SWU Engineering Journal (2010) 5(2), 38-42
วารสารวิศวกรรมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ
ปีที่ 5 ฉบับที่ 2 เดือนกรกฎาคม - ธันวาคม พ.ศ.2553

การตรวจจับไวรัสข้อความสื่อประสมโดยใช้เทคนิคการทำเหมืองข้อมูล

Detecting MMS Virus Using Data Mining Technique

อัณศยา เกิดคล้าย [1] และนำคุณ ศรีสนิท[2]
[1]สาขาการจัดการทางวิศวกรรมเทคโนโลยีสารสนเทศ คณะวิศวกรรมศาสตร์
[2] ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ
E-mail: namkhun@swu.ac.th

บทคัดย่อ

งานวิจัยนี้ได้นำเทคนิคกฎการค้นหาความสัมพันธ์ ซึ่งเป็นเทคนิคหนึ่งในเทคนิคเหมืองข้อมูล มาประยุกต์ใช้ออกแบบโปรแกรมสำหรับใช้ในการตรวจจับข้อความมัลติมีเดียที่มีไวรัสชนิด CommWarrior ผู้วิจัยได้ทำการทดลองศึกษาโปรแกรม โดยผลของการศึกษาโปรแกรมพบว่าโปรแกรมที่สร้างขึ้นสามารถตรวจจับข้อความมัลติมีเดียที่มีไวรัสได้ ผลของการใช้เทคนิคเหมืองข้อมูลพบว่าโปรแกรมที่สร้างขึ้นสามารถตรวจจับข้อความมัลติมีเดียที่มีไวรัสได้โดยมีความถูกต้องเทียบเท่า Viral Marketing Tool ซึ่งเป็นโปรแกรมเชิงพาณิชย์

คำสำคัญ: กฎการค้นหาความสัมพันธ์ ไวรัสข้อความสื่อประสม การทำเหมืองข้อมูล ไวรัส CommWarrior การตรวจจับไวรัส

ABSTRACT

This research applies one of data mining techniques called ‘association rule discovery’. The objective for this research is to detect MMS containing CommWarrior-type virus. Researchers practically examine the program and achieve the results that the created program is able to detect virus-contained MMS. The result from applying data mining technique is apparently shown that the program is able to detect virus-contained MMS at the same accuracy as Viral Marketing Tool, commercially available program.

Keywords: Association rule, MMS Virus, Data mining, CommWarrior Virus, Virus Detection

1. บทนำ

ปัญหาที่ผู้ให้บริการโครงข่ายโทรศัพท์เคลื่อนที่กำลังประสบอยู่คือ “ไวรัสโทรศัพท์เคลื่อนที่” แม้ในช่วงแรกจะติดต่อผ่านทาง Bluetooth ในโทรศัพท์เคลื่อนที่ระบบปฏิบัติการ Symbian และล่าสุดไวรัสดังกล่าวยังสามารถติดต่อผ่านทางข้อความสื่อประสมได้อีกด้วย โดยไวรัสนี้มีชื่อเรียกว่า CommWarrior[1] ซึ่งก็คือ ไวรัสประเภท Worm ที่ทำงานอยู่บนโทรศัพท์เคลื่อนที่ Symbian Series 60 ซึ่งสามารถแพร่กระจายผ่านทาง Bluetooth และข้อความสื่อประสม เมื่อไวรัสนี้เข้าไปฝังตัวอยู่ในโทรศัพท์เคลื่อนที่แล้ว ไวรัสจะเริ่มทำการค้นหาโทรศัพท์เคลื่อนที่เครื่องอื่นที่เปิด Bluetooth เอาไว้แล้วทำการส่งไฟล์ไวรัสในรูปแบบของ SIS ไปยังโทรศัพท์เคลื่อนที่เครื่องอื่น ซึ่งชื่อไฟล์ที่ส่งจะมาจากการสุ่มขึ้นของไวรัส ทำให้ผู้รับไม่แน่ใจว่าเป็นไฟล์ไวรัสหรือไม่ นอกเหนือจากนี้ไวรัสยังสามารถแพร่กระจาย

