ใบรับรองวิทยานิพนธ์

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์

วิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์)

ปริญญา

วิศวกรรมคอมพิวเตอร์ วิศวกรรมคอมพิวเตอร์

สาขา **ภาควิชา**

เรื่อง ระบบตรวจจับและตอบโต้การติดตั้งแอกเซสพอยต์โดยไม่ได้รับอนุญาต

Rogue Access Point Detection and Counterattack System

นามผู้วิจัย นายทรงฤทธิ์ ศรีลาศักดิ์

ได้พิจารณาเห็นชอบโดย

อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(รองศาสตราจารย์อนันต์ ผลเพิ่ม, Ph.D.)

อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

(อาจารย์กิตติ วงศ์ถาวราวัฒน์, Ph.D.)

หัวหน้าภาควิชา

(ผู้ช่วยศาสตราจารย์เขมะฑัต วิภาตะวนิช, Ph.D.)

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์รับรองแล้ว

(รองศาสตราจารย์กัญจนา ธีระกุล, D.Agr.)

คณบดีบัณฑิตวิทยาลัย

วันที่ ..... **เดือน** ..... **พ.ศ.** .....

วิทยานิพนธ์

เรื่อง

ระบบตรวจจับและตอบโต้การติดตั้งแอกเซสพอยต์โดยไม่ได้รับอนุญาต

Rogue Access Point Detection and Counterattack System

โดย

นายทรงฤทธิ์ ศรีลาศักดิ์

เสนอ

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์

เพื่อความสมบูรณ์แห่งปริญญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์)

พ.ศ. 2552

ทรงฤทธิ์ ศรีลาศักดิ์ 2552: ระบบตรวจจับและตอบโต้การติดตั้งแอกเซสพอยต์โดยไม่ได้รับอนุญาต ปริญญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์) สาขาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก: รองศาสตราจารย์อนันต์ ผลเพิ่ม, Ph.D. 85 หน้า

โดยทั่วไปพนักงานในองค์กรสามารถเข้าถึงเครื่องแม่ข่ายภายในองค์กรผ่านทางเครือข่ายแลนมีสาย ซึ่งไม่ได้รับความสะดวกเท่ากับการใช้งานผ่านเครือข่ายแลนไร้สาย ได้ไม่สะดวกนัก เนื่องจากหน่วยงานจะมีการกำหนดนโยบายด้านความปลอดภัยซึ่งเป็นสาเหตุหนึ่งที่ทำให้พนักงานมีการนำแอกเซสพอยต์มาติดตั้งในองค์กรโดยไม่ได้แจ้งให้แก่ผู้ดูแลเครือข่ายทราบ ซึ่งส่วนใหญ่ไม่ได้มีการตั้งค่าที่มีความปลอดภัยที่เหมาะสม และ ส่งผลให้เป็นช่องทางให้เกิดการบุกรุก หรือ ดักจับข้อมูลภายในองค์กรได้ นอกจากนี้ยังอาจมีการติดตั้งแอกเซสพอยต์จากผู้บุกรุกภายนอกโดยไม่เชื่อมต่อกับเครือข่ายองค์กร

งานวิจัยนี้เสนอระบบที่มีความสามารถแก้ปัญหาที่เกิดจากแอกเซสพอยต์ที่ติดตั้งโดยไม่ได้รับอนุญาตด้วยการรายการตรวจจับ และ ระงับการเชื่อมต่อแบบอัตโนมัติ ระบบนี้ได้รับการออกแบบให้ทำงานแบบรวมศูนย์ โดยใช้แอกเซสพอยต์ขององค์กรที่มีอยู่ทำหน้าที่ดักจับข้อมูลที่แพร่กระจายในอากาศ ที่มีรูปแบบการสื่อสารตามมาตรฐาน IEEE 802.11 เมื่อแอกเซสพอยต์ได้รับข้อมูลในอากาศจะทำการส่งข้อมูลกลับไปที่เครื่องแม่ข่ายเพื่อทำหน้าที่วิเคราะห์โดยเปรียบเทียบกับฐานข้อมูลแอกเซสพอยต์องค์กร หากพบข้อมูลที่แตกต่างจากฐานข้อมูล ระบบจะทำการส่งคำสั่งควบคุมสวิตช์เพื่อระงับการเชื่อมต่อ จากการทดลอง โดยมีการติดตั้งแอกเซสพอยต์ที่ไม่ได้รับอนุญาตทั้งหมด 4 ประเภททั้งแบบติดตั้งภายในและภายนอกองค์กร เพื่อทดสอบความสามารถในการตรวจจับ พบว่าระบบนี้สามารถตรวจจับแอกเซสพอยต์ได้อย่างถูกต้องในทุกการทดลอง และ มีความสามารถระงับการเชื่อมต่อได้ในแบบอัตโนมัติหากแอกเซสพอยต์นั้นเชื่อมกับเครือข่ายภายในองค์กร

_____ _____ ___ / ___ / ___

ลายมือชื่อนิสิต ลายมือชื่ออาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

Songrit Srilasak 2009: Rogue Access Point Detection and Counterattack System. Master of Engineering (Computer Engineering), Major Field: Computer Engineering, Department of Computer Engineering. Thesis Advisor: Associate Professor Anan Phonphoem, Ph.D. 85 pages.

Normally a user can access an internal server via wireless LAN with some restriction due to the organization security policy. The user may intentionally install an unregistered access point without administrative awareness for his or her convenient which causes backdoors for eavesdrop or attack from the intruders. The rouge access point may also be installed by the intruder himself without connected to the organization's network.

In this thesis, the rouge access point detection and counterattack system has been proposed. The system is designed as a centralize control by utilizing the existing registered access points to capture the broadcasting data, e.g. the identity of the access point, according to the IEEE802.11 standard. The captured data is then sent to the central server for analysis. If the received data does not match with the registered access point, the system sends control commands to the edge switch for shutting down the port that the unregistered access point is connected to. From the experiment, 4 types of unauthorized access point, both inside and outside the organization, can be correctly detected while the system is able to automatically block the internal rouge access point.

_____ _____ ___ / ___ / ___

Student's signature Thesis Advisor's signature

กิตติกรรมประกาศ

ผู้วิจัยขอกราบขอบพระคุณ รศ.ดร. อนันต์ ผลเพิ่ม ประธานกรรมการที่ปรึกษาวิทยานิพนธ์ ที่ให้คำปรึกษาในการเรียน การค้นคว้าวิจัย ตลอดจนช่วยตรวจแก้ไขวิทยานิพนธ์จนกระทั่งเสร็จสมบูรณ์ และ กราบขอบพระคุณ ดร. กิตติ วงศ์ถาวราวัฒน์ กรรมการที่ปรึกษาสาขาวิชาเอก ที่คอยให้ความรู้ คำแนะนำ ทั้งด้านการเรียน และ การทำงาน ตลอดจนเป็นแบบอย่างและแรงบันดาลใจแก่ผู้วิจัย

ขอกราบขอบพระคุณอาจารย์ภาควิชาวิศวกรรมคอมพิวเตอร์ทุกท่าน ที่ได้อบรมสั่งสอนและมอบความรู้อันเป็นประโยชน์อย่างยิ่ง และ ขอบคุณเจ้าหน้าที่ภาควิชาวิศกรรมคอมพิวเตอร์ทุกท่าน ที่ได้ให้ความช่วยเหลือและให้คำแนะนำต่าง ๆ

ด้วยความดีหรือประโยชน์อันใดเนื่องจากวิทยานิพนธ์เล่มนี้ ขอมอบแด่คุณพ่อ คุณแม่ และคุณอุ๊ ที่ได้ให้กำลังใจผู้วิจัยมาตลอดในทุกเรื่อง

ทรงฤทธิ์ ศรีลาศักดิ์

พฤษภาคม 2550

สารบัญ

หน้า

สารบัญตาราง

สารบัญภาพ

สารบัญภาพ (ต่อ)

คำอธิบายสัญลักษณ์และคำย่อ

AP	=	Access Point
BSSID	=	Basic Service Set ID
CTS	=	Clear To Send
CWIDS	=	Cisco Wireless Intrusion Detection System
ICV	=	Integrity Check Value
OSI	=	Open System Interconnection
RTS	=	Request To Send

ระบบตรวจจับและตอบโต้การติดตั้งแอกเซสพอยต์โดยไม่ได้รับอนุญาต

Rogue Access Point Detection and Counterattack System

คำนำ

เครือข่ายแลนไร้สายที่ใช้งานในปัจจุบันมีประสิทธิภาพการส่งข้อมูลได้ด้วยความเร็วสูง และ ยังคงสามารถพัฒนาความเร็วในการสื่อสารได้เพิ่มขึ้นได้อีก สังเกตได้จากมาตรฐานแรกที่เสนอในปี พ.ศ. 2542 ซึ่งเป็นปีที่มาตรฐาน IEEE802.11 ได้เผยแพร่ฉบับสมบูรณ์ ในขณะนั้นเครือข่ายแลนไร้สายใช้เทคโนโลยี DSSS (Direct Sequence Spread Spectrum) และ FHSS (Frequency Hoping Spread Spectrum) ที่ความถี่ 2.4กิกะเฮิร์ต (GHz) สามารถสื่อสารได้ด้วยความเร็วสูงสุด 11 เมกะบิตต่อวินาที (Mbps) ถึงแม้ในขณะนั้นเครือข่ายแลนไร้สายสื่อสารได้ช้ากว่าแลนมีสาย แต่เครือข่ายแลนไร้สายให้ความสะดวกไม่ต้องใช้สายสัญญาณซึ่งเป็นข้อดีที่เข้ามาทดแทน ทำให้เครือข่ายแลนไร้สายเริ่มได้รับความนิยมเรื่อยมา จนกระทั่งในปี พ.ศ. 2546 ทีมพัฒนามาตรฐาน IEEE802.11 คณะทำงานกลุ่มจี (IEEE802.11g) ได้เสนอเทคโนโลยี OFDM (Orthogonal Frequency Division Multiplexing) สำหรับความถี่ 2.4 กิกะเฮิร์ตฉบับสมบูรณ์ เทคโนโลยีที่ใช้เทคนิคการมอดูเลชันแบบ OFDM นี้ทำให้เครือข่ายแลนไร้สายสามารถสื่อสารได้ด้วยความเร็วสูงกว่าเดิม จากเดิมสามารถสื่อสารได้สูงสุด 11เมกะบิตต่อวินาทีกลายเป็น 54เมกะบิตต่อวินาที และในอนาคตถ้าหากเทคโนโลยี IEEE802.11n เสนอฉบับสมบูรณ์ระบบเครือข่ายแลนไร้สายจะสามารถสื่อสารได้ด้วยความเร็วมากกว่า 300เมกะบิตต่อวินาที สังเกตได้ว่าความเร็วในการสื่อสารเครือข่ายแลนไร้สายเริ่มใกล้เคียงกับเครือข่ายแลนมีสายด้วยระยะเวลาเพียงไม่ถึง 10 ปี นอกจากนี้เครือข่ายแลนไร้สายมีความสามารถที่ดีกว่าเครือข่ายแลนมีสายอีกหลายประการ เช่น ความสามารถที่ส่งสัญญาณได้ทะลุกำแพงทำให้ผู้ใช้สามารถสื่อสารกันได้ข้ามห้องแบบไม่ต้องลากสายสัญญาณหรือ ความสามารถจากการไม่จำกัดจุดเชื่อมต่อเพราะเครือข่ายแลนไร้สายใช้การแพร่สัญญาณแบบคลื่นวิทยุไม่ว่าอยู่ที่จุดใดที่สัญญาณครอบคลุมก็สามารถเชื่อมต่อได้ จากข้อดีเหล่านี้ ทำให้องค์กรต่าง ๆ เริ่มเห็นประโยชน์จากการใช้งานเครือข่ายแลนไร้สาย และ คุณสมบัติของแลนไร้สายที่สามารถเชื่อมเข้ากับแลนมีสายทำให้เครือข่ายทั้งสองสามารถสื่อสารกันได้อย่างดี ส่งผลให้เครือข่ายแลนไร้สายได้รับความนิยมอย่างรวดเร็ว ทั้งนี้องค์กรที่ต้องการใช้งานเครือข่ายแลนไร้สายเพียงนำแอกเซสพอยต์ไปเชื่อมกับจุดเชื่อมต่อเครือข่ายแลนมีสายเดิมหลังจากนั้นจะสามารถใช้คอมพิวเตอร์

โน๊ตบุ๊คที่มีการ์ดเครือข่ายแลนไร้สายมาพร้อมกับเครื่อง ทำให้สามารถสื่อสารกับเครือข่ายแลนมีสายผ่านทางเครือข่ายแลนไร้สายได้ทันที

การสื่อสารข้อมูลในอดีตใช้สายสัญญาณเพื่อเป็นสื่อกลางในการรับส่งข้อมูล ระบบเครือข่ายในสมัยก่อนจึงถูกออกแบบบนพื้นฐานการรับส่งข้อมูลผ่านสายสัญญาณซึ่งรวมไปถึงการพัฒนาอุปกรณ์ทางด้านความปลอดภัยของข้อมูลก็ได้รับการออกแบบให้ป้องกันเฉพาะข้อมูลที่เดินทางตามสายสัญญาณเท่านั้น จนกระทั่งเทคโนโลยีการสื่อสารข้อมูลแบบไร้สายได้รับความนิยม ทำให้ข้อมูลไม่จำเป็นต้องส่งผ่านสายสัญญาณเพียงทางเดียว หากใช้เทคโนโลยีเครือข่ายแลนไร้สายทำให้ข้อมูลสามารถแพร่กระจายรอบบริเวณโดยไม่ถูกจำกัดสัญญาณที่สายสัญญาณเพียงอย่างเดียว นำไปสู่ปัญหาที่เกิดขึ้นกับเครือข่ายในองค์กร ปัญหาหนึ่งที่อยู่เหนือความคาดหมาย และเทคโนโลยีการเข้ารหัสข้อมูลไม่อาจป้องกัน เช่น ปัญหาจากพนักงานนำแอกเซสพอยต์มาติดตั้งในเครือข่ายด้วยตนเองโดยที่ผู้ดูแลเครือข่ายไม่ทราบมาก่อน ปัญหาจากผู้บุกรุกลักลอบนำแอกเซสพอยต์มาติดตั้งในเครือข่ายขององค์กร เป็นต้น ปัญหาเหล่านี้จำเป็นต้องได้รับการแก้ไข สำหรับองค์กรที่ยังคงใช้งานเครือข่ายคอมพิวเตอร์

เทคโนโลยีเครือข่ายแลนไร้สายช่วยเพิ่มความสะดวกในการใช้งาน ผู้ใช้งานสามารถใช้งานได้รอบบริเวณที่สัญญาณครอบคลุมถึง และ ในปัจจุบันแอกเซสพอยต์ซึ่งเป็นอุปกรณ์ทำหน้าที่กระจายสัญญาณมีราคาถูกจนสามารถซื้อไปใช้งานได้ง่าย พนักงานที่ต้องการความสะดวกจึงซื้อแอกเซสพอยต์แล้วนำไปเชื่อมต่อกับเครือข่ายองค์กรโดยผู้ดูแลเครือข่ายไม่ล่วงรู้ การกระทำดังกล่าวเป็นการละเมิดนโยบายความปลอดภัยในการสื่อสารข้อมูลภายในองค์กร และ เป็นช่องทางนำไปสู่การบุกรุกเครือข่ายจากบุคคลภายนอก แอกเซสพอยต์ที่เกิดจากการติดตั้งโดยไม่ได้รับอนุญาตหรือเรียกว่าแอกเซสพอยต์เถื่อน สามารถทำได้โดยง่ายเพียงนำแอกเซสพอยต์ไปเชื่อมกับเครือข่ายองค์กรที่ใช้งานปกติในองค์กร แต่ก่อให้เกิดผลเสียหายได้เป็นอย่างมาก เพราะแอกเซสพอยต์ดังกล่าวไม่ได้รับการปรับแต่งค่าอย่างเหมาะสม และ ไม่ได้ปฏิบัติตามนโยบายด้านความปลอดภัยขององค์กร ถูกนำไปติดตั้งอยู่ด้านหลังไฟร์วอลล์ เป็นสาเหตุให้ผู้บุกรุกเลือกโจมตีผ่านทางแอกเซสพอยต์แทนที่จะโจมตีผ่านไฟร์วอลล์ แอกเซสพอยต์เถื่อนเป็นตัวการทำให้ข้อมูลเครือข่ายองค์กรกระจายในอากาศรอบทิศทางในรูปแบบคลื่นวิทยุ เป็นสาเหตุให้เกิดการบุกรุกเครือข่ายองค์กร ด้วยเหตุนี้การติดตั้งแอกเซสพอยต์โดยไม่ได้รับอนุญาตจึงเป็นการทำลายความปลอดภัยของเครือข่ายองค์กรในทันที ปัญหาที่เกิดจากแอกเซสพอยต์เถื่อนไม่ได้เกิดจากการติดตั้งของพนักงานที่ไม่ล่วงรู้ผลเสียหายจากแอกเซสพอยต์เถื่อนเพียงอย่างเดียว แต่แอกเซสพอยต์เถื่อนยังเกิดจากผู้บุกรุกที่เห็นถึงช่องโหว่ของการสื่อสารผ่านเครือข่ายแลนไร้สาย ทำการติดตั้งแอกเซสพอยต์ขึ้นเองเพื่อ

หลอกล่อให้พนักงานภายในองค์กรส่งข้อมูลผ่านตน การกระทำนี้ส่งผลให้ผู้บุกรุกสามารถ ดักฟัง เปลี่ยนแปลง ปลอมแปลง ข้อมูลได้ นอกจากนี้แอกเซสพอยต์เถื่อนยังเกิดขึ้นได้จากพนักงานภายในองค์กรเป็นผู้เจตนาติดตั้งแอกเซสพอยต์ขึ้นเองเพื่อใช้เป็นช่องการสำหรับตนเองเข้าใช้เครือข่ายภายในองค์กรได้ในทุกที่ตลอดเวลา ด้วยเหตุนี้ระบบที่มีความสามารถแก้ไขปัญหาที่เกิดจากแอกเซสพอยต์เถื่อนจึงมีความจำเป็นสำหรับองค์กรที่ต้องการการสื่อสารอย่างปลอดภัย

วิทยานิพนธ์นี้เสนอระบบที่มีความสามารถตรวจจับและตอบโต้การติดตั้งแอกเซสพอยต์เถื่อนด้วยวิธีการควบคุมแบบรวมศูนย์ ระบบนี้ถูกออกแบบให้ใช้ประโยชน์จากอุปกรณ์เครือข่ายที่มีอยู่เดิม วิธีการทำงานของระบบเริ่มจากเครื่องแม่ข่ายควบคุมส่งคำสั่งเพื่อสั่งงานให้แอกเซสพอยต์องค์กรทำหน้าที่ดักฟังข้อมูลในเครือข่ายแลนไร้สายแล้วส่งข้อมูลนั้นกลับมายังเครื่องแม่ข่ายควบคุมผ่านเครือข่ายองค์กร หลังจากที่เครื่องแม่ข่ายควบคุมได้รับข้อมูลจะนำข้อมูลที่ได้เปรียบเทียบกับฐานข้อมูลแอกเซสพอยต์องค์กร หากพบว่ามีความแตกต่างจากข้อมูลในเบื้องต้นจะทำการตรวจสอบถึงการเชื่อมต่อของแอกเซสพอยต์ดังกล่าว หากพบว่ามีการเชื่อมต่อกับเครือข่ายแลนองค์กร จะทำการส่งคำสั่งเพื่อไประงับการเชื่อมต่อในทันที ระบบนี้ได้ออกแบบให้สามารถตรวจจับและระงับการสื่อสารในแบบอัตโนมัติ ทำให้ช่วยลดภาระงานของผู้ดูและระบบ และเพิ่มความปลอดภัยให้แก่เครือข่ายในองค์กร

วัตถุประสงค์

1. สร้างระบบตรวจจับแอกเซสพอยต์ที่ไม่ได้รับอนุญาต

2. พัฒนาวิธีการค้นหาตำแหน่งเพื่อใช้ตรวจสอบแอกเซสพอยต์ที่ไม่ได้รับอนุญาต

3. สร้างระบบป้องกันการบุกรุกจากแอกเซสพอยต์ที่ไม่ได้รับอนุญาต

การตรวจเอกสาร

การตรวจเอกสารของวิทยานิพนธ์นี้ประกอบไปด้วยความรู้พื้นฐานที่สำคัญ และ งานวิจัยที่เกี่ยวข้อง

ความรู้พื้นฐานที่สำคัญ

1. รูปแบบเฟรมตามมาตรฐาน IEEE 802.11

การติดต่อสื่อสารแบบแลนไร้สายมีข้อจำกัดที่แตกต่างจากการติดต่อสื่อสารผ่านแลนมีสาย เช่น ปัญหาโหนดซ่อน (Hidden Node) ปัญหาการกระจายสัญญาณผ่านอากาศ(RF Propagation) หรือ ปัญหาจากการสื่อสารสองทางครึ่งอัตรา (Half Duplex) ปัญหาโหนดซ่อนทำให้มาตรฐาน IEEE802.11 เสนอเฟรมควบคุมแบบ RTS/CTS เพื่อใช้แก้ปัญหาการได้ยินข้อมูลไม่ถึงกันของสถานีลูก ปัญหาการกระจายสัญญาณผ่านอากาศทำให้ข้อมูลดักฟังได้ง่าย ในมาตรฐานจึงได้ออกแบบวิธีการเข้ารหัสข้อมูลเพื่อป้องกันการลักลอบดักฟัง และ ปัญหาที่เกิดจากการสื่อสารสองทางครึ่งอัตราทำให้ไม่อาจใช้กลไกตรวจสอบการชน(Collision Detection) เช่นเดียวกับ IEEE802.3 ได้ จนต้องออกแบบให้มีการส่ง ACK ร่วมกับ RTS/CTS ในชั้น MAC (Medium Access Control) ใช้ควบคุมการเข้าใช้สื่อ เพื่อใช้ตรวจสอบและป้องกันการชนกันของข้อมูล ตัวอย่างข้างต้นเป็นเพียงตัวอย่างข้อหนึ่งที่ทำให้มาตรฐาน IEEE802.11 เสนอรูปแบบเฟรมสื่อสารจำนวนมาก เพื่อแก้ปัญหาเหล่านั้น เฟรมกลุ่มหลักที่สำคัญในเครือข่ายแลนไร้สายประกอบด้วยเฟรม ต่อไปนี้

1.1 เฟรมการจัดการ

การสื่อสารแบบแลนไร้สาย ได้เสนอรูปแบบการสร้างเครือข่ายแลนไร้สายหลายรูปแบบ เช่น เครือข่ายที่มีโครงสร้างแบบแอดฮอก(Ad-hoc) เครือข่ายที่มีโครงสร้างแบบโครงสร้างพื้นฐาน(Infrastructure) และ เครือข่ายที่มีโครงสร้างแบบกระจาย(Wireless Distribution) เป็นต้น วิธีการสร้างเครือข่ายแลนไร้สายแบบโครงสร้างพื้นฐานเป็นทางเลือกหนึ่งได้รับความนิยมสูงในองค์กร โครงสร้างเครือข่ายแบบนี้อาศัยแอกเซสพอยต์เป็นศูนย์กลาง แอกเซสพอยต์มีเฟรมบางชนิดที่สถานีลูกไม่ได้ส่งออกมา เช่น บีคอน เฟรมควบคุมชนิด CTS เป็นต้น ข้อมูลเหล่านี้สามารถใช้เป็นข้อมูลสำหรับการตรวจจับแอกเซสพอยต์ได้ ในภาพที่ 1 ได้แสดงถึงเฟรมการจัดการ เฟรมดังกล่าวใช้สำหรับอ้างอิงถึงรูปแบบเฟรมที่พบทั่วไป ภายในเฟรมการจัดการ มีเฟรมย่อยอีกจำนวน 14 เฟรม

ซึ่งใช้ประโยชน์ในการจัดการเครือข่ายแลนไร้สาย ภายในเฟรมเหล่านี้มีเฟรมที่สำคัญชื่อว่า เฟรมบีคอน ซึ่งเป็นเฟรมที่ใช้เพื่อเป็นประโยชน์ต่อการตรวจจับแอกเซสพอยต์สำหรับวิทยานิพนธ์นี้

2 octets	2 octets	6 octets	6 octets	6 octets	2 octets	0-2312 octets	4 octets
Frame Control	Duration	DA	SA	BSSID	Seq Control	Frame Body	FCS

ภาพที่ 1 รูปแบบของเฟรมการจัดการ

Frame Control มีขนาดเท่ากับ 16 บิต ทำหน้าที่ระบุชนิดของเฟรม การระบุชนิดของเฟรมใช้วิธีปรับเปลี่ยนข้อมูลใน Type และ Subtype ดังแสดงในตารางหมายเลข 1 และ 2

Duration มีขนาด 2 ไบต์ทำหน้าที่บอกระยะเวลาการรอให้แก่สถานีซึ่งมีหน่วยเป็นมิลลิวินาที

DA มีขนาด 6 ไบต์ ทำหน้าที่บอกค่าหมายเลขอุปกรณ์เครือข่ายแลนไร้สายปลายทาง หากเฟรมนั้นเป็นเฟรมการจัดการค่านี้จะมีค่าเป็น $FF\text{-}FF\text{-}FF\text{-}FF\text{-}FF\text{-}FF_{16}$

SA มีขนาด 6 ไบต์ ทำหน้าที่บอกค่าหมายเลขอุปกรณ์เครือข่ายแลนไร้สายต้นทาง หากเฟรมนั้นเป็นเฟรมการจัดการจะได้รับการเซตค่าให้ตรงกับค่าหมายเลขอุปกรณ์เครือข่ายแลนไร้สายของแอกเซสพอยต์นั้น

BSSID หรือ หมายเลขอุปกรณ์เครือข่ายแลนไร้สาย มีขนาด 6 ไบต์ ทำหน้าที่บอกค่าหมายเลขอุปกรณ์เครือข่ายแลนไร้สายของเจ้าของเครือข่าย หากเฟรมดังกล่าวเป็นเฟรมการจัดการจะได้รับการเซตค่าให้ตรงกับค่าหมายเลขอุปกรณ์เครือข่ายแลนไร้สายของแอกเซสพอยต์นั้น

