

สารบัญ

	หน้า
<u>บทคัดย่อ</u>	(1)
ABSTRACT	(2)
กิตติกรรมประกาศ	(3)
สารบัญ	(4)
สารบัญตาราง	(6)
สารบัญภาพ	(8)
สารบัญกราฟ	(10)
<u>บทที่ 1</u> บทนำ	1
1.1 ความเป็นมาของปัญหา	1
1.2 ลักษณะของงานวิจัย	2
1.3 ขอบเขตงานวิจัย	2
1.4 วิธีดำเนินงานวิจัย	2
<u>บทที่ 2</u> เอกสารและงานวิจัยที่เกี่ยวข้อง	3
2.1 Intrusion Detection System (IDS)	3
2.2 ชุดข้อมูลมาตรฐาน KDD Cup'99	4
2.3 Singular Value Decomposition (SVD)	7
2.4 Artificial Neural Network (ANN)	10
2.5 งานวิจัยที่เกี่ยวข้อง	17
<u>บทที่ 3</u> การวิเคราะห์และออกแบบระบบ	22
3.1 สถาปัตยกรรมระบบ	22
3.2 การประมวลผลข้อมูลเบื้องต้น (Preprocessor)	23
3.3 การลดขนาดข้อมูลสำหรับการสร้างชุดข้อมูลการสอน (SVD)	24
3.4 การลดขนาดข้อมูลสำหรับสร้างชุดข้อมูลทดสอบ (Reducer)	27

3.5	การแยกประเภทรูปแบบข้อมูล (ANN)	c4-1	28
<u>บทที่ 4</u>	การทดลองและผลการทดลอง		33
4.1	การตรวจสอบคุณสมบัติของ SVD		33
4.2	การประยุกต์ใช้ SVD กับ FFN	<u>c4-3</u>	39
4.3	การประยุกต์ใช้ SVD กับ SOM		52
<u>บทที่ 5</u>	สรุปผลการวิจัยและข้อเสนอแนะ		61
5.1	สรุปผลการทดลองเรื่องการตรวจสอบคุณสมบัติของ SVD		61
5.2	สรุปผลการทดลองเรื่องการประยุกต์ใช้ SVD กับ FFN		62
5.3	สรุปผลการทดลองเรื่องการประยุกต์ใช้ SVD กับ SOM		63
5.4	ข้อเสนอแนะ		64
	<u>บรรณานุกรม</u>		65
	<u>ประวัติผู้ทำวิทยานิพนธ์</u>		67

สารบัญตาราง

ตารางที่		หน้า
2.1	คุณลักษณะที่ใช้ในชุดข้อมูลมาตรฐาน KDDcup'99	5
3.1	ความหมายของสถานะการติดต่อที่ใช้ในชุดข้อมูล KDDcup'99	24
4.1	ชนิดและจำนวนของข้อมูลที่ใช้ในการทดลองที่หนึ่ง	34
4.2	ชนิดและจำนวนของข้อมูลที่ใช้ในการทดลองที่สอง	40
4.3	ส่วนหนึ่งของ FBN ลักษณะต่างๆ ที่ใช้ในการสอน	44
4.4	Mean Square Error (MSE) ของ FBN แต่ละตัวภายหลังการสอน	44
4.5	ผลการตรวจจับของ FBN แบบ 1 อินพุต 1 เอาพุต	49
4.6	ผลการตรวจจับของ FBN แบบ 1 อินพุต 4 เอาพุต	49
4.7	ผลการตรวจจับของ FBN แบบ 2 อินพุต 1 เอาพุต	49
4.8	ผลการตรวจจับของ FBN แบบ 2 อินพุต 4 เอาพุต	50
4.9	ผลการตรวจจับของ FBN แบบ 3 อินพุต 1 เอาพุต	50
4.10	ผลการตรวจจับของ FBN แบบ 3 อินพุต 4 เอาพุต	50
4.11	ผลการตรวจจับของ FBN แบบ 41 อินพุต 1 เอาพุต	51
4.12	ผลการตรวจจับของ FBN แบบ 41 อินพุต 4 เอาพุต	51
4.13	เวลาที่ใช้ในการสอน SOM ที่มีอินพุต = 41 มิติ	54
4.14	เวลาที่ใช้ในการสอน SOM ที่มีอินพุต = 1 มิติ	54
4.15	เวลาที่ใช้ในการสอน SOM ที่มีอินพุต = 2 มิติ	54
4.16	เวลาที่ใช้ในการสอน SOM ที่มีอินพุต = 3 มิติ	55
4.17	ผลการทดสอบ SOM ขนาด 5x5 (41 อินพุต)	56
4.18	ผลการทดสอบ SOM ขนาด 10x10 (41 อินพุต)	56
4.19	ผลการทดสอบ SOM ขนาด 15x25 (41 อินพุต)	56
4.20	ผลการทดสอบ SOM ขนาด 20x20 (41 อินพุต)	56
4.21	ผลการทดสอบ SOM ขนาด 5x5 (1 อินพุต)	56
4.22	ผลการทดสอบ SOM ขนาด 10x10 (1 อินพุต)	57

