รายงานการวิจัยฉบับสมบูรณ์

เรื่อง

วิธีการแบบผสมสำหรับการสกัดคุณลักษณะของชุดข้อมูลบนเครือข่ายเพื่อระบุผู้บุกรุกแบบเวลาจริง

(A Hybrid Method for Feature Extraction in Real-time Intrusion Detection)

โครงการวิจัยนี้ได้รับการสนับสนุนทุนวิจัย
จาก
สำนักงานคณะกรรมการวิจัยแห่งชาติ
ปีงบประมาณ พ.ศ. ๒๕๕๔

คณะผู้วิจัย

นายกฤษณะ ชินสาร หัวหน้าโครงการวิจัย
นางสาวสุวรรณา รัศมีขวัญ ผู้ร่วมวิจัย
นางสาวสุนิสา ริมเจริญ ผู้ร่วมวิจัย

ศูนย์วิจัย Knowledge and Smart Technology
คณะวิทยาการสารสนเทศ มหาวิทยาลัยบูรพา

บทคัดย่อ

วิธีการของการตรวจจับการบุกรุกสามารถแบ่งออกได้เป็น 2 ชนิด คือ วิธีการตรวจจับการบุกรุกแบบอโนมาลี (anomaly intrusion detection method) และวิธีการตรวจจับการบุกรุกแบบมิสยูส (*misuse intrusion detection method*) โดยที่วิธีการตรวจจับการบุกรุกแบบอโนมาลีนั้นเป็นวิธีการหาผู้บุกรุกโดยการวิเคราะห์การใช้งานของผู้ใช้งาน หรือตัวระบบเองที่เบี่ยงเบนไปจากระดับการใช้งานโดยปกติ ส่วนการตรวจจับการบุกรุกแบบมิสยูสนั้น เป็นวิธีการหาผู้บุกรุกโดยการเปรียบเทียบข้อมูลที่เข้ามากับรูปแบบของผู้บุกรุกที่มีอยู่เดิม ซึ่งทั้งสองวิธีนี้มีจุดแข็งและจุดอ่อนที่แตกต่างกัน ปัญหาที่เด่นชัดที่สุดของการตรวจจับการบุกรุกแบบมิสยูส คือ ไม่สามารถตรวจจับการบุกรุกแบบใหม่ หรือการบุกรุกที่ไม่มีในชุดรูปแบบของผู้บุกรุกที่มีได้ ส่วนการตรวจจับการบุกรุกแบบอโนมาลีนั้น จะสามารถตรวจจับการบุกรุกจากผู้บุกรุกที่ไม่มีในฐานข้อมูลการบุกรุกได้ แต่ปัญหาที่สำคัญในการตรวจจับการบุกรุกแบบอโนมาลี คือ ทำอย่างไรถึงจะสร้างเค้าโครงของการใช้งานปกติที่ดีได้

ในงานวิจัยนี้ คณะผู้วิจัยได้แสดงให้เห็นแล้วว่าการสกัดคุณลักษณะของชุดข้อมูลบนเครือข่าย มีความสำคัญต่อการพัฒนาการระบุผู้บุกรุกเป็นอย่างมาก ในการได้มาซึ่งตัวแทนชุดคุณลักษณะของชุดข้อมูลที่เหมาะสม เพื่อใช้ในการระบุผู้บุกรุกโดยอาศัยวิธีการแบบผสมในการสกัดคุณลักษณะของชุดข้อมูลเครือข่าย ซึ่งจะเพิ่มความสามารถในการระบุผู้บุกรุกได้เหมาะสมมากกว่า การพัฒนาการสกัดคุณลักษณะชุดข้อมูลเครือข่าย ประกอบด้วย 2 ขั้นตอน คือ 1.การหาคุณลักษณะของชุดข้อมูลที่สามารถแทนข้อมูลได้และมีจำนวนคุณลักษณะที่เหมาะสม และขั้นตอนที่ 2.การรู้จำรูปแบบการบุกรุกเพื่อระบุผู้บุกรุกจากชุดข้อมูลบนเครือข่ายจากคุณลักษณะที่ได้จากการสกัดคุณลักษณะของชุดข้อมูล โดยวัดประสิทธิภาพจากอัตราความเร็วในการตรวจจับผู้บุกรุก และเปอร์เซ็นต์ความผิดพลาดของการตรวจจับผู้บุกรุก

Abstract

Detection of Network Intrusion can be categorized into two groups. The First one is Anomaly Intrusion Detection Method. The second one is Misuse Intrusion Detection Method. For the first method is to inspect the irregular behavior on the usage of the network or on the computer systems. For the second method is to inspect the mis-matching with those patterns store in the database. This brings the discussion of improper way to detect the intrusion as the intruders keep on changing their ways to intrude the networks or computer systems.

In this research report, we have demonstrated how the use of feature selection on those data traffic will help in improving the detection of intrusion more efficient. There are two steps in extract feature on data traffic to detect intrusion. First step is to extract features. And then use pattern recognition to validate whether there is any anomaly behavior for those data traffic. We compare the speed in detecting the intrusion and measure the percentage of the misclassification.

สารบัญ

บทที่ 1 บทนำ

1.1 ที่มาและความสำคัญของปัญหา

จากการพัฒนาอย่างรวดเร็วของโครงข่ายอินเทอร์เน็ตนั้น ทำให้คนส่วนใหญ่หันมาตระหนักถึงการรักษาความปลอดภัยกันมากขึ้น โดยปกติแล้วการบุกรุกจะเน้น 3 ด้านคือ การละเมิดความเป็นส่วนตัวหรือความลับ การแก้ไขความถูกต้องของข้อมูล และการทำให้ไม่สามารถใช้งานระบบคอมพิวเตอร์ได้ วิธีการหนึ่งที่นิยมนำมาใช้ในการสร้างความปลอดภัยให้กับระบบเครือข่ายคอมพิวเตอร์ คือ การตรวจจับการบุกรุก (Intrusion Detection) ซึ่งการตรวจจับการบุกรุก สามารถแบ่งออกได้เป็น 2 ชนิดคือ ระบบการตรวจจับการบุกรุกแบบโฮสเบส (host-based intrusion detection systems) และระบบตรวจจับการบุกรุกแบบเน็ตเวิร์คเบส (network-based intrusion detection systems) โดยที่ระบบตรวจจับการบุกรุกแบบเน็ตเวิร์คเบสนั้นจะติดตั้งที่ระบบเครือข่ายเพื่อทำการตรวจสอบและวิเคราะห์ชุดข้อมูลที่ใช้งานบนเครือข่าย ซึ่งมีความแตกต่างจากระบบการตรวจจับการบุกรุกแบบโฮสเบส ที่จะทำงานอยู่บนระบบเพื่อตรวจสอบและวิเคราะห์ชุดคำสั่งเพื่อระบุการทำงานที่น่าสงสัย วิธีการของการตรวจจับการบุกรุกสามารถแบ่งออกได้เป็น 2 ชนิด คือ วิธีการตรวจจับการบุกรุกแบบอโนมาลี (anomaly intrusion detection method) และวิธีการตรวจจับการบุกรุกแบบมิสยูส (misuse intrusion detection method) โดยที่วิธีการตรวจจับการบุกรุกแบบอโนมาลี นั้นเป็นวิธีการหาผู้บุกรุกโดยการวิเคราะห์การใช้งานของผู้ใช้งาน หรือตัวระบบเองที่เบี่ยงเบนไปจากระดับการใช้งานโดยปกติ ส่วนการตรวจจับการบุกรุกแบบมิสยูสนั้น เป็นวิธีการหาผู้บุกรุกโดยการเปรียบเทียบข้อมูลที่เข้ามากับรูปแบบของผู้บุกรุกที่มีอยู่เดิม ซึ่งทั้งสองวิธีนี้มีจุดแข็งและจุดอ่อนที่แตกต่างกัน ปัญหาที่เด่นชัดที่สุดของการตรวจจับการบุกรุกแบบมิสยูส คือ ไม่สามารถตรวจจับการบุกรุกแบบใหม่ หรือการบุกรุกที่ไม่มีในชุดรูปแบบของผู้บุกรุกที่มีได้ ส่วนการตรวจจับการบุกรุกแบบอโนมาลีนั้น จะระบุว่าการใช้งานที่ตรวจสอบนั้นเป็นผู้บุกรุกหรือไม่นั้นจะตรวจสอบจากการใช้งานนั้นว่ามีการเบี่ยงเบนจากกิจกรรมปกติมากหรือไม่ ดังนั้นการตรวจจับการบุกรุกแบบอโนมาลีจะสามารถตรวจจับการบุกรุกจากผู้บุกรุกที่ไม่มีในฐานข้อมูลการบุกรุกได้ แต่ปัญหาที่สำคัญในการตรวจจับการบุกรุกแบบอโนมาลีคือ ทำอย่างไรถึงจะสร้างเค้าโครงของการใช้งานปกติที่ดีได้ เพราะถ้าสร้างเค้าโครงการใช้งานปกติกว้างไป การบุกรุกบางชนิดอาจจะไม่สามารถถูกตรวจพบ ซึ่งเป็นผลให้การตรวจจับมีประสิทธิผลค่อนข้างต่ำ แต่ในทางกลับกันถ้ากำหนดเค้าโครงการใช้งานปกติแคบเกินไป อาจจะทำให้การใช้งานปกติบางอย่าง ถูกตรวจพบว่าเป็นการบุกรุกได้ เป็นผลทำให้มีโอกาสเกิดข้อผิดพลาดมากและ อาจทำให้ลดประสิทธิภาพการทำงานของระบบโดยรวมได้