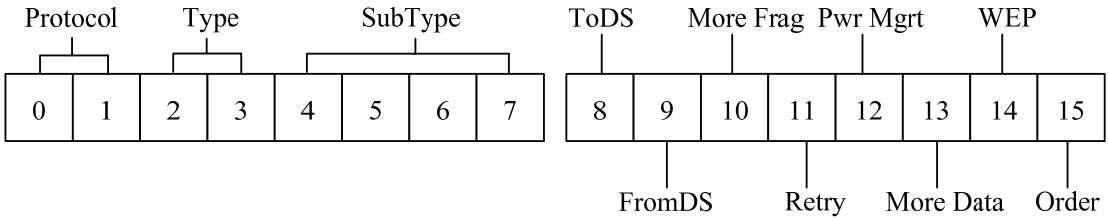
Seq Control field ทำหน้าที่สองหน้าที่ ได้แก่ กำหนดลำดับข้อมูลเพื่อให้เฟรมที่ได้รับการแบ่งข้อมูล (fragment) สามารถรวมกันได้ถูกต้อง และ มีหน้าที่ป้องกันการส่งเฟรมซ้ำ ภายในข้อมูล 16 บิตนี้ได้แบ่งออกเป็นสองกลุ่ม 4 บิตแรกทำหน้าที่กำหนดเลขหมายของเฟรมที่ได้รับการแบ่งและ 12 บิตที่เหลือทำหน้าที่แสดงลำดับของเฟรม

Frame Body มีขนาดเปลี่ยนแปลงได้ขึ้นอยู่กับชนิดของเฟรม โดยมีขนาดตั้งแต่ 0 ถึง 2312 ไบต์ หากเฟรมดังกล่าวเป็นเฟรมบีคอน ข้อมูลที่อยู่ภายใน Frame Body ประกอบด้วยข้อมูลเพิ่มเติมขึ้นอยู่กับชนิดของเฟรมที่อธิบายตามตารางหมายเลข 1 และ 2

FCS มีขนาด 4 ไบต์ได้รับการออกแบบให้เป็นข้อมูลเพื่อใช้ตรวจสอบความสมบูรณ์ของเฟรม

1.2 Frame Control

Frame Control มีหน้าที่ระบุชนิดของเฟรม ด้วยการเปลี่ยนแปลงค่า Type และ Subtype และรายละเอียดอื่น ๆ ซึ่งได้จัดเรียงตามบิตดังแสดงในภาพที่ 2 หมายเลขที่กำกับจาก 0 ถึง 15 หรือเขียนแทนด้วย b_0 - b_{15}ใช้อธิบายถึงลำดับหมายเลขบิตของข้อมูล ต่อไปเป็นคำอธิบายหน้าที่การทำงาน



ภาพที่ 2 รายละเอียดภายใน Frame Control

Protocol มีขนาด 2 บิต ทำหน้าที่บอกหมายเลขรุ่นของการใช้สื่อ (MAC) ตามมาตรฐาน IEEE 802.11 ซึ่งในปัจจุบันมีค่าเท่ากับ 0 ดังนั้นข้อมูลในบิตนี้จึงมีค่าเท่ากับ $b_0b_1=00_2$

Type มีขนาด 2 บิตทำหน้าที่บอกชนิดของเฟรมซึ่งจำเป็นต้องใช้งานร่วมกับ Subtype การระบุชนิดเฟรมแสดงดังตารางที่ 1

Subtype มีขนาด 4 บิต ทำหน้าที่ระบุรายละเอียดของเฟรม ซึ่งมีความสัมพันธ์กับ Type ภายใน Subtype นี้ได้ระบุชนิดของเฟรมที่มีความจำเป็นสำหรับการตรวจจับแอกเซสพอยต์ เพราะเป็นข้อมูลที่ส่งออกจากแอกเซสพอยต์เพียงอย่างเดียว เช่น เฟรมบีคอน เป็นต้น รายละเอียดของ Subtype แสดงในตารางที่ 2

ตารางที่ 1 คำอธิบายหน้าที่ของเฟรมการจัดการ

Type		คำอธิบาย
b3	b2	
0	0	เฟรมการจัดการ
0	1	เฟรมควบคุม
1	0	เฟรมข้อมูล
1	1	สำรอง ไม่ใช้งาน

ตารางที่ 2 คำอธิบายหน้าที่ย่อยของเฟรมการจัดการ

Subtype	คำอธิบาย
$b_7b_6b_5b_4$	
0000	Association request
0001	Association response
0010	Reassociation request
0011	Reassociation response
0100	Probe request
0101	Probe response
0110	-
0111	-
1000	Beacon
1001	Announcement traffic indication message (ATIM)
1010	Disassociation
1011	Authentication
1100	Deauthentication
1101	Acknowledgment(ACK)

ตารางที่ 2 (ต่อ)

Subtype $b_7b_6b_5b_4$	คำอธิบาย
1110	Contention-Free(CF)-End
1111	CF-End+CF-Ack

จากตารางที่ 2 เห็นได้ว่าเฟรมบีคอนมีค่า Subtype เท่ากับ 0001_2 ($b_4b_5b_6b_7$) ซึ่งในการส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์ใช้การอ่านข้อมูลครั้งละ 1 ไบต์ (8 บิต) เรียงในแบบ MSB (Most Significant Bit) ทำให้ข้อมูลที่ได้รับเปลี่ยนแปลงโดยเรียงลำดับใหม่ดังนี้ $b_7b_6b_5b_4b_3b_2b_1b_0$ ดังนั้นซอฟต์แวร์จึงอ่านข้อมูลได้เท่ากับ $1000\ 0000_2$ เมื่อแปลงเป็นเลขฐาน 16 ตรงกับ $0x80_{16}$ ค่าดังกล่าวนี้ถูกนำไปใช้เป็นข้อมูลสำหรับการระบุเฟรมบีคอน ซึ่งเป็นข้อมูลที่แอกเซสพอยต์ดักจับข้อมูลจากอากาศ

ToDS มีขนาด 1 บิต และ FromDS มีขนาด 1 บิต ข้อมูลบิตนี้ใช้สำหรับระบุทิศทางของข้อมูล หากเป็นข้อมูลที่ส่งออกจากสถานีลูกค่า ToDS จะรับการเซตค่าให้มีค่าเป็น 1 และค่า FromDS จะได้รับการเซตค่าให้เท่ากับ 0 เมื่อข้อมูลนั้นส่งมาจากแอกเซสพอยต์ไปยังสถานีลูก ค่า ToDS จะมีค่าเท่ากับ 0 และ FromDS จะมีค่าเท่ากับ 1 แต่เมื่อไรก็ตามที่ข้อมูลนั้นเป็นข้อมูลที่แอกเซสพอยต์ส่งออกมาเพื่อใช้ควบคุมการสื่อสารเช่นเฟรมจัดการค่าทั้งสองจะมีค่าเท่ากับ 0

More Frag มีขนาด 1 บิต บิตนี้ได้รับการเซตค่าเท่ากับ 1 เมื่อเฟรมนั้นเป็นเฟรมข้อมูล หรือเฟรมการจัดการที่มีข้อมูลอื่นแทรก แต่โดยทั่วไปมีค่าเท่ากับ 0

Retry มีขนาด 1 บิต ได้รับการเซตให้เป็น 1 กรณีที่มีการส่งข้อมูลซ้ำ แต่โดยทั่วไปมีค่าเท่ากับ 0

Pwr Mgrt มีขนาด 1 บิต บิตนี้จะถูกเซตให้เป็น 1 ในกรณีที่มีการตั้งค่าใช้งานการประหยัดพลังงาน เฟรมนี่จะเป็นเฟรมที่ส่งออกจากสถานีลูกถึงแอกเซสพอยต์เท่านั้น บิตนี้ถูกเซตให้เป็น 0 เพื่อเฟรมดังกล่าวเป็นเฟรมการจัดการ

More Data มีขนาด 1 บิต บิตนี้ใช่ร่วมกับโหมดประหยัดพลังงานซึ่งแอกเซสพอยต์จะทำหน้าที่เซตบิตให้มีค่าเป็น 1 เพื่อบอกว่ามีข้อมูลอยู่เก็บที่ตนเองเพื่อรอส่งให้สถานีลูก

WEP หรือ Protected Frame มีขนาด 1 บิต เมื่อข้อมูลที่ส่งมีการเข้ารหัส บิตนี้จะถูกเซตค่าให้เป็น 1 แต่ ถ้าเป็นเฟรมการจัดการซึ่งเป็นข้อมูลที่ไม่เข้ารหัส บิตนี้จึงมีค่าเป็น 0 เสมอ

Order มีขนาด 1 บิต ได้รับการเซตค่าให้เป็น 1 เมื่อใช้งาน ต้องการกำหนดลำดับข้อมูล (StrictlyOrdered) ปกติถูกเซตค่าเท่ากับ 0

1.3 เฟรมบีคอน

เฟรมนี้เป็นเฟรมชนิดหนึ่งของเฟรมการจัดการซึ่งถูกส่งออกมาจากแอกเซสพอยต์ด้วยคาบเวลาคงที่ เพื่อส่งข้อมูลที่มีความจำเป็นในการสร้างการเชื่อมต่อ ภายในเฟรมประกอบด้วยข้อมูลที่จำเป็น เช่น ชื่อเครือข่าย หมายเลขอุปกรณ์เครือข่ายแลนไร้สายของแอกเซสพอยต์ ช่องสัญญาณ เป็นต้น โดยมีรูปแบบเฟรมในภาพที่ 3 ซึ่งเป็นภาพที่แสดงถึงรายละเอียดการจัดรูปแบบเฟรมซึ่งอยู่ภาย Frame Body ของเฟรมการจัดการ

8 octets	2 octets	2 octets	2-34 octets	2-10 octets	3 octets	
Time Stamp	Beacon Interval	Capability Info	SSID	Support rate	DS Parameter	More..

ภาพที่ 3 รายละเอียดเฟรมบีคอน

Time Stamp มีขนาดคงที่ 8 ไบต์ มีไว้เพื่อให้สถานีลูกใช้ซิงโครนัสเวลา

Beacon Interval มีขนาดคงที่ 2 ไบต์ ใช้สำหรับบอกสถานีลูกถึงคาบเวลาการมาของเฟรมบีคอน

Capability Info มีขนาดคงที่ 2 ไบต์ ใช้สำหรับบอกคุณสมบัติของเครือข่าย

SSID หรือ ชื่อเครือข่ายแลนไร้สาย มีขนาดเปลี่ยนแปลงได้อยู่ระหว่าง 2 - 34 ไบต์ มีไว้สำหรับบอกชื่อเครือข่ายแลนไร้สาย ค่า SSID เป็นข้อมูลขนาดความยาวที่ทำให้ทราบว่า สามารถกำหนดชื่อเครือข่ายไร้สายได้ 32 ตัวอักษรเมื่อหักลบออก 2 ไบต์จากส่วนบอกความยาวเฟรม

Support rate มีขนาดเปลี่ยนแปลงได้อยู่ระหว่าง 2-10 ไบต์ ทำหน้าที่บอกการรองรับความเร็วในการสื่อสารของเครือข่าย

DS Parameter มีขนาดคงที่ 3 ไบต์ ใช้สำหรับบอกค่าหมายเลขช่องสัญญาณของเครือข่ายแลนไร้สาย

More ... ใช้อธิบายบายถึงข้อมูลที่เหลือ ซึ่งเป็นข้อมูลที่ได้รับการใช้งานในวิทยานิพนธ์นี้

1.4 เฟรมข้อมูล

หน้าที่หลักของเฟรมข้อมูลได้แก่การบรรจุข้อมูลเพื่อส่งไปยังปลายทาง โดยที่เฟรมข้อมูลสามารถบรรจุข้อมูลได้สูงสุดขนาด 2326 ไบต์ เมื่อข้อมูลมีขนาดใหญ่กว่าที่กำหนดจะทำการแบ่ง เพื่อส่งต่อในเฟรมถัดไป รูปแบบเฟรมข้อมูลแสดงในภาพที่ 4

2 octets	2 octets	6 octets	6 octets	6 octets	2 octets	6 octets	0-2326 octets	4 octets
Frame Control	Duration	Addr1	Addr2	Addr3	Seq Control	Addr4	Frame Body	FCS

ภาพที่ 4 รูปแบบของเฟรมข้อมูล

เฟรมข้อมูลได้รับการออกแบบให้จัดรูปแบบเฟรมคล้ายกับเฟรมการจัดการ แต่มีรายละเอียดข้อมูลที่มีความแตกต่างจากเฟรมการจัดข้อมูลภายใน Addr1 Addr2 Addr3 และ Addr4 ข้อมูลทั้ง 4 ข้อมูลนี้ใช้อธิบายถึงหมายเลขอุปกรณ์เครือข่ายแลนไร้สายของสถานีลูก และ หมายเลขอุปกรณ์เครือข่ายแลนไร้สายของแอกเซสพอยต์ ค่าทั้ง 4 ค่านี้ถูกกำหนดขึ้นโดยมีความสัมพันธ์กับค่าข้อมูลใน ToDS และ FromDS ที่ปรากฏใน Frame Control ตารางที่ 3 ได้แสดงถึงความสัมพันธ์ของ Addr1 Addr2 Addr3 และ Addr4 กับ ToDS และ FromDS โดยที่ Addr1 ใช้อ้างถึงหมายเลขอุปกรณ์เครือข่ายแลนไร้สายที่เป็นผู้รับข้อมูล (RA) และ Addr2 ใช้อ้างถึงหมายเลขอุปกรณ์เครือข่ายแลนไร้สายที่เป็นผู้ส่งข้อมูล (TA)

จากตารางที่ 3 แสดงให้เห็นว่าค่าหมายเลขอุปกรณ์เครือข่ายสามารถเปลี่ยนแปลงได้ขึ้นอยู่กับทิศทางการเดินทางของข้อมูลที่กำหนดด้วย ToDS และ FromDS รายละเอียดในตารางสามารถอธิบายได้ดังต่อไปนี้

RA = DA หมายถึง หมายเลขอุปกรณ์เครือข่ายแลนไร้สายผู้รับ มีค่าเท่ากับ หมายเลขอุปกรณ์เครือข่ายแลนไร้สายของสถานีผู้รับ

TA = SA หมายถึง หมายเลขอุปกรณ์เครือข่ายแลนไร้สายผู้ส่ง มีค่าเท่ากับ หมายเลขอุปกรณ์เครือข่ายแลนไร้สายของสถานีผู้ส่ง

BSSID หมายถึง หมายเลขอุปกรณ์เครือข่ายแลนไร้สายของแอกเซสพอยต์เจ้าของเครือข่าย

TA = BSSID หมายถึง หมายเลขอุปกรณ์เครือข่ายแลนไร้สายผู้ส่งเท่ากับหมายเลขอุปกรณ์เครือข่ายแลนไร้สายเจ้าของเครือข่าย

RA (Receiver Address) หมายถึง หมายเลขอุปกรณ์เครือข่ายแลนไร้สายที่เป็นผู้รับข้อมูล

TA (Transmitting Address) หมายถึง หมายเลขอุปกรณ์เครือข่ายแลนไร้สายผู้ส่งข้อมูล

SA (Source Address) หมายถึง หมายเลขอุปกรณ์เครือข่ายแลนไร้สายของสถานีลูกที่เป็นผู้ส่งข้อมูล

DA (Destination Address) หมายถึง หมายเลขอุปกรณ์เครือข่ายแลนไร้สายผู้รับข้อมูล

BSSID หมายถึง หมายเลขอุปกรณ์เครือข่ายแลนไร้สายของเจ้าของเครือข่าย

N/A หมายถึง ไม่ได้ใช้งาน

ตารางที่ 3 ความสัมพันธ์ของค่าหมายเลขอุปกรณ์เครือข่ายแลนไร้สายในเฟรมข้อมูล

Frame Control		Addr1	Addr2	Addr3	Addr4
ToDS	FromDS				
0	0	RA = DA	TA = SA	BSSID	N/A
0	1	RA = DA	TA = BSSID	SA	N/A

ตารางที่ 3 (ต่อ)

Frame Control		Addr1	Addr2	Addr3	Addr4
ToDS	FromDS				
1	0	RA = BSSID	TA = SA	DA	N/A
1	1	RA	TA	DA	SA

จากตารางที่ 3 มีเฟรมชนิดพิเศษที่มีความแตกต่างจากเฟรมอื่นได้แก่ กรณีที่ ToDS และ FromDS เท่ากับ 1 ซึ่งจะทำให้เฟรมข้อมูลมีความอุปกรณ์เครือข่ายทั้งหมด 4 ค่า (Addr1 - Addr4) โดยที่เฟรมดังกล่าวถูกใช้ในกรณีที่ส่งข้อมูลที่ไม่ได้ผ่านเครือข่ายแลนมีสาย เป็นการสื่อสารระหว่างแอกเซสพอยต์ด้วยกันทางไร้สาย ซึ่งเรียกว่า WDS (Wireless Distribution System)

1.5 เฟรมควบคุม

เฟรมควบคุมทำหน้าที่จัดการตรวจสอบการเข้าใช้เครือข่ายและสำหรับจองช่องสื่อสาร เฟรมดังกล่าวนี้เป็นเฟรมที่ได้รับสิทธิในการส่งข้อมูลเร็วที่สุด ด้วยความเร็ว SIFS (Short Inter Frame Spacing) รูปแบบเฟรมมีความคล้ายกับเฟรมการจัดการดังแสดงในภาพที่ 1 แต่บิตของ Type มีค่า $b_3b_2 = 01_2$ ตามลำดับ

2. ความรู้พื้นฐานด้านความปลอดภัยเครือข่ายแลนไร้สาย

เพื่อให้เกิดการสื่อสารอย่างปลอดภัยในเครือข่ายแลนไร้สาย หน่วยงาน NIST (National Institute of Standards and Technology) (Scarfone *et al.,* 2008) ได้มีข้อเสนอแนะเพื่อช่วยให้ผู้ดูแลเครือข่ายแลนไร้สายได้เลือกใช้เทคโนโลยีด้านความปลอดภัยอย่างถูกต้อง ภายในเอกสารได้เสนอวิธีการเลือกใช้เทคโนโลยีที่รองรับการทำงานภายในข้อกำหนด 3 ประการดังนี้ 1). การรักษาความลับ (Confidentiality) 2). การป้องกันการแก้ไข (Integrity) และสุดท้าย 3). การให้บริการได้ตลอดเวลาที่ต้องการใช้งาน (Availability) ข้อกำหนดทั้ง 3 ประการนี้สามารถใช้เป็นเกณฑ์ในการพิจารณาเพื่อเลือกคุณสมบัติของระบบสื่อสารเครือข่ายคอมพิวเตอร์ ที่ต้องการสื่อสารได้อย่างปลอดภัย สำหรับคำอธิบายข้อกำหนดด้านความปลอดภัยได้เขียนอธิบายรายละเอียดไว้ดังคำอธิบายต่อไปนี้

การรักษาความลับ หมายถึง การปกป้องข้อมูลไม่ให้ผู้อื่นที่ไม่เกี่ยวข้องล่วงรู้ ซึ่งสามารถทำได้ด้วยการเข้ารหัสข้อมูลที่มีความซับซ้อนเพียงพอ รวมไปถึงการควบคุมสิทธิการเข้าใช้งานเครือข่าย

การป้องกันการแก้ไข หมายถึง การป้องกันไม่ให้ข้อมูลที่สื่อสารได้รับการแก้ไข หรือเปลี่ยนแปลงจากต้นฉบับที่ส่งออกไป การป้องกันการแก้ไขที่ดีจะต้องมีกลไกการพิสูจน์ตัวตนของผู้รับและผู้ส่ง และ ช่องทางการแลกเปลี่ยนข้อมูลที่ปลอดภัยเพียงพอ

การให้บริการได้ตลอดเวลาที่ต้องการใช้งาน หมายถึง ระบบที่ใช้งานจริงจำเป็นต้องให้บริการได้เมื่อมีการร้องขอ ระบบที่มีความปลอดภัยจึงต้องสามารถให้บริการได้ด้วย

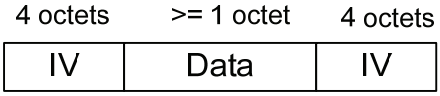
จากข้อกำหนดทั้ง 3 ประการสามารถใช้เป็นเกณฑ์ในการตัดสินใจเลือกใช้เทคโนโลยีเครือข่ายแลนไร้สายสำหรับองค์กรที่ต้องการความปลอดภัยว่ามีความสามารถครบทั้ง 3 ประการหรือไม่ ถึงแม้ในปัจจุบันมาตรฐานความปลอดภัยสำหรับการสื่อสารผ่านเครือข่ายสาย IEEE802.11i ยังไม่ได้เปิดเผยฉบับสมบูรณ์ แต่ก็สามารถเลือกใช้เทคโนโลยีในปัจจุบันที่มีความปลอดภัยเพียงพอได้ ดังรายละเอียดที่ได้จะกล่าวต่อไป

3. เทคโนโลยีความปลอดภัยสำหรับมาตรฐาน IEEE802.11

เทคโนโลยีด้านความปลอดภัยสำหรับเครือข่ายแลนไร้สาย ได้รับการเสนอพร้อมกับมาตรฐานการสื่อสารตั้งแต่ปี ค.ศ. 1999 ภายในมาตรฐานนั้นได้เสนอเทคโนโลยีด้านความปลอดภัยมีชื่อว่า WEP (Wired Equivalent Privacy) ภายในเทคโนโลยี WEP ได้เสนอวิธีการเข้ารหัสข้อมูลด้วยวิธีเข้ารหัสแบบ RC4 ซึ่งการเข้ารหัสชนิดนี้ถูกจัดอยู่ในกลุ่มการเข้ารหัสแบบ Stream Cipher และ ในปี ค.ศ. 2000 หน่วยงานที่เกิดจากความร่วมมือของผู้ผลิตอุปกรณ์เครือข่ายแลนไร้สายชื่อว่า Wi-Fi Alliance ได้เสนอเทคโนโลยีเพื่อแก้ปัญหาด้านความปลอดภัยที่เกิดกับ WEP ด้วยเทคโนโลยี WPA (Wi-Fi Protected Access) ซึ่งยังคงใช้การเข้ารหัสแบบ RC4 เช่นเดิมแต่ได้ปรับปรุงเทคนิคการปรับเปลี่ยนค่า IV (Initial Vector) และ เพิ่ม MIC (Message Integrity Code) ต่อมาปี ค.ศ. 2004 หน่วยงาน Wi-Fi Alliance ได้เสนอ WPA2 (Wi-Fi Protected Access version 2) ซึ่งได้ปรับปรุงเทคนิคการเข้ารหัสจากเดิมที่ใช้ RC4 เป็น AES (Advanced Encryption Standard) การเข้ารหัสชนิดนี้ถูกจัดอยู่ในกลุ่ม Block Cipher

3.1 เทคโนโลยีความปลอดภัยด้วย WEP

มาตรฐานได้กำหนดให้สามารถใช้งาน WEP ได้ 2 แบบได้แก่ WEP-40 และ WEP-104 ตัวเลขที่อยู่ด้านหลังจากถึงจำนวนบิตที่ใช้เป็นกุญแจเข้ารหัส สำหรับ WEP-40 หมายถึงใช้ข้อมูล 40 บิตในเป็นกุญแจเข้ารหัส รูปแบบการจัดเฟรมของ WEP อยู่ในการเข้ารหัสข้อมูลของเฟรมข้อมูลซึ่งข้อมูลนี้เรียกว่า MSDU (MAC Service Data Unit) โดยมีการจัดรูปแบบดังนี้



ภาพที่ 5 เฟรมการเข้ารหัสในแบบ WEP

จากภาพที่ 5 ได้อธิบายถึงเฟรมข้อมูลที่ได้รับการเข้ารหัสด้วยเทคโนโลยี WEP เฟรมนี้ถูกนำไปใช้กับเฟรมข้อมูล ซึ่งอธิบายรายละเอียดได้ดังนี้ IV หมายถึง หมายเลขที่ใช้เพื่อกำหนดลำดับการเข้ารหัส, DATA หมายถึง ข้อมูลที่ผ่านการเข้ารหัสแล้ว, ICV หมายถึง ชุดข้อมูลที่ใช้สำหรับตรวจสอบความสมบูรณ์ของเฟรม

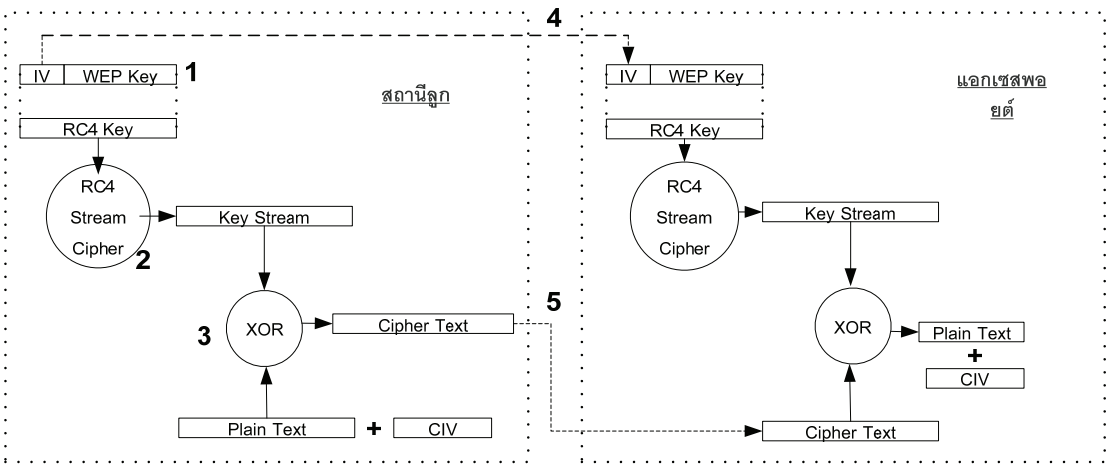
จากภาพที่ 6 เมื่อสถานีลูกต้องการสื่อสารข้อมูลกับแอกเซสพอยต์ เริ่มต้นจาก 1) นำค่ากุญแจที่ได้รับการกำหนดให้ตรงกับแอกเซสพอยต์มาสร้างรหัสกระแส (Stream Cipher) 2) นำรหัสที่ได้จากการสร้างรหัสกระแสมาทำการแบ่งข้อมูลออกเป็นท่อนแล้วนำไปเข้าวิธีการ XOR กับข้อมูลที่ต้องการเข้ารหัส (Plain Text Packet) และ ICV โดยที่ ICV คือข้อมูลที่ได้จากการนำเอาข้อมูลที่ต้องการเข้ารหัสไปเข้าขั้นตอนวิธี CRC32 หลังจากนั้นจึงได้ข้อมูลที่เข้ารหัสพร้อมส่งไปยังแอกเซสพอยต์ โดยข้อมูลที่ส่งให้แก่แอกเซสพอยต์มี 2 ข้อมูลได้แก่ 4) ค่า IV ซึ่งได้แนบไปพร้อมกับข้อมูลเข้ารหัส 5) ข้อมูลที่ได้รับการเข้ารหัสแล้ว เมื่อแอกเซสพอยต์ได้รับข้อมูล (4) และ (5) จะทำการถอดรหัสด้วยกลไกย้อนกลับ จนสุดท้ายได้รับข้อมูลที่เหมือนกับข้อมูลต้นทาง