ด้วยวิธีส่งข้อความสื่อประสมไปยังหมายเลขอื่นที่ได้บันทึกในสมุดโทรศัพท์อีกด้วย โดยที่ผู้ใช้โทรศัพท์เคลื่อนที่จะไม่รู้ตัวว่าเครื่องของตนเองกำลังทำการส่งข้อความสื่อประสมไปยังโทรศัพท์เคลื่อนที่เครื่องอื่นอยู่เรื่อยๆ ซึ่งทำให้ต้องเสียค่าบริการส่งข้อความสื่อประสมเพิ่มขึ้นมากกว่าปกติอย่างมาก ซึ่งปัจจุบันมีผู้ใช้มือถือสมาร์ทโฟนประมาณ 10% ที่ตกเป็นเหยื่อไวรัส

เนื่องด้วยจำนวนผู้ใช้สมาร์ทโฟนเพิ่มขึ้นอย่างรวดเร็ว จึงมีผู้ใช้ที่ตกเป็นเหยื่อไวรัสโทรศัพท์เคลื่อนที่จำนวนมาก รวมทั้งยังสร้างปัญหาให้แก่ผู้ให้บริการ ยกตัวอย่างเช่น โทรศัพท์เคลื่อนที่ที่ติดไวรัสจะส่งข้อความสื่อประสมไปให้ผู้อื่น โดยที่ผู้ใช้บริการไม่รู้ตัวว่ามีการส่งข้อความสื่อประสมออกไป ทำให้ต้องเสียค่าบริการ ทั้งที่ตนเองไม่ได้ใช้งาน ในด้านของผู้ให้บริการจะได้รับการร้องเรียนปัญหาจากผู้ใช้บริการเป็นจำนวนมาก โดยไม่สามารถแก้ปัญหานี้ได้ เนื่องจากผู้ให้บริการสามารถรู้แต่เพียงว่าผู้ใช้บริการมีพฤติกรรมการส่งข้อความสื่อประสมที่ผิดปกติเท่านั้น และยังเพิ่มปริมาณทราฟฟิกให้กับเครือข่ายโดยไม่จำเป็น อีกทั้งยังมีต้นทุนที่ต้องจ่ายให้กับบริษัทที่เก็บค่าใบอนุญาตของทราฟฟิกที่วิ่งผ่านระบบบริการรับส่งข้อความสื่อประสม (MMSC System) โดยไร้ประโยชน์ เพราะผู้ใช้บริการส่วนใหญ่ที่ร้องเรียนปัญหานี้จะไม่ยอมชำระค่าบริการ หรือในบางรายอาจถึงขั้นยกเลิกการใช้บริการทั้งหมดกับผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่เจ้านั้นๆ ซึ่งการสูญเสียผู้ใช้บริการไปนั้น ถือเป็นเรื่องที่ร้ายแรงมากสำหรับผู้ให้บริการ และสิ่งที่ต้องสูญเสียไปโดยไร้ประโยชน์อีกอย่างก็คือทรัพยากรบุคคลที่ทำหน้าที่รับปัญหาร้องเรียนจากผู้ใช้บริการ

ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่รายหนึ่ง พบปัญหาไวรัสโทรศัพท์เคลื่อนที่ โดยการใช้ Viral Marketing Tool [2] ซึ่งเป็นเครื่องมือที่บริษัทเอกชนผลิตขึ้นเพื่อขายให้กับผู้ให้บริการที่ต้องการจะนำมาใช้วิเคราะห์ทราฟฟิกข้อความสื่อประสม โดยวัตถุประสงค์ของเครื่องมือนี้คือ เพื่อหาเนื้อหาข้อความที่มีการส่งกันมากๆ และผู้ใช้งานที่มีการส่งข้อความสื่อประสมมากๆ ซึ่งผลลัพท์ของการทดลองใช้วิเคราะห์ทราฟฟิกข้อความสื่อประสมพบว่าเนื้อหาข้อความที่มีการส่งต่อกันมากที่สุดเป็นอันดับ 1-3 คือ ไวรัส CommWarrior จากผลการใช้งาน Viral Marketing Tool และผลกระทบของปัญหาไวรัสที่ผู้วิจัยได้กล่าวไปข้างต้น ผู้วิจัยจึงสนใจที่จะออกแบบโปรแกรมไว้ใช้ตรวจจับข้อความสื่อประสมที่มีไวรัสชนิด CommWarrior ที่มีประสิทธิภาพทัดเทียมกับ Viral Marketing Tool โดยที่ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ไม่ต้องเสียค่าใช้จ่ายในการเก็บรวบรวม ทราฟฟิก เพราะข้อมูลที่ใช้ในการวิเคราะห์เป็นข้อมูลที่มีการเก็บรวบรวมไว้อยู่แล้ว และเป็นข้อมูลที่มีรายละเอียดเพียงพอ เมื่อผู้วิจัยพิจารณาจากคุณสมบัติของไวรัสชนิดนี้ ซึ่งต่างจาก Viral Marketing Tool ที่สามารถวิเคราะห์ข้อมูลได้ถึงเนื้อหาภายในของข้อความสื่อประสม จึงส่งผลทำให้อัตราการตรวจจับไวรัสมีความถูกต้องร้อยละ 100 แต่ข้อมูลที่ Viral Marketing Tool ต้องเก็บเพื่อนำไปเข้ากระบวนการวิเคราะห์นั้น ทำให้อุปกรณ์ที่ไปเชื่อมต่อเพื่อทำการรวบรวมทราฟฟิก ต้องมีขนาดความจุที่ใหญ่เพียงพอกับการเก็บรวบรวมทราฟฟิกในแต่ละวัน ซึ่งผู้ให้บริการต้องเสียค่าใช้จ่ายเพิ่มขึ้น อีกทั้งยังต้องสูญเสียเวลาในการดึงและอ่านข้อมูลขนาดใหญ่ เพื่อนำมาใช้ในการวิเคราะห์

ในงานวิจัยนี้ยังสนใจการนำคลังข้อมูลและเทคนิคการทำเหมืองข้อมูลมาใช้ในการออกแบบโปรแกรม โดยเหตุผลของการเลือกใช้เทคนิคนี้ เนื่องจากข้อมูลของระบบบริการรับส่งข้อความสื่อประสมที่เก็บรวบรวมในแต่ละวันมีขนาดใหญ่ การทำเหมืองข้อมูลจึงเป็นวิธีที่เหมาะสมในการค้นหา วิเคราะห์ หรือสร้างองค์ความรู้ใหม่จากข้อมูลที่มีขนาดใหญ่ ที่จะช่วยนำข้อมูลออกมาใช้งานให้เกิดประโยชน์สูงสุดได้

2. วรรณกรรมที่เกี่ยวข้อง

จากหลักทฤษฎีทั่วไปที่มีการตีพิมพ์เผยแพร่ทางหนังสือและทางอินเตอร์เน็ต รวมทั้งจากงานวิจัยที่เคยมีผู้นำเสนอมาแล้ว ผู้วิจัยพบว่าวิธีการทำเหมืองข้อมูลมีความเหมาะสมกับข้อมูลในระบบบริการรับส่งข้อความสื่อประสม เนื่องจากข้อมูลของระบบบริการ