จากปัญหาที่พบข้างต้นนั้น ได้มีความพยายามที่จะพัฒนาประสิทธิภาพของการตรวจจับการบุกรุกโดยนำวิธีการต่างๆ เพื่อมาช่วยในการแทนข้อมูลและการรู้จำหรือระบุผู้บุกรุก โดยมุ่งเน้นที่ความสัมพันธ์ 2 ด้านคือ การระบุผู้บุกรุกที่ถูกต้องและมีประสิทธิภาพที่ดี และการหาวิธีการแทนข้อมูลที่ดี โดยทั่วๆ ไปมีหลายวิธีถูกนำมาสร้างเป็นต้นแบบเพื่อระบุผู้บุกรุก โดยใช้องค์ประกอบหลักหรือคุณลักษณะเด่นในการศึกษาและการตรวจจับผู้บุกรุก ตัวอย่างเช่น การวิเคราะห์ค่าตัวแปรแบบเบย์ (Bayesian Parameter Estimation) การรวมข้อมูล (Data Fusion) และเครือข่ายประสาทเทียม (Neural Network) ทำให้ปัญหาการตรวจจับการบุกรุกสามารถพิจารณาได้ในลักษณะเดียวกับปัญหาการแบ่งกลุ่ม (Classification Problem) โดยที่ปัญหาการแบ่งกลุ่มนั้นวิธีการที่ให้ผลลัพธ์ที่ดี คือ วิธีการเครือข่ายประสาทเทียม แต่อย่างไรก็ตามการตรวจจับการบุกรุกนั้นควรจะประมวลผลข้อมูลที่ต้องการตรวจสอบทั้งที่เป็นกรณีที่เป็นการบุกรุก และกรณีที่ไม่ใช่การบุกรุก ซึ่งการตรวจสอบดังกล่าวทำให้ข้อมูลที่ตรวจสอบมีปริมาณมากทั้งจำนวนข้อมูล และจำนวนคุณลักษณะของข้อมูล เป็นผลทำให้เกิดความล่าช้าในการระบุผู้บุกรุก และอาจเป็นสาเหตุให้การบุกรุกบางชนิดสามารถบุกรุกเข้าสู่ระบบเครือข่ายได้

จากที่ได้กล่าวมาทั้งหมดนั้น ผู้วิจัยได้แสดงให้เห็นแล้วว่าการสกัดคุณลักษณะของชุดข้อมูลบนเครือข่าย มีความสำคัญต่อการพัฒนาการระบุผู้บุกรุกเป็นอย่างมาก จึงจำเป็นที่จะต้องหาวิธีการที่ดีในการสกัดคุณลักษณะของชุดข้อมูลบนเครือข่าย เพื่อให้ได้ตัวแทนชุดคุณลักษณะของชุดข้อมูลที่เหมาะสมเพื่อใช้ในการระบุผู้บุกรุกโดยอาศัยวิธีการแบบผสมในการสกัดคุณลักษณะของชุดข้อมูลเครือข่าย ซึ่งขั้นตอนนี้จะมีความซับซ้อนมากกว่าวิธีการสกัดคุณลักษณะของชุดข้อมูลแบบปกติทั่วไป แต่อาจจะสามารถเพิ่มความสามารถในการระบุผู้บุกรุกได้เหมาะสมมากกว่า การพัฒนาการสกัดคุณลักษณะชุดข้อมูลเครือข่าย ประกอบไปด้วย 2 ขั้นตอน คือ 1.ขั้นตอนการหาคุณลักษณะของชุดข้อมูลที่สามารถแทนข้อมูลได้และมีจำนวนคุณลักษณะที่เหมาะสม และขั้นตอนที่ 2 การรู้จำรูปแบบการบุกรุกเพื่อระบุผู้บุกรุกจากชุดข้อมูลบนเครือข่าย จากคุณลักษณะที่ได้จากการสกัดคุณลักษณะของชุดข้อมูล โดยวัดประสิทธิภาพจากอัตราความเร็วในการตรวจจับผู้บุกรุก และเปอร์เซ็นต์ความผิดพลาดของการตรวจจับผู้บุกรุก

1.2 วัตถุประสงค์ของโครงการวิจัย

1. เพื่อศึกษาเทคนิคการสกัดคุณลักษณะเด่นของชุดข้อมูล
2. เพื่อศึกษาวิธีการแบบผสมสำหรับการสกัดคุณลักษณะเด่นของชุดข้อมูล
3. เพื่อศึกษาการรู้จำคุณลักษณะของการระบุผู้บุกรุกเครือข่าย
4. เพื่อศึกษาและพัฒนาโปรแกรมที่ใช้วิธีการแบบผสมสำหรับการสกัดคุณลักษณะของชุดข้อมูลบนเครือข่าย เพื่อนำไปใช้กับการระบุผู้บุกรุกในสถานการณ์จริง

5. เพื่อให้ผู้ที่สนใจสามารถนำแนวความคิดที่นำเสนอ ไปศึกษาเพื่อทำการพัฒนาหรือประยุกต์ใช้ในงานวิจัยของตนเองต่อไป

1.3 ขอบเขตของโครงการวิจัย

การวิจัยครั้งนี้มุ่งที่จะศึกษาและพัฒนาการนำวิธีการแบบผสมสำหรับการสกัดคุณลักษณะชุดข้อมูลเครือข่าย การรู้จำเพื่อระบุผู้บุกรุกเครือข่าย มาใช้งานร่วมกันเพื่อสกัดคุณลักษณะของข้อมูลและการรู้จำผู้บุกรุกที่เป็นลักษณะของการบุกรุกเครือข่าย โดยมีขอบเขตดังต่อไปนี้

ชุดข้อมูลเครือข่าย เป็นข้อมูลมาตรฐานที่ใช้ในการทำแบบทดลองการตรวจจับการบุกรุก สามารถดาวน์โหลดได้เว็บไซต์ http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