เทคโนโลยี WEP เป็นเทคโนโลยีที่ได้รับการเสนอในช่วงเวลาที่มีข้อจำกัดหลายประการ เช่น เทคโนโลยีทางด้านการผลิตหน่วยประมวลผล ที่มีความสามารถในการประมวลผลการเข้าและถอดรหัสได้อย่างรวดเร็ว รวมไปถึงความซับซ้อนของเทคโนโลยีด้านความปลอดภัย ทำให้เมื่อนำไปใช้งานจริงจึงพบจุดโหว่หลายประการ การศึกษาของ (Borisov *et al.,* 2001) พบว่าเทคโนโลยีความปลอดภัยของ WEP ไม่เพียงพอสำหรับการนำไปใช้ในเครือข่ายแลนไร้สายที่ต้องการความปลอดภัย

3.2 เทคโนโลยีความปลอดภัยด้วย WPA

เทคโนโลยีความปลอดภัยด้วย WPA ได้รับการเสนอจาก Wi-Fi Alliance เพื่อนำมาใช้แก้ปัญหาเฉพาะหน้า จากความไม่ปลอดภัยในการสื่อสารของเทคโนโลยี WEP ซึ่ง WPA ได้เสนอเทคโนโลยีหลัก 2 รูปแบบโดยได้แบ่งตามขนาดขององค์กรที่ต้องการใช้งานได้แก่ WPA-Personal และ WPA-Enterprise

WPA-Personal หรือบางครั้งเรียกว่า WPA-PSK เป็นเทคโนโลยีที่ออกแบบเพื่อให้สามารถสร้างเครือข่ายแลนไร้สายที่มีความปลอดภัยได้อย่างง่าย ด้วยการใช้กุญแจรหัสร่วมกัน เทคโนโลยีนี้คล้ายกับ WEP แต่ได้ปรับปรุงด้านการเปลี่ยนกุญแจหลักก่อนที่ผู้บุกรุกจะนำไปใช้เพื่อถอดรหัสได้ พร้อมกับเสนอวิธีการตรวจสอบความสมบูรณ์ของข้อมูลด้วย MIC (Message Integrity Code) เพื่อป้องกันการแก้ไขข้อมูลต้นฉบับ WPA-Personal ได้เสนอเทคโนโลยีความปลอดภัยสำหรับเครือข่ายแลนไร้สายที่ตรงตามความต้องการ 3 ประการได้แก่ การรักษาความลับด้วยการเข้ารหัสแบบ RC4 ที่ได้รับการปรับปรุงแล้ว การป้องกันการแก้ไขข้อมูลด้วย MIC การควบคุมการเข้าใช้ด้วยรหัสกุญแจหลัก เทคโนโลยีนี้มีความปลอดภัยเพียงพอสำหรับเครือข่ายแลนไร้สายขนาดเล็กแต่เมื่อต้องการนำไปใช้งานกับเครือข่ายแลนไร้สายขนาดใหญ่จะพบปัญหาจากการควบคุมการแจกจ่ายรหัสกุญแจหลัก เพราะเทคโนโลยี WPA-Personal ใช้วิธีให้เครื่องลูกข่ายใช้กุญแจหลักเหมือนกันทั้งเครือข่าย ซึ่งทำให้กุญแจหลักมีโอกาสรั่วไหลสู่บุคคลภายนอกและติดตามได้ยาก ดังนั้นเมื่อต้องการใช้งานเครือข่ายแลนไร้สายในองค์กรขนาดใหญ่จึงควรใช้เทคโนโลยี WPA-Enterprise



ภาพที่ 6 กลไกการเข้ารหัสข้อมูลของ WEP

WPA-Enterprise หรือบางครั้งเรียกว่า WPA-EAP ได้เสนอวิธีการพิสูจน์ตัวจริงด้วยกลไก EAP (Extensible Authentication Protocol) วิธีการนี้ช่วยให้การดูแลด้านการแจกจ่ายกุญแจหลักทำได้ง่ายขึ้นด้วยการกำหนดรหัสกุญแจหลักสำหรับสถานีลูกได้แตกต่างกัน ความสามารถของ EAP ช่วยให้การพิสูจน์ตัวจริงสำหรับเครือข่ายแลนไร้สายมีความหลากหลายมากขึ้น โดยที่ผู้ดูแลเครือข่ายสามารถเลือกวิธีพิสูจน์ตัวจริงได้ตามตารางที่ 4

เทคโนโลยีพิสูจน์ตัวตนสำหรับ WPA-Enterprise ที่ได้รับความนิยมในปัจจุบันได้แก่ เทคโนโลยี EAP-PEAP ซึ่งเป็นเทคโนโลยีที่ได้รับการติดตั้งมาพร้อมกับระบบปฏิบัติการวินโดว์ XP หรือใหม่กว่า กลไกการทำงานของ EAP-PEAP ได้อ้างอิงการพิสูจน์ตัวตนตามมาตรฐาน IEEE 802.1x โดยกำหนดให้แอกเซสพอยต์ทำหน้าที่เป็น NAS (Network Access Server) และส่งข้อมูลตรวจสอบพิสูจน์ตัวตนกับโพรโทคอลพิสูจน์ตัวตนแบบ RADIUS (Remote Authentication Dial In User Service)

3.3 เทคโนโลยีความปลอดภัยด้วย WPA2

เทคโนโลยีความปลอดภัยด้วย WPA2 ได้เสนอเทคนิคการเข้ารหัสแบบใหม่ด้วยเทคนิคเข้ารหัสแบบ AES เทคนิคเข้ารหัสแบบนี้ได้รับการจัดกลุ่มให้อยู่ในชนิดการเข้ารหัสแบบ Block Cipher เพื่อใช้แก้ปัญหาการโจมตีด้วยการถอดรหัสข้อมูลของ RC4 ซึ่ง WPA2 ได้เสนอเทคโนโลยี 2 แบบโดยได้แบ่งตามขนาดขององค์กรที่ต้องการใช้งานได้แก่ WPA2-Personal และ WPA2-Enterprise ซึ่งใช้วิธีพิสูจน์ตัวตนเช่นเดียวกับ WPA แต่แตกตรงที่ใช้วิธีเข้ารหัสแบบ AES

ตารางที่ 4 รายการเทคโนโลยีพิสูจน์ตัวตน

ลำดับ	ชื่อเทคโนโลยี	ผู้พัฒนา
1	LEAP	ซิสโก้
2	EAP-TLS	RFC 5216
3	EAP-MD5	RFC 3748
4	EAP-PSK	RFC 4764
5	EAP-TTLS	RFC 5281

ตารางที่ 4 (ต่อ)

ลำดับ	ชื่อเทคโนโลยี	ผู้พัฒนา
6	EAP-IKEv2	RFC 5106
7	EAP-PEAP	ไมโครซอฟต์ ซิสโก้ และ RSA
8	EAP-FAST	RFC 4851
9	EAP-SIM	RFC 4186
10	EAP-AKA	RFC 4187

3.4 เทคโนโลยีความปลอดภัยด้วย IEEE 802.11i

ปัญหาจากรูปแบบมาตรฐานสื่อสารเครือข่ายแลนไร้สายของ IEEE802.11 แบบเดิมในปี ค.ศ. 1999 ที่มีปัญหาด้านความปลอดภัยจนไม่อาจยอมรับได้ (Borisov *et al*., 2001) มาตรฐาน IEEE 802.11-2007 ได้ออกแบบวิธีการสื่อสารอย่างปลอดภัยในเครือข่ายแลนไร้สายด้วยการเสนอเทคโนโลยี 2 รูปแบบได้แก่ Pre-RSNA และ RSNA (Robust Security Network Association)

ในปัจจุบัน (กุมภาพันธ์, 2552) เทคโนโลยีความปลอดภัยมาตรฐาน IEEE802.11i ยังไม่แล้วเสร็จจึงไม่ถูกนำไปรวมในมาตรฐานหลัก แต่ผู้ผลิตอุปกรณ์ได้คัดเลือกความสามารถบางส่วนของ IEEE802.11i มาผลิตอุปกรณ์ให้ได้ใช้งานก่อน รายละเอียดที่เสนอในหัวข้อนี้อ้างอิงตามมาตรฐาน IEEE802.11-2007

Pre-RSNA เทคโนโลยี Pre-RSNA เป็นเทคโนโลยีที่ออกแบบเพื่อให้มีการสื่อสารอย่างปลอดภัยสำหรับอุปกรณ์ที่ยังไม่รองรับเทคโนโลยีที่มีความปลอดภัยสูงกว่า(RSNA) ภายใน Pre-RSNA ประกอบด้วยเทคโนโลยีหลัก 2 เทคโนโลยีที่อ้างอิงตามเทคโนโลยีเดิม ประกอบด้วย การพิสูจน์ตัวตน และ การเข้ารหัส pre-RSNA ได้เสนอวิธีพิสูจน์ตัวตนไว้ 2 รูปแบบได้แก่ Open System และ Share Key โดยที่ Open System หมายถึง วิธีการที่ไม่มีระบบพิสูจน์ตัวตน สถานีลูกที่ส่งข้อมูลมาเพื่อขอพิสูจน์ตัวตน จะได้รับการตอบรับ วิธีนี้เป็นวิธีที่เป็นค่าโดยปริยายสำหรับอุปกรณ์ที่รองรับ pre-RSNA และ Shared key หมายถึง วิธีการพิสูจน์ตัวจริง ด้วยการส่งข้อมูลแลกเปลี่ยนกุญแจของสถานี ผ่านทางช่องสื่อสารที่มีความปลอดภัย ขึ้นอยู่กับการเลือกใช้เทคโนโลยีเข้ารหัสในมาตรฐาน IEEE802.11 การพิสูจน์ตัวจริงสำหรับ pre-RSNA ยังคงทับซ้อนกับการเข้ารหัสข้อมูลซึ่งไม่ได้เกิดประโยชน์ในด้านความปลอดภัย ดังนั้น Share Key จึงถูก

กำหนดขึ้นเพื่อให้รองรับกับเทคโนโลยีเดิม โดยที่ระบบความปลอดภัยแบบใหม่ได้รับคำแนะนำให้ใช้ Open System

การเข้ารหัสข้อมูลของ pre-RSNA ได้เสนอรูปแบบเข้ารหัสแบบเดียวกับมาตรฐาน IEEE802.11-1999 ด้วยการใช้วิธีเข้ารหัสตามแบบ Stream Cipher ด้วยเทคนิค RC4

RSNA (Robust Security Network Association) ได้เสนอวิธีสื่อสารที่ปลอดภัยสูงกว่า pre-RSNA ด้วยการนำเทคโนโลยี WPA และ WPA2 มารวมกลุ่มแล้วเสนอเทคโนโลยี 2 เทคโนโลยีหลักประกอบด้วย TKIP (Temporal Key Integrity Protocol) ซึ่งอ้างอิงจาก WPA และ CCMP (CTR with CBC-MAC Protocol) ซึ่งอ้างอิงจาก WPA2 โดยที่ TKIP ยังคงรองรับเทคโนโลยีเก่าซึ่งใช้งาน WEP แต่ได้ทำการปรับปรุงให้มีความปลอดภัยที่สูงขึ้นด้วยการปรับเปลี่ยนวิธีส่งค่า IV แต่สำหรับ CCMP ได้เสนอเทคโนโลยีเข้ารหัสด้วยการเข้ารหัสแบบ Blocking Cipher โดยเลือกใช้เทคโนโลยี AES (Advanced Encryption Standard)

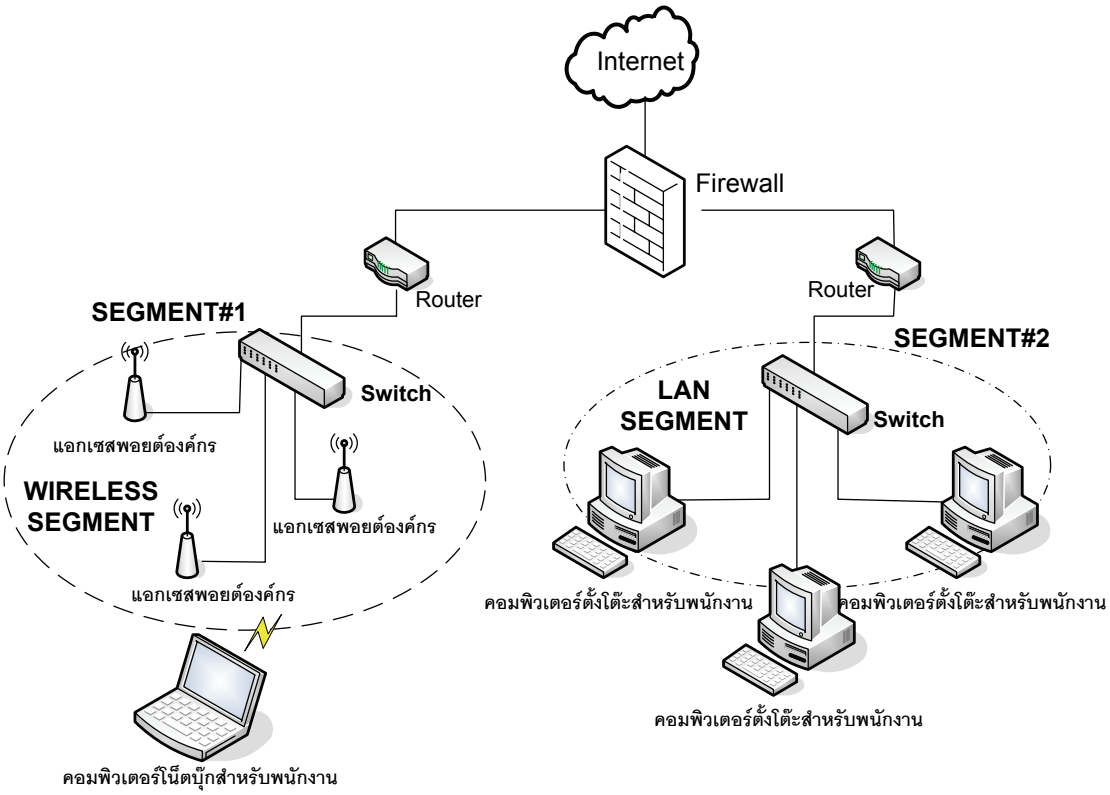
TKIP ออกแบบเพื่อให้รองรับอุปกรณ์เก่าที่ยังไม่มีความสามารถในการประมวลผลการเข้ารหัสแบบ AES วิธีการนี้ได้ปรับปรุงปัญหาที่เกิดกับ WEP ซึ่งยังคงใช้งาน RC4 ในการเข้ารหัส โดยเลือกการยืนยันตัวตนแบบ Open System เพื่อให้รองรับเทคโนโลยีเก่า สำหรับอุปกรณ์ที่รองรับ RSN ไม่จำเป็นต้องรองรับการทำงาน TKIP

CCMP ออกแบบเพื่อให้ใช้เป็นเทคโนโลยีการเข้ารหัสหลักของ RSNA ด้วยการเลือกใช้ AES ซึ่งเป็นวิธีเข้ารหัสแบบ Block Cipher เพื่อทำการเข้ารหัสข้อมูล สำหรับอุปกรณ์ที่รองรับการทำงานแบบ RSN จำเป็นต้องรองรับการใช้งาน CCMP

4. โครงสร้างเครือข่ายสำหรับองค์กรที่ต้องการความปลอดภัยในการสื่อสาร

การออกแบบระบบเครือข่าย ที่ต้องการใช้งานเครือข่ายแลนไร้สายและเครือข่ายแลนร่วมกัน เพื่อให้เกิดความปลอดภัยในการสื่อสารควรแยกเส้นทางข้อมูลทั้งสองออกจากกันมีลักษณะดังภาพที่ 7 ในกรณีที่ในชั้นหรืออาคารมีสวิตช์เพียงเครื่องเดียว อาจใช้เทคโนโลยีแลนเสมือน หรือหากมีสวิตช์เพียงพอ สามารถใช้วิธีการแยกกลุ่มข้อมูลจากกันโดยชัดเจนด้วยสวิตช์ เพื่อประโยชน์ในการบริหารจัดการความปลอดภัยเครือข่าย ซึ่งการแยกเครือข่ายเช่นนี้เป็นที่ยอมรับใช้งานโดยทั่วไป

ประโยชน์จากการแยกเส้นทางข้อมูลในด้านการบริหารจัดการเครือข่าย ได้แก่ การจัดลำดับความสำคัญข้อมูลจากที่มาของข้อมูล เพื่อ นำไปสู่การกำหนดใช้นโยบายความปลอดภัยที่เหมาะสม ดังนั้นข้อกำหนดขั้นต่ำสำหรับองค์กรที่มีความต้องการในการสื่อสารอย่างปลอดภัยควรออกแบบระบบเครือข่ายในองค์กรให้มีลักษณะดังภาพที่ 7 จากภาพที่ 7 ระบบจะทำงานถูกต้องก็ต่อเมื่ออุปกรณ์ในเครือข่ายได้อยู่ในกลุ่มเครือข่าย (SEGMENT) ที่ตรงตามหน้าที่ของอุปกรณ์นั้น ๆ แต่การใช้งานในความเป็นจริงไม่อาจป้องกันการลักลอบนำอุปกรณ์แอกเซสพอยต์ติดตั้งที่เครือข่ายแลน (SEGMENT#2)ได้ มีความเป็นไปได้ที่พนักงานในองค์กรนำแอกเซสพอยต์ไปเชื่อมกับเครือข่ายแลน ผลจากการติดตั้งแอกเซสพอยต์โดยไม่ได้รับอนุญาตทำให้ข้อมูลในเครือข่ายแลนมิได้ส่งผ่านสายนำสัญญาณเท่านั้นแต่ข้อมูลกลับถูกส่งออกในอากาศ และทำให้ข้อมูลที่ส่งผ่านแอกเซสพอยต์ที่ติดตั้งโดยไม่ได้รับอนุญาตผ่านแนวป้องกันของไฟร์วอลล์ซึ่งถูกออกแบบให้ป้องกันข้อมูลที่ส่งในสายสัญญาณได้โดยสะดวก การติดตั้งแอกเซสพอยต์โดยไม่ได้รับอนุญาตจึงทำลายความปลอดภัยขององค์กรในทันที นอกจากกรณีที่ยกตัวอย่างไปแล้ว แอกเซสพอยต์สามารถเกิดขึ้นในเครือข่ายได้หลายตำแหน่ง เช่น ในกรณีที่แอกเซสพอยต์เถื่อนที่เกิดจากผู้บุกรุกที่อยู่ภายนอกองค์กรทำการติดตั้งแอกเซสพอยต์ขึ้น ซึ่งจะกล่าวถึงรายละเอียดในหัวข้อต่อไป



ภาพที่ 7 โครงสร้างเครือข่ายแบบปกติ

5. แอกเซสพอยต์เถื่อน

แอกเซสพอยต์เถื่อน ในวิทยานิพนธ์นี้มีความหมายเดียวกับ แอกเซสพอยต์ที่เกิดจากการติดตั้งโดยไม่ได้รับอนุญาต ซึ่งใช้อ้างถึงแอกเซสพอยต์ที่อยู่ภายในคำจำกัดความของแอกเซสพอยต์เถื่อนที่ได้อธิบายไว้ในหัวข้อวิธีการ และเพื่อให้เกิดความเข้าใจภัยคุกคามที่เกิดจากแอกเซสพอยต์เถื่อน ในหัวข้อต่อไปนี้ได้กล่าวถึง จุดเชื่อมต่อของแอกเซสพอยต์ในรูปแบบต่าง ที่สามารถเกิดขึ้นได้ภายในองค์กร

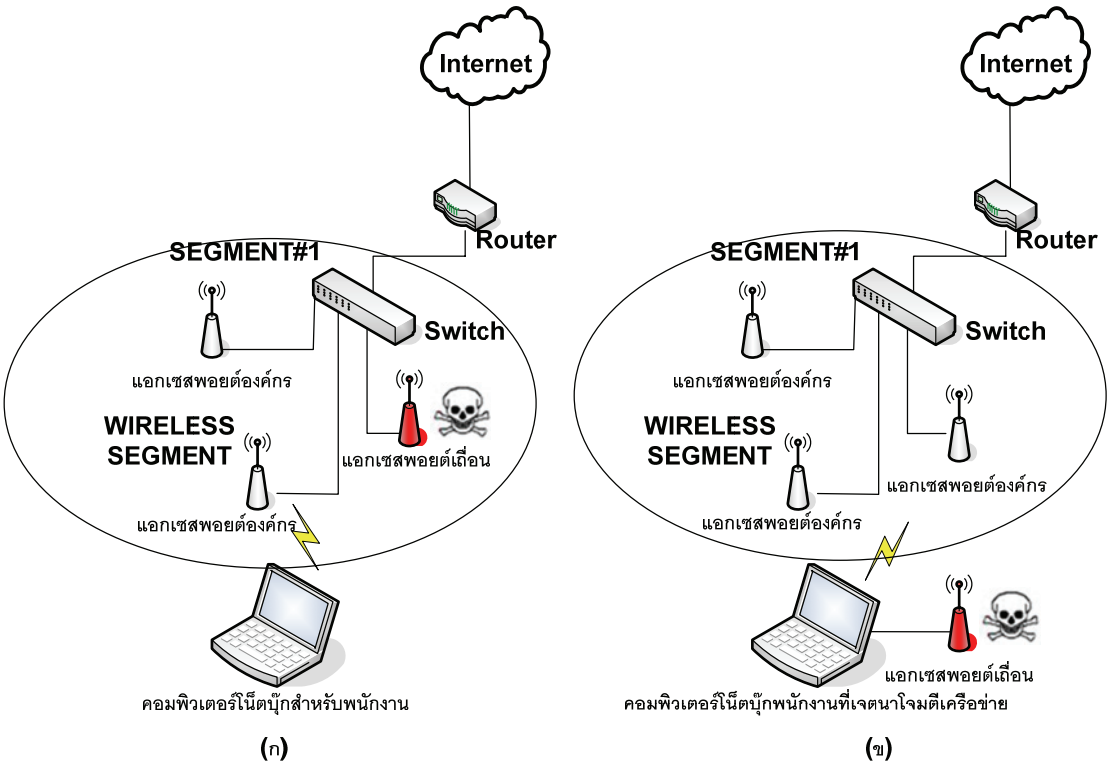
5.1 การเกิดแอกเซสพอยต์เถื่อนในตำแหน่งที่ข้อมูลส่งผ่านเครือข่ายแลนไร้สายขององค์กร

การโจมตีลักษณะนี้เกิดจากการติดตั้งแอกเซสพอยต์ในสวิตช์ที่อยู่ในเครือข่ายแลนไร้สาย ปกติแล้วมีโอกาสเกิดขึ้นได้ยากเพราะสวิตช์ที่ใช้สำหรับเครือข่ายแลนไร้สายถูกเก็บไว้ที่ห้องควบคุมและได้รับการกำหนดพอร์ตเฉพาะสำหรับแอกเซสพอยต์ ส่วนมากพบการโจมตีในลักษณะนี้จากกรณีที่แอกเซสพอยต์ขององค์กรเกิดชำรุด และ ถูกถอด โดยทิ้งสายสัญญาณไว้ในจุดที่ผู้บุกรุกสามารถเข้าถึงได้ง่าย การโจมตีจึงเกิดขึ้นจากการนำแอกเซสพอยต์ไปเชื่อมต่อกับสายสัญญาณดังกล่าวโดยมากเกิดขึ้นจากพนักงานภายในที่มีสิทธิเข้าถึงอุปกรณ์เป็นผู้นำแอกเซสพอยต์มาติดตั้งติดตั้ง ถึงแม้ว่าวิธีนี้ทำได้ยาก แต่สามารถเกิดขึ้นได้หากไม่มีการป้องกันที่ดีพอ ความเสียหายที่เกิดขึ้นนี้ทำให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าใช้เครือข่ายแลนไร้สายโดยไม่ผ่านการตรวจสอบ และหากแอกเซสพอยต์ดังกล่าวเกิดจากการติดตั้งของผู้บุกรุกที่มีความชำนาญทำการตั้งค่าแอกเซสพอยต์เพื่อหลีกเลี่ยงการตรวจจับ เช่น การซ่อนชื่อเครือข่าย การปลอมแปลงข้อมูล เป็นต้น จะทำให้การตรวจจับทำได้ยากยิ่งขึ้น การโจมตีลักษณะนี้แสดงไว้ในภาพที่ 8 (ก)

การโจมตีด้วยแอกเซสพอยต์ผ่านทางเครือข่ายแลนไร้สายภายในองค์กรยังสามารถเกิดขึ้นจากผู้บุกรุกที่เป็นพนักงานภายในองค์กรเป็นผู้ที่ได้รับสิทธิใช้งานเครือข่ายแลนไร้สายและมีเจตนาบุกรุกด้วยการตั้งแอกเซสพอยต์กระจายสัญญาณต่อ ดังแสดงในภาพที่ 8ข การโจมตีในลักษณะนี้จำเป็นต้องใช้ความรู้และทักษะการตั้งค่าเครือข่ายเพื่อใช้ในการเชื่อมต่อและปล่อยข้อมูลกระจายสู่แอกเซสพอยต์ของตน การโจมตีลักษณะนี้ย่อมมีเจตนาที่ไม่ดีดังนั้นจึงสามารถสร้างความเสียหายได้สูง หากข้อมูลถูกส่งผ่านเครื่องของผู้โจมตี ข้อมูลนั้นสามารถปลอมแปลง หรือ ดักข้อมูลได้ ภาพที่ 8ข แสดงลักษณะการเชื่อมเครือข่ายที่ผู้บุกรุกซึ่งเป็นพนักงานภายในที่ได้รับสิทธิใช้งานเครือข่ายแลนไร้สายเป็นผู้บุกรุกเครือข่ายเสียเอง