รับส่งข้อความสื่อประสมที่เก็บรวบรวมมีขนาดใหญ่ คือ ระดับหลายล้านรายการต่อวัน ซึ่งเทคนิคเหมืองข้อมูลเป็นเทคนิคที่ใช้จัดการกับข้อมูลขนาดใหญ่โดยเฉพาะอยู่แล้ว และงานวิจัยหลายงานที่เคยนำเสนอ มีลักษณะของข้อมูลคล้ายกับข้อมูลในระบบบริการรับส่งข้อความสื่อประสม ก็มีการนำเทคนิคเหมืองข้อมูลไปประยุกต์ใช้ และได้ผลลัพธ์ที่มีประสิทธิภาพ ตัวอย่างเช่น การเพิ่มอัตราการพบในระบบพร็อกซี่โดยใช้เทคนิคเหมืองข้อมูล [3] การทำนายปริมาณการจราจรในเครือข่ายโดยใช้เทคนิคเหมืองข้อมูล [4] และพัฒนาระบบตรวจจับการบุกรุก [5] ผู้วิจัยจึงได้เลือกนำเทคนิคการทำเหมืองข้อมูล กฎการวิเคราะห์ความสัมพันธ์ (Association Rule) แบบวิธีค้นหารูปแบบ (Frequent Pattern Mining) มาใช้ค้นหาความสัมพันธ์ระหว่างข้อมูลที่รวบรวม โดยใช้ค่าสนับสนุน (Support) และค่าความเชื่อมั่น (Confidence) เป็นเกณฑ์ในการตัดสินว่ารูปแบบใดสมควรกำหนดเป็นกฎ [6] แม้ว่างานวิจัยทั้งหมดที่ผู้วิจัยได้ศึกษาจะไม่ได้ประยุกต์ใช้บนระบบระบบบริการรับส่งข้อความสื่อประสม แต่ผู้วิจัยยังสามารถนำมาเป็นแนวทางในการออกแบบและพัฒนาโปรแกรมได้ ส่วน Viral Marketing Tool นั้นมีความสามารถในการตรวจจับข้อความสื่อประสมที่มีไวรัสได้ โดยมีความถูกต้อง ร้อยละ 100 ซึ่งมีข้อด้อยตรงที่ผู้ให้บริการต้องเสียค่าใช้จ่ายเพิ่มนอกเหนือจากค่าใบอนุญาตการใช้ Viral Marketing Tool เพราะต้องจัดหาอุปกรณ์สำหรับรวบรวมทราฟฟิกที่มีขนาดความจุใหญ่เพียงพอกับทราฟฟิกในแต่ละวัน เพื่อนำไปใช้เป็นข้อมูลเริ่มต้นของ Viral Marketing Tool ซึ่งในอนาคตการใช้งานข้อความสื่อประสมมีแนวโน้มจะเพิ่มขึ้นอย่างก้าวกระโดด ผู้ให้บริการจึงอาจต้องเสียค่าใช้จ่ายในส่วนนี้เพิ่มอยู่เรื่อยๆ

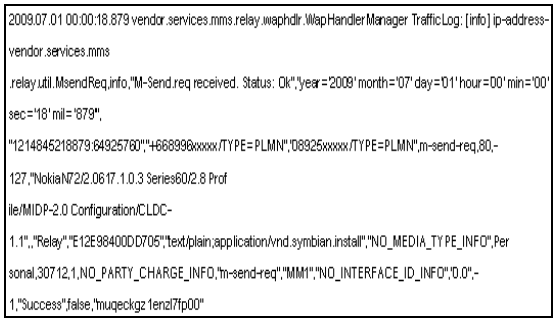
3. วิธีการดำเนินการวิจัย

3.1 เตรียมข้อมูล

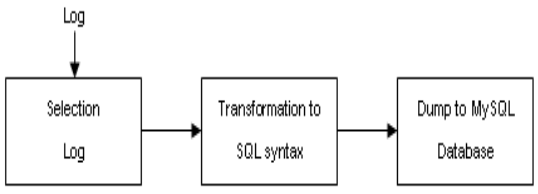
เตรียมข้อมูลเพื่อใช้สำหรับออกแบบและพัฒนาโปรแกรม โดยแปลงข้อมูลจาก Log ดังภาพที่ 1 และโหลดลงคลังข้อมูลที่ใช้ฐานข้อมูลมายเอสคิวแอล (MySQL) ด้วยโปรแกรมที่มีขั้นตอนการทำงานดังภาพที่ 2 สำหรับข้อมูลที่โหลดลงคลังข้อมูลจะประกอบด้วยข้อมูล 9 ข้อมูล ดังภาพที่ 3 ซึ่งแบ่งการจัดเก็บข้อมูล

3.1.1 ชุดฝึกสอน (Training set) คือข้อมูลการส่งข้อความสื่อประสมของผู้ใช้งานภายในระบบบริการรับส่งข้อความสื่อประสม จำนวน 4 Server ระหว่างวันที่ 1-30 มิถุนายน 2552 ที่ใช้ในการสร้างโปรแกรม

