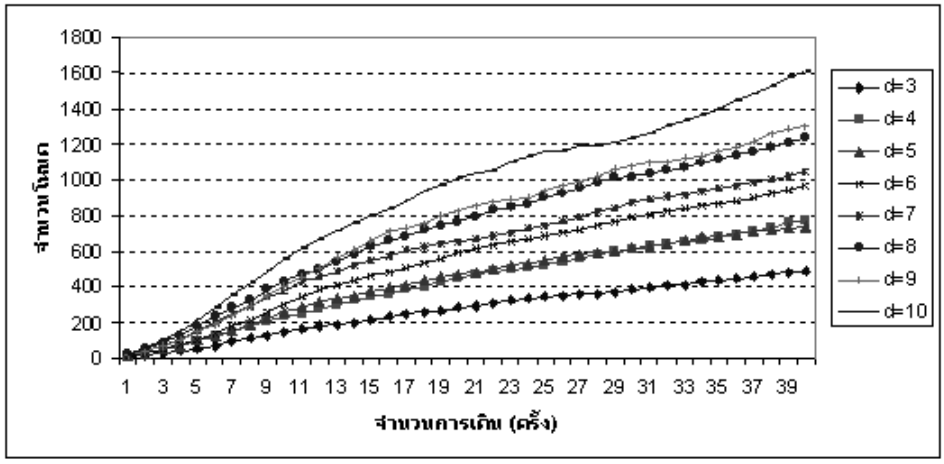

**ภาพที่16** จำนวนการเพิ่มของโหนดที่รู้จักตามจำนวนการเดินแบบสุ่มสำหรับกราฟสุ่มดีกรีสม่ำเสมอ (random d-regular graph) 50000 โหนด

2. ทดลองด้วยกราฟที่สร้างด้วยอัลกอริทึมแบบจำลองพรีเฟอร์เรนเชียล (Preferential Model)

พิจารณาผลที่ได้จากภาพที่17 และภาพที่18 เป็นการทดลองด้วยแบบจำลองพรีเฟอร์เรนเชียลที่ใช้พารามิเตอร์ d ต่างๆ และมีขนาดของกราฟคือ 5000 โหนดและ 50000 โหนดตามลำดับ ใช้การเดินแบบสุ่มความยาว 40 ในการร้องขอโหนด




**ภาพที่17** จำนวนการเพิ่มของโหนดที่รู้จักตามจำนวนการเดินแบบสุ่มสำหรับกราฟแบบพรีเฟอร์เรนเชียล 5000 โหนด




**ภาพที่18** จำนวนการเพิ่มของโหนดที่รู้จักตามจำนวนการเดินแบบสุ่มสำหรับกราฟแบบพรีเฟอร์เรนเชียล 50000 โหนด

จากการทดลองในการเดินสุ่มเพื่อร้องขอโหนดใหม่ พบว่าอัตราการขยายตัวอย่างรวดเร็วทั้งกราฟสุ่มดีกรีสม่ำเสมอและแบบจำลองพรีเฟอร์เรนเชียล ด้วยอัตราการขยายใกล้ๆกับค่า $d$ สำหรับกราฟสุ่มดีกรีสม่ำเสมอ และใกล้กับ $2d$ สำหรับแบบจำลองพรีเฟอร์เรนเชียลซึ่งถือว่าดีกว่า $d/2$ มาก

**ทดสอบเพื่อหาความยาวของการเดินสุ่มที่เหมาะสม**

จะเป็นการทดลองเพื่อวิเคราะห์หาความยาวของการเดินสุ่มที่เหมาะสมสำหรับนำมาใช้ในอัลกอริทึมสำหรับการตรวจสอบการบุกรุกแบบอิคลิปส์ สำหรับกราฟสุ่มดีกรีสม่ำเสมอ และแบบจำลองพรีเฟอร์เรนเชียล จะต้องเดินสุ่มด้วยความยาวเท่าไรที่จะสามารถรับประกันความสำเร็จของอัลกอริทึมได้

