

สารบัญ

	หน้าที่
บทคัดย่อ	(2)
กิตติกรรมประกาศ	(4)
สารบัญตาราง	(9)
สารบัญภาพประกอบ	(10)
บทที่	
1 บทนำ.....	1
1.1 ความเป็นมาและความสำคัญของงานวิจัย.....	1
1.2 วัตถุประสงค์ของงานวิจัย.....	4
1.3 สมมุติฐานของงานวิจัย.....	4
1.4 ขอบเขตงานวิจัย.....	4
1.5 นิยามตัวแปร.....	5
1.6 ประโยชน์ที่ได้รับจากงานวิจัย.....	7
1.7 รายละเอียดของวิทยานิพนธ์.....	7
2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง.....	8
2.1 ทฤษฎีการทำงานของระบบจดหมายอิเล็กทรอนิกส์.....	8
2.1.1 ระบบการทำงานของจดหมายอิเล็กทรอนิกส์.....	8
2.1.2 พื้นฐานการทำงานของโปรโตคอล SMTP.....	10
2.1.3 จดหมายอิเล็กทรอนิกส์สแปม.....	11
2.2 ทฤษฎีการทำงานของบอตเน็ต.....	12
2.2.1 ลักษณะการแพร่กระจายของบอตเน็ต.....	13

2.3	งานวิจัยที่เกี่ยวข้องกับจดหมายอิเล็กทรอนิกส์สแปมและบอตเน็ต	14
3	วิธีการดำเนินการวิจัย.....	20
3.1	การออกแบบระบบ DSDSE	20
3.1.1	ระบบ DETECTION	22
3.1.2	ระบบ TRAFFIC CONTROL	25
3.1.3	อัลกอริทึมของระบบ DSDSE	26
3.2	การเตรียมการทดลอง.....	27
3.2.1	การเตรียมการทดลองในส่วนการร้องขอข้อมูล DOMAIN NAME จากระบบ DNS	27
3.2.2	การเตรียมการทดลองในส่วนของการส่งจดหมายอิเล็กทรอนิกส์.....	27
3.2.3	การเตรียมการทดลองในส่วนการลดอัตราการส่งจดหมายอิเล็กทรอนิกส์ สแปม	28
3.2.4	รายละเอียดฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ในการเตรียมทดลอง.....	28
3.3	การดำเนินการทดลอง.....	29
3.3.1	การทดลองการร้องขอข้อมูล DOMAIN NAME จากระบบ DNS	29
3.3.2	การทดลองการส่งจดหมายอิเล็กทรอนิกส์	30
3.3.3	การทดลองการลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจากเครื่อง บอตเน็ต	30
3.4	ข้อมูลเพิ่มเติมที่ใช้ในการทดลอง.....	32
3.4.1	ข้อมูลเกี่ยวกับจดหมายอิเล็กทรอนิกส์	32
3.4.2	ข้อมูลบอตเน็ตที่นำมาทดลอง	33
3.4.3	รายละเอียดการส่งงาน SDBOT	34
3.4.4	คำสั่งในการสั่งให้บอตเน็ตทำงาน.....	35
4	ผลของการวิจัย.....	37