5.2 การเกิดแอกเซสพอยต์เถื่อนในตำแหน่งที่ข้อมูลส่งผ่านเครือข่ายแลนขององค์กร

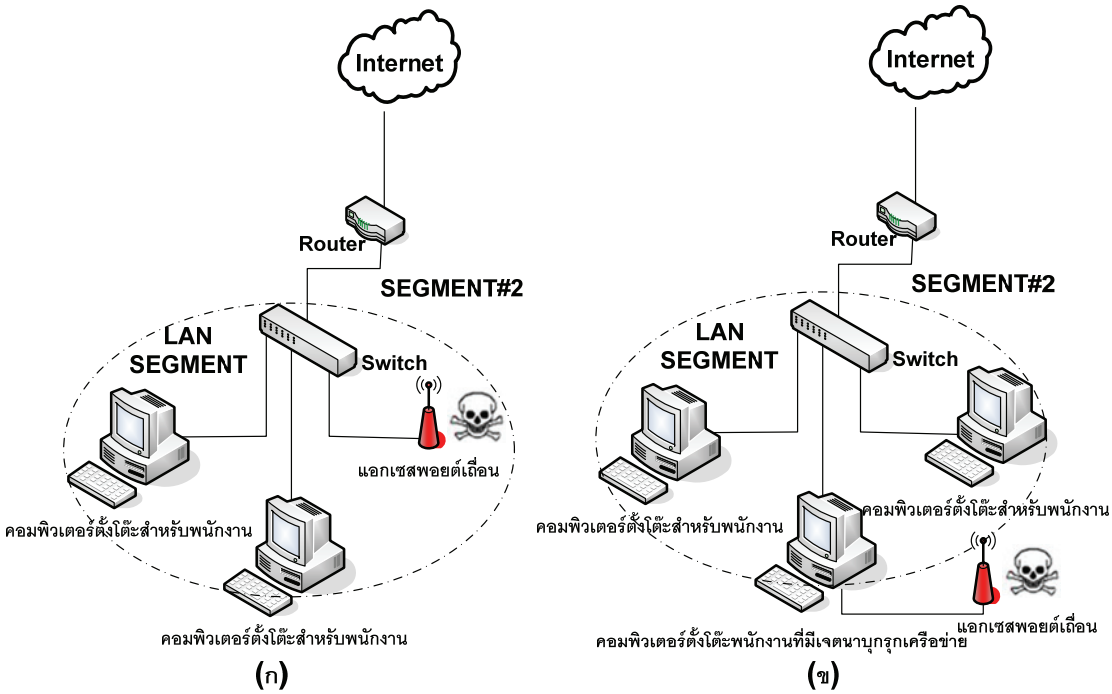
การติดตั้งแอกเซสพอยต์ที่สร้างความเสียหายให้แก่องค์กรได้สูงสุดเกิดจากการติดตั้งแอกเซสพอยต์ที่ไม่ได้รับอนุญาตบนเครือข่ายแลน ข้อมูลที่สื่อสารในเครือข่ายแลนถือได้ว่าเป็นข้อมูลที่ได้รับความไว้วางใจเพราะข้อมูลถูกกำหนดให้ส่งผ่านทางสายสัญญาณเท่านั้นดังนั้นผู้ดูแลเครือข่ายจึงกำหนดให้เครื่องแม่ข่ายที่ให้บริการแก่พนักงาน ถูกติดตั้งในเครือข่ายแลน และพนักงานทุกคนมีสิทธิเข้าใช้เครื่องแม่ข่ายดังกล่าวผ่านทางสายแลน แต่ทั้งนี้แอกเซสพอยต์สามารถติดตั้งได้ง่าย ทำให้พนักงานที่ต้องการความสะดวกแต่ละเลยด้านความปลอดภัยนำแอกเซสพอยต์ไปแทนที่เครื่องคอมพิวเตอร์ของตนเพื่อใช้กระจายสัญญาณในแบบคลื่นวิทยุ ทำให้เกิดช่องโหว่ให้ผู้บุกรุกเข้าโจมตีเครือข่ายแลนขององค์กร การโจมตีผ่านแอกเซสพอยต์ที่ไม่ได้รับการตั้งค่าความปลอดภัยตามนโยบายขององค์กรทำได้ง่ายกว่าการโจมตีผ่านอุปกรณ์ความปลอดภัยของเครือข่ายแลน ภาพที่ 9 แสดงถึงลักษณะการเชื่อมต่อของแอกเซสพอยต์ในเครือข่ายแลนขององค์กรในรูปแบบต่าง ๆ การเชื่อมแอกเซสพอยต์เข้ากับเครือข่ายแลนดังภาพที่ 9ก



ภาพที่ 8 การติดตั้งแอกเซสพอยต์เถื่อนบนเครือข่ายแลนไร้สายในองค์กร

หากเกิดจากการติดตั้งของพนักงานที่ไม่ตระหนักถึงความปลอดภัยในการสื่อสารข้อมูลภายในองค์กร และไม่ทราบถึงผลเสียหายที่ตามมาจากการติดตั้งแอกเซสพอยต์โดยที่ผู้ดูแลเครือข่าย

ไม่ทราบ ทำการติดตั้งโดยไม่ได้ตั้งค่าความปลอดภัยที่เพียงพอ สามารถสร้างความเสียหายได้สูงสุด เพราะเป็นการเปิดช่องให้ผู้บุกรุกเข้าโจมตีเครือข่ายแลนโดยไม่ผ่านการตรวจสอบ



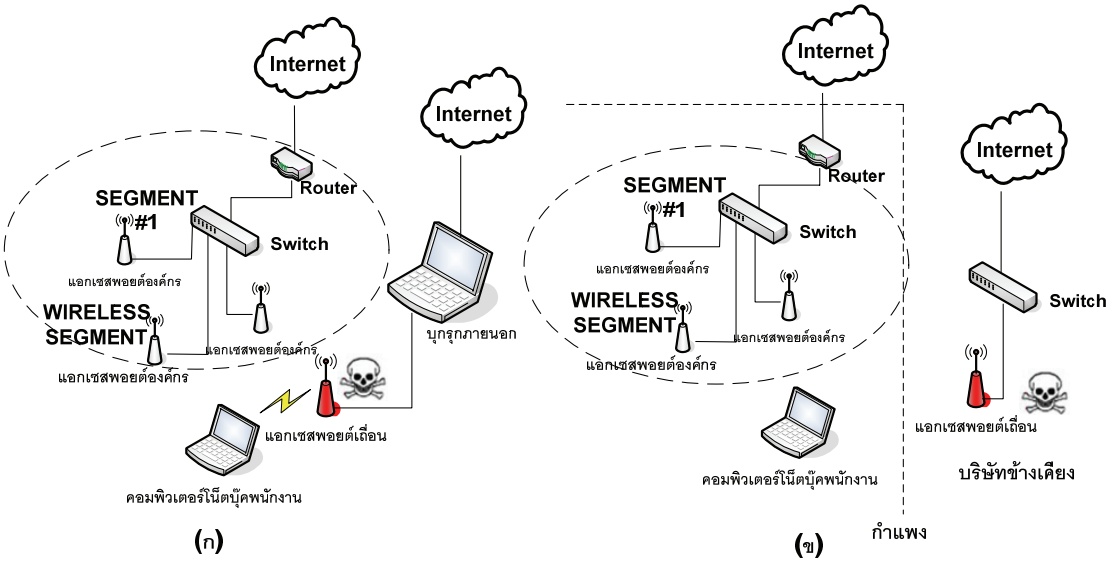
ภาพที่ 9 ติดตั้งแอกเซสพอยต์เถื่อนบนสวิตช์ของเครือข่ายแลน

ในการเชื่อมอุปกรณ์ตามภาพที่ 9ข เกิดจากพนักงานเป็นผู้บุกรุกเสียเอง การโจมตีในรูปแบบนี้เกิดจากพนักงานมีเจตนาเพื่อบุกรุกเครือข่าย ด้วยการปลอมแปลงข้อมูลแอกเซสพอยต์ของตนให้คล้ายกับแอกเซสพอยต์ขององค์กร เพื่อกระทำการใด ๆ ที่ส่งผลเสียหายแก่องค์กร เป้าหมายการโจมตีลักษณะนี้เพื่อดักจับข้อมูล หรือ หลอกลวง หากองค์กรได้ตั้งค่าความปลอดภัยเครือข่ายแลนไร้สายด้วยเทคโนโลยีความปลอดภัยที่ออกแบบสำหรับองค์กร เช่น การใช้เทคโนโลยี WPA-Enterprise หรือ WPA2-Enterprise สามารถป้องกันการโจมตีในลักษณะนี้ได้

5.3 การเกิดแอกเซสพอยต์เถื่อนในตำแหน่งที่ข้อมูลส่งผ่านเครือข่ายภายนอกองค์กร

แอกเซสพอยต์เถื่อนที่ตรงตามหัวข้อนี้ได้แก่ แอกเซสพอยต์ที่ไม่ได้ทำการเชื่อมเครือข่ายองค์กร แต่ส่งสัญญาณในรูปแบบคลื่นวิทยุมายังองค์กร สัญญาณเครือข่ายไร้สายนี้มีโอกาสเกิดจากเครือข่ายไร้สายใกล้เคียง หรือ เกิดจากผู้ที่มีเจตนาบุกรุกเครือข่าย หากเกิดจากผู้ที่มีเจตนาบุกรุกเครือข่ายอาจเป็นช่องทางผู้บุกรุกสามารถดัดแปลง ปลอมแปลงข้อมูลเพื่อทำให้เครื่องเป้าหมาย

หลงเชื่อ ภาพที่ 10ก แสดงถึงตัวอย่างลักษณะการโจมตีที่เกิดจากผู้บุกรุกที่ไม่ใช่พนักงาน ทำการตั้งค่าแอกเซสพอยต์ให้คล้ายกับเครือข่ายแลนไร้สายขององค์กรเพื่อทำให้พนักงานในองค์กรหลงเชื่อแล้วเชื่อมเข้าสู่เครือข่ายของตน การโจมตีลักษณะนี้จำเป็นต้องใช้ความรู้และทักษะการสร้างเครือข่ายแลนไร้สายและการปลอมแปลงข้อมูล ความเสียหายที่เกิดขึ้นเทียบเท่ากับการดักฟังข้อมูลความลับและการหลอกลวง ซึ่งสามารถป้องกันได้จากการใช้เทคโนโลยีความปลอดภัยในการสื่อสารผ่านเครือข่ายแลนไร้สายสำหรับองค์กร เช่น WPA-Enterprise, WPA2-Enterprise เทคโนโลยีเหล่านี้มีคุณสมบัติในด้านการพิสูจน์ตัวจริงของทั้งสองด้าน ได้แก่การพิสูจน์ตัวจริงของเครือข่ายไร้สายเพื่อให้พนักงานเชื่อใจ และ การพิสูจน์ตัวจริงของพนักงานเพื่อให้เครือข่ายไร้สายอนุญาตสิทธิการเข้าใช้



ภาพที่ 10 การติดตั้งแอกเซสพอยต์จากเครือข่ายผู้บุกรุก และ เครือข่ายใกล้เคียง

สำหรับการโจมตีจากแอกเซสพอยต์ในเครือข่ายภายนอก ดังที่แสดงในภาพที่ 10ข เกิดจากแอกเซสพอยต์จากองค์กรอื่นที่อยู่ใกล้เคียงได้ปล่อยสัญญาณเครือข่ายแลนไร้สายผ่านกำแพงเข้ามาถึงเครือข่ายแลนไร้สายในองค์กร แอกเซสพอยต์ที่เกิดขึ้นในลักษณะนี้มักเกิดในที่ซึ่งมีรูปแบบการจัดหน่วยงานให้มีองค์กรติดกันโดยกั้นด้วยกำแพง แอกเซสพอยต์ลักษณะนี้เกิดจากการกระจายสัญญาณจากแอกเซสพอยต์ภายนอกซึ่งมีความแรงของสัญญาณสูง ความเสียหายที่เกิดขึ้นทำให้มีสัญญาณรบกวนซึ่งหากติดตั้งช่องสัญญาณที่ตรงกันจะทำให้เกิดการรบกวนของสัญญาณแต่ยังไม่สร้างความเสียหายที่ร้ายแรง

6. เครื่องมือที่เกี่ยวข้องกับงานวิจัย

6.1 โปรแกรมช่วยควบคุมอุปกรณ์แบบอัตโนมัติ

โปรแกรม Expect (Libes., 2006) ได้รับการพัฒนาให้มีหน้าที่รับ-ตอบคำสั่งแบบอัตโนมัติ ผ่านโพรโทคอลที่ได้รับความนิยมในการใช้ควบคุมอุปกรณ์ในเครือข่ายแบบระยะไกล โดยมากนิยมใช้กับระบบปฏิบัติการคล้ายยูนิกซ์ เช่น ลินุกซ์ ฟรีบีเอสดี โอเพ่นบีเอสดี เป็นต้น โปรแกรมนี้ถูกนำไปใช้ประยุกต์เพื่อควบคุมอุปกรณ์ในเครือข่ายที่รองรับการทำงานแบบควบคุมระยะไกลผ่านทางโพรโทคอล telnet หรือ ssh เช่น สวิตช์ แอกเซสพอยต์ เราท์เตอร์ หรือ เครื่องแม่ข่าย เป็นต้น

วิธีใช้งานโปรแกรม Expect สามารถใช้โปรแกรมชื่อ autoexpect ซึ่งโปรแกรมนี้ถูกติดตั้งมาพร้อมกับโปรแกรม Expect ทำการบันทึกชุดคำสั่งในครั้งแรกเพียงครั้งเดียว หลังจากนั้นเมื่อนำไปใช้งานระบบจะทำคำสั่งเช่นเดียวกับที่บันทึกเอาไว้ในครั้งแรก ภาพที่ 11 แสดงถึงตัวอย่างลำดับชุดคำสั่งเพื่อใช้ควบคุมแอกเซสพอยต์ซิสโก้ รุ่น AP1121 รายละเอียดคำสั่งเหล่านี้พบได้จากคู่มือของอุปกรณ์ ตัวอย่าง ในภาพที่ 12 แสดงให้เห็นถึงการควบคุมแอกเซสพอยต์ผ่านทางการสื่อสารเทลเน็ตในรูปแบบปกติ โปรแกรม Expect นี้มีประโยชน์ช่วยลดการป้อนคำสั่งด้วยมือเปลี่ยนเป็นการตอบสนองต่อคำสั่งจากข้อมูลที่เคยบันทึกไว้แล้ว

```
1   telnet 172.16.0.1
2   admin
3   password
4   config terminal
5   int dot11Radio 0
6   station-role scanner
7   monitor frames endpoint ip address 172.16.0.1 port 5222 truncate
    128
8   channel 1
9   channel 6
10  channel 11
11  exit
12  exit
13  reload
14  no
15  yes
```

ภาพที่ 11 ตัวอย่างชุดคำสั่งควบคุมแอกเซสพอยต์ให้ดักจับข้อมูลไร้สาย

จากภาพที่ 11 รายชื่อคำสั่งนั้นหมายถึงคำสั่งที่ผู้ควบคุมจะต้องป้อนด้วยตนเองทุกครั้งเมื่อต้องการสั่งให้แอกเซสพอยต์เปลี่ยนสถานะเป็นอุปกรณ์ดักฟังข้อมูลไร้สาย โดยที่ภาพที่ 12 แสดงถึงการใช้โปรแกรมอรรถประโยชน์ โปรแกรมอรรถประโยชน์ทำหน้าที่ช่วยในการบันทึกคำสั่ง ในรูปแบบภาษา Expect จากภาพที่ 12 แสดงถึง คำสั่งที่ผู้ควบคุมป้อนด้วยตนเองผ่านทางแป้นพิมพ์เพื่อสั่งงานแอกเซสพอยต์เปลี่ยนสถานะให้ดักจับข้อมูลไร้สาย โดยมีคำสั่งเปลี่ยนช่องสัญญาณที่ต้องการรับฟังตั้งแต่ช่องสัญญาณหมายเลข 1 ไปจนกระทั้งช่องสัญญาณหมายเลข 11 คำสั่งเหล่านี้ได้รับการสั่งงานในลักษณะพิมพ์ข้อมูลจากผู้ดูแลเครือข่าย และเมื่อต้องการให้มีการจดจำคำสั่งและนำชุดคำสั่งนั้นกลับมาทำงานใหม่ในรูปแบบอัตโนมัติสามารถทำได้จากการใช้คำสั่ง autoexpect เพื่อทำการบันทึกชุดคำสั่ง ดังแสดงไว้ในภาพที่ 13

ภาพที่ 13 ได้แสดงถึงวิธีการใช้งาน autoexpect ผลจากการทำงานจะทำให้ได้ไฟล์ในรูปแบบแฟ้มข้อความสามารถอ่านรู้เรื่องโดยบันทึกในไฟล์ที่ชื่อ script.exp ภายในไฟล์ที่ได้จากการใช้โปรแกรม auotoexpect ได้รวบรวมชุดคำสั่งทั้งหมดที่จำเป็นเพื่อควบคุมแอกเซสพอยต์ให้เปลี่ยนสถานะในการดักจับข้อมูลไร้สาย หลังจากนี้เมื่อต้องการให้แอกเซสพอยต์ดักจับข้อมูลก็สามารถเรียกคำสั่งนี้ได้ทันที โดยโปรแกรมจะทำหน้าที่สั่งให้โดยอัตโนมัติ ตัวอย่างการใช้งานแสดงในภาพที่ 15

```
1   rds@rds:~$ telnet 172.16.1.44
    Trying 172.16.1.44...
    Escape character is '^]'.
    User Access Verification
2   Username: admin
3   Password: *****
4   APFL4-4_CH01#config terminal
    Enter configuration commands, one per line.  End with CNTL/Z.
5   APFL4-4_CH01(config)#int dot11Radio 0
6   APFL4-4_CH01(config-if)#station-role scanner
7   APFL4-4_CH01(config-if)#monitor frames endpoint ip address
    172.16.0.1 port 5222 truncate 128
8   APFL4-4_CH01(config-if)#channel 1
9   APFL4-4_CH01(config-if)#channel 6
10  APFL4-4_CH01(config-if)#channel 11
11  APFL4-4_CH01(config-if)#exit
12  APFL4-4_CH01(config)#exit
13  APFL4-4_CH01#reload
14  System configuration has been modified. Save? [yes/no]: no
15  Proceed with reload? [confirm]yes
```

ภาพที่ 12 คำสั่งอย่างควบคุมแอกเซสพอยต์ระยะไกลผ่านทางเทลเน็ต

ตัวอักษร (expect script.exp) ที่แสดงในภาพที่ 15 แสดงถึงคำสั่งเพียงคำสั่งเดียวที่ผู้ควบคุมป้อนเพื่อสั่งงานให้แอกเซสพอยต์เปลี่ยนสถานะเป็นอุปกรณ์ดักฟังข้อมูลหลังจากสั่งงานโปรแกรมจะทำการป้อนคำสั่งให้ในแบบอัตโนมัติ ซึ่งแตกต่างจากภาพที่ 11 เห็นได้ว่าการใช้งานโปรแกรม Expect ช่วยลดภาระงานของผู้ควบคุมได้เป็นอย่างมาก

```
1   rds@rds:~$ autoexpect telnet 172.16.1.44
    Trying 172.16.1.44...
    Connected to 172.16.1.44.
    Escape character is '^]'.

    User Access Verification
2   Username: admin
3   Password: *****
4   APFL4-4_CH01#config terminal
    Enter configuration commands, one per line.  End with CNTL/Z.
5   APFL4-4_CH01(config)#int dot11Radio 0
6   APFL4-4_CH01(config-if)#station-role scanner
7   APFL4-4_CH01(config-if)#monitor frames endpoint ip address
    172.16.0.1 port 5222 truncate 128
8   APFL4-4_CH01(config-if)#channel 1
9   APFL4-4_CH01(config-if)#channel 6
10  APFL4-4_CH01(config-if)#channel 11
11  APFL4-4_CH01(config-if)#exit
12  APFL4-4_CH01(config)#exit
13  APFL4-4_CH01#reload
14  System configuration has been modified. Save? [yes/no]: no
15  Proceed with reload? [confirm]yes
```

ภาพที่ 13 ตัวอย่างการใช้โปรแกรมอรรถประโยชน์

```
1   #!/usr/bin/expect -f
2
3   set force_conservative 0  ;
4
5   if {$force_conservative} {
6           set send_slow {1 .1}
7           proc send {ignore arg} {
8                   sleep .1
9                   exp_send -s -- $arg
10          }
11  }
12  set timeout -1
```

ภาพที่ 14 ชุดคำสั่งที่ได้หลังจากการสร้างไฟล์อัตโนมัติของ autoexpect

```
13  spawn telnet 172.16.1.44
14  match_max 100000
15  expect -exact "Trying 172.16.1.44...\r
16  Connected to 172.16.1.44.\r
17  Escape character is '^\]'.\r
18  \r
19  \r
20  User Access Verification\r
21  \r
22  Username: "
23  send -- "admin\r"
24  expect -exact "admin\r
```

ภาพที่ 14 (ต่อ)

```
1   rds@rds:~$ expect script.exp
2   Username: admin
3   Password:
4   APFL4-4_CH01#config terminal
    Enter configuration commands, one per line.  End with CNTL/Z.
5   APFL4-4_CH01(config)#int dot11Radio 0
6   APFL4-4_CH01(config-if)#station-role scanner
7   APFL4-4_CH01(config-if)#monitor frames endpoint ip address
    172.16.0.1 port 5222 truncate 128
8   APFL4-4_CH01(config-if)#channel 1
9   APFL4-4_CH01(config-if)#channel 6
10  APFL4-4_CH01(config-if)#channel 11
11  APFL4-4_CH01(config-if)#exit
12  APFL4-4_CH01(config)#exit
13  APFL4-4_CH01#reload
14  System configuration has been modified. Save? [yes/no]: no
15  Proceed with reload? [confirm]yes
    Connection closed by foreign host.
```

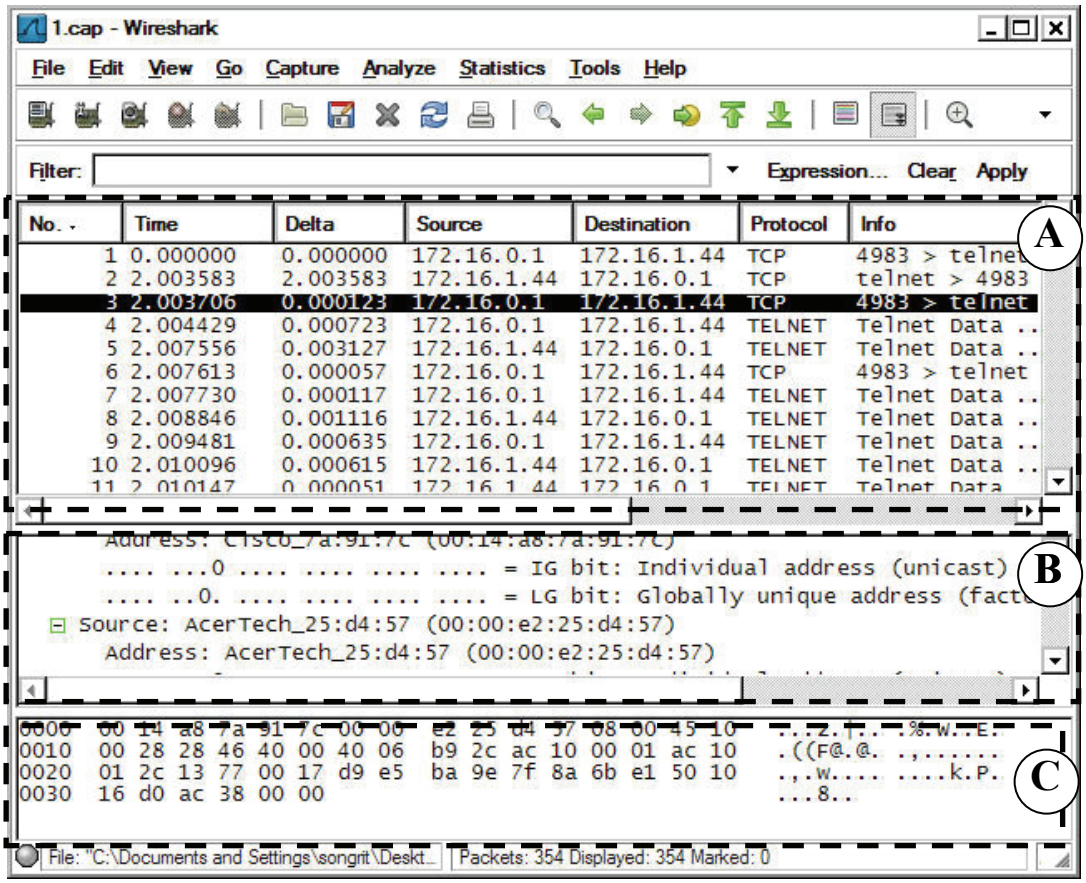
ภาพที่ 15 การเรียกใช้ชุดคำสั่งที่ได้จากการบันทึกด้วยโปรแกรมอรรถประโยชน์

6.2 โปรแกรมวิเคราะห์ข้อมูลเครือข่ายคอมพิวเตอร์

งานวิจัยนี้ได้เลือกโปรแกรม WireShark [network protocol analyzer, http://www.wireshark.org] เพื่อการวิเคราะห์ข้อมูลที่ส่งมาจากแอกเซสพอยต์ และนำไปใช้ในการถอดรหัสข้อมูลของ CWIDS ซึ่งเป็นรูปแบบเฟรมที่ส่งจากแอกเซสพอยต์ โปรแกรม WireShark มีความสามารถในการถอดรหัสข้อมูล เพื่อให้อยู่ในรูปแบบที่เข้าใจง่าย ภาพที่ 16 ได้แสดงถึงหน้า

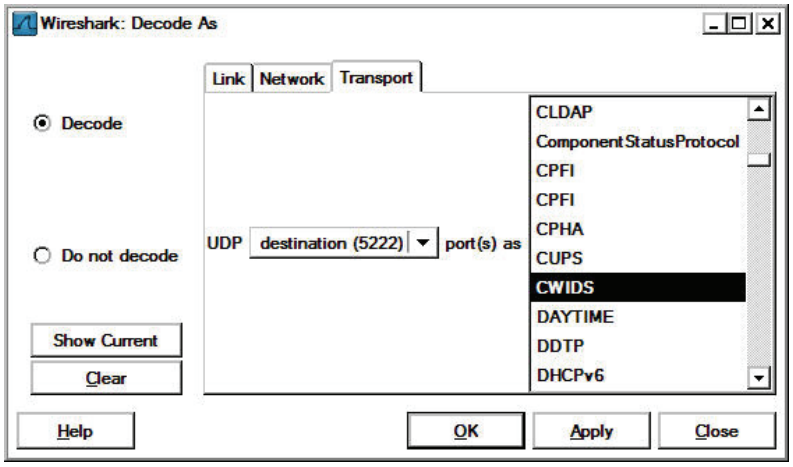
แสดงผลของโปรแกรม WireShark เมื่อทำการสั่งงานให้โปรแกรมทำการดักฟังข้อมูลในเครือข่าย จะทำให้มีข้อมูลแสดงผล และ เพื่อให้อ่านข้อมูลที่ส่งออกจากแอกเซสพอยต์ซิสโก้