ในกรณีที่ไม่มีผู้มุ่งร้ายในระบบการร้องขอโหนด $K_t$ โหนด สำหรับการวิเคราะห์หาจำนวนความยาว $w$ ที่ใช้ในการเดินสุ่มจะวิเคราะห์ด้วยการคำนวนและการทดลองสำหรับ กราฟสุ่มดีกรีสม่ำเสมอ และการทดลองเพียงอย่างเดียวสำหรับแบบจำลองพรีเฟอร์เรนเชียล โดยจะใช้ค่า $K_t$ เท่ากับ 100, 500 และ 1000 ในการทดลอง

1. การวิเคราะห์เชิงทฤษฎีเพื่อหาความยาวการเดินสุ่มที่เหมาะสมสำหรับกราฟสุ่มดีกรีสม่ำเสมอ

สำหรับการวิเคราะห์หาจำนวนการเดินที่เหมาะสมสำหรับอัลกอริทึม สำหรับแก้ปัญหา การบุกรุกแบบอิคลิปส์ โดยในหัวข้อนี้จะวิเคราะห์เชิงทฤษฎีสำหรับแบบจำลองกราฟสุ่มดีกรีสม่ำเสมอ (random d-regular graph) โดยจะอาศัยคุณสมบัติของการขยายตัวที่ดีเพื่อแสดงว่าสำหรับการตรวจสอบ

**ทฤษฎีบทย่อยที่ 1** *สำหรับกราฟสุ่มดีกรีสม่ำเสมอ* $G=(V,E)$ *ที่มีดีกรีเท่ากับ d การตรวจสอบว่าถูกโจมตีแบบอิคลิปส ด้วยการร้องขอเพียร์ด้วยการเดินแบบสุ่มความยาว w ถ้าไม่ได้มีผู้มุ่งร้ายจำนวนโหนดที่รู้จักจะเพิ่มขึ้นไม่น้อยไปกว่า* $(1+d/2)*w$ *ด้วยความน่าจะเป็นที่สูง*

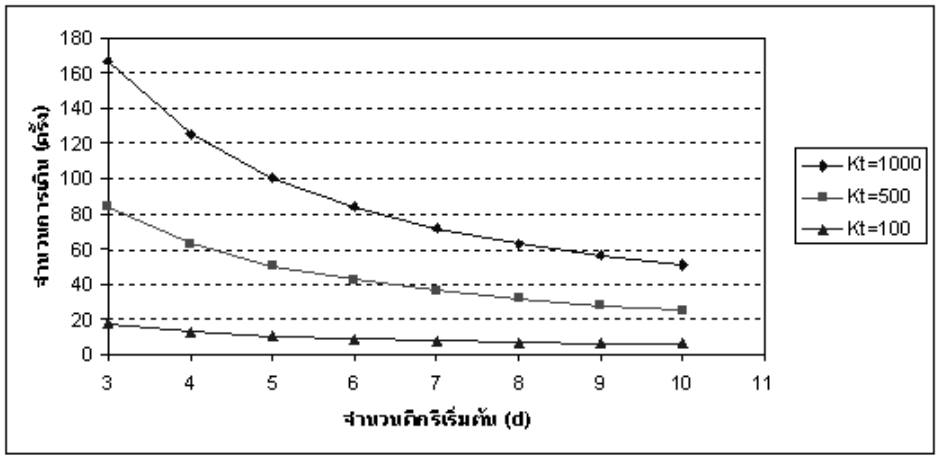
**พิสูจน์** สำหรับกราฟสุ่มดีกรีสม่ำเสมอ $G=(V,E)$ ที่ $|V|=n$ และมีดีกรีเท่ากับ $d$ จากทฤษฎีบทที่ 3 อัตราการขยายตัว $h(G)$ ไม่น้อยไปกว่า $d/2$ ด้วยความน่าจะเป็นที่สูง ให้ $S_1$ เป็นเซตของกลุ่มเล็กๆในกราฟที่ $|S_1|\le n/2$ จำนวนดโหนดที่รู้จักจะไม่น้อยไปกว่า $(1+d/2)*|S_1|$ ทำการเดินแบบสุ่มความยาว $w$ ให้ $S_2$ เป็นเซตของกลุ่มเล็กๆหลังเดินสุ่มความยาว w จะได้ว่า $|S_2|=|S_1|+w$ ดังนั้นหลังจากเดินแบบสุ่มเพื่อร้องขอโหนดสิ้นสุดลงจำนวนโหนดที่รู้จักจะไม่น้อยไปกว่า $(1+d/2)*|S_2|$ จะได้โหนดที่รู้จักเพิ่มขึ้นไม่น้อยไปกว่า $(1+d/2)*|S_2|-(1+d/2)*|S_1|$ คือ $(1+d/2)*w$ เนื่องจากทฤษฎีบทที่ 3 จะเป็นจริงด้วยความน่าจะเป็นที่สูงดังนั้น การร้องขอโหนดด้วยการเดินแบบสุ่มความยาว w จะได้โหนดที่รู้จักเพิ่มไม่น้อยไปกว่า $(1+d/2)*w$ ด้วยความน่าจะเป็นที่สูง ■