ลักษณะของข้อมูลที่นำมาทำแบบทดสอบ จะประกอบด้วยข้อมูล 5 กลุ่มหลัก ซึ่งได้แก่ Normal, DoS, Probe, R2L และ U2R และมีรูปแบบของฟีเจอร์ (Feature) ดังแสดงตามรูปที่ 1-1

```
0,tcp,pop_3,RSTO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,211,6,0.00,0.00,1.00,1.00,0.03,0.07,0.00,255,6,0.02,0.07,0.00,0.00,0.00,0.00,1.00,1.00,neptune.
0,tcp,pop_3,RSTO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,231,16,0.00,0.00,1.00,1.00,0.07,0.06,0.00,255,16,0.06,0.07,0.00,0.00,0.00,0.00,1.00,1.00,neptune.
0,tcp,pop_3,RSTO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,232,5,0.00,0.00,1.00,1.00,0.02,0.06,0.00,255,5,0.02,0.07,0.00,0.00,0.00,0.00,1.00,1.00,neptune.
0,tcp,pop_3,RSTO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,254,15,0.00,0.00,1.00,1.00,0.06,0.07,0.00,255,15,0.06,0.07,0.00,0.00,0.00,0.00,1.00,1.00,neptune.
0,tcp,pop_3,RSTO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,252,6,0.00,0.00,1.00,1.00,0.02,0.07,0.00,255,6,0.02,0.08,0.00,0.00,0.00,0.00,1.00,1.00,neptune.
0,tcp,pop_3,RSTO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,272,16,0.00,0.00,1.00,1.00,0.06,0.06,0.00,255,16,0.06,0.07,0.00,0.00,0.00,0.00,1.00,1.00,neptune.
0,tcp,pop_3,SH,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1.00,1.00,0.00,0.00,1.00,0.00,0.00,255,1,0.00,1.00,1.00,0.00,1.00,1.00,0.00,0.00,nmap.
0,tcp,pop_3,SH,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1.00,1.00,0.00,0.00,1.00,0.00,0.00,255,1,0.00,1.00,1.00,0.00,1.00,1.00,0.00,0.00,nmap.
5,tcp,pop_3,SF,6,151,0,0,0,0,0,0,0,0,0,0,0,0,0,0,511,1,0.07,0.00,0.91,0.00,0.00,1.00,0.00,255,1,0.00,1.00,0.00,0.00,0.00,0.07,0.00,0.90,0.00,satan.
40339,tcp,pop_3,RSTR,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,2,0.00,0.00,1.00,1.00,1.00,0.00,0.00,255,2,0.01,0.44,0.86,0.00,0.00,0.00,0.86,1.00,portsweep.
```

รูปที่ 1-1 ตัวอย่างของข้อมูลที่ใช้ในงานวิจัย

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ขั้นตอนวิธีการสกัดคุณลักษณะของชุดข้อมูลเครือข่าย โดยอาศัยวิธีการแบบผสมสำหรับการสกัดคุณลักษณะชุดข้อมูลเครือข่าย และการรู้จำการระบุผู้บุกรุก ซึ่งเป็นการสกัดคุณลักษณะในรูปแบบใหม่ที่แตกต่างจากการสกัดคุณลักษณะแบบเดิม โดยการนำการสกัดแบบเดิมผสมกับตัวแบบโครงข่ายประสาทเทียม
2. สามารถนำไปพัฒนาระบบตรวจจับการบุกรุกบนระบบเครือข่ายได้ ซึ่งจะทำให้ช่วยรักษาความปลอดภัยเครือข่ายและให้การใช้งานเครือข่ายมีประสิทธิภาพมากขึ้น
3. ขั้นตอนวิธีที่นำเสนอจะสามารถใช้เป็นต้นแบบในการศึกษาขั้นสูงต่อไป

1.5 ระยะเวลาทำการวิจัยและแผนการดำเนินงานตลอดโครงการวิจัย

ดำเนินการวิจัยแบบ 2 ปีต่อเนื่อง (ปีงบประมาณ 2554-2555)

แผนการดำเนินงานปีที่ 1 (ปีงบประมาณ 2554-2555)

แผนการดำเนินงานวิจัย	เดือนที่											
	1	2	3	4	5	6	7	8	9	10	11	12
การจัดเตรียมเครื่องมือ อุปกรณ์และวัสดุวิจัย	⇨											
การศึกษาการสกัดคุณลักษณะชุดข้อมูล	→	→	→	→	→	→	→					
การจัดทำรายงานความก้าวหน้าครั้งที่ 1							⇨					
การศึกษาวิธีการแบบผสมสำหรับการสกัดคุณลักษณะชุดข้อมูล							→	→	→	→	→	→
การจัดทำรายงานความก้าวหน้าครั้งที่ 2												⇨

แผนการดำเนินงานปีที่ 2 (ปีงบประมาณ 2555-2556)

แผนการดำเนินงานวิจัย	เดือนที่											
	1	2	3	4	5	6	7	8	9	10	11	12
การศึกษาระบบโครงข่ายประสาทเทียมเพื่อการรู้จำและระบุผู้บุกรุก	→	→	→	→	→	→	→					
การจัดทำรายงานความก้าวหน้าครั้งที่ 3							⇨					
พัฒนาเป็นโปรแกรม Application สำหรับผู้ใช้ทั่วไป								→	→	→	→	
จัดส่งรายงาน												⇨

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ลักษณะของข้อมูลที่ใช้ในการทำแบบทดลอง

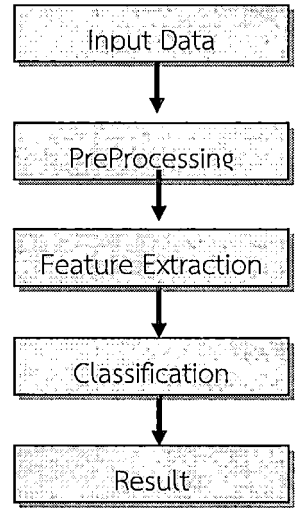
ข้อมูลที่นำมาใช้ในการทำแบบทดลอง เป็นข้อมูลที่ได้จากฐานข้อมูลความรู้ (Knowledge Discovery in Database (KDD) Cup data) ซึ่งเป็นชุดข้อมูลในปี 1999 โดยชุดข้อมูลนี้ได้มาจากความร่วมมือของโครงการวิจัยและพัฒนาเพื่อการทหารของประเทศสหรัฐอเมริกา (Defense Advanced Research Projects Agency: DARPA) ซึ่งร่วมมือกับทางมหาวิทยาลัยเมตซาชูเซตส์ สหรัฐอเมริกา ชุดข้อมูลนี้ถูกสร้างตามการจำลองการโจมตีของผู้บุกรุกจาก U.S. Air Force local area network ตั้งขึ้นที่ Lincoln Labs โดยข้อมูลนั้นมีระยะเวลาในการจัดทำนานถึง 9 สัปดาห์ จากการเก็บข้อมูลจากแพ็กเก็ต TCP ผ่านโปรแกรม TCP Dump ประกอบด้วยข้อมูลขนาดใหญ่มาก ซึ่งมี 41 แอทริบิวต์ (มิติ) ที่ได้จากแพ็กเก็ต TCP (Raw TCP Packet) รวมถึงชนิดของโปรโตคอลซึ่งมีค่า “TCP”, “ICMP”, “UDP” ซึ่งเป็นแอทริบิวต์ที่มีความต่อเนื่องเป็นในลักษณะข้อความ (Nominal) ซึ่งจะมีสถานะ (Label) กำกับไว้เสมอในแต่ละบรรทัด (Record) ว่าข้อมูลชุดนี้เป็นสถานะปกติ (Normal) หรือว่าเป็นชุดข้อมูลที่ถูกโจมตี (Malicious) ทางผู้จัดทำได้คัดเลือก ชุดข้อมูลที่มีมากถึง 5 ล้านบรรทัด ออกมาประมาณ 10% เท่านั้นเพื่อสะดวกในการจัดทำชุดข้อมูลเรียนรู้ (Training Set) และชุดข้อมูลทดสอบ (Test Set)

ชุดข้อมูลที่ได้นำมาทำแบบทดลองนี้ อยู่ในรูปแบบของเครื่องกลเรียนรู้ (Machine Learning Pattern) โดยสามารถแบ่งออกเป็นกลุ่มหลักๆ ได้ 5 กลุ่มคือ Normal, DoS, Probe, R2L และ U2R โดยแต่ละกลุ่มยังมีชนิดของข้อมูลย่อย ๆ อีก โดยแอทริบิวต์ขวามือสุดคือ คลาสแอทริบิวต์ (Class Attribute) ที่เป็นตัวบอกสถานะว่าถูกโจมตีหรือไม่ ซึ่งหากไม่ถูกโจมตีจะมีค่าเป็นปกติ

2.2 กระบวนการรู้จำทางคอมพิวเตอร์

โดยทั่วไปกระบวนการรู้จำทางคอมพิวเตอร์นั้น จะมีขั้นตอนการทำงานหลักๆ คือ การประมวลผลเบื้องต้น (Processing) การวิเคราะห์แยกองค์ประกอบเฉพาะของข้อมูล (Feature Extraction) และการจำแนกข้อมูล (Classification) แสดงดังรูปที่ 2-1 ซึ่งในแต่ละส่วนมีรายละเอียดเบื้องต้นดังนี้