จากภาพที่ 16 กรอบ A อธิบายถึงภาพรวมของข้อมูลที่โปรแกรม WireShark ถอดข้อมูลที่ได้รับจากแอกเซสพอยต์ซิสโก้ ซึ่งประกอบด้วย ข้อมูลต้นทาง-ปลายทาง และรายละเอียดวิธีการสื่อสาร เช่น หมายเลขไอพีที่มีการสื่อสาร และ ชนิดโพรโทคอล รวมถึงพอร์ตที่ใช้ติดต่อ กรอบ B อธิบายถึงรายละเอียดของข้อมูลในแต่ละแพ็คเกต ซึ่งภายในได้จัดเรียงข้อมูลตามรูปแบบของโพรโทคอลนั้น ๆ จากภาพที่ 16 แสดงให้เห็นถึงรายละเอียดข้อมูลที่อยู่ภายในเฟรม TCP ซึ่งประกอบด้วยหมายเลขอุปกรณ์เครือข่ายแลนของต้นทางและปลายทาง และ กรอบ C ใช้อธิบายถึงข้อมูลดิบในรูปแบบเลขฐาน 16 ที่ยังไม่ได้ทำการถอดรหัสข้อมูล โดยด้านซ้ายมือใช้อธิบายถึงเลขฐาน 16 และ ด้านขวามือเป็นข้อมูลเลขฐาน 16 ที่ได้รับการถอดรหัสในแบบ ASCII



ภาพที่ 16 โปรแกรมวิเคราะห์ข้อมูลในเครือข่ายคอมพิวเตอร์

ในการทำงานปกติของโปรแกรม WireShark จะไม่ได้ทำการถอดรหัสข้อมูลตามโพรโทคอลที่ได้รับจากแอกเซสพอยต์ ดังนั้น เมื่อต้องการให้โปรแกรม WireShark แสดงผลตามโพรโทคอลจำเป็นต้องทำการสั่งงานด้วยการเปลี่ยนแปลงรูปแบบการถอดโพรโตคอล ให้โปรแกรมทำการถอดข้อมูลที่ได้รับจากแอกเซสพอยต์ซิสโก้เพื่อใช้ในการศึกษาโพรโทคอล สามารถทำได้จากการเลือกเมนู Analyze แล้วเลือก Decode As... หลังจากนั้นเลือก รูปแบบโพรโทคอลในการถอดรหัสชื่อว่า CWIDS ดังแสดงในภาพที่ 17

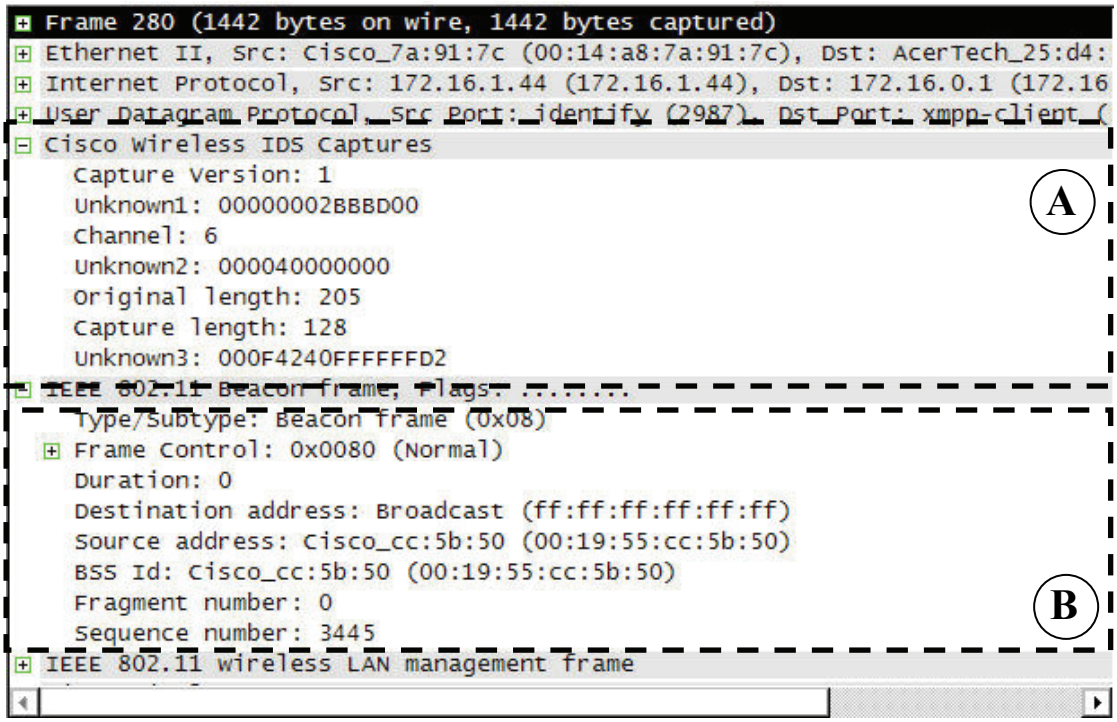


ภาพที่ 17 หน้าต่างการเลือกโพรโทคอล CWIDS ในการถอดรหัส

ภาพที่ 17 ได้อธิบายถึงหน้าต่างของซอฟต์แวร์ WireShark ที่ใช้สำหรับการเลือกโพรโทคอลสำหรับถอดรหัสข้อมูล ซึ่งจำเป็นจะต้องทราบชนิดของโพโทคอลก่อนจึงสามารถเลือกได้ถูกต้อง จากภาพแถบสีดำหมายถึงได้เลือกรูปแบบการถอดโพรโทคอลให้มีรูปแบบข้อมูลตามการจัดเรียงของ CWIDS

จากภาพที่ 18 กรอบ B ได้แสดงถึงข้อมูล Cisco Wireless IDS Captures ซึ่งเป็นข้อมูลที่ได้รับการถอดรหัสหลังจากได้กำหนดให้โปรแกรมทำการถอดรหัสข้อมูลด้วยโพรโทคอล CWIDS ภายในโพรโทคอล CWIDS ประกอบด้วยข้อมูลหลักจำนวน 2 ชุดได้แก่ ข้อมูลส่วนหัวซึ่งเป็นข้อมูลที่สร้างขึ้นจากแอกเซสพอยต์ซึ่งมีขนาดคงที่เท่ากับ 28 ไบต์ และ ข้อมูลส่วนที่เป็นข้อมูลตามมาตรฐาน IEEE802.11 ซึ่งมีขนาดเปลี่ยนแปลงได้ขึ้นอยู่กับชนิดของเฟรมที่ใช้รับส่งของเครือข่ายแลนไร้สายในขณะนั้น เมื่อแอกเซสพอยต์ดักจับข้อมูลในเครือข่ายไร้สายได้จะทำการนำข้อมูลนั้นมาเพิ่มข้อมูลส่วนหัวแล้วนำข้อมูลนั้นรวบรวมไว้ที่บัพเฟอร์ก่อนส่งออกในรูปแบบข้อมูลแบบ UDP ข้อมูลที่ส่งออกจากแอกเซสพอยต์มายังเครื่องแม่ข่ายควบคุมถูกส่งด้วยรูปแบบ UDP สามารถสังเกต

ได้ข้อมูล UDP ในหนึ่งเฟรม สามารถอดออกเป็นข้อมูลที่อยู่ในรูปแบบ CWIDS ได้จำนวนหลายเฟรม ทำให้เข้าใจได้ว่า แอกเซสพอยต์ได้ทำการบันทึกข้อมูลที่ได้รับจากอากาศเก็บรวบรวมข้อมูลไว้ระยะหนึ่งก่อนส่งออก โดยที่เอกสารด้านเทคนิคของแอกเซสพอยต์ไม่ได้ระบุไว้ว่าเก็บรวบรวมไว้นานเท่าใดจึงส่งออก

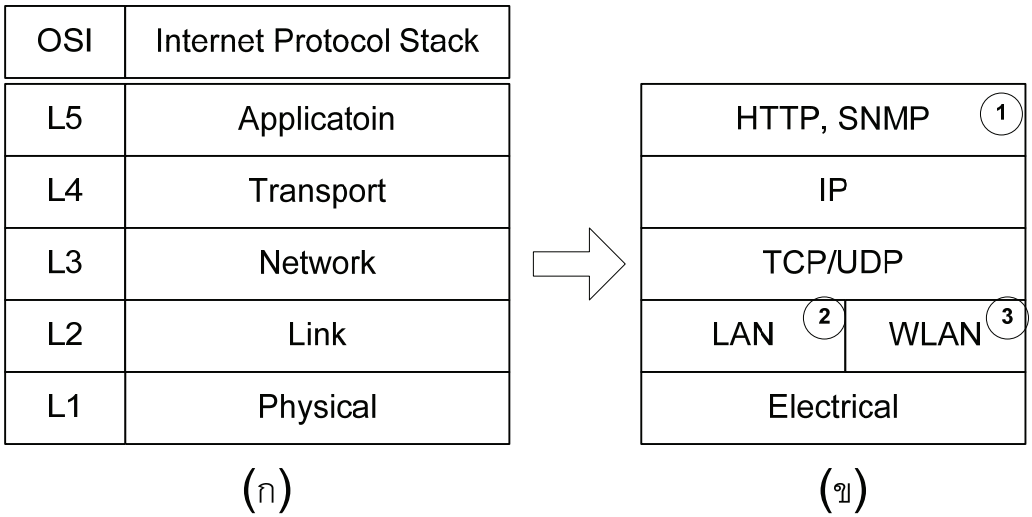


ภาพที่ 18 โปรแกรม WireShark หลังจากถอดรหัสข้อมูลด้วยโพรโทคอล CWIDS

ภาพที่ 18 ในกรอบ A ใช้อธิบายโพรโตคอลในส่วนเฮดเดอร์ของ CWIDS ที่ประกอบด้วยข้อมูล Capture Version , unknown1, Channel, unknown2, Original length, Capture length และ unknown3 โดยหน้าที่การทำงานของแต่ละส่วนได้อธิบายไว้ในหัวข้อต่อไป สังเกตได้ว่ามีข้อมูลบางส่วนที่ยังไม่ได้ทำการถอดรหัส เพราะรูปแบบเฟรมข้อมูลนี้ไม่ได้เผยแพร่จากผู้ผลิต ดังนั้นทีมงาน WireShark จึงได้ทำการแปลและสังเกตการเปลี่ยนแปลงของข้อมูลถึงแม้ว่าข้อมูลไม่ได้รับการแปลครบทั้งหมด แต่ข้อมูลที่มีความจำเป็นสำหรับวิทยานิพนธ์นี้ได้แก่ข้อมูลตามรูปแบบ IEEE802.11 ซึ่งมีการเรียงข้อมูลตามรูปแบบมาตรฐาน ซึ่งได้แสดงไว้ในภาพที่ 18 กรอบ B

งานวิจัยที่เกี่ยวข้อง

งานวิจัยที่เสนอแนวทางการตรวจจับแอกเซสพอยต์เถื่อน สามารถจัดกลุ่มตามลำดับชั้นการสื่อสาร ได้ 3 กลุ่มดังต่อไปนี้ 1) การตรวจจับแอกเซสพอยต์ในชั้นแอพลิเคชั่น 2) การตรวจจับในชั้นแลน 3) การตรวจจับในชั้นแลนไร้สาย ซึ่งแสดงลักษณะการเรียงลำดับตามภาพที่ 18



ภาพที่ 19 ชั้นโพรโทคอล

จากภาพที่ 19กได้แสดงชั้นโพรโทคอล (Protocol stack) ที่เรียงตามลำดับ OSI(Open System Interconnection) และ ชั้นโพรโทคอลอินเตอร์เน็ต (Internet Protocol Stack) ตามลำดับ และภาพที่ 19ข ได้ยกตัวอย่างการใช้งานจริง ในงานวิจัยที่ได้เสนอแนวทางการตรวจจับแอกเซสพอยต์ในเครือข่าย ด้วยการเสนอวิธีการตรวจจับที่สามารถอ้างอิงได้ตาม ชั้นโพรโทคอลภาพที่ 19ข ตามลำดับต่อไปนี้

1. การตรวจจับแอกเซสพอยต์เถื่อนในชั้นแอพลิเคชั่น

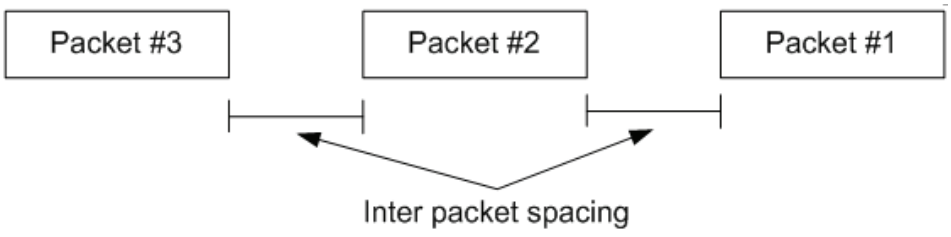
ในการตรวจจับแอกเซสพอยต์เถื่อนด้วยการใช้ข้อมูลในชั้นแอพลิเคชั่น ใช้คุณสมบัติของอุปกรณ์ซึ่งมีการตอบสนองต่อโพรโทคอลที่แตกต่างจากเครื่องคอมพิวเตอร์ทั่วไป เช่น ในภาพที่ 19ข (หมายเลข 1) ใช้การสมมุติฐานว่าแอกเซสพอยต์สามารถตอบสนองต่อการเรียกข้อมูลผ่านทาง HTTP (Hypertext Transfer Protocol) หรือ SNMP (Simple Network Management Protocol) วิธีในการตรวจจับแอกเซสพอยต์เถื่อนลักษณะนี้สามารถประยุกต์ได้จากการศึกษาของ (Wilson, 2003)

ซึ่งได้เสนอวิธีการใช้ซอฟต์แวร์ที่มีความสามารถในการสแกนเครือข่าย เช่น NMAP (Lyon, 1997) ด้วยการคอยส่งคำสั่งสแกนอุปกรณ์ทุกเครื่องที่อยู่ในเครือข่าย ซอฟต์แวร์สแกนเครือข่ายนี้มีความสามารถในการรายงานชนิดของอุปกรณ์ในเครือข่ายจากการวิเคราะห์ข้อมูลที่ได้จากการตอบกลับของอุปกรณ์นั้น ๆ ดังนั้นเมื่อใช้โปรแกรมส่งข้อมูลสุ่มสอบถามหากมีการตอบสนองถือได้ว่าเครื่องนั้นเป็นอุปกรณ์อื่นที่ไม่ใช่คอมพิวเตอร์สำหรับพนักงานที่เปิดขึ้นโดยไม่ได้รับอนุญาต

การตรวจจับแอกเซสพอยต์เถื่อนด้วยเทคนิคนี้สามารถใช้ได้กับแอกเซสพอยต์ที่มีการตอบสนองเท่านั้น ซึ่งจำเป็นต้องทราบล่วงหน้า และ ได้รับการตั้งการให้ตอบกลับเมื่อได้รับการสอบถาม หรือ หากใช้หลักการสุ่มสอบถาม ก็ไม่อาจใช้ได้ผลกับอุปกรณ์ที่ได้รับการตั้งค่าให้ไม่ตอบสนองต่อการสอบถาม

2. การตรวจจับแอกเซสพอยต์เถื่อนในชั้นแลน

ใช้การศึกษาพฤติกรรมการตอบสนองที่แตกต่างกันระหว่างอุปกรณ์แลนไร้สายและแลนมีสาย ช่วยให้ระบุชนิดของอุปกรณ์ที่เชื่อมกับเครือข่ายแลนได้ โดยงานวิจัยเหล่านี้ใช้สมมุติฐานที่แอกเซสพอยต์จะต้องติดตั้งในเครือข่ายแลนเท่านั้น จึงทำให้ข้อมูลที่ส่งผ่านแอกเซสพอยต์วิ่งผ่านเครือข่ายแลนมีสาย การศึกษาของ (Beyah *et al.,* 2004) ได้ใช้ค่า Inter-packet spacing เพื่อแยกชนิดของอุปกรณ์ที่สื่อสารซึ่งผลการทดลองแสดงให้เห็นว่าค่า Inter-packet spacing ของข้อมูลที่มาจากเครือข่ายแลนมากกว่า 80 เปอร์เซนต์ให้ค่าน้อยกว่า 1 ms และค่า Inter-packet time ของข้อมูลที่เดินทางมาจากอุปกรณ์ไร้สายจำนวนมากกว่า 90 เปอร์เซนต์ให้ค่ามากกว่า 1mS สำหรับค่า Inter packet spacing เป็นค่าระยะห่างของการเดินทางแต่ละข้อมูลตัวอย่างของ Inter-packet spacing แสดงในภาพที่ 20 ที่อธิบายถึงข้อมูลจำนวน 3 ชุด โดยที่ packet -1 ถึง packet-3 อธิบายถึงข้อมูลแต่ละชุด และ ระยะห่างของข้อมูลมีค่าเท่ากับ inter-packet spacing



ภาพที่ 20 ตัวอย่างอธิบาย Inter packet spacing

ในงานวิจัยของ (Watkins *et al.*, 2007) ใช้ค่า RTT (Round-Trip Time) ของ TCP (Transmission Control Protocol) ซึ่งให้ผลการทดลองที่สอดคล้องกับการศึกษาของ (Beyah *et al.*, 2004) โดยใช้การทดลองและเปรียบเทียบทางสถิติด้วยส่วนเบี่ยงเบนมาตรฐานและ การแจกแจงสะสม (CDF: Cumulative Distribution Function) เพื่อใช้ระบุความแตกต่างระหว่างอุปกรณ์สื่อสารสำหรับแลนมีสาย และ อุปกรณ์สื่อสารสำหรับแลนไร้สาย นอกจากนี้ได้มีงานวิจัยที่เสนอแนวทางการสร้างชุดข้อมูลขึ้นมาเองเพื่อช่วยให้การระบุถูกต้องมากขึ้น งานวิจัยที่อยู่ในกลุ่มนี้เช่น (Chad *et al.,* 2008) เสนอวิธีการใช้ค่า Local Round Trip Time ร่วมกับ Packet Slicing โดยที่ค่า Local Round Trip Time เกิดจากการทดสอบส่งข้อมูลภายในเครื่องทดสอบ โดยเครื่องนั้นมีการ์ดเครือข่ายจำนวน 2 ใบ อาจเป็นการ์ดเครือข่ายแลน และ การ์ดเครือข่ายแลนไร้สาย โดยใช้การทดสอบค่า Round Trip Time ระหว่างแต่ละการ์ด ผลที่ได้นำไปใช้เป็นประโยชน์ในการประเมินการเดินทางของข้อมูลที่มีการใช้การ์ดเครือข่ายแตกต่างกันได้ ด้วยวิธีที่คล้ายกันในงานวิจัยของ (Wei *et al.,* 2007) ใช้ TCP ACK-Pairs ซึ่งเป็นค่า Round Trip Time ชนิดหนึ่งของ TCP เพื่อใช้ระบุแอกเซสพอยต์ในเครือข่ายแลนโดยที่งานวิจัยนี้เสนอแนวทางตรวจจับ 2 รูปแบบที่ใช้ค่า TCPACK-Pairs เหมือนกัน แต่แตกต่างกันที่มีการฝึกให้ระบบเรียนรู้ และ ไม่มีการฝึกให้ระบบเรียนรู้ จากการทดลองสำหรับระบบที่ได้รับการฝึกสามารถระบุแอกเซสพอยต์ได้ถูกต้องภายในเวลาที่น้อยกว่า 10 วินาทีโดยมีค่า false positive และ false negative ที่ต่ำมาก สำหรับระบบที่ไม่ได้รับการฝึกสามารถระบุแอกเซสพอยต์ได้ถูกต้อง 60 - 76 เปอร์เซนต์โดยปราศจาก false positive

นอกจากนี้ยังมีงานวิจัยอื่น ๆ ที่ใช้ข้อมูลจากเครือข่ายแลนเพียงอย่างเดียว ดังนี้ (Yin *et al.*, 2007) (Ma *et al.,* 2007) (Sachin *et al.,* 2007) ผู้วิจัยเหล่านี้ศึกษาความแตกต่างของแลนไร้สายและแลนมีสายในชั้น MAC-Layer ของมาตรฐาน IEEE802.3 โดยอาศัยพื้นฐานที่ในการใช้งานจริงในองค์กรจะทำการติดตั้งเครือข่ายแลนไร้สายเชื่อมเข้ากับเครือข่ายแลนมีสาย ดังนั้นเครือข่ายแลนไร้สายจึงจำเป็นต้องสื่อสารผ่านเครือข่ายแลน ในการสื่อสารผ่านเครือข่ายแลนไร้สายจะเสียเวลาในกระบวนการทำงานในระดับ MAC Layer เช่นการทำงานของ exponential backoff รวมถึงข้อจำกัดในระดับชั้นกายภาพที่ไม่สามารถส่งข้อมูลพร้อมกันกับรับข้อมูล จึงทำให้อุปกรณ์ในเครือข่ายแลนไร้สาย สื่อสารได้ช้ากว่าอุปกรณ์เครือข่ายแลนมีสาย

การตรวจจับแอกเซสพอยต์ด้วยข้อมูลในเครือข่ายแลนตรวจจับได้เฉพาะเวลาที่แอกเซสพอยต์นั้นกำลังสื่อสารในเครือข่ายแลนขององค์กร ไม่อาจตรวจพบแอกเซสพอยต์ที่เชื่อมต่ออยู่และไม่ได้ส่งข้อมูลสื่อสาร หรือ แอกเซสพอยต์ที่เกิดจากการโจมตีโดยที่ข้อมูลส่งผ่านเครือข่ายภายนอกองค์กร

3. การตรวจจับแอกเซสพอยต์เถื่อนในชั้นแลนไร้สาย

การตรวจจับด้วยวิธีนี้ใช้อุปกรณ์ที่มีคุณสมบัติฟังข้อมูลที่แพร่กระจายในอากาศ โดยให้อุปกรณ์ดักจับข้อมูลติดตั้งในบริเวณที่ต้องการตรวจจับ ข้อมูลที่ได้จากตรวจจับสามารถจัดกลุ่มได้ 2 กลุ่มได้แก่ ข้อมูลตามรูปแบบ IEEE 802.11 และ ข้อมูลที่ไม่อยู่ในรูปแบบ IEEE 802.11

งานวิจัยของ (Adya *et al.,* 2004) ได้เสนอให้มีซอฟต์แวร์ที่ติดตั้งที่เครื่องคอมพิวเตอร์ขององค์กร โดยที่ซอฟต์แวร์ดังกล่าว มีความสามารถในการเปลี่ยนการ์ดแลนไร้สาย ให้ดักจับข้อมูลได้ชั่วคราว แล้วส่งข้อมูลนั้นผ่านโพรโทคอลที่พัฒนาขึ้นเองโดยให้ชื่อว่า Client Conduit ถึงแม้งานวิจัยนี้มีวัตถุประสงค์เพื่อเสนอวิธีการรายงานและวิเคราะห์ปัญหาที่เกิดขึ้นในเครือข่ายแลนไร้สาย แต่ภายในงานวิจัยนี้ได้เสนอวิธีการระบุแอกเซสพอยต์เถื่อนด้วย ในการศึกษาเพื่อตรวจจับแอกเซสพอยต์เถื่อนใช้วิธีการเก็บข้อมูลของแอกเซสพอยต์ในองค์กรไว้ที่ฐานข้อมูลกลาง ข้อมูลที่บันทึกในฐานข้อมูลกลางประกอบไปด้วย หมายเลขอุปกรณ์เครือข่ายแลนไร้สาย ที่ตั้งของคอมพิวเตอร์ ชื่อเครือข่าย และ หมายเลขช่องสัญญาณ โดยข้อมูลเหล่านี้เป็นข้อมูลที่พบในเฟรมบีคอน เมื่อใดก็ตามที่สถานีลูกพบเฟรมบีคอนที่มีความแตกต่างจากฐานข้อมูลกลางจึงทำให้สามารถระบุข้อมูลนั้นได้ว่าเป็นข้อมูลที่เกิดจากแอกเซสพอยต์ที่ติดตั้งโดยไม่ได้รับอนุญาต ในการศึกษาของ (Bahl *et al*., 2006) ได้เสนอแนวทางการติดตั้งอุปกรณ์ดักจับข้อมูลไร้สายที่เครื่องคอมพิวเตอร์ในองค์กรโดยวิธีการนี้ได้นำข้อมูลที่ดักจับได้มาวิเคราะห์และระบุชนิดของการโจมตี ได้สองรูปแบบ ได้แก่ การโจมตีภายในเครือข่าย และ การก่อกวนระบบ พร้อมกับเสนอแนวทางการวิเคราะห์จำนวนอุปกรณ์ดักจับข้อมูลเพื่อให้เพียงพอสำหรับการใช้ดักจับทั่วทั้งองค์กร นอกจากนี้ในการศึกษาของ (Srilasak *et al.*, 2008) ได้เสนอวิธีการใช้แอกเซสพอยต์ที่มีอยู่เดิมขององค์กรให้ทำหน้าที่ในการดักจับข้อมูลในเครือข่ายแลนไร้สายชั่วคราว แล้วนำข้อมูลนั้นส่งผ่านเครือข่ายเดิมขององค์กรเพื่อมาวิเคราะห์ค้นหาแอกเซสพอยต์เถื่อน ซึ่งในงานวิจัยนี้ได้เสนอแนวทางการระบุชนิดแอกเซสพอยต์เถื่อนด้วยการจัดกลุ่มตามความรุนแรงของการโจมตีวิธีการนี้ประสิทธิภาพสูง เนื่องจากสามารถตรวจจับแอกเซสพอยต์เถื่อนได้ทุกชนิด รวมถึงวิธีการระงับการเชื่อมต่อของแอกเซสพอยต์เถื่อน โดยได้ทดลองบนระบบที่มีการใช้งานจริง และ ได้พัฒนาแอพลิเคชั่นสำหรับบริหารจัดการระบบผ่านทางเว็บเพจ

อุปกรณ์และวิธีการ

อุปกรณ์

1. ฮาร์ดแวร์

1. คอมพิวเตอร์แม่ข่าย ความเร็ว 3.00GHz
2. แอกเซสพอยต์ซิสโก้ รุ่น AP1121
3. สวิตช์ SMC รุ่น 6726AL2

2. ซอฟต์แวร์

1. ระบบปฏิบัติการลินุกซ์ Ubuntu 8.10
2. คอมไพเลอร์ภาษาซีสำหรับใช้ในการแปลงโปรแกรมให้รันได้
3. โปรแกรม Expect (Libes, 2006) สำหรับใช้ควบคุมอุปกรณ์