**ทฤษฎีบทที่ 7** *สำหรับการตรวจสอบด้วยการเดินสุ่มในกราฟสุ่มดีกรีสม่ำเสมอ* $G=(V,E)$ *ที่มีดีกรีเท่ากับ d เพื่อร้องขอเพื่อให้ได้โหนด* $K_t$ *โหนดจะใช้ความยาวในการเดินสุ่มอย่างน้อย* $K_t/(1+d/2)$ *ด้วยความน่าจะเป็นที่สูง*

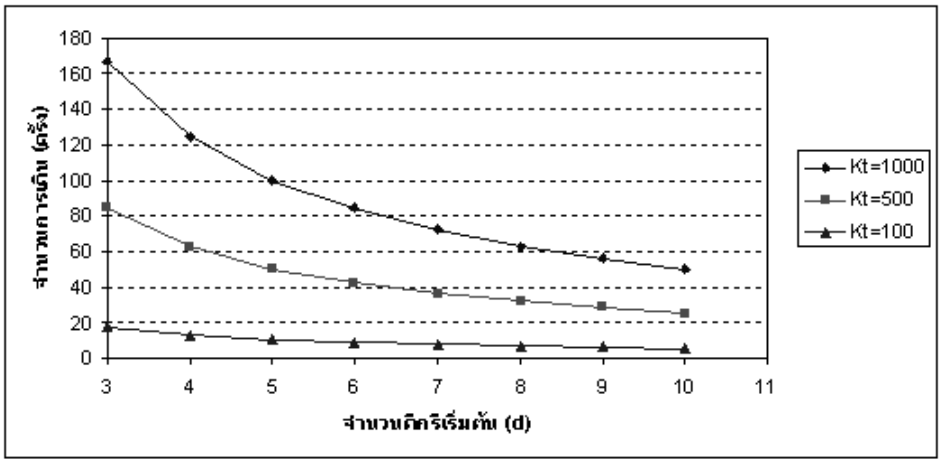
**พิสูจน์** จากทฤษฎีย่อยที่ 1 การเดินสุ่มความยาว $w$ เพื่อร้องขอโหนดจะได้รับโหนดเพิ่มไม่น้อยไปกว่า $(1+d/2)*w$ เป็นจริงด้วยความน่าจะเป็นที่สูง ดังนั้นถ้าจะทำการเดินสุ่มเพื่อร้องขอเพื่อให้ได้โหนด $K_t$ โหนด จะต้องเดินสุ่มความยาวอย่างน้อย $K_t/(1+d/2)$ จะเป็นจริงด้วยความน่าจะเป็นที่สูง ■

2. การทดสอบเพื่อหาความยาวการเดินสุ่มที่เหมาะสมสำหรับกราฟสุ่มดีกรีสม่ำเสมอ

วิเคราะห์ในแบบจำลองกราฟสุ่มดีกรีสม่ำเสมอ (random d-regular graph) เพื่อหาค่าพารามิเตอร์ที่เหมาะสมสำหรับอัลกอริทึมการป้องกันการโจมตีแบบอิคลิปส์ที่ได้นำเสนอในการวิจัยนี้ จะพบว่า ความยาวสำหรับการเดินสุ่ม จะแปรผันตามค่า $K_t$ แต่จะแปรผกผันกับดีกรีของกราฟดังแสดงตามภาพที่ 19 และ 20