Input Data เป็นข้อมูลที่มีลักษณะหลายรูปแบบตามความต้องการของระบบ เช่น ในการรู้จำตัวอักขระ อาจจะใช้ภาพที่มีลักษณะเป็นข้อความบรรทัดเดียว ข้อความหลายบรรทัด หรือ ภาพตัวอักขระจำนวน 1 อักขระ เป็นต้น ซึ่งข้อมูลอาจได้จากการเก็บข้อมูล หรือนำเอาเอกสารที่เป็นกระดาษไปสแกนเพื่อเปลี่ยนเป็นข้อมูลทางคอมพิวเตอร์ เช่น แฟ้มข้อมูลชนิด txt , xls, bitmap หรือ ได้จากการป้อนข้อมูลผ่านอุปกรณ์อินพุต เช่น เมาส์หรือปากกาอิเล็กทรอนิกส์



รูปที่ 2-1 กระบวนการรู้จำสำหรับปัญหา Intrusion Detection

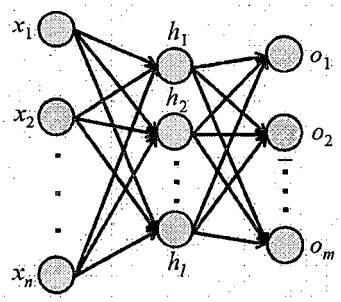
Preprocessing เป็นการประมวลผลเบื้องต้นเพื่อปรับเปลี่ยนลักษณะรูปแบบบางอย่างของข้อมูลอินพุต ทั้งนี้เพื่อปรับอินพุตให้มีความเหมาะสมและตรงตามที่ระบบต้องการ เช่น ปรับขนาด (Resize) ปรับลดจำนวนมิติ (Reduce Dimension) หรือการกำจัดสัญญาณรบกวน (Noise Remove)

Feature Extraction เป็นขั้นตอนของการสกัดเอาลักษณะเฉพาะของแต่ละอินพุตออกมาเป็นเวกเตอร์เพื่อนำไปใช้เป็นอินพุตในการเรียนรู้ระบบและทดสอบระบบ

Classification เป็นขั้นตอนในการจำแนกและตัดสินใจว่าอินพุตที่เข้ามานั้นเป็นการบุกรุกแบบใด โดยในขั้นตอนนี้มีหลายวิธีด้วยกัน เช่นการเปรียบเทียบอินพุตกับโครงสร้างของตัวต้นแบบการบุกรุกในฐานข้อมูลการเปรียบเทียบอินพุตกับกฎเพื่อการตัดสินใจ การใช้โครงข่ายประสาทเทียม หรือการใช้ตัวแบบฮิดเดนมาร์คอฟ เป็นต้น

2.2.1 ระบบโครงข่ายประสาทเทียมแบบวิธีการแพร่กระจายย้อนกลับ (Back propagation Algorithm)

ขั้นตอนวิธีการแพร่กระจายย้อนกลับ เป็นขั้นตอนวิธีที่ใช้ในการเรียนรู้ของเครือข่ายประสาทเทียมวิธีหนึ่งที่นิยมใช้ในโครงข่ายประสาทเทียมหลายชั้น (Multilayer neural network) เพื่อใช้ในการปรับค่าน้ำหนักในเส้นเชื่อมต่อระหว่างโหนดให้เหมาะสม โดยการปรับค่านี้จะขึ้นกับความแตกต่างของค่าเอาต์พุตที่คำนวณได้กับค่าเอาต์พุตที่ต้องการ พิจารณารูปต่อไปนี้ประกอบ



รูปที่ 2-2 ตัวอย่างข่ายงานประสาทเทียมแบบหลายชั้น

ตัวอย่างในรูปด้านบนแสดงข่ายงานป้อนไปหน้าแบบหลายชั้นซึ่งประกอบไปด้วยชั้นอินพุต ชั้นฮิดเดนหรือชั้นซ่อน และชั้นเอาต์พุต ในรูปแสดงชั้นฮิดเดนเพียงชั้นเดียวแต่อาจมีมากกว่าหนึ่งชั้นก็ได้ เส้นเชื่อมจะเชื่อมต่อเป็นชั้น ๆ ไม่ข้ามชั้นจากชั้นอินพุตไปชั้นฮิดเดน ถ้ามีชั้นฮิดเดนมากกว่าหนึ่งชั้นก็เชื่อมต่อกันไป และสุดท้ายจากชั้นฮิดเดนไปชั้นเอาต์พุต

ในการปรับค่าน้ำหนักโดยขั้นตอนวิธีการแพร่กระจายย้อนกลับนั้น เราต้องนิยามค่าผิดพลาดสำหรับการเรียนรู้ของข่ายงาน $MSE(\vec{w})$ จากนั้นจะหาค่าน้ำหนักที่ให้ค่าผิดพลาดต่ำสุด นิยามค่าผิดพลาดดังนี้

$$MSE(\vec{w}) = \frac{1}{2}\sum_{p\in P}\sum_{k\in outputs}(d_{p,k} - o_{p,k})^2 \qquad ...(1)$$

โดยที่ *outputs* คือ เซตของเอาต์พุตโหนดในข่ายงานประสาทเทียม $d_{p,k}$ และ $o_{p,k}$ เป็นค่าเอาต์พุตเป้าหมายและเอาต์พุตที่ได้จากข่ายงานประสาทเทียมตามลำดับของเอาต์พุตโหนดที่ k ของตัวอย่างที่ p ขั้นตอนการแพร่กระจายย้อนกลับจะค้นหาค่าน้ำหนักที่ให้ค่าผิดพลาดกำลังสองเฉลี่ยต่ำสุด

ขั้นตอนของ Back-propagation Algorithm มีดังนี้

Algorithm Backpropagation;

Start with randomly chosen weights;

while MSE is unsatisfactory

and computational bounds are not exceeded, do

for each input pattern x_p, $1 \le p \le P$,

Compute hidden node inputs ($net_{p,j}^{(1)}$);

Compute hidden node outputs ($x_{p,j}^{(1)}$);

Compute inputs to the output nodes ($net_{p,k}^{(2)}$);

Compute the network outputs ($o_{p,k}$);

Modify outer layer weights:

$$\Delta w_{k,j}^{(2,1)} = \eta(d_{p,k} - o_{p,k})\mathcal{S}'(net_{p,k}^{(2)})x_{p,j}^{(1)}$$

Modify weights between input & hidden nodes:

$$\Delta w_{j,i}^{(1,0)} = \eta \sum_{k} \left((d_{p,k} - o_{p,k})\mathcal{S}'(net_{p,k}^{(2)})w_{k,j}^{(2,1)} \right) \mathcal{S}'(net_{p,j}^{(1)})x_{p,i}$$

end-for

end-while.

Note: if S is a logistic function, then
$S'(x) = S(x)(1 - S(x))$

2.2.2 วิธีการรู้จำแบบซัพพอร์ตเวกเตอร์แมชชีน (Support Vector Machine : SVM)

Support Vector Machine หรือ SVM จุดมุ่งหมายที่สำคัญของแนวคิด SVM คือการหาเส้นแบ่ง Hyperplane ซึ่งใช้แบ่งข้อมูลออกเป็นคลาส เพื่อให้ได้ผลลัพธ์ที่ดี โดยพิจารณาจากสมการเส้นตรง Hyper planes และ SVM จะทำการค้นหาจุดของข้อมูลที่อยู่ใกล้เส้นแบ่ง Hyper planes ซึ่งจุดนี้เรียกว่า "Support Vector" มีหลักการดังนี้