4.1	การตรวจสอบเครื่องบอตเน็ตจากพฤติกรรมการร้องขอตรวจสอบ DOMAIN NAME จากระบบ DNS	37
4.2	การตรวจสอบเครื่องบอตเน็ตจากการตรวจสอบการส่งจดหมายอิเล็กทรอนิกส์ สแปมโดยวิธีกำหนดค่า THRESHOLD	44
4.2.1	การจำลองข้อมูลจดหมายอิเล็กทรอนิกส์ปกติและจดหมาย อิเล็กทรอนิกส์สแปม.....	44
4.2.2	การตรวจสอบข้อมูลจดหมายอิเล็กทรอนิกส์ปกติและจดหมาย อิเล็กทรอนิกส์สแปมโดยวิธีการกำหนดค่า THRESHOLD.....	45
4.2.3	การทดลองการส่งจดหมายอิเล็กทรอนิกส์สแปมโดยวิธีการกำหนดค่า THRESHOLD	46
4.2.4	ผลการวิเคราะห์ข้อมูลการตรวจสอบจดหมายอิเล็กทรอนิกส์สแปม โดยวิธีกำหนดค่า THRESHOLD.....	51
4.2.5	ผลการวิเคราะห์ค่า FALSE POSITIVE ของการกำหนดค่า THRESHOLD	57
4.2.6	ผลการวิเคราะห์ค่า FALSE NEGATIVE ของการกำหนดค่า THRESHOLD ...	62
4.3	การลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปม (TRAFFIC CONTROL)	69
4.3.1	การลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมโดยวิธีกำหนด ค่าเริ่มต้น	70
4.3.2	การลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจากประวัติการใช้งาน	71
4.3.3	การลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมแบบกำหนดค่ากลาง .	72
5	สรุปผลการศึกษา.....	73
5.1	สรุปผลการทดสอบสมมุติฐาน	73
5.1.1	สรุปผลการทดสอบสมมุติฐานที่ 1	73
5.1.2	สรุปผลการทดสอบสมมุติฐานที่ 2	74
	ภาคผนวก.....	75
	ภาคผนวก ก	76

ข้อมูลค่า A, B, C สำหรับการคำนวณค่า SIMILARITY	76
ภาคผนวก ข	79
การทดสอบระบบ DSDSE ที่เงื่อนไขต่างๆ	79
ภาคผนวก ค	97
โปรแกรมที่ใช้ในงานวิจัยนี้	97
บรรณานุกรม	102
ประวัตินักศึกษา	105

สารบัญตาราง

ตารางที่	หน้าที่
4.1 แสดงข้อมูลการหาค่า Threshold.....	38
4.2 แสดงการหาค่า Similarity จาก Domain Name	41
4.3 แสดงข้อมูลตัวอย่างการส่งจดหมายอิเล็กทรอนิกส์ของเครื่อง 100 เครื่องโดยมีเครื่อง บอตเน็ต 10 % ความน่าจะเป็น 0.2 และ Threshold = $\frac{1}{2}$ Threshold.....	46
4.4 แสดงข้อมูลจำนวนบอตเน็ตที่ตรวจพบ ณ Threshold = $\frac{1}{4}$ Threshold.....	51
4.5 แสดงข้อมูลจำนวนบอตเน็ตที่ตรวจพบ ณ Threshold = $\frac{1}{2}$ Threshold.....	53
4.6 แสดงข้อมูลจำนวนบอตเน็ตที่ตรวจพบ ณ Threshold = $\frac{3}{4}$ Threshold.....	54
4.7 แสดงข้อมูลจำนวนบอตเน็ตที่ตรวจพบ ณ Threshold = 1 Threshold	56
4.8 แสดงข้อมูล False Positive ของการกำหนดค่า Threshold = $\frac{1}{4}$ Threshold.....	58
4.9 แสดงข้อมูล False Positive ของการกำหนดค่า Threshold = $\frac{1}{2}$ Threshold.....	59
4.10 แสดงข้อมูล False Positive ของการกำหนดค่า Threshold = $\frac{3}{4}$ Threshold.....	60
4.11 แสดงข้อมูล False Positive ของการกำหนดค่า Threshold = 1 Threshold	62
4.12 แสดงข้อมูล False Negative ของการกำหนดค่า Threshold = $\frac{1}{4}$ Threshold.....	63
4.13 แสดงข้อมูล False Negative ของการกำหนดค่า Threshold = $\frac{1}{2}$ Threshold.....	64
4.14 แสดงข้อมูล False Negative ของการกำหนดค่า Threshold = $\frac{3}{4}$ Threshold.....	65
4.15 แสดงข้อมูล False Negative ของการกำหนดค่า Threshold = 1 Threshold	67
4.16 สรุปข้อเปรียบเทียบของการกำหนดค่า Threshold.....	68
ก.1 แสดงค่า A, B และ C สำหรับการคำนวณค่า Similarity	76