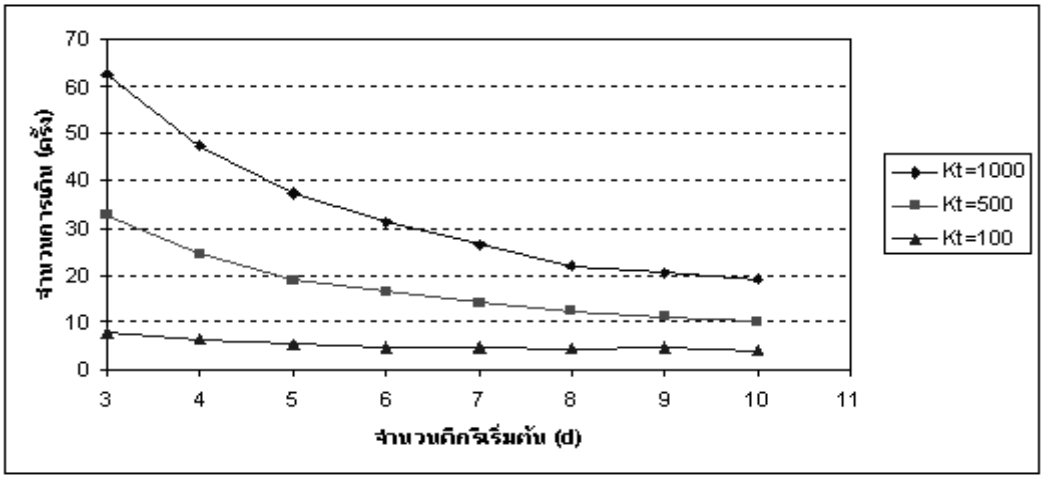

**ภาพที่19** จำนวนการเดินเมื่อเทียบกับจำนวนดีกรีที่ใช้ในการเดินพบโหนดขนาด $K_t$ ต่างๆสำหรับกราฟสุ่มดีกรีสม่ำเสมอ (random d-regular graph) 5000 โหนด



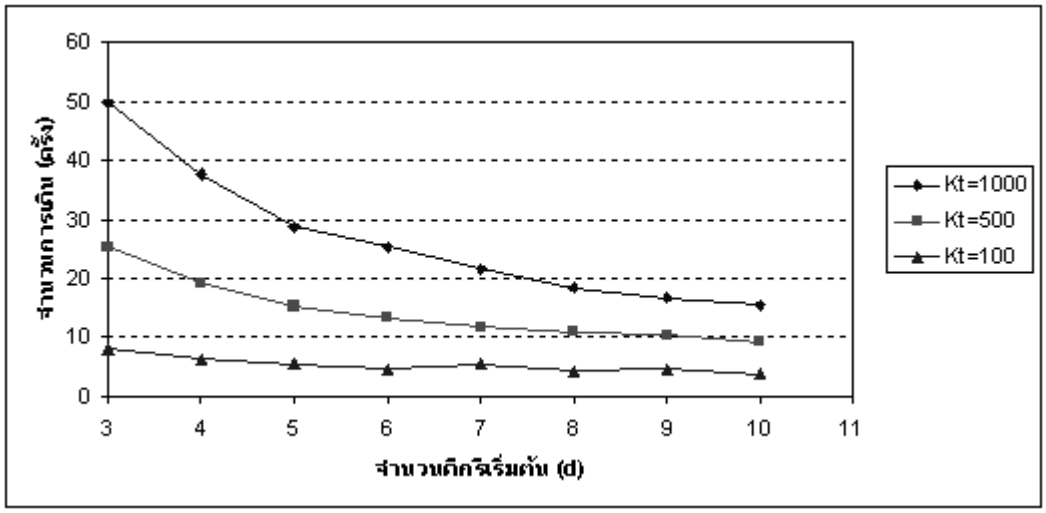

**ภาพที่20** จำนวนการเดินเมื่อเทียบกับจำนวนดีกรีที่ใช้ในการเดินพบโหนดขนาด $K_t$ ต่างๆสำหรับกราฟสุ่มดีกรีสม่ำเสมอ (random d-regular graph) 50000 โหนด