นำข้อมูลมาคำนวณหาค่า y ซึ่งค่า $y \in \{-1,1\}$ จากสมการ

$$y = w^T x + b \qquad \text{...(2)}$$

คำนวณหาเส้นแบ่ง ซึ่งเรียกว่าเส้น Optimal Hyperplane จากสมการ

$$w^T x + b = 0 \qquad \text{...(3)}$$

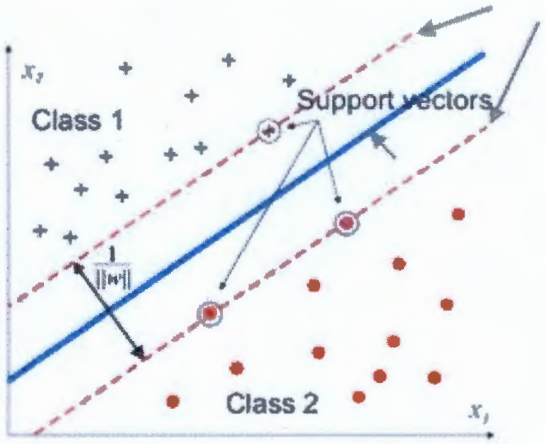
ระยะทาง (d) หรือ maximum margin จากเส้นขอบ ณ จุด x_i ไปยัง hyperplane แสดงดังสมการ

$$d = \frac{|w^T x_i + b|}{\|w\|} \qquad ...(4)$$

w คือ เวกเตอร์น้ำหนัก (Weight Vector)

x_i คือ Input

b คือ ค่าคงที่ที่กำหนดขึ้นเพื่อให้เหมาะสมกับการจัดกลุ่ม



รูปที่ 2-3 การแบ่งกลุ่มข้อมูลโดย Support Vector Machine

เลือกจุดที่อยู่ใกล้เส้นตรง Optimal Hyperplane ทั้งเหนือเส้นซึ่งเรียกว่า "ขอบล่าง" ซึ่งเป็นขอบล่างสุดของคลาสเอกสารที่อยู่เหนือเส้นตรง Optimal Hyperplane และใต้เส้นเรียกว่า "ขอบบน" ซึ่งเป็นขอบบนสุดของคลาสเอกสารที่อยู่ใต้เส้นตรง Optimal Hyperplane เพื่อที่จะหาระยะทางระหว่างเส้นขอบทั้งสองโดยจะเลือกเอาค่าระยะทางที่ห่างจากเส้นตรงOptimal Hyperplane ที่น้อยที่สุดเป็นตัวเลือกในการจัดกลุ่มเอกสาร

2.3 วิธีการวิเคราะห์องค์ประกอบหลัก

วิธีการวิเคราะห์องค์ประกอบหลัก Principal Component Analysis (PCA) เป็นวิธีการทางสถิติ เพื่อใช้ในการสกัดปัจจัยที่อาศัยหลักความสัมพันธ์เชิงเส้นตรงระหว่างตัวแปรที่ใช้เป็นข้อมูล องค์ประกอบหลักตัวแปร คือ การผสมเชิงเส้นตรง (Linear Combination) ของตัวแปรที่อธิบายการผันแปรของข้อมูลได้มากที่สุด จากนั้นหาการผสมเชิงเส้นครั้งที่สองที่สามารถอธิบายการผันแปรได้มากที่สุดเป็นอันดับที่สอง โดยที่ไม่สัมพันธ์กับการผสมครั้งแรก การวิเคราะห์องค์ประกอบหลักถูกนำไป

ประยุกต์ใช้งานต่างๆ เช่น การบีบอัดข้อมูล , การสร้างภาพใบหน้าไอเกนเพื่อใช้ในระบบจดจำ และ การลบออกของพื้นหลังโดยใช้ไอเกน เป็นต้นวิธีการวิเคราะห์องค์ประกอบหลักสามารถนำมาใช้ในการลดมิติของข้อมูลโดย การวิเคราะห์ข้อมูลและเลือกเฉพาะข้อมูลที่มีความสำคัญเท่านั้น ส่วนข้อมูลที่ไม่สำคัญจะถูกตัดทิ้งไป ดังนั้นเมื่อข้อมูลผ่านกระบวนการ *PCA* แล้ว จะได้ผลลัพธ์เป็นไอเกนเวกเตอร์และค่าไอเกน ซึ่งไอเกนเวกเตอร์ที่มีค่าสมนัยกับค่าไอเกนที่มีค่าสูงๆ จะเป็นการดึงข้อมูลที่มีความถี่ต่ำ ส่วนไอเกนเวกเตอร์ที่สมนัยกับค่าไอเกนที่ต่ำๆ จะเป็นการดึงข้อมูลที่มีความถี่สูง

2.3.1 การหาค่าไอเกน และไอเกนเวกเตอร์ (Eigen Value and Eigen Vector)

ความหมายของค่าไอเกน และไอเกนเวกเตอร์ กำหนดให้ A เป็นค่าเมทริกซ์จัตุรัส

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

และ v เป็นเวกเตอร์หลัก (Column Vector) และ λ เป็นค่าคงที่ใดๆ โดยที่

$$v = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_3 \end{bmatrix}$$

ที่ทำให้

$$Av = \lambda v \qquad \text{...(5)}$$

เมื่อ A แทน ค่าเมตทริกซ์

λ แทน เป็นค่าคงที่ใดๆ เป็นสเกลาร์

v แทน ค่าไอเกนเวกเตอร์

จากสมการจะเห็นว่า $v = 0$ ที่ทำให้สมการ เป็นจริงทุกๆ ค่าของ λ สมการที่ (5) อาจเขียนให้อยู่ในอีกรูปหนึ่งคือ

$$(\lambda I - A)v = \bar{0} \qquad \text{...(6)}$$

เมื่อ A แทน ค่าเมทริกซ์

I แทน เมทริกซ์เอกลักษณ์

λ แทน เป็นค่าคงที่ใดๆ เป็นสเกลาร์

v แทน ค่าไอเกนเวกเตอร์

เราจะคำนวณค่าไอเกน และเวคเตอร์ไอเกน ของสมการ (6) โดย

$$\det(\lambda I - A) = 0 \qquad \text{...(7)}$$

จากนั้นก็ใช้วิธีแก้สมการแบบปกติ

2.4 การสกัดคุณลักษณะสำคัญ (*Feature Extraction)*

การสกัดคุณลักษณะสำคัญเป็นอีกขบวนการหนึ่งที่สำคัญมาก ตำราส่วนใหญ่จะแยกส่วนนี้ออกจากการประมวลผลเบื้องต้น คือจะอยู่ระหว่างขั้นตอนการประมวลผลเบื้องต้นกับขั้นตอนการรู้จำ การสกัดคุณลักษณะสำคัญเป็นการดึงเอาโครงสร้างพื้นฐานที่สำคัญของข้อมูลนั้นออกมา โดยโครงสร้างพื้นฐานที่ว่าจะต้องมีการกำหนดไว้ก่อนว่าจะมีอะไรบ้าง มีการนิยามอย่างไร ตัวอย่างเช่น สำหรับภาษาไทยเราอาจกำหนดว่าตัวอักษรภาษาไทยทั้งหมดประกอบด้วยโครงสร้างพื้นฐานคือ เส้นตรง (แนวตั้ง/นอน) เส้นเอียง หัว (วงกลม) ส่วนโค้ง ส่วนเว้า จุดแตกกิ่ง จุดตัด เป็นต้น เมื่อเราสามารถแยกเอาองค์ประกอบของตัวอักษรแต่ละตัวออกมาได้แล้ว จากนั้นเราก็นำเสนอรูปภาพของตัวอักษรนั้นในรูปแบบของรายการขององค์ประกอบพื้นฐานต่างๆ แทน ซึ่งจะถูกส่งต่อเป็นอินพุตสำหรับขั้นตอนการรู้จำต่อไป

2.5 การทบทวนวรรณกรรม/สารสนเทศ (*Information)* ที่เกี่ยวข้อง

Dong Seong Kim, Ha-nam Nguyen, Thanda Thein และ Jong Sou Park (2005) ได้นำเสนองานวิจัยเรื่อง An Optimized Intrusion Detection System Using PCA and BNN โดยได้นำเสนอการหาค่าที่เหมาะสมสำหรับการตรวจจับการบุกรุกโดยอาศัยการวิเคราะห์องค์ประกอบหลัก (Principal Component Analysis: PCA) และโครงข่ายประสาทเทียมแบบแพร่ย้อนกลับ (Backpropagation Neural Network: BNN) โดยมุ่งเน้นในการแก้ปัญหา 2 ปัญหาด้วยกันคือ การกำหนดจำนวนของ Hidden Layer และการจัดการค่าของน้ำหนัก เพื่อใช้ในการกำหนดรูปแบบของโครงข่ายประสาทเทียม และการประมวลผลข้อมูลที่ตรวจสอบที่มีปริมาณมาก โดยพิจารณาถึงการเพิ่มอัตราการตรวจจับและลดเวลาการประมวลผล โดยนำข้อดีของ Genetic Algorithm (GA) มาใช้ โดยการทำงานของ GA จะทำงานบนการทำงานที่รวมกันระหว่าง PCA และ BNN แต่ผลการทดลองยัง