3.1.2 ชุดทดสอบ (Test set) คือข้อมูลการส่งข้อความสื่อประสมของผู้ใช้งานภายในระบบบริการรับส่งข้อความสื่อประสม จำนวน 4 Servers ระหว่างวันที่ 1-31 กรกฎาคม 2552 ที่ใช้ในการตรวจสอบความถูกต้องของโปรแกรมที่สร้างขึ้นคัดเลือกข้อมูลเพื่อนำไปสร้างโมเดลของเทคนิคเหมืองข้อมูล โดยผู้วิจัยเลือกเฉพาะข้อมูลที่มีความสัมพันธ์กับคุณสมบัติของไวรัสชนิด CommWarrior และทำการแปลงข้อมูลที่อยู่ในฐานข้อมูลให้เป็นหมวดหมู่ เพื่อเอื้อต่อขั้นตอนในการประเมินรูปแบบของการทำเหมืองข้อมูลที่จะไม่เกิดการกระจายรูปแบบ


2009.07.01 00:00:18.879 vendor.services.mms.relay.waphdlr.WapHandlerManager TrafficLog: [info] ip-address-vendor.services.mms
.relay.util.MsendReq,info,"M-Send.req received. Status: Ok","year='2009' month='07' day='01' hour='00' min='00' sec='18' mil='879'",
"12148452188 79:64925760","+668996xxxxx/TYPE=PLMN","08925xxxxx/TYPE=PLMN",m-send-req,80,-127,"NokiaN72/2.0617.1.0.3 Series60/2.8 Profile/MIDP-2.0 Configuration/CLDC-1.1",,"Relay","E12E98400DD705","text/plain;application/vnd.symbian.install","NO_MEDIA_TYPE_INFO",Personal,30712,1,NO_PARTY_CHARGE_INFO,"m-send-req","MM1","NO_INTERFACE_ID_INFO","0.0",-1,"Success",false,"muqeckgz1enzl7fp00"

รูปที่ 1 ตัวอย่าง Log ของระบบบริการรับส่งข้อความสื่อประสม



รูปที่ 2 กระบวนการโหลดข้อมูล Log สู่ฐานข้อมูล

Field	Type	Null	Key	Default	Extra
year	int(11)	YES		NULL	
month	int(11)	YES		NULL	
day	int(11)	YES		NULL	
hour	int(11)	YES		NULL	
min	int(11)	YES		NULL	
sec	int(11)	YES		NULL	
mil	int(11)	YES		NULL	
sender	text	YES		NULL	
recipient	text	YES		NULL	
phoneModel	text	YES		NULL	
contentType	text	YES		NULL	
contentSize	int(11)	YES		NULL	
triggerPoint	varchar(20)	YES		NULL	
status	text	YES		NULL	
messageID	varchar(25)	YES		NULL	

รูปที่ 3 ข้อมูลที่จัดเก็บลงคลังข้อมูล

3.2 ออกแบบโปรแกรม

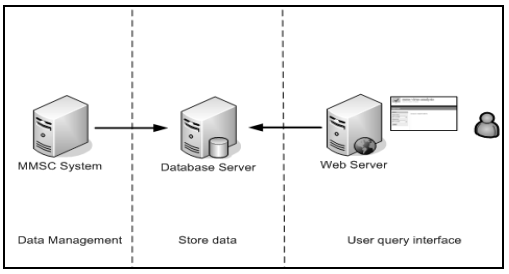
ออกแบบโปรแกรมเพื่อใช้ตรวจจับข้อความสื่อประสมที่มีไวรัสโดยใช้เทคนิคเหมืองข้อมูล กฎการวิเคราะห์ความสัมพันธ์ (Association Rule) แบบวิธีค้นหารูปแบบ (Frequent Pattern Mining) โดยใช้ข้อมูลชุดฝึกสอน และเลือกกฎความสัมพันธ์โดยพิจารณาตามหลักเกณฑ์การจำแนกดังนี้