3. การทดสอบเพื่อหาความยาวการเดินสุ่มที่เหมาะสมสำหรับแบบจำลองพรีเฟอร์เรนเชียล

วิเคราะห์ในแบบจำลองพรีเฟอร์เรนเชียล (Preferential Model) เพื่อหาค่าพารามิเตอร์ที่เหมาะสมสำหรับอัลกอริทึม เนื่องจากแบบจำลองนี้มีคุณสมบัติในการขยายตัวได้ใกล้เคียงกับระบบเครือข่ายแบบเพียร์ทูเพียร์ จะพบว่าความยาวที่ใช้สำหรับการเดินสุ่มจะใช้น้อยกว่าในแบบจำลองกราฟสุ่มดีกรีสม่ำเสมอมาก ดังแสดงตามภาพที่ 21 และ 22




**ภาพที่21** แสดงจำนวนการเดินที่จะเทียบกับจำนวนดีกรีในค่า $K_t$ ต่างๆสำหรับกราฟแบบพรีเฟอร์เรนเชียล 5000 โหนด




**ภาพที่22** แสดงจำนวนการเดินที่จะเทียบกับจำนวนดีกรีในค่า $K_t$ ต่างๆสำหรับกราฟแบบพรีเฟอร์เรนเชียล 50000 โหนด

ในการวิเคราะห์พารามิเตอร์ที่เหมาะสมของอัลกอริทึม สำหรับแบบจำลองแบบต่างๆ ด้วยพารามิเตอร์บางค่าพบว่าสำหรับการโจมตีที่มีผู้มุ่งร้ายไม่ถึงครึ่งของจำนวนโหนดทั้งหมดพบว่าความยาวที่ใช้ในการเดินสุ่ม สำหรับจำนวนโหนดทั้งหมดใดๆ จะใกล้เคียงกัน โดยในการทดลองพบว่าพารามิเตอร์ที่มีผลต่อความยาวของการเดินสุ่ม $w$ คือจำนวนโหนดในแบบจำลอง ค่า $K_t$ และค่า $d$ สำหรับความยาวของการเดินสุ่ม $w$ ในการทดลองด้วยกราฟสุ่มดีกรีสม่ำเสมอ และแบบจำลองพรีเฟอร์เรนเชียลจำนวนโหนด 5000 และ 50000 โหนด จะสรุปได้ผลดังตารางที่ 3 และตารางที่ 4

**ตารางที่ 3** แสดงค่าความยาวที่ใช้ในการเดินสุ่มสำหรับกราฟสุ่มดีกรีสม่ำเสมอขนาด 5000 และ 50000 โหนด

| $K_t$ | $d$ | *วิเคราะห์* | 5000 โหนด | | | 50000 โหนด | | |
|---|---|---|---|---|---|---|---|---|
| | | $W$ | E(w) | Var(w) | $w$ | $E(w)$ | $Var(w)$ | $w$ |
| 100 | 3 | 25 | 17 | 0 | 17 | 17 | 0 | 17 |
| | 4 | 20 | 13 | 0 | 13 | 13 | 0 | 13 |
| | 5 | 16.67 | 10 | 0 | 10 | 10 | 0 | 10 |
| | 6 | 14.29 | 9 | 0 | 9 | 9 | 0 | 9 |
| | 7 | 12.5 | 8 | 0 | 8 | 8 | 0 | 8 |
| | 8 | 11.11 | 7 | 0 | 7 | 7 | 0 | 7 |
| | 9 | 10 | 6 | 0 | 6 | 6 | 0 | 6 |
| | 10 | 9.09 | 5.7 | 0.48 | 6.18 | 5 | 0 | 5 |
| 500 | 3 | 125 | 84 | 0 | 84 | 84 | 0 | 84 |
| | 4 | 100 | 63 | 0 | 63 | 63 | 0 | 63 |
| | 5 | 83.33 | 50 | 0 | 50 | 50.3 | 0.48 | 50.78 |
| | 6 | 71.43 | 42.6 | 0.52 | 43.12 | 42 | 0 | 42 |
| | 7 | 62.5 | 36 | 0 | 36 | 36 | 0 | 36 |
| | 8 | 55.56 | 32 | 0 | 32 | 32 | 0 | 32 |
| | 9 | 50 | 28 | 0 | 28 | 28 | 0 | 28 |
| | 10 | 45.45 | 25 | 0 | 25 | 25 | 0 | 25 |
| 1000 | 3 | 250 | 167 | 0 | 167 | 167 | 0 | 167 |
| | 4 | 200 | 125.8 | 0.42 | 126.22 | 125.3 | 0.48 | 125.78 |
| | 5 | 166.67 | 100.6 | 0.52 | 101.12 | 100.2 | 0.42 | 100.62 |
| | 6 | 142.86 | 84 | 0 | 84 | 84 | 0 | 84 |
| | 7 | 125 | 72 | 0 | 72 | 72 | 0 | 72 |
| | 8 | 111.11 | 63 | 0 | 63 | 63 | 0 | 63 |
| | 9 | 100 | 56 | 0 | 56 | 56 | 0 | 56 |
| | 10 | 90.91 | 50.9 | 0.32 | 51.22 | 50.2 | 0.42 | 50.62 |