ออกมาไม่เป็นที่น่าพอใจตามที่คาดหวังไว้ ในส่วนงานในอนาคตได้มีการชี้ถึงประเด็นว่า ถ้ามีการปรับเปลี่ยนตัว PCA และ BPN น่าจะทำให้ได้ผลการทดลองที่ดีขึ้น

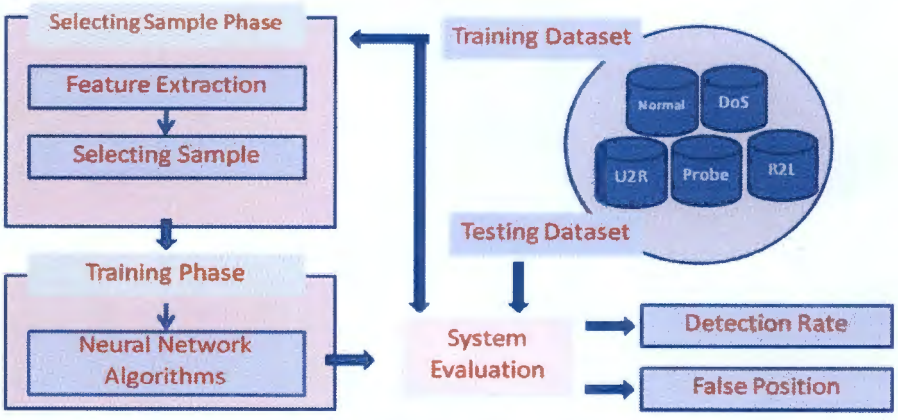
Hai-Hua Gao, Hui-Hua Yang และ Xing-Yu Wang (2005) ได้นำเสนองานวิจัยเรื่อง Kernel PCA Based Network Intrusion Feature Extraction and Detection Using SVM โดยได้นำเสนอวิธีการใหม่ในการตรวจจับการบุกรุกด้วยการประยุกต์ Kernel Principal Component Analysis: KPCA สำหรับการสกัดคุณลักษณะและใช้ Support Vector Machine: SVM ในการแบ่งประเภท โดยทำการเปรียบเทียบผลกับข้อมูลที่ไม่ได้ผ่านการสกัดคุณลักษณะ และการสกัดคุณลักษณะด้วยวิธีการ PCA โดยผลการทดลองชี้ให้เห็นว่าการสกัดคุณลักษณะของข้อมูลสามารถลดขนาดของข้อมูลนำเข้าโดยไม่ทำให้ประสิทธิภาพในการแบ่งกลุ่มลดลง ซึ่งการทดลองด้วย SVM ใช้ข้อมูลเพียง 4 คุณลักษณะหลักที่สกัดได้จาก KPCA ก็ทำให้ได้ผลลัพธ์ที่ดีกว่าชุดข้อมูลที่ไม่ผ่านการสกัด และชุดข้อมูลที่ผ่านการสกัดด้วย PCA

Hai-Hua Gao, Hui-Hua Yang และ Xing-Yu Wang (2005) ได้นำเสนองานวิจัยเรื่อง Principal Component Neural Networks Based Intrusion Feature Extraction and Detection Using SVM โดยได้นำเสนอวิธีการใหม่ในการสกัดคุณลักษณะชุดข้อมูลการบุกรุก โดยการประยุกต์ใช้ Principal Component Neural Network: PCNN และนำผลลัพธ์ที่ได้จากการสกัดคุณลักษณะ มาทำการแบ่งกลุ่มด้วย SVM โดยที่ใช้อัลกอริทึม Adaptive Principal Component Extraction: APEX มาดัดแปลงให้เหมาะสมในการทำงานของ PCNN โดยผลที่ได้จากการทดลองนำมาเปรียบเทียบกับ SVM ที่ไม่ได้ทำการสกัดคุณลักษณะชุดข้อมูล ผลการทดลองแสดงให้เห็นชัดว่า การสกัดคุณลักษณะด้วย PCNN สามารถลดจำนวนมิติของข้อมูลนำเข้า และไม่ทำให้ประสิทธิภาพในการตรวจจับการบุกรุกลดลง

Zhu Xiaorong, Wang Dianchun และ Ye Changguo (2009) ได้นำเสนองานวิจัยเรื่อง A New Feature Extraction Method of Intrusion Detection โดยได้นำเสนอวิธีการนำเอา Kernel Principal Component Analysis: KPCA มาทำการสกัดคุณลักษณะจากการตัวอย่างของข้อมูลการบุกรุกที่จะใช้ฝึกฝน โดยที่วิธีการนี้สกัดคุณลักษณะและลดจำนวนมิติของข้อมูลได้อย่างมีประสิทธิผล โดยได้นำเสนอวิธีการนำ Reduce SVM: RSVM ร่วมกับวิธีการ nonlinear proximal SVM ซึ่งวิธีการที่นำเสนอนี้สามารถลดความซับซ้อนในการคำนวณของ Kernel Matrix ได้ และยังส่งผลให้ความเร็วในการฝึกฝนและผลลัพธ์ของการแบ่งกลุ่มดีขึ้น

บทที่ 3 วิธีดำเนินการวิจัย

การดำเนินการวิจัยมีขอบเขตการวิจัย ดังแสดงในรูปที่ 3-1 เพื่อให้เกิดความเข้าใจในวิธีการดำเนินการวิจัย ผู้วิจัยจะอธิบายการดำเนินการวิจัยเป็นส่วนๆ ดังต่อไปนี้



รูปที่ 3-1 Feature Extraction Framework ซึ่งใช้ในงานวิจัยนี้

3.1 การจัดการชุดข้อมูล

ในงานวิจัยนี้จะใช้ข้อมูล 10% ของชุดข้อมูลทั้งหมดมาทำการวิจัย โดยชุดข้อมูลนี้แบ่งออกได้เป็น 5 ชนิด คือ Normal, Dos, Probe, U2R และ R2L ซึ่งแต่ละชนิดก็จะสามารถแบ่งแยกย่อยออกเป็นชนิดย่อยๆ อีก เมื่อได้ข้อมูลมาแล้วทำการแบ่งข้อมูลออกเป็นสองกลุ่มเพื่อทำแบบทดลอง โดยกลุ่มที่ 1 ใช้ในการฝึกฝน และกลุ่มที่ 2 ใช้ในการทดสอบ ซึ่งวิธีการแบ่งจะใช้วิธีการสุ่มข้อมูลจากข้อมูลทั้งหมด ออกเป็นข้อมูลเพื่อทำแบบทดลอง

3.1.1 การสกัดคุณลักษณะชุดข้อมูล

การสกัดคุณลักษณะชุดข้อมูล จะใช้วิธีการที่ได้ศึกษาจากวิธีการสกัดคุณลักษณะชุดข้อมูล แบบต่าง ๆ มาทำการสกัดคุณลักษณะชุดข้อมูล เพื่อนำไปทดสอบในขั้นตอนการฝึกฝนต่อไป

3.1.2 การรู้จำด้วยโครงข่ายประสาทเทียม

ในขั้นตอนนี้จะทำการเรียนรู้ด้วยโครงข่ายประสาทเทียมแบบแพร่ย้อนกลับ และ Support Vector Machine ที่มีการปรับปรุงการทำงานให้สามารถทำงานได้ดีในการฝึกฝนและการทดสอบ

3.1.3 การประเมินระบบ

นำผลจากการเรียนรู้ที่ได้มาทำการประเมินระบบโดยนำข้อมูลที่ผ่านการเรียนรู้และไม่เคยผ่านการเรียนรู้มาทดสอบระบบ จากนั้นวัดค่าอัตราการตรวจจับ และค่าความผิดพลาด เพื่อประเมินตัวระบบต้นแบบต่อไป เพื่อให้ได้ตัวต้นแบบที่เหมาะสมทั้งการเลือกวิธีการผสมสำหรับการสกัดคุณลักษณะชุดข้อมูลเครือข่าย และตัวแบบการรู้จำเพื่อระบุผู้บุกรุก

บทที่ 4 ผลการทดลอง

ในบทนี้ จะกล่าวถึงผลการทดลองเบื้องต้นที่ได้ศึกษามา โดยผลการทดลองที่นำเสนอจะประกอบด้วย ผลการทดลองจากการสกัดคุณลักษณะข้อมูล และ ขั้นตอนการรู้จำประเภทของผู้บุกรุกโดยใช้โครงข่ายประสาทเทียมแบบแพร่ย้อนกลับ