วิธีการ

1. เป้าหมายการออกแบบระบบ

1.1 สามารถตรวจจับ ค้นหาจุดเชื่อมต่อ และ ระงับการสื่อสารผ่านแอกเซสพอยต์เถื่อนได้

1.2 ใช้ร่วมกับเครือข่ายเดิมได้

2. ชนิดของแอกเซสพอยต์เถื่อน และ การวิเคราะห์ความเสี่ยง

2.1 คำจำกัดความแอกเซสพอยต์เถื่อน

แอกเซสพอยต์เถื่อนเกิดขึ้นได้ในเครือข่ายแลน เครือข่ายแลนไร้สาย หรือแม้กระทั้งในเครือข่ายภายนอก ทั้งที่เกิดจากพนักงานที่ไม่มีเจตนาบุกรุกเครือข่าย หรือ เกิดจากผู้บุกรุก เห็นได้ว่า

แอกเซสพอยต์เถื่อนมีหลายรูปแบบดังนั้นเพื่อให้เข้าใจได้ชัดเจนจึงสรุปคำจำกัดความของแอกเซสพอยต์เถื่อนได้ 2 แบบดังนี้

<u>คำจำกัดความที่ 1</u> แอกเซสพอยต์เถื่อน คือ แอกเซสพอยต์ที่ถูกติดตั้งโดยไม่ได้รับอนุญาตหรือ ไม่ได้ปฏิบัติตามกฎด้านความปลอดภัยขององค์กร

<u>คำจำกัดความที่ 2</u> แอกเซสพอยต์เถื่อน คือ แอกเซสพอยต์ที่เกิดจากผู้บุกรุกที่มีประสงค์ร้ายแก่องค์กร

จากคำจำกัดความของแอกเซสพอยต์เถื่อน ทำให้สามารถจำแนกชนิดของแอกเซสพอยต์ออกได้ 4 ชนิดดังที่ได้อธิบายต่อไปนี้

2.2 ชนิดของแอกเซสพอยต์เถื่อน

2.2.1 แอกเซสพอยต์เถื่อนชนิดที่ 1

แอกเซสพอยต์เถื่อนชนิดที่ 1 ได้แก่แอกเซสพอยต์ที่ตรงตามคำจำกัดความที่ 1 ซึ่งเกิดจากการติดตั้งของพนักงานภายในองค์กร แอกเซสพอยต์เถื่อนชนิดนี้เกิดขึ้นจากพนักงานซื้อแอกเซสพอยต์ด้วยตนเอง นำมาติดตั้งแทนที่เครื่องคอมพิวเตอร์ของตนเอง หรือ ที่ช่องเสียบสายแลน (outlet) ที่ยังว่าง แอกเซสพอยต์เถื่อนชนิดนี้ติดตั้งได้ง่ายแต่กลับสร้างความเสียหายแก่องค์กรได้สูง เพราะหากเป็นพนักงานที่มีความเข้าใจในด้านความปลอดภัยจะไม่ทำการลักลอบติดตั้งด้วยตนเอง การติดตั้งแอกเซสพอยต์ในลักษณะนี้เกิดจากการติดตั้งที่ไม่คำนึงในด้านความปลอดภัยจึงไม่ได้ตั้งค่าความปลอดภัยที่เพียงพออาจเป็นช่องทางให้ผู้บุกรุกเข้าโจมตีและเข้าสู่เครือข่ายภายในได้ง่าย ตัวอย่างของแอกเซสพอยต์เถื่อนตามรูปแบบนี้ที่พบเห็นบ่อย ๆ เช่น เป็นแอกเซสพอยต์ที่ปล่อยค่าชื่อเครือข่ายที่ไม่ได้เปลี่ยนแปลงจากโรงงานผู้ผลิต และ ไม่มีการเข้ารหัสข้อมูล

2.2.2 แอกเซสพอยต์เถื่อนชนิดที่ 2

แอกเซสพอยต์เถื่อนชนิดที่ 2 ได้แก่แอกเซสพอยต์ที่เกิดจากการติดตั้งของผู้บุกรุกตรงตามคำจำกัดความที่ 2 คือ แอกเซสพอยต์ตั้งอยู่ภายนอกองค์กร แต่เป็นแอกเซสพอยต์ที่ได้รับการปรับแต่งให้มีกำลังส่งสูงกว่าปกติ และ ปลอมแปลงให้แอกเซสพอยต์ดังกล่าวมีข้อมูลคล้ายแอกเซสพอยต์องค์กร การป้องกันการโจมตีลักษณะนี้ทำได้ง่ายด้วยการตั้งค่าความปลอดภัยของแอกเซส

พอยต์ในองค์กรให้ทำการเข้ารหัสและมีระบบพิสูจน์ตัวจริง เช่น เลือกใช้เทคโนโลยี WPA2 ตัวอย่างของแอกเซสพอยต์เถื่อนตามรูปแบบนี้ที่พบบ่อย ๆ เช่น แอกเซสพอยต์ที่จงใจกำหนดค่าแอกเซสพอยต์ให้ชื่อเครือข่ายหรือ ชื่อเครือข่ายแลนไร้สาย ตรงกับขององค์กร (เพื่อจุดประสงค์เพื่อหลอกลวงให้พนักงานองค์กรเข้าใจผิด และ มาเชื่อมต่อโดยปราศจากข้อสงสัยใด ๆ)

2.2.3 แอกเซสพอยต์เถื่อนชนิดที่ 3

แอกเซสพอยต์เถื่อนชนิดที่ 3 เป็นแอกเซสพอยต์ที่ตรงตามคำจำกัดความที่ 1 และ คำจำกัดความที่ 2 ซึ่ง ผู้บุกรุกที่สามารถเข้าถึงเครือข่ายภายในองค์กรได้ (สูญเสียความปลอดภัยทางด้านกายภาพ) แอกเซสพอยต์ดังกล่าวถูกติดตั้งเข้ากับเครือข่ายขององค์กร และ ทำการอำพรางร่องรอยโดยการตั้งค่าเครือข่ายแลนไร้สายให้เหมือนกับเครือข่ายจริง ซึ่งหลังจากติดตั้งแล้วผู้บุกรุกสามารถเข้าถึงเครือข่ายภายในองค์กรได้จากภายนอกและเข้าถึงได้ทุกเวลา ตัวอย่างที่พบเห็นบ่อย ๆ เช่น แอกเซสพอยต์ที่จงใจกำหนดค่าแอกเซสพอยต์ให้มีชื่อเครือข่ายแลนไร้สายตรงกับชื่อเครือข่ายแลนไร้สายขององค์กร โดยจุดประสงค์เพื่ออำพรางไม่ให้ผู้ดูแลระบบสามารถตรวจจับได้

2.2.4 แอกเซสพอยต์เถื่อนชนิดที่ 4

แอกเซสพอยต์เถื่อนชนิดที่ 4 เป็นแอกเซสพอยต์ที่เกิดจากเครือข่ายใกล้เคียง แอกเซสพอยต์นี้ไม่ได้ถูกจัดให้ตรงตามคำจำกัดความที่กำหนด เพราะความถี่ที่ใช้งานในเครือข่ายไร้สายตามรูปแบบมาตรฐาน IEEE 802.11 ได้เลือกใช้งานในย่านความถี่ที่ได้รับการยอมรับในระดับสากลให้เป็นย่านความถี่ที่สามารถใช้งานได้โดยไม่จำเป็นต้องขออนุญาต ซึ่งหมายถึงความถี่ดังกล่าวไม่ได้รับการคุมครองด้านการรบกวนสัญญาณ และ อุปกรณ์ที่ใช้งานย่านความถี่นั้น ๆ สามารถซื้อได้โดยไม่จำเป็นต้องขออนุญาต แต่บางครั้งอาจจะมีผลกระทบต่อประสิทธิภาพการใช้งานเครือข่ายแลนไร้สายขององค์กร เพราะสัญญาณเครือข่ายไร้สายมีรูปแบบการแพร่กระจายผ่านทางคลื่นวิทยุที่สามารถแพร่กระจายสัญญาณทะลุกำแพง ดังนั้นในกรณีที่องค์กรหรือหน่วยงานที่ตั้งอยู่บริเวณใกล้กันจึงมีโอกาสที่มีสัญญาณจากแอกเซสพอยต์ใกล้เคียงทำการแพร่กระจายสัญญาณส่งถึงกัน เป็นสาเหตุให้เกิดการรบกวนสัญญาณระหว่างกัน ตัวอย่างที่พบบ่อย เช่น แอกเซสพอยต์ในบริเวณใกล้เคียงโดยที่ไม่ได้ปลอมแปลงข้อมูลใด ๆ แต่การสร้างเครือข่ายขึ้นนี้เป็นการทำให้เกิดการรบกวนทางความถี่ได้ ตัวอย่างของแอกเซสพอยต์เถื่อนตามรูปแบบนี้ที่พบบ่อย ๆ เช่น แอกเซสพอยต์ที่ส่งสัญญาณเข้ามาถึงเครือข่ายแลนไร้สายภายในองค์ โดยข้อมูลจากแอกเซสพอยต์นั้นไม่มีความเหมือนกับข้อมูลภายในองค์กรเลย

2.3 การวิเคราะห์ความเสี่ยงจากแอกเซสพอยต์เถื่อนในเชิงคุณภาพ (Qualitative Risk Analysis)

การวิเคราะห์ความเสี่ยงเชิงคุณภาพนั้น ใช้เพื่อจัดลำดับความสำคัญของการกำหนดมาตรการในการแก้ไขปัญหาของแอกเซสพอยต์เถื่อน มีการแบ่งระดับของภัยคุกคาม (Threat) ออกเป็น 3 ระดับ คือ สูง กลาง ต่ำ ซึ่งเกณฑ์การกำหนดระดับของภัยคุกคามกำหนดขึ้นจากเจตนาของการบุกรุก หากเป็นการสร้างเครือข่ายของผู้บุกรุกที่มีเจตนาร้ายจะได้รับการกำหนดให้มีระดับของภัยคุกคามที่สูง และ แอกเซสพอยต์ที่เกิดจากการติดตั้งโดยไม่ได้มีเจตนาบุกรุกเครือข่ายแต่ติดตั้งโดยไม่ได้ตระหนักถึงความปลอดภัยอยู่ในระดับการสร้างช่องโหว่ให้แก่องค์กรหากไม่มีการบุกรุกจะยังไม่เกิดภัยคุกคามดังนั้นจึงจัดให้อยู่ในภัยคุกคามระดับกลาง และ ในกรณีที่แอกเซสพอยต์นั้นเป็นแอกเซสพอยต์เครือข่ายใกล้เคียงที่เกิดจากการส่งสัญญาณรบกวนไม่ได้มีเจตนาบุกรุกเครือข่าย รวมถึงอุปกรณ์นั้นไม่ได้เชื่อมกับเครือข่ายภายในองค์กรจึงถูกจัดกลุ่มให้อยู่ในภัยคุกคามระดับต่ำ

ปัจจัยที่ใช้ในการพิจารณาระดับความเสี่ยงเพิ่มเติม ได้แก่ โอกาสของการเกิดภัยคุกคามของแอกเซสพอยต์เถื่อนแต่ละประเภท ซึ่งกำหนดให้มี 3 ระดับได้แก่ โอกาสเกิดสูง โอกาสเกิดปานกลาง โอกาสเกิดน้อย วิธีการกำหนดเกณฑ์พิจารณาโดยเปรียบเทียบจากความง่ายในการสร้างเครือข่าย ในกรณีที่เป็นแอกเซสพอยต์ที่ไม่ได้รับการปรับแต่งใด ๆ ได้รับการกำหนดให้อยู่ในระดับความเสี่ยงที่โอกาสเกิดสูง ในขณะที่ แอกเซสพอยต์ที่ได้รับการปรับแต่ง หากแอกเซสพอยต์นั้นใช้วิธีปรับแต่งอย่างง่ายจะได้รับการจัดกลุ่มให้อยู่ในแอกเซสพอยต์ที่มีโอกาสเกิดปานกลาง และ แอกเซสพอยต์ที่ได้รับการปรับแต่งจากผู้บุกรุกที่มีความชำนาญด้วยการปรับแต่งข้อมูลทั้งหมดเหมือนกับแอกเซสพอยต์ในองค์กรถูกจัดให้อยู่ในกลุ่มแอกเซสพอยต์โอกาสเกิดน้อย ตารางที่ 5 แสดงถึงผลการวิเคราะห์ความเสี่ยงของแอกเซสพอยต์เถื่อนแต่ละประเภท เห็นได้ว่า แอกเซสพอยต์เถื่อนชนิดที่ 1 และชนิดที่ 2 มีความเสี่ยงสูงกว่าแอกเซสพอยต์ชนิดอื่น ๆ

3. ระบบการตรวจจับและตอบโต้ที่นำเสนอ

การตรวจจับสัญญาณแอกเซสพอยต์เถื่อนนั้นสามารถใช้การตรวจจับผ่านทางคลื่นวิทยุที่แอกเซสพอยต์ปล่อยออกมา ระบบดังกล่าวจะทำการแยกแยะความแตกต่างของสัญญาณที่ได้รับเทียบกับแอกเซสพอยต์ที่ติดตั้งดูแลโดยองค์กร อุปกรณ์ตรวจจับที่ใช้ทั่วไปมีทั้งแบบติดตั้งอยู่กับที่

เพื่อตรวจสอบแอกเซสพอยต์แปลกปลอมเข้ามาในบริเวณเฝ้าระวัง หรือ ใช้แรงงานคนถืออุปกรณ์ในการเดินตรวจตรา

วิทยานิพนธ์นี้นำเสนอวิธีการตรวจจับแอกเซสพอยต์เถื่อนด้วยการใช้แอกเซสพอยต์ที่มีการติดตั้งอยู่เดิม ทำหน้าที่ในการตรวจจับคลื่นวิทยุของอุปกรณ์แปลกปลอมเหล่านั้น ซึ่งได้รับประโยชน์ 2 ทาง

1. ไม่ต้องซื้ออุปกรณ์เพิ่มเติมใหม่ เช่น อุปกรณ์ดักจับข้อมูล สวิตช์
2. ลดเวลาสำหรับผู้ดูแลเครือข่าย ที่ต้องเดินตรวจตราทั่วบริเวณขององค์กร เพราะ แอกเซสพอยต์ได้ติดตั้งอยู่ทั่วบริเวณอยู่แล้ว

ดังนั้นแอกเซสพอยต์ที่จะถูกนำมาใช้กับระบบที่นี้จึง สามารถให้บริการเป็นแอกเซสพอยต์ตามปกติ และ มีคุณสมบัติที่สามารถเปลี่ยนสถานะให้ดักฟังคลื่นวิทยุได้ด้วย วิทยานิพนธ์นี้เลือกใช้แอกเซสพอยต์ซิสโก้รุ่น AP1121 ที่เป็นแอกเซสพอยต์ที่ได้รับความนิยมใช้งานในองค์กร เช่น มหาวิทยาลัยเกษตรศาสตร์ สำนักงานวิทยาศาสตร์และเทคโนโลยีแห่งชาติ เป็นต้น ซึ่งงานวิจัยนี้ได้เลือกใช้คุณสมบัติของแอกเซสพอยต์ที่มีอยู่แล้วมาทำให้เกิดประโยชน์

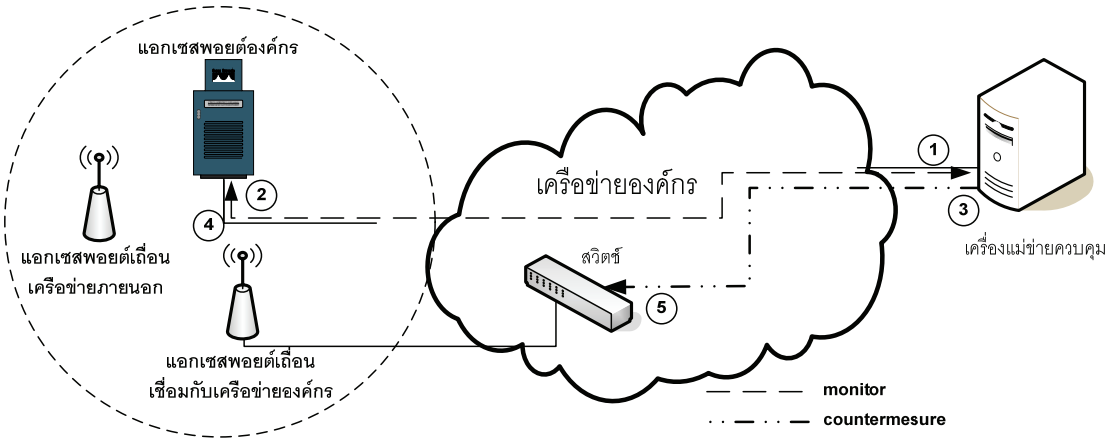
ตารางที่ 5 ผลการวิเคราะห์ระดับของความเสี่ยง

ประเภทแอกเซสพอยต์เถื่อน	ระดับภัยคุกคาม	โอกาสเกิดภัยคุกคาม	ระดับของความเสี่ยง
ชนิดที่ 1	กลาง (2)	โอกาสเกิดสูง (3)	2x3 = 6
ชนิดที่ 2	สูง (3)	โอกาสเกิดปานกลาง (2)	3x2 = 6
ชนิดที่ 3	สูง (3)	โอกาสเกิดน้อย (1)	3x1 = 3
ชนิดที่ 4	ต่ำ (1)	โอกาสเกิดสูง (3)	1x3 = 3

3.1 การทำงานโดยรวมของระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน

การทำงานของระบบสามารถอ้างอิงภาพที่ 21 โดยระบบเริ่มต้นทำงานจาก 1) เครื่องแม่ข่ายควบคุม ส่งคำสั่งไปควบคุมแอกเซสพอยต์ขององค์กร (Exist AP) ให้เปลี่ยนสถานะเป็นอุปกรณ์ดักฟังข้อมูลไร้สาย 2) เมื่อแอกเซสพอยต์องค์กรได้รับคำสั่งเปลี่ยนสถานะจะเริ่มทำการดัก

ฟังข้อมูลที่สื่อสารในอากาศแล้วส่งข้อมูลกลับมายังเครื่องแม่ข่ายส่วนกลางผ่านทางเครือข่ายขององค์กร ต่อมา 3) เมื่อเครื่องแม่ข่ายได้รับข้อมูลจากแอกเซสพอยต์ครบถ้วน ขั้นตอนไปจึงทำการส่งคำสั่งเพื่อคืนสถานะเป็นปกติให้แก่แอกเซสพอยต์ ในขั้นตอนที่ 4) แอกเซสพอยต์ได้คืนสู่สถานะปกติแล้ว หลังจากนั้นจึงเริ่มต้นวิเคราะห์ข้อมูล เมื่อเครื่องแม่ข่ายควบคุมตรวจจับแอกเซสพอยต์เถื่อนจากการวิเคราะห์ข้อมูลเปรียบเทียบกับฐานข้อมูลในเบื้องต้น หากพบข้อมูลแอกเซสพอยต์เถื่อนจะทำการค้นหาว่าข้อมูลจากแอกเซสพอยต์ที่จับได้นั้นเป็นแอกเซสพอยต์ที่เชื่อมกับเครือข่ายภายในหรือไม่ หากพบกว่ามีการเชื่อมในเครือข่ายภายใน เข้าสู่ขั้นตอนที่ 5) ทำการส่งคำสั่งควบคุมสวิตช์ให้ระงับการเชื่อมต่อ



ภาพที่ 21 ภาพรวมของระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน

อุปกรณ์ที่เกี่ยวข้องกับระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อนนี้ประกอบด้วยอุปกรณ์หลัก 3 อุปกรณ์ได้แก่ แอกเซสพอยต์ สวิตช์ และ เครื่องแม่ข่ายควบคุม อุปกรณ์เหล่านี้เป็นอุปกรณ์ที่มีอยู่เดิมในเครือข่าย ดังนั้นผู้ดูแลระบบสามารถควบคุมสั่งงานอุปกรณ์ทั้งหมดได้จากระยะไกล ผ่านทางโพรโทคอลที่ได้รับความนิยม เช่น telnet หรือ ssh เป็นต้น สำหรับหน้าที่การทำงานโดยละเอียดของอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องกับระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อนมีดังต่อไปนี้

3.2 แอกเซสพอยต์

แอกเซสพอยต์สำหรับระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน มีหน้าที่คอยรับคำสั่งจากเครื่องแม่ข่ายเพื่อให้เปลี่ยนสถานะ ใน 2 รูปแบบ ได้แก่ สถานะทำหน้าที่ใช้งานปกติ หรือทำหน้าที่ในการดักฟัง

3.2.1 สถานะปกติ

สถานะนี้เป็นสถานะปกติของแอกเซสพอยต์ ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายแลนไร้สาย การทำงานเกือบตลอดเวลาจะอยู่ในสถานะนี้

3.2.2 สถานะดักฟังข้อมูลไร้สาย

สถานะนี้เป็นสถานะที่ต้องการฟังข้อมูลในเครือข่ายแลนไร้สายเพื่อนำข้อมูลมาวิเคราะห์เพื่อค้นหาแอกเซสพอยต์ที่มีโอกาสเป็นแอกเซสพอยต์เถื่อน ช่วงเวลาที่เสียไปในการดักฟังข้อมูลเมื่อเทียบกับเวลาการให้บริการมีค่าแตกกันมากจนสามารถถือได้ว่าไม่สูญเสียการให้บริการ อย่างไรก็ตาม วิทยานิพนธ์นี้ได้เสนอแนวทางการวิเคราะห์เวลาที่เหมาะสมในการเปลี่ยนสถานะของแอกเซสพอยต์ในแต่ละวัน เพื่อช่วยให้ผู้ดูแลเครือข่ายตัดสินใจได้ง่ายขึ้น

3.3 สวิตช์

ทำหน้าที่กระจายสัญญาณโดยกระจายข้อมูลสำหรับเครือข่ายแลน อุปกรณ์นี้สามารถทำงานร่วมกับแอกเซสพอยต์ได้เป็นอย่างดี แอกเซสพอยต์ที่ติดตั้งโดยไม่รับอนุญาตโดยมากถูกเชื่อมต่อกับสวิตช์โดยตรง เครื่องแม่ข่ายมีหน้าที่คอยควบคุมสวิตช์ให้เปลี่ยนการทำงาน ใน 2 รูปแบบ ได้แก่ การทำงานแบบสวิตช์ปกติ และ ควบคุมการเข้าใช้งานของอุปกรณ์ที่เชื่อมต่อ

3.3.1 การทำงานแบบสวิตช์ปกติ

สวิตช์จะทำหน้าที่กระจายข้อมูลในเครือข่าย ทั้งนี้สวิตช์มีความแตกต่างจากแอกเซสพอยต์ในด้านการสั่งงานควบคุมอุปกรณ์ เพราะเมื่อสั่งงานให้สวิตช์ควบคุมการเข้าใช้งานอุปกรณ์ที่เชื่อมต่อในพอร์ตใด ๆ พอร์ตอื่นยังคงใช้งานได้ปกติโดยไม่มีผลกระทบใด ๆ

3.3.2 ควบคุมการเข้าใช้งานของอุปกรณ์ที่เชื่อมต่อ

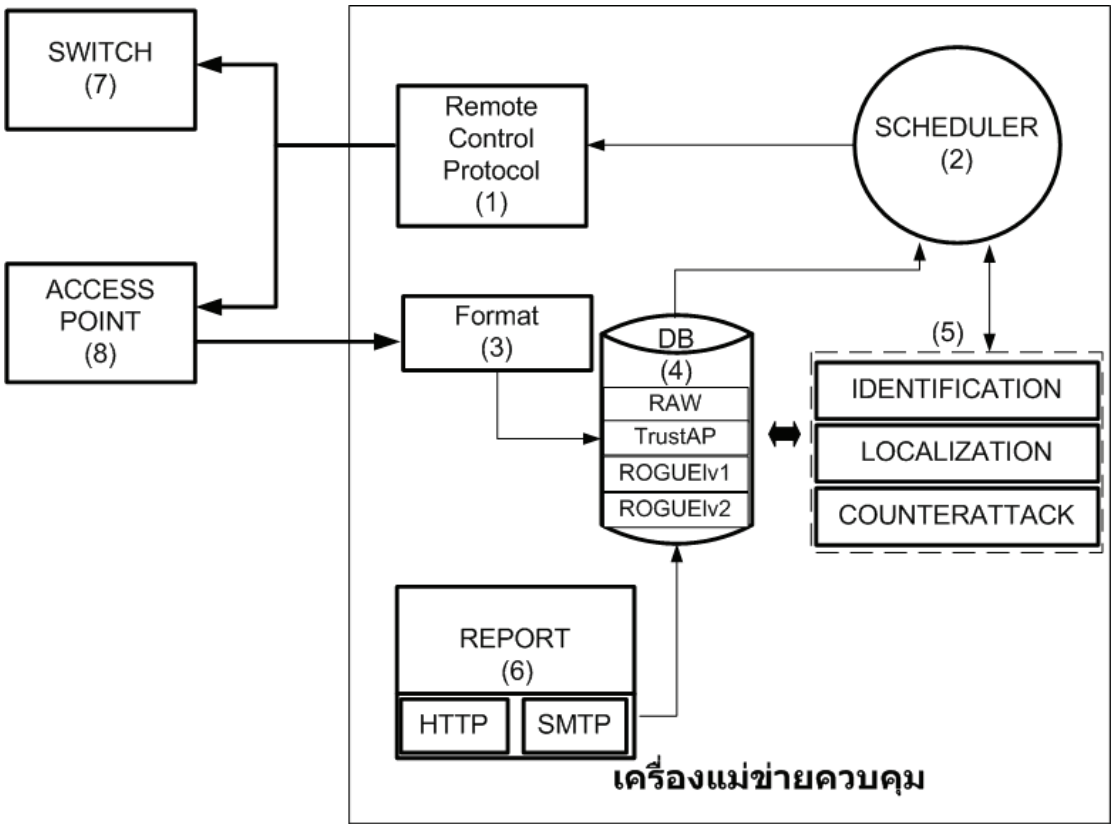
สวิตช์สามารถดำเนินการระงับการเชื่อมต่อของแอกเซสพอยต์หรืออุปกรณ์ที่เชื่อมต่ออื่นโดยรับคำสั่งควบคุมจากเครื่องแม่ข่ายควบคุมโดยข้อมูลที่ส่งมาระงับการเชื่อมต่อจะเป็นข้อมูลที่ผ่านการวิเคราะห์และระบุได้ว่าอุปกรณ์ที่กำลังเชื่อมต่อนั้นเป็นอุปกรณ์แอกเซสพอยต์เถื่อน