**ตารางที่ 4** แสดงความยาวที่ใช้ในการเดินสุ่มสำหรับแบบจำลองพรีเฟอร์เรนเชียลขนาด 5000 และ 50000 โหนด

| $K_t$ | $d$ | 5000 โหนด | | | 50000 โหนด | | |
|---|---|---|---|---|---|---|---|
| | | E(w) | Var(w) | $w$ | $E(w)$ | $Var(w)$ | $w$ |
| 100 | 3 | 7.9 | 0.99 | 8.89 | 7.9 | 1.60 | 9.50 |
| | 4 | 6.3 | 0.67 | 6.97 | 6.4 | 1.17 | 7.57 |
| | 5 | 5.4 | 0.84 | 6.24 | 5.4 | 0.84 | 6.24 |
| | 6 | 4.6 | 0.70 | 5.30 | 4.7 | 1.06 | 5.76 |
| | 7 | 4.8 | 0.79 | 5.59 | 5.4 | 1.07 | 6.47 |
| | 8 | 4.4 | 1.26 | 5.66 | 4.3 | 0.82 | 5.12 |
| | 9 | 4.7 | 0.82 | 5.52 | 4.5 | 0.85 | 5.35 |
| | 10 | 4 | 0.82 | 4.82 | 3.8 | 1.14 | 4.94 |
| 500 | 3 | 32.5 | 2.99 | 35.49 | 25.3 | 3.40 | 28.70 |
| | 4 | 24.7 | 1.06 | 25.76 | 19.2 | 1.14 | 20.34 |
| | 5 | 19 | 1.15 | 20.15 | 15.3 | 1.64 | 16.94 |
| | 6 | 16.5 | 1.43 | 17.93 | 13.1 | 1.91 | 15.01 |
| | 7 | 14.2 | 1.40 | 15.60 | 11.8 | 1.55 | 13.35 |
| | 8 | 12.4 | 0.84 | 13.24 | 10.8 | 1.62 | 12.42 |
| | 9 | 11.1 | 0.99 | 12.09 | 10.3 | 1.34 | 11.64 |
| | 10 | 10.2 | 1.03 | 11.23 | 9.3 | 1.89 | 11.19 |
| 1000 | 3 | 62.7 | 5.50 | 68.20 | 49.6 | 4.67 | 54.27 |
| | 4 | 47.3 | 4.99 | 52.29 | 37.7 | 2.67 | 40.37 |
| | 5 | 37.3 | 3.37 | 40.67 | 28.6 | 2.41 | 31.01 |
| | 6 | 31.4 | 2.12 | 33.52 | 25.3 | 2.00 | 27.30 |
| | 7 | 26.5 | 1.96 | 28.46 | 21.4 | 2.01 | 23.41 |
| | 8 | 21.9 | 1.73 | 23.63 | 18.3 | 1.49 | 19.79 |
| | 9 | 20.4 | 1.78 | 22.18 | 16.7 | 1.25 | 17.95 |
| | 10 | 19.2 | 1.93 | 21.13 | 15.4 | 1.43 | 16.83 |

