

กิตติกรรมประกาศ	ก
บทคัดย่อภาษาไทย	ง
บทคัดย่อภาษาอังกฤษ	จ
สารบัญตาราง	ฉ
สารบัญภาพ	ญ
บทที่ 1 บทนำ	1
1.1 ที่มาและความสำคัญของปัญหา	1
1.2 แนวทางการแก้ปัญหา	5
1.3 สรุปสาระสำคัญจากเอกสารที่เกี่ยวข้อง	6
1.4 วัตถุประสงค์ของการวิจัย	11
1.5 ขอบเขตการทำวิจัย	11
1.6 ประโยชน์ที่ได้รับจากการศึกษาเชิงทฤษฎีและเชิงประยุกต์	11
1.7 ระเบียบวิธีวิจัย	11
บทที่ 2 ทฤษฎีที่ใช้ในการแก้ปัญหา	13
2.1 การวิเคราะห์ข้อมูลจากคุณลักษณะ (Feature Analysis)	13
2.2 ขั้นตอนวิธีเคมีนและการเลือกจุดศูนย์กลางเริ่มต้น	14
2.2.1 ขั้นตอนการเลือกจุดศูนย์กลางเริ่มต้น	16
2.2.2 ตัวอย่างการจัดกลุ่มข้อมูลโดยใช้ขั้นตอนวิธีเคมีน	17
2.3 การตัดสินใจบอตเน็ต (Botnet Decision)	20

บทที่ 3 แนวคิดในการแก้ไขปัญหาและขั้นตอนการพัฒนา	22
3.1 การเตรียมข้อมูลแพ็กเก็ต (Packet)	23
3.2 การวิเคราะห์ข้อมูลจากคุณลักษณะ (Feature Analysis)	26
3.3 กระบวนการแบ่งกลุ่ม (Clustering)	27
3.4 กระบวนการรวมกลุ่มข้อมูลและการตัดสินใจ (Botnet Decision)	30
บทที่ 4 การทดลองและผลการทดลอง	32
4.1 ระบบที่ใช้ในการทดลอง	32
4.2 ข้อมูลที่ใช้ในการทดลอง	32
4.3 การเตรียมการทดลอง	33
4.3.1 การทดลองขั้นตอนวิธีการจำแนกบอตเน็ตโดยใช้ขั้นตอนวิธีเคมีนแบบขนานที่ปรับปรุงใหม่ ขั้นตอนวิธีเคมีนแบบเดิม และขั้นตอนวิธีเคมีนแบบขนานโดยใช้จุดศูนย์กลางร่วม	33
4.3.2 การทดลองการจำแนกบอตเน็ตโดยใช้ขั้นตอนวิธีเคมีนแบบขนานที่นำเสนอ โดยการทดลองเพิ่มจำนวนโปรเซสเซอร์ขึ้นทีละหนึ่ง	33
4.4 ผลการทดลอง	34
4.4.1 ผลการทดลองขั้นตอนวิธีการจำแนกบอตเน็ตโดยใช้ขั้นตอนวิธีเคมีนแบบขนานที่ปรับปรุงใหม่ ขั้นตอนวิธีเคมีนแบบเดิม และขั้นตอนวิธีเคมีนแบบขนานโดยใช้จุดศูนย์กลางร่วม	34
4.4.2 ผลการทดลองการจำแนกบอตเน็ตโดยใช้ขั้นตอนวิธีเคมีนแบบขนานที่นำเสนอ โดยการทดลองเพิ่มจำนวนโปรเซสเซอร์ขึ้นทีละหนึ่ง	35
4.4.3 ผลการทดลองเพิ่มเติม การจำแนกบอตเน็ตโดยใช้ขั้นตอนวิธีเคมีนแบบขนานที่นำเสนอ โดยการทดลองเปรียบเทียบข้อมูลแพ็กเก็ตของ Botnet Traffic และ Normal Traffic จำนวน 10,000 และ 30,000 แพ็กเก็ตรวมกัน เมื่อเพิ่มจำนวนโปรเซสเซอร์ขึ้นทีละหนึ่ง	36

4.4.4 ผลการทดลองเพิ่มเติม การจำแนกบอตเน็ตโดยใช้ขั้นตอนวิธีเคมีน	36
แบบขนานที่นำเสนอ โดยการทดลองเปรียบเทียบข้อมูลแพ็กเก็ตของ Botnet Traffic และ Normal Traffic จำนวน 20,000 และ 40,000 แพ็กเก็ตรวมกัน เมื่อเพิ่มจำนวนโปรเซสเซอร์ขึ้นทีละหนึ่ง	
4.5 สรุปผลการทดลอง	37
บทที่ 5 สรุปผลการทำวิจัย	38
5.1 สรุปผลการทำวิจัย	38
5.2 ข้อเสนอแนะ	39
เอกสารอ้างอิง	40
ประวัติผู้เขียน	43