4.1 การสกัดคุณลักษณะข้อมูล

จากตัวอย่างข้อมูล KDDcup99 ซึ่งเป็นฐานข้อมูลมาตรฐานและนำมาใช้เป็นตัวอย่างในการทดลองในงานวิจัยนี้ โดยข้อมูลชุดนี้มีจำนวนประมาณ 4,900,000 ระเบียน เป็นข้อมูล 41 มิติ โดยในแต่ละชุดข้อมูล (pattern) ของ KDDcup99 นี้ จะแบ่งออกเป็นสามกลุ่มใหญ่ คือ

1. Basic Features คุณลักษณะ (attributes/features) ของข้อมูลในกลุ่มนี้จะบอกได้ว่าเป็นข้อมูลที่ได้มาจาก TCP/IP
2. Traffic Features คุณลักษณะของข้อมูลในกลุ่มนี้จะเป็นค่าของเวลาที่ได้จากการคำนวณ โดยแบ่งออกเป็นสองประเภทย่อย คือ Same host features และ same service features
3. Content Features คุณลักษณะของข้อมูลในกลุ่มนี้จะไว้บอกลักษณะของการบุกรุก เนื่องจาก DoS และ Probing จะมีพฤติกรรมการบุกรุกที่แตกต่างจาก R2L และ U2L เช่น DoS และ Probing จะมีพฤติกรรมในการโจมตีเครื่องแม่ข่ายบางเครื่อง (some hosts) ในช่วงเวลาสั้น ๆ แต่ในขณะที่การโจมตีของ R2L และ U2L จะถูกรวมมากับส่วนของข้อมูล ซึ่งโดยปกติแล้วจะโจมตีมาเพียงครั้งเดียว

```
0,tcp,pop_3,RSTO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,211,6,0.00,0.00,1.00,1.00,0.03,0.07,0.00,255,6,0.02,0.07,0.00,0.00,0.00,0.00,1.00,1.00,neptune.
0,tcp,pop_3,RSTO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,231,16,0.00,0.00,1.00,1.00,0.07,0.06,0.00,255,16,0.06,0.07,0.00,0.00,0.00,0.00,1.00,1.00,neptune.
0,tcp,pop_3,RSTO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,232,5,0.00,0.00,1.00,1.00,0.02,0.06,0.00,255,5,0.02,0.07,0.00,0.00,0.00,0.00,1.00,1.00,neptune.
0,tcp,pop_3,RSTO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,254,15,0.00,0.00,1.00,1.00,0.06,0.07,0.00,255,15,0.06,0.07,0.00,0.00,0.00,0.00,1.00,1.00,neptune.
0,tcp,pop_3,RSTO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,252,6,0.00,0.00,1.00,1.00,0.02,0.07,0.00,255,6,0.02,0.08,0.00,0.00,0.00,0.00,1.00,1.00,neptune.
0,tcp,pop_3,RSTO,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,272,16,0.00,0.00,1.00,1.00,0.06,0.06,0.00,255,16,0.06,0.07,0.00,0.00,0.00,0.00,1.00,1.00,neptune.
0,tcp,pop_3,SH,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1.00,1.00,0.00,0.00,1.00,0.00,0.00,255,1,0.00,1.00,1.00,0.00,1.00,1.00,0.00,0.00,nmap.
0,tcp,pop_3,SH,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1.00,1.00,0.00,0.00,1.00,0.00,0.00,255,1,0.00,1.00,1.00,0.00,1.00,1.00,0.00,0.00,nmap.
5,tcp,pop_3,SF,6,151,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,511,1,0.07,0.00,0.91,0.00,0.00,1.00,0.00,255,1,0.00,1.00,0.00,0.00,0.07,0.00,0.90,0.00,satan.
40339,tcp,pop_3,RSTR,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,2,0.00,0.00,1.00,1.00,1.00,0.00,0.00,255,2,0.01,0.44,0.86,0.00,0.00,0.00,0.86,1.00,portsweep.
```

รูปที่ 4-1 ตัวอย่างข้อมูล Intrusion สำหรับการทดสอบการรู้จำ

เนื่องจากข้อมูล KDDcup99 มีจำนวนมาก ดังนั้น ในงานวิจัยส่วนใหญ่จึงแนะนำให้เลือกข้อมูลเพียงร้อยละ 10 สำหรับเป็นข้อมูลในการสอนและทดสอบประสิทธิภาพของระบบการรู้จำ และจาก

ข้อมูลที่เลือกมาร้อยละ 10 นั้น จะทำการสุ่มมาทำข้อมูลในการสอนประมาณ 13,499 ชุด (Patterns) ทำการสกัดคุณลักษณะโดยใช้ขั้นตอนวิธีการวิเคราะห์องค์ประกอบหลัก (Principal Component Analysis) ซึ่งได้คุณลักษณะเด่นจากข้อมูลทั้งหมด 37 มิติ สำหรับการรู้จำด้วยโครงข่ายประสาทเทียม จำนวน 19 มิติ โดยเราจะพิจารณาจากค่าไอเกนของข้อมูล (จากที่กล่าวไว้ก่อนหน้านี้ว่าข้อมูล KDDcup99 เป็นข้อมูลทั้งหมด 41 มิติ แต่มิติที่เป็น Basic Features และมิติที่เป็นคำตอบจะไม่นำมาพิจารณา ดังนั้น จึงเหลือเพียง 37 มิติ)

4.2 การรู้จำประเภทของผู้บุกรุกเบื้องต้น

ในการทดลองเบื้องต้นสำหรับการรู้จำประเภทของผู้บุกรุกในงานวิจัยนี้ ผู้วิจัยเลือกวิธีการรู้จำแบบมีผู้สอน (Supervised learning) ที่ได้รับความนิยมในการใช้ทดสอบการรู้จำ คือ โครงข่ายประสาทเทียมแบบแพร่ย้อนกลับ และ Support Vector Machine โดยมีข้อมูลนำเข้าสำหรับการรู้จำ 2 ประเภท คือ ข้อมูลทั้งหมด 37 มิติ และ ข้อมูลที่ผ่านขั้นตอนการลดมิติข้อมูล (PCA) 19 มิติ ทำให้เราสามารถแบ่งการทดลองออกเป็น 4 การทดลอง ดังนี้

1. **All+BPNN** (ข้อมูลทั้งหมด 37 มิติ และรู้จำด้วยโครงข่ายประสาทเทียมแบบแพร่ย้อนกลับ)
   - Number of hiddenLayers = (attribs + classes) / 2
   - LearningRate=0.3
   - Momentum=0.2
   - TrainingTime=500
   - Training 100%
2. **All+SVM** (ข้อมูลทั้งหมด 37 มิติ และรู้จำด้วย Support Vector Machine)
   - The polynomial kernel
3. **PCA+BPNN** (ข้อมูลผ่าน PCA 19 มิติ และรู้จำด้วยโครงข่ายประสาทเทียมแบบแพร่ย้อนกลับ)
   - Number of hiddenLayers = (attribs + classes) / 2
   - LearningRate=0.3
   - Momentum=0.2
   - TrainingTime=500
   - Training 100%
4. **PCA+SVM** (ข้อมูลผ่าน PCA 19 มิติ และรู้จำด้วย Support Vector Machine)
   - The polynomial kernel

ตารางที่ 4-1 นำเสนอรายละเอียดของข้อมูลที่ใช้ในการทดลองนี้ โดยข้อมูลที่ใช้นี้ ชื่อ KDDcup99 ทำการสุ่มเลือกมาทั้งหมด 13,499 ชุดทดสอบ โดยข้อมูลมี 37 มิติ โดยรายละเอียดของข้อมูลแต่ละคลาสเป็นดังนี้

คลาสที่ 1 (ประเภทข้อมูล Normal) จำนวนข้อมูลที่สุ่มมาได้ 4,107 ชุดข้อมูล
คลาสที่ 2 (ประเภทผู้บุกรุก DoS) จำนวนข้อมูลที่สุ่มมาได้ 4,107 ชุดข้อมูล
คลาสที่ 3 (ประเภทผู้บุกรุก Probe) จำนวนข้อมูลที่สุ่มมาได้ 4,107 ชุดข้อมูล
คลาสที่ 4 (ประเภทผู้บุกรุก R2L) จำนวนข้อมูลทั้งหมด 1,126 ชุดข้อมูล
คลาสที่ 5 (ประเภทผู้บุกรุก U2L) จำนวนข้อมูลทั้งหมด 52 ชุดข้อมูล