# สรุป

ในงานวิจัยนี้เสนอการแก้ปัญหาการบุกรุกแบบไซบิลและการบุกรุกแบบอิคลิปส์ สำหรับการแก้ปัญหาการบุกรุกแบบไซบิล โดยจะปรับปรุงโปรโตคอลไซบิลการ์ดที่รับประกันความถูกต้องสำหรับโหนดเริ่มต้นที่หยิบมาด้วยการสุ่ม แต่ไม่ได้รับประกันโหนดที่อยู่ติดผู้มุ่งร้าย ในงานวิจัยโหนดที่ถูกเลือกสำหรับเริ่มต้น จะใช้การตรวจสอบว่ารอบข้างในระยะ k ช่วงความสัมพันธ์มีผู้มุ่งร้ายหรือไม่ ด้วยวิธีการเดียวกับการตรวจสอบในระบบใช้ศูนย์กลางตรวจสอบ ผลจากการทดลองจะได้ว่า ถ้าถอยโหนดเริ่มต้นสร้างเส้นทางตรวจสอบให้ไกลจากผู้มุ่งร้ายได้ไกลประมาณ k = 3 โอกาสที่เส้นทางตรวจสอบจะเดินตกไปยังกลุ่มผู้มุ่งร้ายจะมีค่าโดยเฉลี่ยน้อยมาก ซึ่งจะช่วยให้การรับประกันความถูกต้องดีขึ้น ซึ่งในงานวิจัยนี้โหนดต่างๆในระบบจะถูกกำหนดว่ามีขีดความสามารถเท่ากัน ดังนั้นวิธีการสำหรับตรวจสอบโหนดตรวจสอบโหนดรอบข้างที่มีขีดความสามารถต่างกันจึงเป็นงานที่น่าสนใจ

สำหรับงานวิจัยการแก้ปัญหาการบุกรุกแบบอิคลิปส์ ได้เสนออัลกอริทึมสำหรับตรวจสอบผู้มุ่งร้ายขนาด $k$ โดยใช้การร้องขอโหนดที่ติดกับผู้มุ่งร้าย ในกรณีที่ผู้มุ่งร้ายคืนโหนดที่น่าเชื่อถือกลับมาบ้าง สำหรับโหนดที่ได้รับคืนกลับมา $K_t$ โหนด อัลกอริทึมจะทำการเลือกโหนดที่ได้รับคืนมา มาเป็นโหนดที่เชื่อมต่อด้วยแทนโหนดเดิม ซึ่งโอกาสที่กระบวนการนี้จะทำให้หลุดจากการโจมตีเท่ากับ $(K_t - k)/K_t$ ภายในงานวิจัยจะทดลองเพื่อหาค่าพารามิเตอร์ความยาวของการเดินสุ่ม $w$ ที่เหมาะสมสำหรับค่า $K_t$ บางค่า ในการทดลองอัลกอริทึมจะใช้แบบจำลองกราฟสุ่มดีกรีสม่ำเสมอ และแบบจำลอง
พรีเฟอร์เรนเชียล ซึ่งจะได้ค่าตามตารางที่ 3 และตารางที่ 4 เนื่องจากในระบบเครือข่ายจริงๆจำนวนผู้มุ่งร้ายเราไม่ทราบแน่นอน ดังนั้นในการตั้งค่า $k$, $W$ และ $K_t$ ถ้าการตั้งค่า $k$ หากสูงเกินไป เมื่อต้องการโอกาสที่อัลกอริทึมจะทำงานสำเร็จจำเป็นต้องตั้งค่า $K_t$ และ $W$ ให้สูงขึ้นตาม แต่ถ้าตั้งค่า k น้อยเกินไปโอกาสที่อัลกอริทึมจะทำงานผิดก็จะมีสูงมาก ดังนั้นการตั้งค่า $k$, $W$ และ $K_t$ จึงเป็นปัญหาที่น่าสนใจอยู่

# เอกสารและสิ่งอ้างอิง

Abraham, I. and Malkhi, D. 2003. **Probabilistic quorums for dynamic systems**. In the 17th International Symposium on Distributed Computing (DISC)., pages 60-74.