สารบัญตาราง

ตาราง	หน้า
1.1 ผลการทดลองการแบ่งกลุ่มของข้อมูล Botnet Traffic ออกจากข้อมูล Normal Traffic โดยใช้ K-means Algorithm	9
1.2 ผลการทดลองการแบ่งกลุ่มของข้อมูล Botnet Traffic ออกจากข้อมูล Normal Traffic โดยใช้ Merged X-means Algorithm	10
1.3 ผลการทดลองการแบ่งกลุ่มของข้อมูล Botnet Traffic ออกจากข้อมูล Normal Traffic โดยใช้ Unmerged X-means Algorithm	10
2.1 ตัวอย่างข้อมูลในการจัดกลุ่มข้อมูลของขั้นตอนวิธีเคมีน	17
2.2 การคำนวณจุดศูนย์กลาง (Centroid) รอบที่ 2	19
2.3 การคำนวณจุดศูนย์กลาง (Centroid) รอบที่ 3	19
4.1 ผลการทดสอบการจำแนกบอตเน็ต	34
4.2 ผลการทดลองเปรียบเทียบเวลาในการประมวลผลข้อมูลแพ็กเก็ตเกิดของ Botnet Traffic และ Normal Traffic จำนวน 10,000 และ 30,000 แพ็กเก็ตรวมกัน เมื่อเพิ่มจำนวนโปรเซสเซอร์ขึ้นทีละหนึ่ง	36
4.3 ผลการทดลองเปรียบเทียบเวลาในการประมวลผลข้อมูลแพ็กเก็ตเกิดของ Botnet Traffic และ Normal Traffic จำนวน 20,000 และ 40,000 แพ็กเก็ตรวมกัน เมื่อเพิ่มจำนวนโปรเซสเซอร์ขึ้นทีละหนึ่ง	37

สารบัญภาพ

รูป	หน้า
1.1 กระบวนการทำงานของบอตเน็ต (Botnet)	2
1.2 ผลกระทบของภัยคุกคามจากบอตเน็ต (Botnet)	4
1.3 Detection Botnet Framework	7
1.4 Average byte frequency over 256 ASCII for Normal IRC flows	8
1.5 Average byte frequency over 256 ASCII for Botnet IRC flows	9
2.1 ตัวอย่างการแบ่งกลุ่มของขั้นตอนวิธีเคมีน (K-means-Algorithm)	14
2.2 ขั้นตอนวิธีเคมีน (K-means-Algorithm)	16
3.1 กระบวนการจำแนกบอตเน็ตโดยใช้ขั้นตอนวิธีเคมีนแบบขนาน	22
3.2 การดักจับข้อมูลแพ็กเก็ตเกิดของ Botnet Traffic และ Normal Traffic ของโปรแกรม Wireshark	24
3.3 ข้อมูล Packet Analyzer ของ Botnet Traffic และ Normal Traffic	24
3.4 การจัดเรียงข้อมูล Packet Analyzer ของ Botnet Traffic และ Normal Traffic	25
3.5 การนับข้อมูล Packet Analyzer ของ Botnet Traffic และ Normal Traffic	25
3.6 กราฟแสดงค่าความถี่เฉลี่ยในแต่ละไบต์ (Byte) ของตัวอักษรแอสกี (ASCII) ข้อมูล 1,000 แพ็กเก็ตเกิดของ Botnet Traffic และ Normal Traffic	26
3.7 กระบวนการจำแนกบอตเน็ต	27
3.8 ขั้นตอนวิธีเคมีนแบบขนานโดยใช้จุดศูนย์กลางร่วมกัน	28
3.9 กระบวนการจำแนกบอตเน็ตโดยใช้ขั้นตอนวิธีเคมีนแบบขนานในรูปแบบที่นำเสนอ	29
4.1 กราฟแสดงเวลาในการประมวลผลเมื่อมีการเพิ่มขึ้นของจำนวนโปรเซสเซอร์ของข้อมูลแพ็กเก็ตเกิด Botnet Traffic และ Normal Traffic จำนวน 40,000 แพ็กเก็ตรวมกัน	35