สารบัญภาพประกอบ

ภาพที่	หน้าที่
2.1 แสดงการรับ-ส่งจดหมายอิเล็กทรอนิกส์ผ่านระบบอินเทอร์เน็ต	8
2.2 แสดงการติดต่อสื่อสารผ่านโปรโตคอล SMTP	10
2.3 แสดงการแพร่กระจายของบอตเน็ต	13
2.4 แสดงอัตราส่วนการส่งจดหมายอิเล็กทรอนิกส์สแปมจากแหล่งต่างๆ	15
2.5 อัลกอริทึมในการตรวจสอบบอตเน็ตจากการร้องขอผ่านระบบ DNS	16
2.6 แสดงภาพ Domain Name ที่มีค่า Similarity สูงๆ	17
3.1 การทำงานของระบบ DSDSE	21
3.2 โครงสร้างระบบ DSDSE	21
3.3 การทำงานของระบบ Detection Module ในระบบ DSDSE	22
3.4 อัลกอริทึมระบบ DSDSE	26
3.5 แสดงการวางระบบเครือข่ายที่ใช้สำหรับการทดลอง	28
3.6 อัตราส่วนการส่งจดหมายอิเล็กทรอนิกส์จากบอตเน็ตแต่ละประเภท	33
4.1 แสดงการหาค่า Threshold ของกลุ่มเครื่องที่สอบถามระบบ DNS	40
4.2 แสดงค่า Similarity ของแต่ละ Domain Name	43
4.3 แสดงข้อมูลค่าความถูกต้องของ บอตเน็ต 10 เปอร์เซ็นต์ ความน่าจะเป็น 0.2 และการกำหนดค่า Threshold = $\frac{1}{2}$ Threshold	50
4.4 แสดงจำนวนบอตเน็ตที่ถูกตรวจพบเมื่อกำหนด Threshold = $\frac{1}{4}$ Threshold	51
4.5 แสดงจำนวนบอตเน็ตที่ถูกตรวจพบเมื่อกำหนด Threshold = $\frac{1}{2}$	52
4.6 แสดงจำนวนบอตเน็ตที่ถูกตรวจพบเมื่อกำหนด Threshold = $\frac{3}{4}$ Threshold	54
4.7 แสดงจำนวนบอตเน็ตที่ถูกตรวจพบ เมื่อกำหนด Threshold = 1 Threshold	55
4.8 แสดงจำนวนค่า False Positive ของการกำหนดค่า Threshold = $\frac{1}{4}$ Threshold	57
4.9 แสดงจำนวนค่า False Positive ของการกำหนดค่า Threshold = $\frac{1}{2}$ Threshold	59
4.10 แสดงจำนวนค่า False Positive ของการกำหนดค่า Threshold = $\frac{3}{4}$ Threshold	60
4.11 แสดงจำนวนค่า False Positive ของการกำหนดค่า Threshold = 1 Threshold	61
4.12 แสดงจำนวนค่า False Negative ของการกำหนดค่า Threshold = $\frac{1}{4}$ Threshold	63
4.13 แสดงจำนวนค่า False Negative ของการกำหนดค่า Threshold = $\frac{1}{2}$ Threshold	64