(7)

4.23	ผลการทดสอบ SOM ขนาด 15x25 (1 อินพุท)	57
4.24	ผลการทดสอบ SOM ขนาด 20x20 (1 อินพุท)	57
4.25	ผลการทดสอบ SOM ขนาด 5x5 (2 อินพุท)	57
4.26	ผลการทดสอบ SOM ขนาด 10x10 (2 อินพุท)	58
4.27	ผลการทดสอบ SOM ขนาด 15x25 (2 อินพุท)	58
4.28	ผลการทดสอบ SOM ขนาด 20x20 (2 อินพุท)	58
4.29	ผลการทดสอบ SOM ขนาด 5x5 (3 อินพุท)	58
4.30	ผลการทดสอบ SOM ขนาด 10x10 (3 อินพุท)	59
4.31	ผลการทดสอบ SOM ขนาด 15x25 (3 อินพุท)	59
4.32	ผลการทดสอบ SOM ขนาด 20x20 (3 อินพุท)	59

สารบัญภาพ

ภาพที่		หน้า
2.1	ลักษณะของชุดข้อมูล KDDcup'99	7
2.2	ตัวอย่างแสดงการใช้ SVD อัลกอริทึมกับเมตริก	8
2.3	สถาปัตยกรรมของ FBN	11
2.4	ตัวแบบทางคณิตศาสตร์ของชั้นใด ๆ ใน FBN	12
2.5	สถาปัตยกรรมของ Self-Organizing maps	15
2.6	การเรียงตัวแบบพิกัดสี่เหลี่ยม (ก) และหกเหลี่ยม (ข)	15
2.7	ตัวแบบทางคณิตศาสตร์ของ SOM	16
2.8	(ก) ANN ในลำดับชั้นที่ 1 2 และ 3 (ข) ANN ในลำดับชั้นที่ 4 และ 5	18
2.9	สถาปัตยกรรมของ Agent	19
2.10	สถาปัตยกรรมของ SOM	21
3.1	สถาปัตยกรรมระบบ	22
3.2	ตัวอย่างของเมตริก Attribute-Connection	25
3.3	การใช้ SVD อัลกอริทึมกับเมตริก Attributes-Connections	25
3.4	เมตริก A_k ที่เกิดจากการประมาณค่าเมตริกดั้งเดิมด้วยค่า Singular k ตัวใด ๆ	26
3.5	ตัวอย่างการประมาณค่าเมตริก A ด้วย A_k ที่ $k = 1$	27
3.6	การลดขนาด Connection Vector	27
3.7	ตัวอย่างการคำนวณการลดขนาด Connection Vector	28
3.8	สถาปัตยกรรมในส่วนของ Detector สำหรับ SOM	31
3.9	ตัวอย่างของ SOM Table สำหรับใช้เป็นตารางอ้างอิงให้กับ Detector	32
4.1	เมตริก Attribute-Connection	35
4.2	ผลการใช้ SVD อัลกอริทึมที่ Rank = 1	36
4.3	ผลการใช้ SVD อัลกอริทึมที่ Rank = 2	37

4.4	ผลการใช้ SVD อัลกอริทึมที่ Rank = 3	38
4.5	Connection Vector บนแกนหนึ่งมิติแกนใหม่ที่เกิดขึ้น	41
4.6	Connection Vector บนแกนสองมิติแกนใหม่ที่เกิดขึ้น	42
4.7	Connection Vector บนแกนสามมิติแกนใหม่ที่เกิดขึ้น	42
4.8	ภาพขยายของ Attack Connection Vector ทั้งสี่ประเภท (ก) Back (ข) Neptune (ค) Smurf และ (ง) Teardrop	43
4.9	ตำแหน่งของชุดข้อมูลทดสอบบนชุดข้อมูลการสอนบนแกนใหม่ 1 มิติ	46
4.10	ตำแหน่งของชุดข้อมูลทดสอบบนชุดข้อมูลการสอนบนแกนใหม่ 2 มิติ	47
4.11	ตำแหน่งของชุดข้อมูลทดสอบบนชุดข้อมูลการสอนบนแกนใหม่ 3 มิติ	48
4.12	ค่าน้ำหนักของโหนดแต่ละโหนดบนระนาบ 2 มิติที่ได้จาก SVD Rank = 2	53

สารบัญกราฟ

กราฟที่		หน้า
4.1	ความสัมพันธ์ระหว่างค่า Singular ในลำดับต่างๆ ทั้ง 41 ตัว	40