3.4 เครื่องแม่ข่ายควบคุม

เครื่องแม่ข่ายควบคุมมีหน้าที่ควบคุมการทำงานของระบบ เริ่มตั้งแต่ควบคุมให้แอกเซสพอยต์เปลี่ยนสถานะชั่วคราวให้ดักจับข้อมูลในเครือข่ายไร้สายแล้วนำข้อมูลนั้นส่งกลับมายังเครื่องแม่ข่ายควบคุม และ ส่งคำสั่งควบคุมให้แอกเซสพอยต์คืนสู่สถานะปกติ ทำการถอดรหัสข้อมูลที่ได้รับจากแอกเซสพอยต์แล้วนำไปเก็บลงฐานข้อมูล วิเคราะห์เพื่อระบุแอกเซสพอยต์เถื่อน ควบคุมสวิตช์เพื่อค้นหาจุดเชื่อมต่อของแอกเซสพอยต์เถื่อน และ ระงับการเชื่อมต่อของแอกเซสพอยต์เถื่อน เป็นต้น การทำงานของเครื่องแม่ข่ายควบคุมได้อธิบายรายละเอียดในหัวข้อต่อไป

การทำงานของเครื่องแม่ข่ายควบคุม

เครื่องแม่ข่ายควบคุมทำหน้าที่ควบคุมการทำงานของอุปกรณ์ในระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน โดยมีหน้าที่การทำงานดังแสดงในแผนผังการทำงานในภาพที่ 22



ภาพที่ 22 ภาพฟังก์ชั่นการทำงานของเครื่องแม่ข่ายควบคุม

1. โมดูลควบคุมระยะไกล

โมดูลควบคุมระยะไกล (Remote Control Protocol) มีหน้าที่ส่งคำสั่งควบคุมแอกเซสพอยต์และสวิตช์ขององค์กร โมดูลควบคุมระยะไกลจะคอยรับคำสั่งจาก โมดูลจัดการเวลา(2)ซึ่งทำหน้าที่ในการควบคุมเวลาในการทำงานของระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน ภายในโมดูลควบคุมระยะไกลจะบรรจุชุดคำสั่งสำหรับควบคุมอุปกรณ์ไว้ภายใน เช่น คำสั่งเปลี่ยนสถานะของแอกเซสพอยต์จากสถานะปกติให้ทำงานดักฟังข้อมูลในเครือข่ายไร้สาย คำสั่งสำหรับสั่งงานให้แอกเซสพอยต์คืนสู่สถานะปกติ และ คำสั่งควบคุมการทำงานของสวิตช์ เป็นต้น โมดูลควบคุมระยะไกลนี้ประกอบด้วยโมดูลสำหรับควบคุมอุปกรณ์ซึ่งขึ้นอยู่กับชนิดและรูปแบบคำสั่งที่ใช้ติดต่อ ซึ่งในงานวิจัยนี้เลือกใช้โปรแกรม Expect เพื่อใช้ควบคุมอุปกรณ์ที่อยู่ในเครือข่าย

1.1 ชุดคำสั่งสำหรับแอกเซสพอยต์เพื่อใช้เปลี่ยนเป็นสถานะการดักจับข้อมูล

ชุดคำสั่งนี้พัฒนาขึ้นสำหรับสั่งงานแอกเซสพอยต์เพื่อให้เปลี่ยนสถานะของแอกเซสพอยต์องค์กร จากสถานะปกติให้เปลี่ยนเป็นดักจับข้อมูลในเครือข่ายไร้สาย รวมถึงชุดคำสั่งสำหรับสั่งงานให้แอกเซสพอยต์คืนสู่สถานะปกติ ชุดคำสั่งสำหรับควบคุมแอกเซสพอยต์จะขึ้นอยู่กับโพรโทคอลที่ใช้สำหรับสื่อสารกับอุปกรณ์นั้น ๆ โดยขึ้นกับคำสั่งจากผู้ผลิตแอกเซสพอยต์ ซึ่งชุดคำสั่งสำหรับแอกเซสพอยต์ซิสโก้ตัวอย่างได้แสดงไว้ในภาคผนวก

1.2 ชุดคำสั่งติดต่อสวิตช์เพื่อใช้ค้นหาตำแหน่งจุดเชื่อมต่อ

ชุดคำสั่งสำหรับติดต่อสวิตช์เพื่อสอบถามตำแหน่งการเชื่อมต่อ ซึ่งเป็นชุดคำสั่งที่เรียกใช้โพรโทคอลที่นิยมใช้งานในการบริหารจัดการอุปกรณ์ชื่อว่า SNMP (Simple Network Management Protocol)

1.3 ชุดคำสั่งติดต่อสวิตช์เพื่อใช้ควบคุมการเข้าใช้พอร์ต

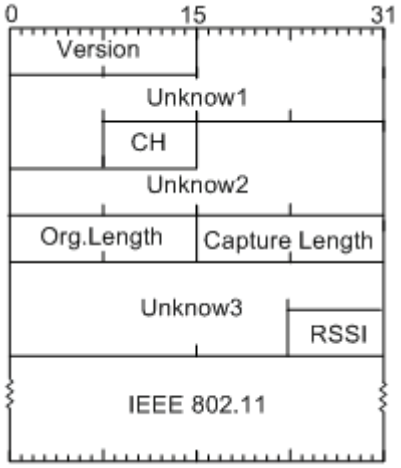
ชุดคำสั่งสำหรับติดต่อสวิตช์ถูกพัฒนาขึ้นเพื่อใช้ส่งคำสั่งควบคุมสวิตช์ที่อยู่ในเครือข่ายองค์กร ชุดคำสั่งที่ใช้ควบคุมนี้ มีรูปแบบการส่งคำสั่งเช่นเดียวกับ คำสั่งที่ผู้ดูแลระบบป้อนสั่งควบคุมสวิตช์ ซึ่งชุดคำสั่งควบคุมจะขึ้นอยู่กับโพรโทคอล และ ชนิดของสวิตช์

2. โมดูลจัดการเวลา

โมดูลจัดการเวลา (Scheduler) ทำหน้าที่กำหนดเวลาเพื่อสั่งงานควบคุมการเปลี่ยนสถานะของแอกเซสพอยต์ซึ่งในระบบจะมีการเลือกช่วงเวลาและระยะในการเปลี่ยนสถานะให้เหมาะสมที่สุด พร้อมกับส่งคำสั่งควบคุมอุปกรณ์ไปยังโมดูลควบคุมระยะไกล วิทยานิพนธ์นี้เลือกใช้โปรแกรม cron [Joey, http://www.linuxhelp.net/guides/cron] ซึ่งเป็นโปรแกรมที่ได้รับการติดตั้งมาพร้อมกับระบบปฏิบัติการลินุกซ์อยู่แล้ว

3. โมดูลจัดรูปแบบ

โมดูลจัดรูปแบบ (Format) ทำหน้าที่รับข้อมูลจากแอกเซสพอยต์ และ จัดรูปแบบของเฟรมก่อนเก็บลงฐานข้อมูล ข้อมูลที่ได้รับจากแอกเซสพอยต์ถูกส่งในรูปแบบ UDP ซึ่งมีการจัดเฟรมตามภาพที่ 23 ในโมดูลจัดรูปแบบนี้จะทำการคัดเลือกข้อมูลเฉพาะเฟรมที่สำคัญประกอบด้วย เฟรมบีคอน และ เฟรมข้อมูล เพื่อนำไปเก็บลงฐานข้อมูล



ภาพที่ 23 รูปแบบเฟรมจากแอกเซสพอยต์ซิสโก้

รูปแบบการจัดเฟรมตามภาพที่ 23 ถูกเปิดเผยโดยนักพัฒนาโปรแกรม WireShark ภายใต้ชื่อว่า CWIDS [WireShark, http://www.wireshark.org/docs/dfref/c/cwids.html] เนื่องจากเป็นการศึกษาด้วยการถอดรหัสโพรโทคอลแบบวิศวกรรมย้อนกลับ (Reverse Engineering) รายละเอียดของเฟรมอาจไม่ครบถ้วน แต่ยังคงมีรายละเอียดข้อมูลที่มีความสำคัญต่อวิทยานิพนธ์ รายละเอียดต่อไปนี้ได้สรุปการทำงาน ของโพรโทคอล CWIDS

Version มีขนาดคงที่ 2 ไบต์ ทำหน้าที่กำหนดหมายเลขโพรโทคอล CWIDS

Unknown1 มีขนาดคงที่ 7 ไบต์ เป็นข้อมูลที่ยังไม่ได้รับการถอดรหัส

CH มีขนาดคงที่ 1 ไบต์ ใช้อธิบายช่องสัญญาณที่แอกเซสพอยต์นั้นกำลังดักฟังข้อมูล

Unknown2 มีขนาดคงที่ 6 ไบต์ เป็นข้อมูลที่ยังไม่ได้รับการถอดรหัส

Org.Length มีขนาดคงที่ 2 ไบต์ ใช้อธิบายถึงขนาดความยาวจริงของข้อมูลเครือข่ายแลนไร้สาย

Capture Length มีขนาดคงที่ 2 ไบต์ ใช้อธิบายถึงขนาดความยาวที่แอกเซสพอยต์ส่งข้อมูลมายังเครื่องแม่ข่ายควบคุม

Unknown3 มีขนาดคงที่ 7 ไบต์ เป็นข้อมูลที่ยังไม่ได้รับการถอดรหัส

RSSI มีขนาด 1 ไบต์ ใช้อธิบายค่าความแรงของสัญญาณไร้สายที่แอกเซสพอยต์ได้รับ

IEEE 802.11 มีขนาดเปลี่ยนแปลงได้ อยู่ระหว่าง 0 - 2288 ไบต์

ขนาดเฮดเดอร์ของ CWIDS มีขนาดคงที่ 28 ไบต์ เมื่อนำข้อมูลนี้ไปรวมกับ ขนาดของข้อมูลที่จำเป็นสำหรับวิทยานิพนธ์นี้ที่ประกอบด้วย เฟรมการจัดการ (24 ไบต์) และ เฟรมบีคอน (59 ไบต์) รวมได้ขนาด 83 ไบต์ เป็นค่าความยาวที่สามารถควบคุมให้แอกเซสพอยต์ตัดข้อมูลที่ไม่จำเป็นก่อนส่งข้อมูลนั้นมายังเครื่องแม่ข่ายควบคุม จากการคำนวณทำให้ได้ค่าความยาวข้อมูลที่จำเป็นสำหรับการตรวจจับแอกเซสพอยต์เถื่อน (28 ไบต์ + 83 ไบต์) เท่ากับ 111 ไบต์ ซึ่งค่าดังกล่าวนี้ถูกนำไปใช้ในคำสั่งกำหนดขนาดข้อมูลซึ่งควบคุมด้วยโมดูลควบคุมระยะไกลเพื่อควบคุมแอกเซสพอยต์

4. โมดูลฐานข้อมูล

โมดูลฐานข้อมูล(Database) ทำหน้าที่เก็บข้อมูลที่ได้รับจากโมดูลจัดรูปแบบ(3) โมดูลนี้ทำ

หน้าที่บันทึกข้อมูลเพียงอย่างเดียว โดยข้อมูลภายในฐานข้อมูลประกอบด้วยตารางฐานข้อมูลที่สำคัญ 5 ตารางดังนี้ raw roguelv1 roguelv2 และ trustAP

ตารางที่ 6 ได้แสดงถึงโครงร่างตาราง raw ทำหน้าที่เก็บบันทึกเฟรมตามรูปแบบ IEEE802.11 ข้อมูลที่บันทึกภายใน raw เกิดจากข้อมูลข้อมูลที่แอกเซสพอยต์องค์กรดักจับได้จากอากาศ และ ถูกส่งผ่านเครือข่ายแลนในรูปแบบ UDP มายังเครื่องแม่ข่ายควบคุมหลังจากที่ได้รับการถอดข้อมูลให้อยู่ในรูปแบบ IEEE802.11 จะได้รับการคัดกรองอีกครั้งเพื่อให้เหลือเฉพาะเฟรมบีคอนและนำข้อมูลนั้นบันทึกลงในตารางฐานข้อมูล raw

ตารางที่ 7 ได้อธิบายถึงโครงร่างตารางฐานข้อมูล roguelv1 ซึ่งทำหน้าที่เก็บบันทึกข้อมูลแอกเซสพอยต์เถื่อนที่ผ่านการวิเคราะห์เบื้องต้นจากการเปรียบเทียบข้อมูลกับข้อมูลที่มีอยู่เดิม โดยใช้ข้อมูลที่นำมาเปรียบเทียบ 4 ข้อมูลประกอบด้วย ชื่อเครือข่ายไร้สาย(SSID) หมายเลขอุปกรณ์เครือข่ายไร้สาย (Wireless MAC Address) หมายเลขช่องสัญญาณ (Channel) และ หมายเลขไอพีของแอกเซสพอยต์องค์กร

ตารางที่ 8 แสดงถึงโครงร่างตารางของ roguelv2 ทำหน้าที่เก็บบันทึกข้อมูลแอกเซสพอยต์เถื่อนที่เชื่อมในเครือข่ายภายในองค์กร

ตารางที่ 9 ได้แสดงถึง trustAP ทำหน้าที่เก็บบันทึกข้อมูลแอกเซสพอยต์ขององค์กรข้อมูลที่อยู่ในตารางนี้ประกอบด้วยข้อมูลแอกเซสพอยต์องค์กรที่มีคุณสมบัติในการดักจับข้อมูลในอากาศแล้วส่งกลับมายังเครื่องแม่ข่ายควบคุม

5. โมดูลวิเคราะห์

โมดูลวิเคราะห์ เป็นโมดูลหัวใจหลักของระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน โมดูลนี้ทำหน้าที่อ่านข้อมูลจากฐานข้อมูล แล้วนำข้อมูลที่อยู่ในฐานข้อมูลมาจัดเรียงรูปแบบเพื่อนำไปวิเคราะห์เพื่อค้นหาแอกเซสพอยต์เถื่อน หน้าที่ของโมดูลนี้ได้รวมถึงการส่งคำสั่งเพื่อติดต่อกับสวิตช์เพื่อค้นหาจุดเชื่อมต่อของแอกเซสพอยต์เถื่อนด้วยการส่งคำสั่ง SNMP เพื่อสอบถามหมายเลขอุปกรณ์เครือข่ายไร้สาย ที่เชื่อมอยู่กับสวิตช์ภายในองค์กร รายละเอียดหน้าที่ของโมดูลวิเคราะห์ สามารถสรุปได้ดังต่อไปนี้

5.1 หน้าที่ตรวจจับ (Identification)

การตรวจจับเริ่มต้นทำงานเมื่อแอกเซสพอยต์ส่งข้อมูลจนเสร็จสิ้น หลังจากนั้นจึงเริ่มต้นอ่านข้อมูลในตารางฐานข้อมูล raw ข้อมูลที่อยู่ภายในตารางฐานข้อมูล raw ประกอบด้วยข้อมูลที่ดักจับได้จากเครือข่ายไร้สาย โดยมีข้อมูลหลักได้แก่เฟรมบีคอน หน้าที่ตรวจจับนี้จะนำข้อมูลที่อยู่ในตารางฐานข้อมูล raw มาจัดกลุ่ม ตามชื่อเครือข่าย หมายเลขอุปกรณ์เครือข่ายแลนไร้สาย และ หมายเลขไอพีของแอกเซสพอยต์ที่ใช้ตรวจจับ ข้อมูลที่ได้รับนี้จะถูกนำไปเปรียบเทียบกับตารางฐานข้อมูลแอกเซสพอยต์องค์กรซึ่งข้อมูลที่อยู่ในตารางนี้ได้ถูกบันทึกไว้ก่อนล่วงหน้า ผลของการเปรียบเทียบเพื่อค้นหาแอกเซสพอยต์ที่มีข้อมูลที่แตกต่างจากข้อมูลแอกเซสพอยต์องค์กรถ้าพบความแตกต่างจะนำข้อมูลที่ได้นั้นไปเก็บที่ตารางฐานข้อมูล roguelv1 เพื่อใช้เป็นข้อมูลในการค้นหาจุดเชื่อมต่อในขั้นตอนต่อไป

ตารางที่ 6 โครงร่างตารางฐานข้อมูล raw

Field	Type
ID	bigint(20)
apview	varchar(15)
rssi	mediumint(9)
unknown1	varchar(14)

ตารางที่ 6 (ต่อ)

Field	Type
FrameControl	varchar(16)
Duration	varchar(8)
DA	varchar(24)
SA	varchar(24)
BSSID	varchar(24)
SeqNumber	varchar(8)
TimeStamp	varchar(32)

ตารางที่ 7 โครงร่างตารางฐานข้อมูล roguelv1

Field	Type
id	bigint(20)
apview	varchar(20)
ssid	varchar(128)
mac	varchar(256)
channel	varchar(128)
rssi	varchar(20)
status	tinyint(4)
location	varchar(1024)
extended	varchar(1024)
DateTime	datetime

ตารางที่ 8 โครงร่างตารางฐานข้อมูล roguelv2

Field	Type
id	bigint(20)
macap	varchar(20)
macclient	varchar(20)
switch	varchar(20)
port	varchar(10)
investigate	int(2)
DateTime	datetime

ตารางที่ 9 โครงร่างตารางฐานข้อมูล trustAP

Field	Type
id	bigint(20)
apview	varchar(20)

ตารางที่ 9 (ต่อ)

Field	Type
ssid	varchar(20)
mac	varchar(256)
channel	varchar(128)
rssi	varchar(20)
location	varchar(1024)
extended	varchar(1024)

วิธีการตรวจจับแอกเซสพอยต์เถื่อนในวิทยานิพนธ์นี้ได้เลือกใช้ข้อมูลไร้สายที่ได้รับจากแอกเซสพอยต์องค์กรมาเปรียบเทียบกับฐานข้อมูลในแอกเซสพอยต์องค์กร โดยใช้วิธีคิดตามรหัสเทียม ดังแสดงในภาพที่ 24 รายละเอียดการทำงานของรหัสเทียมตามภาพที่ 24 มีดังนี้ เริ่มต้นจากเครื่องแม่ข่ายควบคุมได้รับข้อมูลจากแอกเซสพอยต์องค์กร ซึ่งประกอบด้วย ชื่อเครือข่าย และหมายเลขอุปกรณ์เครือข่ายแลนไร้สาย แล้วทำการนำข้อมูลนั้นเปรียบเทียบกับฐานข้อมูล เมื่อพบว่าตรงกับฐานข้อมูลระบบจะทำการตรวจสอบอีกครั้งว่าเป็นการปลอมแปลงหรือไม่ (spoofing) (ซึ่งตรงตามบรรทัดที่ 3) วิธีที่วิทยานิพนธ์นี้เลือกใช้ในการตรวจจับการปลอมแปลงได้แก่การเลือกใช้ค่าหมายเลขไอพีของแอกเซสพอยต์องค์กรที่ใช้ดักจับข้อมูลเป็นปัจจัยสำคัญในการวิเคราะห์ ด้วยเหตุผลที่เกิดจากในขณะที่แอกเซสพอยต์องค์กรอยู่ในสถานะดักฟัง จะทำให้แอกเซสพอยต์ดังกล่าวหยุดส่งบีคอน เมื่อไรก็ตามที่แอกเซสพอยต์นั้นได้รับเฟรมบีคอนที่เป็นข้อมูลของตนเองจึงทำให้สามารถระบุได้ว่าข้อมูลนั้นเป็นข้อมูลที่ส่งจากแอกเซสพอยต์เถื่อนเมื่อพบว่าเป็นการปลอมแปลงข้อมูลจะถือว่าเป็นแอกเซสพอยต์เถื่อนชนิดที่ 2 แต่ถ้าไม่พบการปลอมแปลงก็ถือว่าเป็นข้อมูลจากแอกเซสพอยต์ขององค์กร

ในบรรทัดที่ 9-18 ใช้วิเคราะห์ข้อมูลเครือข่ายแลนไร้สายที่มีข้อมูลบางข้อมูลที่ตรงกับฐานข้อมูล โดยเริ่มต้นด้วยการตรวจสอบว่ามีการเชื่อมสู่เครือข่ายภายในหรือไม่ หากเชื่อมต่อเครือข่ายภายในถือว่าเป็นการบุกรุกของผู้บุกรุกที่เป็นพนักงานภายในองค์กรซึ่งตรงกับแอกเซสพอยต์เถื่อนชนิดที่ 3 หากไม่เชื่อมกับเครือข่ายภายในถือว่าเป็นการบุกรุกของผู้บุกรุกจากภายนอกตรงกับแอกเซสพอยต์เถื่อนชนิดที่ 2 และ ในกรณีที่พบข้อมูลที่ไม่ตรงกับแอกเซสพอยต์ภายในองค์กรเลย ระบบจะทำการตรวจสอบการเชื่อมเข้าสู่เครือข่ายภายในหรือไม่ ด้วยวิธีตามรหัสเทียม

ในภาพที่ 25 หากพบว่าเชื่อมเข้าสู่เครือข่ายภายในถือว่าเป็นแอกเซสพอยต์เถื่อนชนิดที่ 1 และหากพบว่าไม่ได้เชื่อมในเครือข่ายภายในองค์กร ถือว่าเป็นแอกเซสพอยต์เถื่อนชนิดที่ 4

```
1   GET ssid AND bssid from Trust-AP
2   IF (ssid AND bssid) == Authorized_AP THEN
3    IF has spoofing THEN
4     Report Rogue Type2
5     Store data to roguelv1
6    ELSE
7     Report that is Authorized_AP
8    END IF
9   ELSE IF (ssid OR bssid) == Trust-AP THEN
10   IF connect internal THEN
11    Report Rogue Type3
12    Store data to roguelv1
13   ELSE
14    Report Rogue Type2
15    Store data to Rogue tables
16   END IF
17  ELSE
18   IF connected over intranet THEN
19    Report Rogue Type1
20    Store data to roguelv1
21   ELSE
22    Report Rogue Type4
23   END IF
24  END IF
```

ภาพที่ 24 รหัสเทียมเพื่อใช้ระบุแอกเซสพอยต์เถื่อน

5.2 หน้าที่ค้นหาตำแหน่ง (Localization)

การค้นหาตำแหน่งเริ่มต้นโดยใช้ข้อมูลในตารางฐานข้อมูล roguelv1 ตรงกับตารางหมายเลข 7 ซึ่งเป็นตารางที่ใช้บันทึกรายชื่อแอกเซสพอยต์เถื่อน (roguelv1) การทำงานของการคนหาตำแหน่งได้คัดเลือกเฉพาะข้อมูลที่มีแอกเซสพอยต์ได้รับค่าความแรงสัญญาณที่มีค่ามากที่สุด ทำให้ได้ด้วยข้อมูลแอกเซสพอยต์องค์กรที่อยู่ใกล้เคียงกับแอกเซสพอยต์เถื่อนนั้น หลังจากนั้นค้นหาในฐานข้อมูลว่ามีสวิตช์ใดที่อยู่ใกล้บริเวณนั้นบ้าง และสอบถามผ่านโพรโทคอล SNMP เพื่อค้นหาจุดเชื่อมต่อโดยใช้ข้อมูลค่าอุปกรณ์เครือข่ายแลนไร้สายของสถานีลูกที่เชื่อมกับแอกเซสพอยต์ในข้อมูลตารางหมายเลข 7 ตามภาพที่ 25 ได้เสนอวิธีที่ใช้ในการค้นหาตำแหน่งโดยใช้ข้อมูลที่ได้จากโมดูลตรวจจับ

การทำงานของรหัสเทียมในภาพที่ 25 เริ่มต้นจากการอ่านข้อมูลแอกเซสพอยต์เถื่อนจาก จากตารางที่ 7 (roguelv1) พร้อมกับอ่านค่า หมายเลขอุปกรณ์เครือข่ายของสถานีลูก (st_mac) จากนั้น หลังจากนั้นค้นหาค่า st_mac ที่สื่อสารอยู่กับแอกเซสพอยต์เถื่อนซึ่งตรงกับข้อมูลในตาราง ที่ 7 ผลที่ได้เป็นค่าอุปกรณ์เครือข่ายของสถานีลูกที่เกิดเชื่อมกับแอกเซสพอยต์เถื่อน หลังจากที่พบข้อมูลการเชื่อมต่อของแอกเซสพอยต์เถื่อนจึงนำข้อมูลนั้นไปค้นหาจุดเชื่อมต่อของพอร์ตในสวิตช์ ซึ่งผลลัพท์ที่ได้จากการค้นหาได้แก่หมายเลขพอร์ตที่แอกเซสพอยต์เถื่อนเชื่อมอยู่

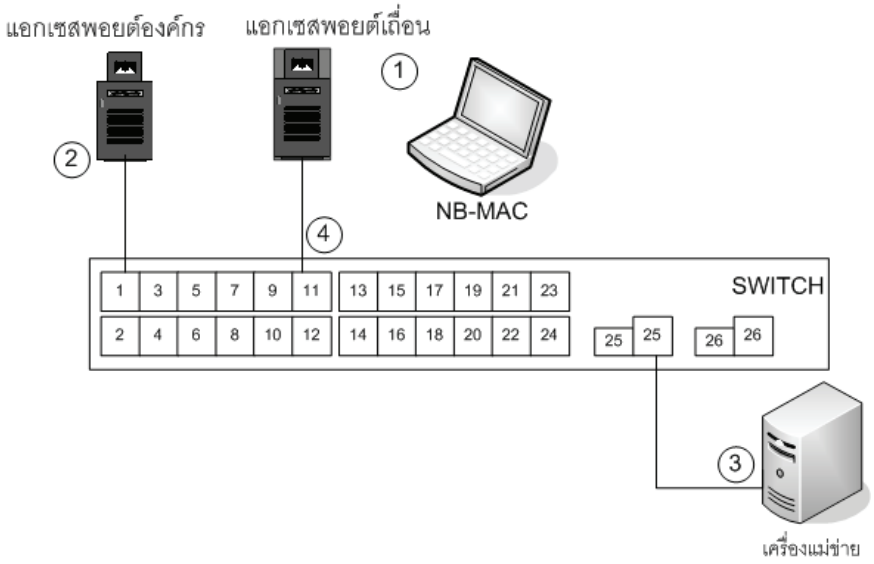
```
1   GET bssid from BSSID table
2   GET st_mac from ST_MAC table
3   WHILE bssid not Empty DO
4    WHILE st_mac not Empty DO
5     IF st_mac associate bssid THEN
6      port = snmp_query (st_mac)
7      IF port = empty THEN
8       Report Not Connect to intranet
9      ELSE
10      Report Connect in intranet
11      Disable Port
12     END IF
13    END DO
14  END DO
```

ภาพที่ 25 รหัสเทียมสำหรับระงับแอกเซสพอยต์เถื่อน

กลไกการค้นหาตำแหน่งที่ใช้ในวิทยานิพนธ์นี้อธิบายได้จากภาพที่ 26 จากภาพหน้าที่ของโมดูลค้นหาตำแหน่งได้แก่การรายงานหมายเลขพอร์ตที่แอกเซสพอยต์เถื่อนเชื่อมอยู่ หากการค้นหาทำงานถูกต้องจะต้องรายงานหมายเลข 11 ซึ่งเป็นหมายเลขพอร์ตที่แอกเซสพอยต์เถื่อนนั้นเชื่อมอยู่