4.14 แสดงจำนวนค่า False Negative ของการกำหนดค่า Threshold = $\frac{3}{4}$ Threshold	65
4.15 แสดงจำนวนค่า False Negative ของการกำหนดค่า Threshold = 1 Threshold.....	66
4.16 แสดงปริมาณ Bandwidth ที่ถูกใช้ไปในขณะที่บอตเน็ตส่งจดหมายอิเล็กทรอนิกส์.....	69
4.17 แสดงปริมาณ Bandwidth ที่ถูกควบคุมในการส่งจดหมายอิเล็กทรอนิกส์ แบบที่ 1 โดยการกำหนดค่าเริ่มต้น	70
4.18 แสดงปริมาณ Bandwidth ที่ถูกควบคุมในการส่งจดหมายอิเล็กทรอนิกส์ แบบที่ 2 โดยการพิจารณาประวัติการใช้งาน	71
4.19 แสดงปริมาณ Bandwidth ที่ถูกควบคุมในการส่งจดหมายอิเล็กทรอนิกส์ แบบที่ 3 โดยการกำหนดค่ากลาง	72
ข.1 แสดงค่า False Positive ของ Threshold = $\frac{1}{4}$ Threshold	79
ข.2 แสดงค่า False Negative ของ Threshold = $\frac{1}{4}$ Threshold	79
ข.3 แสดงค่า True Positive ของ Threshold = $\frac{1}{4}$ Threshold	80
ข.4. แสดงค่า True Negative Positive ของ Threshold = $\frac{1}{4}$ Threshold.....	80
ข.5 แสดงค่า False Positive ของ Threshold = $\frac{1}{2}$ Threshold	81
ข.6 แสดงค่า False Negative ของ Threshold = $\frac{1}{2}$ Threshold.....	81
ข.7 แสดงค่า True Positive ของ Threshold = $\frac{1}{2}$ Threshold	82
ข.8 แสดงค่า True Negative ของ Threshold = $\frac{1}{2}$ Threshold	82
ข.9 แสดงค่า False Positive ของ Threshold = $\frac{3}{4}$ Threshold.....	83
ข.10 แสดงค่า False Negative ของ Threshold = $\frac{3}{4}$ Threshold.....	83
ข.11 แสดงค่า True Positive ของ Threshold = $\frac{3}{4}$ Threshold	84
ข.12 แสดงค่า True Negative ของ Threshold = $\frac{3}{4}$ Threshold	84
ข.13 แสดงค่า False Positive ของ Threshold = 1 Threshold	85
ข.14 แสดงค่า False Negative ของ Threshold = 1 Threshold.....	85
ข.15 แสดงค่า True Positive ของ Threshold = 1 Threshold	86
ข.16 แสดงค่า True Negative ของ Threshold = 1 Threshold	86
ข.17 แสดงค่า False Positive ของความน่าจะเป็นของการส่งจดหมายอิเล็กทรอนิกส์สเปม ที่ 0.1	87
ข.18 แสดงค่า False Negative ของความน่าจะเป็นการส่งจดหมายอิเล็กทรอนิกส์สเปม ที่ 0.1	87

[illegible]

ข.33 แสดงค่า False Positive ของความน่าจะเป็นของการส่งจดหมายอิเล็กทรอนิกส์สแปม ที่ 1	95
ข.34 แสดงค่า False Negative ของความน่าจะเป็นของการส่งจดหมายอิเล็กทรอนิกส์สแปม ที่ 1	95
ข.35 แสดงค่า True Positive ของความน่าจะเป็นของการส่งจดหมายอิเล็กทรอนิกส์สแปม ที่ 1	96
ข.36 แสดงค่า True Negative ของความน่าจะเป็นของการส่งจดหมายอิเล็กทรอนิกส์สแปม ที่ 1	96
ค.1 โปรแกรม Softperfect Bandwidth Manager ใช้สำหรับลดอัตรา Bandwidth	97
ค.2 โปรแกรม WinDump GUI สำหรับการเก็บข้อมูลเครือข่าย	98
ค.3 โปรแกรมเก็บขนาดจดหมายอิเล็กทรอนิกส์ E-mail Statistic	99
ค.4 โปรแกรม Analysis ระบบ DSDSE	100
ค.5 โปรแกรม Speed Test สำหรับดูผลการลดอัตรา Bandwidth และสร้างกราฟข้อมูล ...	101