3.2.1 ผลลัพธ์ของเงื่อนไขต้องมีค่าสนับสนุน (Support) มากกว่าหรือเท่ากับค่าน้อยที่สุดของค่าสนับสนุน (Minimum Support) ที่กำหนดไว้ โดยกำหนดไว้ที่ 1% เนื่องจากจำนวนของไวรัสที่สนใจในงานวิจัยนี้มีอยู่ประมาณ 10% ของข้อมูลทั้งหมดเท่านั้น

3.2.2 ถ้าเงื่อนไขใดมีค่าความเชื่อมั่น (Confidence) มากกว่า 80% ขึ้นไป จะถือว่าเงื่อนไขนั้นเป็นกฎความสัมพันธ์

3.3 พัฒนาโปรแกรม

พัฒนาโปรแกรมเพื่อใช้ตรวจจับข้อความสื่อประสมที่มีไวรัส โดยผู้วิจัยนำกฎความสัมพันธ์ที่ผ่านการจำแนกกฎความสัมพันธ์ทั้ง 2 กฎ ของเงื่อนไขประเภทของเนื้อหาที่ส่งมากับข้อความสื่อประสม มาเป็นกระบวนการทำงานหลัก โดยสถาปัตยกรรมระบบจะเป็นลักษณะเว็บแอพพลิเคชั่น (Web application) ซึ่งพัฒนาขึ้นด้วย ภาษา PHP จาวาสคริปต์ (JavaScript) ฐานข้อมูลมายเอสคิวแอล (MySQL) และอะแพชี เว็บเซิร์ฟเวอร์ (Apache Web Server) ดังรูปที่ 4



รูปที่ 4 สถาปัตยกรรมระบบ

3.4 ทดสอบความถูกต้องของโปรแกรม

ทดสอบความถูกต้องของโปรแกรมที่พัฒนาขึ้น โดยใช้ข้อมูลชุดทดสอบ

รูปที่ 5 แผนผังขั้นตอนการทดสอบโมเดล

3.5 ประเมินผลการตรวจจับข้อความสื่อประสมที่มีไวรัส

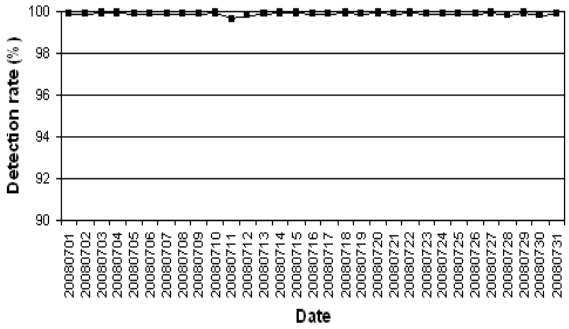
โดยความสำเร็จของงานวิจัยวัดผลได้จาก ความถูกต้องของโปรแกรม คือสามารถตรวจจับข้อความสื่อประสมที่มีไวรัสได้ผลสอดคล้องกับการตรวจจับโดยใช้ Viral Marketing Tool

3.5.1ตัวชี้วัดและสถิติที่ใช้ในการวิจัย

ตัวชี้วัดที่ใช้ในการวิจัย คืออัตราการตรวจจับ (Detection Rate) ระหว่างโปรแกรมที่พัฒนาขึ้น กับ Viral Marketing Tool ภายใต้เงื่อนไขเดียวกัน ซึ่งอัตราการตรวจจับ คืออัตราส่วนระหว่างจำนวนของการตรวจจับข้อความสื่อประสมที่มีไวรัสได้ถูกต้อง กับจำนวนของข้อความสื่อประสมที่มีไวรัสทั้งหมด สถิติที่ใช้ในการวิจัย คือจำนวนของข้อความสื่อประสมที่มีไวรัส เปรียบเทียบกันระหว่างการใช้โปรแกรมที่ออกแบบขึ้นตรวจจับ กับการตรวจจับโดยใช้ Viral Marketing Tool โดยให้การตรวจจับนั้นอยู่ภายใต้เงื่อนไขเดียวกัน

4. ผลการดำเนินงาน

ผลการตรวจจับข้อความสื่อประสมที่มีไวรัสจากข้อมูลการส่งข้อความสื่อประสมของผู้ใช้งานภายในระบบบริการรับส่งข้อความสื่อประสมระหว่างวันที่ 1-31 กรกฎาคม 2552 จำนวน 5,445,348 รายการ ดังรูปที่ 6 และตารางที่ 1