ตารางที่ 4-1 รายละเอียดข้อมูลที่ใช้ในการทดลอง

ประเภทข้อมูล	จำนวนข้อมูล/มิติ (แอทริบิวต์)	จำนวนข้อมูล (Patterns) ในแต่ละคลาส
KDDcup99	13499/37	4107/4107/4107/1126/52

ตารางที่ 4-2 นำเสนอค่าสถิติที่ได้จากการทำการทดลองประกอบด้วย ค่าร้อยละของความถูกต้อง (Accuracy), ค่า F และ ค่า AUC พบว่า ในการทดลองเบื้องต้นในรายงานการวิจัยนี้ ชุดข้อมูลทั้งหมด 37 มิติ ให้ผลการทดลองที่สูงกว่าผลการทดลองที่ได้จากการลดมิติข้อมูลด้วยเทคนิค PCA

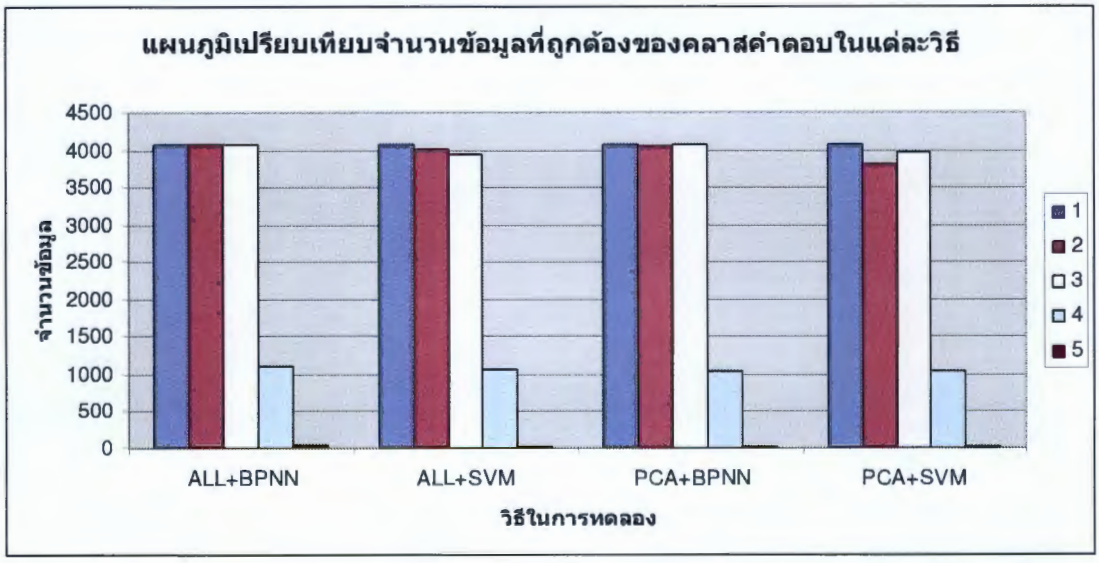
ตารางที่ 4-2 ค่า Accuracy จากการประมวลผล

Learning Method	ข้อมูลทั้งหมด			ข้อมูลที่ผ่านขั้นตอน PCA		
	Accuracy	F	AUC	Accuracy	F	AUC
BPNN	99.17	0.992	0.999	98.45	0.984	0.996
SVM	97.15	0.971	0.988	95.63	0.956	0.983

ตารางที่ 4-3 และ รูปที่ 4-2 ได้แสดงจำนวนชุดข้อมูลที่วิธีการเรียนรู้แต่ละวิธีทำการแบ่งประเภทได้อย่างถูกต้อง ซึ่งพบว่าในการทดลองเบื้องต้นนี้ โครงข่ายประสาทเทียมแบบแพร่ย้อนกลับให้ผลการทดลองที่ดีกว่า Support Vector Machine

ตารางที่ 4-3 จำนวนข้อมูลที่แบ่งประเภทได้ถูกต้องของคลาสคำตอบในแต่ละวิธี

Learning Method	คลาส				
	1 (4107)	2 (4107)	3 (4107)	4 (1126)	5 (52)
ALL+BPNN	4087	4073	4082	1112	34
ALL+SVM	4075	4002	3953	1057	28
PCA+BPNN	4072	4060	4080	1050	28
PCA+SVM	4075	3820	3957	1032	26



รูปที่ 4-2 แผนภูมิเปรียบเทียบจำนวนข้อมูลที่ถูกต้องของคลาสคำตอบในแต่ละวิธี

บทที่ 5 สรุปผลการทดลอง

5.1 สรุปผลการทดลอง

ในงานวิจัยนี้ (ปีงบประมาณ 2554) ได้นำเสนอผลการทดลองเบื้องต้นในส่วนขั้นตอนการสกัดคุณลักษณะเด่นของข้อมูลด้วยเทคนิค Principal Component Analysis และผลการทดลองการรู้จำด้วยเทคนิคโครงข่ายประสาทเทียมแบบแพร่ย้อนกลับ และ Support Vector Machine ผลที่ได้จากการทดลองแสดงให้เห็นว่า ขั้นตอนวิธีที่นำเสนอในขั้นตอนที่หนึ่ง เมื่อลดข้อมูลลงแล้วทำให้ผลการทดลองในส่วนการประมวลผลเพื่อการรู้จำในขั้นตอนที่สองมีประสิทธิภาพที่ต่ำลง ดังนั้น เราจึงสามารถสรุปได้ว่า การสกัดคุณลักษณะด้วย เทคนิค Principal Component Analysis ยังไม่เหมาะสมสำหรับข้อมูล Intrusion ในระบบเครือข่าย ทั้งนี้อาจเนื่องจากการกำหนดค่าไอเกนสำหรับการเลือกลดมิติข้อมูลก็ได้ ซึ่งเป็นปัญหาการวิจัยที่ต้องศึกษาต่อไป และนอกจากนี้เรายังสามารถเพิ่มประสิทธิภาพของการรู้จำได้โดยใช้เทคนิคการรู้จำแบบอื่น ๆ หรืออาจจะเป็นการรู้จำแบบผสมก็ได้

5.2 งานที่ต้องทำต่อไปในปีงบประมาณ พ.ศ. *2555*

1. ศึกษาและพัฒนาขั้นตอนวิธีสำหรับการสกัดคุณลักษณะเด่นสำหรับข้อมูล Intrusion บนระบบเครือข่าย เพื่อเพิ่มความเร็วในการรู้จำ
2. ศึกษาและพัฒนาขั้นตอนวิธีเพื่อการรู้จำแบบอื่น ๆ รวมทั้งการเรียนรู้แบบผสมสำหรับตรวจจับ Intrusion Data Packages ให้มีประสิทธิภาพสูงขึ้น
3. ตีพิมพ์ผลงานวิจัยในประชุมวิชาการระดับนานาชาติ และวารสารวิจัย

บรรณานุกรม

KDD'99 datasets, The UCI KDD Archive, http://kdd.ics.uci.edu/databases/kddcup99/, Irvine, CA, USA, 1999.

Hai-Hua Goa, Hui-Hua Yang, and Xing-Yu Wang (2005), "Kernel PCA Based Network Intrusion Feature Extraction and Detection Using SVM", *Proceedings of ICNC 2005, LNCS 3611*, pp. 89-94.

Hai-Hua Goa, Hui-Hua Yang, and Xing-Yu Wang (2005), "Principal Component Neural Networks Based Intrusion Feature Extraction and Detection Using SVM", *Proceedings of ICNC 2005, LNCS 3611*, pp. 21-27.

Dong Seong Kim, Ha-Nam Nguyen, T. Thein, and Jong Sou Park (2005), "An Optimized Intrusion Detection System Using PCA and BNN", *Proceedings of The 6th Asia-Pacific Sym. on Information and Telecommunication Technologies, IEICE Communications Society*, pp. 356-359.

Zhu Xiaorong, Wang Dianchun, Ye Changguo (2009), "A New Feature Extraction Method of Intrusion Detection," *2009 First International Workshop on Education Technology and Computer Science vol. 2*, pp.504-507.