Alon, N. 1986. **Eigenvalues and expanders**. Combinatorica 6(2)., pages 83-96.

Alon, N. and Milman, V. D. 1985. **isoperimetric inequalities for graphs and superconcentrators**. Journal of Combinatorial Theory, Series B 38(1)., pages 73-88.

Barabasi, A.-L. Albert, R. 1999. **Emergence of scaling in random networks**. Science 286., pages 509-512

Boyd, S. Ghosh, A. Prabhakar, B. and Shah, D. **Gossip algorithms: Design, analysis and applications**. In the 24th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM., vol. 3, pages 1653-1664.

Cheng, A. and Friedman, E. 2005. **Sybilproof Reputation Mechanisms**. In ACM SIGCOMM 2005 Workshop on the Economics of Peer-to-Peer Systems (P2PECON)., pages 128-132.

Douceur, J. 2002. **The Sybil attack**. In Proceeding of 1st International Workshop on Peer-to-Peer System (IPTPS)., pages 251-260

Flaxman, A. D. 2006. **Expansion and lack thereof in randomly perturbed graphs**. Manuscript.

Friedman, J. 2003. **A proof of alon's second eigenvalue conjecture**. ACM Symposium on Theory of Computing (STOC)., 720–724.

Hota, C. Lindqvist, J. Karvonen, K. Yla-Jaaski, A. Mohan, C.K.J. 2007. **Safeguarding Against Sybil Attacks via Social Networks and Multipath Routing**. In Networking, Architecture, and Storage (NAS)., pages 122-132.

Kleinberg, J. 2000. **The small-world phenomenon: An algorithm perspective**. In the 32nd Annual ACM Symposium on Theory of Computing (STOC)., pages 163-170.

Motwani, R. and Raghavan, P. 1995. **Randomized Algorithms**. Cambridge University Press.

Morselli, R. Bhattacharjee, B. Srinivasan, A. and Marsh, M. 2005. **Efficient lookup on unstructured topologies**. In the 32nd Annual ACM Symposium on Principle of Distributed Computing (PODC)., pages 77-86.

Newsome, J. Shi, E. Song, D. and Perrig, A. 2004. **The Sybil attack in sensor networks: Analysis & defenses**. In Third International Symposium on Information Processing in Sensor Networks (IPSN)., pages 259-268.

Singh, A. Castro, M. Druschel, P. and Rowstron, A. 2004. **Defending against the Eclipse attacks in Overlay Networks**. Proceedings of the 11th ACM SIGOPS European Workshop.

Singh, A. Ngan, T. Druschel, Peter. and Wallach, D. S. 2006. **Eclipse Attacks on Overlay Networks: Threats and Defenses**, In the 25th IEEE International Conference on Computer and Communications, Infocom 2006.

Tanner, M. 1984. **Explicit construction of concentrators from generalized N-gons**. SIAM Journal on Algebraic Discrete Methods 5(3)., pages 287-293.

Yu, H. Kaminsky, M. Gibbons, P. B. and Flaxman, A. 2006. **SybilGuard: Defending Against Sybil Attacks via Social Networks**. In ACM SIGCOMM, ACM Press., pages 267-278.

Yu, H. Kaminsky, M. and Gibbons, P. B. 2007. **Toward an Optimal Social Network Defense Against Sybil Attacks**. In the 26th ACM Symposium on Principles of Distributed Computing (PODC)., pages 376-377.

# ประวัติการศึกษา และการทำงาน

| | |
|---|---|
| ชื่อ –นามสกุล | ณัฐวุฒิ กิจบุตราวัฒน์ |
| วัน เดือน ปี ที่เกิด | 29 กรกฎาคม พ.ศ. 2522 |
| สถานที่เกิด | กรุงเทพมหานคร |
| ประวัติการศึกษา | วศ.บ. (วิศวกรรมไฟฟ้า) |
| ตำแหน่งหน้าที่การงานปัจจุบัน | ผู้ช่วยนักวิจัย |
| สถานที่ทำงานปัจจุบัน | ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ |
| ผลงานดีเด่นและรางวัลทางวิชาการ | - |
| ทุนการศึกษาที่ได้รับ | - |