รูปที่ 6 อัตราการตรวจจับข้อความสื่อประสมที่มีไวรัสโดยโปรแกรมที่พัฒนาขึ้นกับข้อมูลชุดทดสอบเป็นรายวัน

ตารางที่ 1 แสดงผลเปรียบเทียบประสิทธิภาพเฉลี่ย

Analyzed by	Virus	Detection rate	SD
Viral Marketing Tool	543,273	100%	0
Program	542,759	99.89%	0.05

จากตารางที่ 1 พบว่าโปรแกรมที่พัฒนาขึ้นสามารถตรวจจับข้อความสื่อประสมที่มีไวรัสได้ 542,759 ข้อความ จากข้อความสื่อประสมที่มีไวรัสทั้งหมด 543,273 ข้อความ นั่นคือยังไม่สามารถตรวจจับได้อีกเฉลี่ย 0.11% ซึ่งคิดเป็น 514 ข้อความ

5. บทสรุป

การออกแบบและสร้างโปรแกรมสำหรับใช้ในการตรวจจับข้อความสื่อประสมที่มีไวรัสในงานวิจัยนี้ ได้นำเสนอการนำเทคนิคการทำเหมืองข้อมูลเข้ามาประยุกต์ใช้ โดยพบว่าโปรแกรมสามารถตรวจจับข้อความสื่อประสมที่มีไวรัสได้ โดยมีความถูกต้องร้อยละ 99.89 หรือเทียบเท่า Viral Marketing Tool ซึ่งเป็นโปรแกรมเชิงพาณิชย์ที่สามารถตรวจจับได้ถูกต้องร้อยละ 100 ทั้งนี้เนื่องจากข้อมูลการส่งข้อความสื่อประสมในระบบบริการรับส่งข้อความสื่อประสมของโปรแกรมที่พัฒนาขึ้นใช้ในการออกแบบ และพัฒนาเป็นข้อมูลที่มีความละเอียดเพียงพอสำหรับการนำไปใช้วิเคราะห์ตรวจจับไวรัส จึงไม่จำเป็นต้องสามารถวิเคราะห์ข้อมูลได้ถึงเนื้อหาภายในของข้อความสื่อประสมเหมือนเช่นการตรวจจับโดยใช้ Viral Marketing Tool ก็สามารถมีประสิทธิภาพทัดเทียมกันได้

6. เอกสารอ้างอิง

[1] Kaspersky Lab ZAO, Worm.*SymbOS.Comwar.a*, Retrieved February 18, 2009, fromhttp://www.securelist.com/en/descriptions/old75541

[2] Mobixell, *Ad-It Ad Serving*, Retrieved February 20, 2009, from http://www.mobixell.com/ad-serving

[3] พิจิตรา จอมศรี และ ปานใจ ธารทัศนวงศ์, “การเพิ่มอัตราการพบในระบบพร๊อกซี่โดยใช้เทคนิคเหมืองข้อมูล,” *ในการประชุมทางวิชาการระดับชาติด้านเทคโนโลยีสารสนเทศ* ครั้งที่ 1 (NCIT2006) 2-3 พฤศจิกายน 2549 หน้า 306-311

[4] ดุลย์วิทย์ ปรางชุมพล และ ปานใจ ธารทัศนวงศ์, “การทำนายปริมาณการจราจรในเครือข่ายโดยใช้เทคนิคเหมืองข้อมูล,” *ในการประชุมทางวิชาการระดับชาติด้านเทคโนโลยีสารสนเทศ* ครั้งที่ 1 (NCIT2006) 2-3 พฤศจิกายน 2549 หน้า 313-317.

[5] Yi H. and Brajendra P., “A Data Mining Approach for Database Intrusion Detection,” *Proceeding of ACM Applies Computing*, pp. 711-716, 2004.

[6] Han Jiawei and Micheline Kamber, *Data Mining Concepts and Techniques*, Morgan Kaufman: USA, 2006.