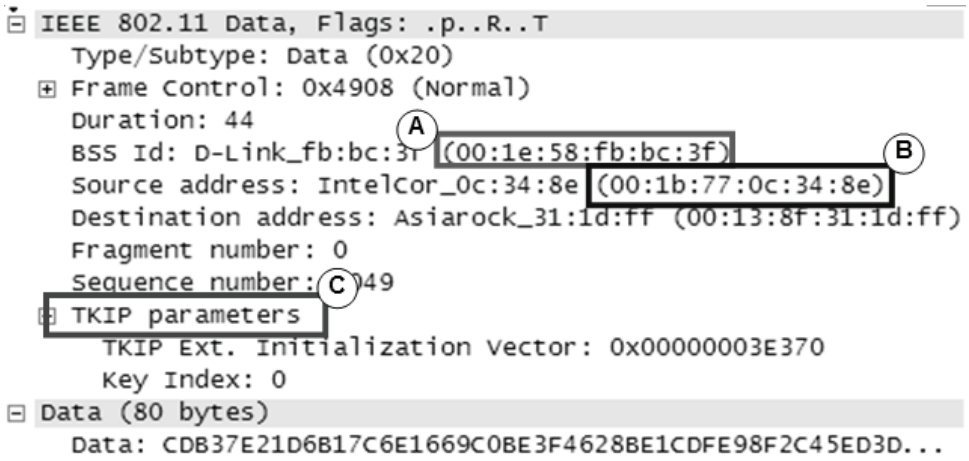
ขั้นตอนการค้นหาจุดเชื่อมต่อ (พอร์ตบนสวิตช์) มีขั้นตอนดังนี้ ลำดับที่ 1 สถานีลูกกำลังสื่อสารกับแอกเซสพอยต์เถื่อน ต่อมาในลำดับที่ 2 ได้รับคำสั่งจากเครื่องแม่ข่ายควบคุมสั่งงานให้แอกเซสพอยต์องค์กรเปลี่ยนสถานะเป็นอุปกรณ์ดักจับข้อมูลเพื่อให้ส่งข้อมูลกลับไปยังเครื่องแม่ข่ายควบคุมในลำดับที่ 3 ข้อมูลที่ส่งไปยังเครื่องแม่ข่ายควบคุมเป็นข้อมูลที่ประกอบด้วย ค่าหมายเลขอุปกรณ์เครือข่ายแลนไร้สายของแอกเซสพอยต์เถื่อนซึ่งได้จากเฟรมบีคอน และ ค่าหมายเลขอุปกรณ์เครือข่ายแลนไร้สายของสถานีลูกซึ่งได้จากเฟรมข้อมูล โดยที่เฟรมข้อมูลมีความสัมพันธ์กับหมายเลขอุปกรณ์เครือข่ายแลนไร้สายของแอกเซสพอยต์เถื่อนดังแสดงในภาพที่ 26 ค่าหมายเลขอุปกรณ์เครือข่ายแลนไร้สายของสถานีลูกได้ปรากฏในสวิตช์ ในลำดับที่ 4 เมื่อ

เครื่องแม่ข่ายทราบหมายเลขพอร์ตที่สถานีลูกเชื่อมอยู่ซึ่งหมายถึงจุดเชื่อมต่อของแอกเซสพอยต์เถื่อน จะทำการส่งคำสั่งไปควบคุมสวิตช์ให้เปลี่ยนหมายเลขแลนเสมือน ถือเป็นการเสร็จสิ้นกระบวนการ



ภาพที่ 26 วิธีค้นหาตำแหน่ง

ภาพที่ 27 ใช้เพื่ออธิบายการทำงานของเฟรมข้อมูลที่สัมพันธ์กับค่าหมายเลขอุปกรณ์เครือข่ายแลนไร้สายของแอกเซสพอยต์เถื่อน ที่สัญลักษณ์ A หมายถึงค่าหมายเลขอุปกรณ์เครือข่าย



ภาพที่ 27 เฟรมข้อมูลที่สัมพันธ์กับหมายเลขอุปกรณ์เครือข่ายแลนไร้สายของแอกเซสพอยต์เถื่อน

แลนไร้สายของแอกเซสพอยต์เถื่อน และ สัญลักษณ์ B หมายถึงค่าหมายเลขอุปกรณ์เครือข่ายแลนไร้สายของสถานีลูก โดยข้อมูลนี้เป็นข้อมูลสถานีลูกสื่อสารกับแอกเซสพอยต์เถื่อนแบบเข้ารหัสดังภาพในสัญลักษณ์ C เห็นได้ว่าการเข้ารหัสเครือข่ายแลนไร้สายไม่ได้ส่งผลต่อการค้นหาตำแหน่งจุดเชื่อมต่อของแอกเซสพอยต์แต่อย่างใด

ด้วยวิธีดังกล่าวนี้ เครื่องแม่ข่ายควบคุมจำเป็นต้องสามารถสื่อสารควบคุมสวิตช์ทุกเครื่องที่อยู่ในเครือข่ายองค์กร

5.3 หน้าที่ตอบโต้ (Countermeasure)

หน้าที่ตอบโต้ มีหน้าที่ในการระงับการเชื่อมต่อของแอกเซสพอยต์เถื่อน ภายในหน้าที่นี้อธิบายส่วนการทำงานแบบอัตโนมัติด้วยการส่งคำสั่งไปควบคุมสวิตช์เพื่อระงับการเชื่อมต่อของแอกเซสพอยต์เถื่อน โดยการนำข้อมูลที่อยู่ในตารางหมายเลข 7 และ 8 เพื่อเลือกวิธีการตอบโต้ ถ้ามีข้อมูลอยู่ในตาราง roguelv2 หมายถึงแอกเซสพอยต์เถื่อนนั้นสามารถส่งคำสั่งไปควบคุมสวิตช์เพื่อระงับการเชื่อมต่อได้ หรือ ในกรณีที่ไม่สามารถค้นหาจุดเชื่อมต่อได้ อาจเกิดจากแอกเซสพอยต์นั้นไม่ได้เชื่อมกับเครือข่ายองค์กร ผู้ดูแลระบบสามารถเลือกวิธีเข้าไปยังพื้นที่ต้องสงสัยโดยใช้ข้อมูลที่ได้รับรายงานจากแอกเซสพอยต์ที่อยู่ใกล้บริเวณนั้นมากที่สุด ซึ่งระบบจะทำการรายงานผลผ่านเว็บเพจแก่ผู้ดูแลเพื่อเข้าให้ไประงับการเชื่อมต่อ

6. โมดูลรายงาน (Report)

โมดูลรายงาน ทำหน้าที่รายงานการทำงานของระบบแก่ผู้ดูแลระบบ สำหรับวิทยานิพนธ์นี้เสนอวิธีการรายงานผ่านทางเว็บเพจโดยโปรแกรมประยุกต์ที่พัฒนาด้วยภาษาพีเอชพี

โปรแกรมประยุกต์สำหรับระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน

วิทยานิพนธ์นี้ได้พัฒนาโปรแกรมประยุกต์ที่พัฒนาด้วยเครื่องมือภาษาพีเอชพี เพื่อใช้ควบคุมระบบตรวจจับ และ ตอบโต้แอกเซสพอยต์เถื่อนผ่านทางเว็บเพจ เมื่อผู้ดูแลไม่ต้องการใช้งานระบบแบบอัตโนมัติ ภาพที่ 28 แสดงให้เห็นถึงส่วนติดต่อกับผู้ใช้งาน (GUI) ที่แสดงรายชื่อแอกเซสพอยต์องค์กร

แอกเซสพอยต์ที่ปรากฏในรายชื่อตามภาพที่ 28 สามารถถูกสั่งงานให้เปลี่ยนสถานะเป็นอุปกรณ์ดักจับข้อมูลไร้สายชั่วคราว โดยเรียกคำสั่งผ่านเมนู Actions และ ภายในเมนู Actions ได้เพิ่มเครื่องมือในการตรวจสอบจำนวนผู้ใช้งานแอกเซสพอยต์องค์กรในขณะนั้น สำหรับค่า -1 หมายถึงแอกเซสพอยต์นั้นไม่พร้อมให้บริการ หมายเลขตั้งแต่ 0 ขึ้นไปแสดงจำนวนผู้ใช้งานในขณะนั้น การตรวจนับจำนวนผู้ใช้งานแอกเซสพอยต์ในขณะนั้น ใช้เป็นทางเลือกให้แก่ผู้ดูแลเครือข่ายก่อนการตัดสินใจเปลี่ยนให้แอกเซสพอยต์ดักจับข้อมูลโดยพิจารณาจากตัวที่มีผลกระทบน้อยที่สุด หลังจากสั่งงานให้แอกเซสพอยต์ดักจับข้อมูลไร้สาย ผลการดักจับข้อมูลได้แสดงในภาพที่ 28

No.	AP	Label	Last Scan	Online	Actions
1	172.16.19.177	APFL7-7_CH01	0000-00-00 00:00:00	-1	
2	172.16.19.155	APFL5-5_CH01	2009-01-28 18:35:09	2	
3	172.16.19.154	APFL5-4_CH11	2008-12-16 23:32:46	5	
4	172.16.19.153	APFL5-3_CH06	2008-12-22 18:57:45	2	
5	172.16.19.152	APFL5-2_CH01	2009-01-08 18:58:16	5	
6	172.16.19.151	APFL5-1_CH11	2008-12-11 17:24:10	12	
7	172.16.19.145	APFL4-5_CH06	2009-01-06 17:53:03	4	
8	172.16.19.144	APFL4-4_CH01	2008-11-28 14:16:19	0	
9	172.16.19.143	APFL4-3_CH11	2008-12-16 23:32:46	6	
10	172.16.19.142	APFL4-2_CH06	2008-11-28 17:57:45	15	

ภาพที่ 28 รายชื่อแอกเซสพอยต์ขององค์กร

No.	APView	SSID	MAC	CH	RSSI	LastTime	Status	Actions
1	172.16.19.155	NTL_ISS	00095bea5f1c	5	170.600000	2009-01-28 18:35:01	Online	
2	172.16.19.123	LSR_thaisarn	001349152f30	7	187.416667	2009-01-28 18:20:20	Online	
3	172.16.19.123	TCLLAB	001563d40f40	4	174.266667	2009-01-28 18:20:12	Online	
4	172.16.19.155	NTL_WiFi6	001839edbbf2	9	169.000000	2009-01-28 18:35:05	Online	

Page : [1/1]

ภาพที่ 29 รายชื่อแอกเซสพอยต์เถื่อนที่ตรวจพบ

จากภาพที่ 29 ในคอลัมน์ SSID แสดงถึงรายชื่อแอกเซสพอยต์เถื่อนที่ระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อนตรวจพบ ภายในเว็บเพจมีเมนูคำสั่งให้ผู้ดูแลระบบตัดสินใจในการจัดการแอกเซสพอยต์เถื่อนนั้นจำนวน 2 ชุดคำสั่งซึ่งประกอบด้วย คำสั่งระงับการสื่อสาร และเพิกเฉย เมื่อผู้ดูแลระบบเลือกคำสั่งระงับการสื่อสาร ระบบจะทำการส่งคำสั่งควบคุมไปยังสวิตช์ที่

อยู่ใกล้แอกเซสพอยต์องค์กรซึ่งเป็นข้อมูลที่มีอยู่ในฐานข้อมูลอยู่แล้ว หลังจากนั้นจึงส่งคำสั่งค้นหาพอร์ตพร้อมกับเปลี่ยนค่าโดยปริยายแลนเสมือนให้เป็นหมายเลขอื่นที่กำหนดขึ้นพิเศษ เทคนิคการเปลี่ยนค่าแลนเสมือนนี้เมื่อใช้งานร่วมกับโปรแกรม Captive Portal (http://nocat.net) ช่วยให้ผู้ใช้งานที่เข้าเชื่อมต่อแอกเซสพอยต์เถื่อนทราบว่ากำลังเชื่อมผ่านเครือข่ายของผู้บุกรุกได้ หรือ เมื่อผู้ดูแลระบบเลือกคำสั่งเพิกเฉย ระบบจะนำข้อมูลแอกเซสพอยต์เถื่อนนั้นเพิ่มลงในรายชื่อแอกเซสพอยต์ที่ได้รับการยกเว้น เมื่อตรวจจับครั้งต่อไป รายชื่อแอกเซสพอยต์ดังกล่าวจะไม่ได้รายงานว่าเป็นแอกเซสพอยต์เถื่อนอีกต่อไป

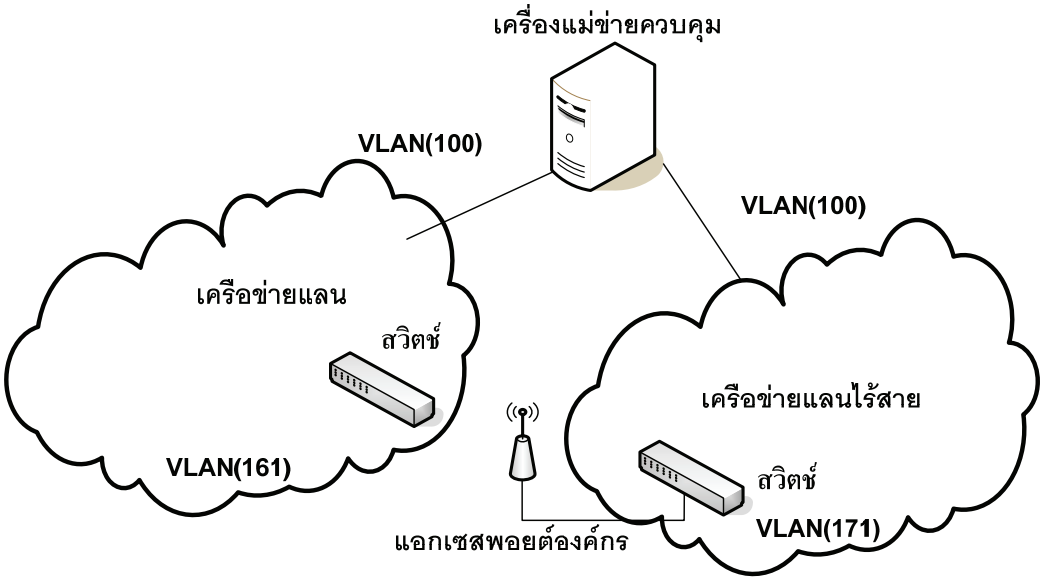
ระบบทดสอบ

ระบบทดสอบ คือ ระบบที่ใช้เพื่อทดสอบระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน สิ่งแวดล้อมที่ใช้อยู่ในระบบทดสอบเป็นสิ่งแวดล้อมจริง ที่ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ และ มหาวิทยาลัยเกษตรศาสตร์

สิ่งสำคัญที่ต้องคำนึงสำหรับระบบทดสอบ คือ สิ่งแวดล้อมที่ใช้ในการทดสอบมาจากสิ่งแวดล้อมใช้งานจริงซึ่งอาจส่งผลให้ผลการทดสอบมีความคลาดเคลื่อน ในการทดลองจึงควรทดลองในระยะเวลาที่เพียงพอเพื่อให้ผลการทดลองใกล้เคียงความเป็นจริงจนสามารถสรุปผลได้ เพื่อให้ผลการทดลองได้รับผลกระทบจากภายนอกน้อยที่สุด ในหัวข้อต่อไปได้รวบรวมสิ่งจำเป็นที่ต้องควบคุมในระบบทดสอบ ควรกำหนดคุณสมบัติสิ่งแวดล้อมให้ใกล้เคียงกัน ดังนี้

- เครื่องคอมพิวเตอร์ที่ใช้งานในระบบทดสอบควรใช้อุปกรณ์ที่มีประสิทธิภาพใกล้เคียงกัน
- ระบบปฏิบัติการที่ใช้ในระบบทดสอบควรเลือกใช้แกนระบบปฏิบัติการรุ่นเดียวกัน
- สวิตช์ที่เลือกใช้ในการทดลองควรเลือกใช้อุปกรณ์และเฟิร์มแวร์ รุ่นเดียวกัน
- แอกเซสพอยต์ที่เลือกใช้ในการทดลองควรเลือกอุปกรณ์และเฟิร์มแวร์ รุ่นเดียวกัน

ไดอะแกรมระบบทดสอบได้แสดงในภาพที่ 30 ระบบทดสอบนี้เป็นระบบที่มีการใช้งานจริง โดยได้แบ่งกลุ่มเครือข่ายแลนมีสายและเครือข่ายแลนไร้สายออกจากกันด้วยเทคโนโลยีแลนเสมือน (VLAN) โดยกำหนดให้เครือข่ายแลนมีสายมีค่าหมายเลขแลนเสมือนเท่ากับ VLAN#161 และ กำหนดให้เครือข่ายแลนไร้สายมีค่าแลนเสมือนเท่ากับ VLAN#171 และหมายเลขแลนเสมือนสำหรับควบคุมอุปกรณ์ในเครือข่ายได้แก่หมายเลข VLAN#100 นอกจากหมายเลขแลนเสมือนที่กล่าวถึงแล้ว ยังมีหมายเลขแลนเสมือนอื่นที่อยู่นอกเหนือการควบคุมรวมอยู่ในสวิตช์ด้วย



ภาพที่ 30 การเชื่อมต่อระบบทดสอบ

จากภาพที่ 30 เครื่องแม่ข่ายควบคุมได้รับการเชื่อมต่อเข้าในกลุ่มแลนเสมือนที่มีค่าหมายเลขแลนเสมือนเท่ากับ VLAN#100 แลนเสมือนในกลุ่มนี้ใช้สำหรับควบคุมอุปกรณ์ที่อยู่ในเครือข่าย เช่น สวิตช์ และ แอกเซสพอยต์ ค่าหมายเลขเสมือนอื่นใด ที่ไม่ได้กล่าวถึงในภาพที่ 30 อาจมีจำนวนมากเพราะอยู่ในระบบจริง ไม่ได้ส่งผลกระทบต่อการทำงานของระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน เพราะ ระบบต้องการเพียงสื่อสารกับอุปกรณ์เครือข่าย ไม่ได้จำเป็นต้องสื่อสารกับสถานีลูก

ผลและวิจารณ์

งานวิจัยนี้ใช้การทดสอบโดยใช้แอกเซสพอยต์ที่ทำงานในระบบจริง ภายในศูนย์เทคโนโลยี อิเล็กทรอนิกส์ และ คอมพิวเตอร์แห่งชาติ ตารางที่ 10 ได้แสดงถึงตัวแปรแอกเซสพอยต์องค์กร ที่อยู่ในการควบคุมของระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อนซึ่งใช้เป็นค่าสภาพแวดล้อมสำหรับการทดลองที่ 1 ถึง การทดลองที่ 3

ตารางที่ 10 ตัวแปรแอกเซสพอยต์องค์กร

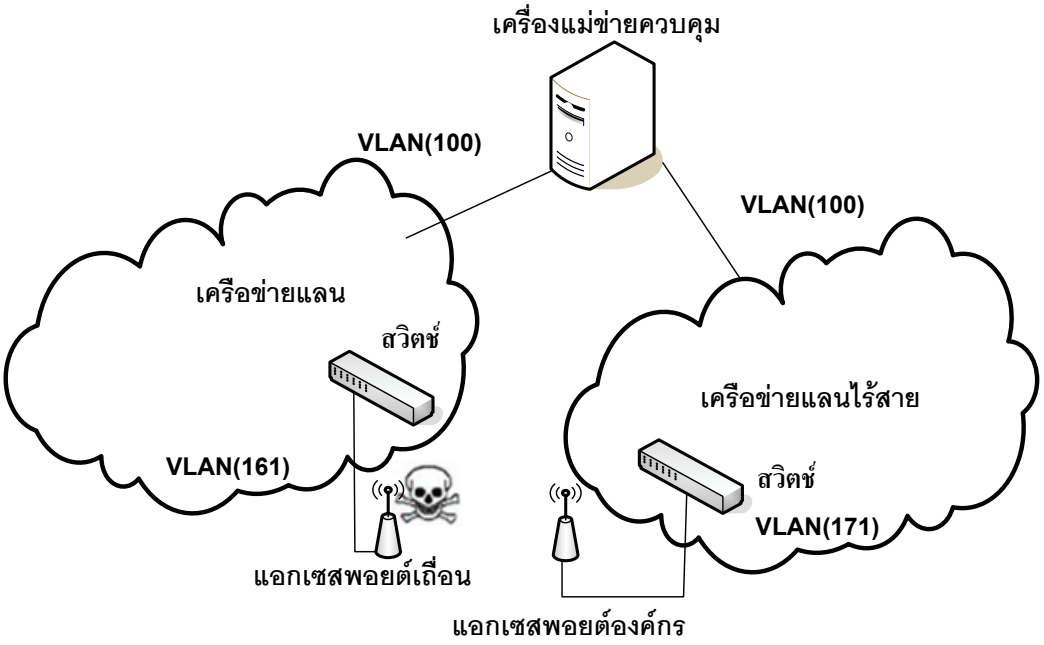
Order	IP address	SSID	Wireless MAC	Channel	Encryption
1	172.16.19.151	NSTDA-WIFI	001955cc4XXX	1	Open
2	172.16.19.152	NSTDA-WIFI	001955cc5XXX	6	Open
3	172.16.19.153	NSTDA-WIFI	001955cc5XXX	11	Open
4	172.16.19.154	NSTDA-WIFI	001955cc5XXX	1	Open
5	172.16.19.155	NSTDA-WIFI	001955cc5XXX	11	Open

การทดลองที่ 1

วัตถุประสงค์ของการทดลองที่ 1 เพื่อศึกษาความสามารถในการตรวจจับ และ ระงับการสื่อสารของแอกเซสพอยต์เถื่อนภายใต้การกำหนดค่าแอกเซสพอยต์เถื่อนในรูปแบบต่าง ๆ ที่ได้เสนอไว้ในหัวข้อชนิดของแอกเซสพอยต์เถื่อน(2.2)

1. แอกเซสพอยต์เถื่อนชนิดที่ 1

แอกเซสพอยต์ชนิดนี้เป็นแอกเซสพอยต์ที่ไม่ได้รับการกำหนดค่าใด ๆ ที่ตรงกับแอกเซสพอยต์ขององค์กร แต่แอกเซสพอยต์เถื่อนนี้ถูกเชื่อมเข้ากับเครือข่ายองค์กร ภาพที่ 31 แสดงถึงภาพการเชื่อมต่อของแอกเซสพอยต์เถื่อนในการทดลองนี้



ภาพที่ 31 แอกเซสพอยต์เถื่อนชนิดที่ 1

แอกเซสพอยต์ชนิดนี้เชื่อมเข้ากับเครือข่ายภายในองค์กร จากภาพที่ 31 ใช้หมายเลขแลนเสมือนหมายเลข VLAN#161 แทนเครือข่ายแลนมีสายของพนักงาน ในการศึกษานี้ระบบควรตรวจจับแอกเซสพอยต์ที่เกิดขึ้นได้ พร้อมกับ สามารถระงับการสื่อสารได้ ซึ่งในการทดลองได้ทำการเปลี่ยนแปลงข้อมูลของ แอกเซสพอยต์เถื่อน ในหลาย ๆ รูปแบบ เพื่อให้เห็นถึงความสามารถการตรวจจับและระงับการสื่อสารของระบบ ดังแสดงผลทดลองในตารางที่ 11 ข้อความ "ไม่ปลอม" ในคอลัมน์ Wireless MAC หมายถึงข้อมูลนั้นไม่ตรงกับแอกเซสพอยต์องค์กร

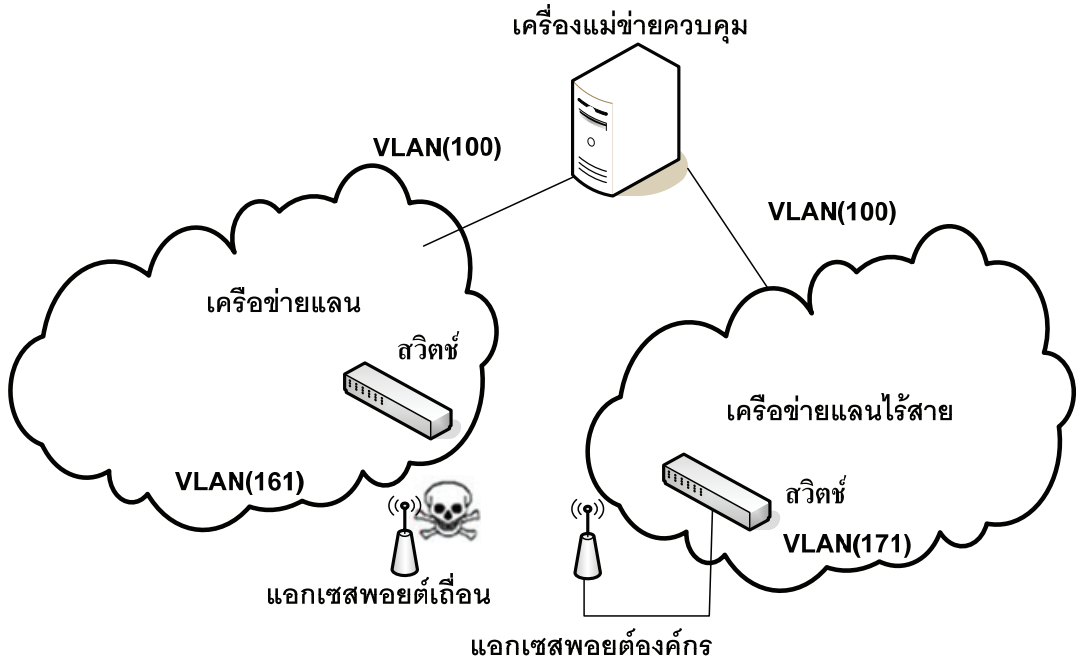
ตารางที่ 11 ผลการตรวจจับแอกเซสพอยต์เถื่อนชนิดที่ 1

ลำดับ	ชื่อเครือข่าย	Wireless MAC	เข้ารหัส	ผลตรวจพบ	ผลระงับ
1	Default	ไม่ปลอม	ไม่	ตรวจพบ	ได้
2	ENC-1	ไม่ปลอม	WPA2	ตรวจพบ	ได้
3	ENC-2	ไม่ปลอม	WPA	ตรวจพบ	ได้
4	ENC-3	ไม่ปลอม	WEP	ตรวจพบ	ได้
5	ซ่อนชื่อ	ไม่ปลอม	ไม่	ตรวจพบ	ได้
6	ซ่อนชื่อ	ไม่ปลอม	WPA	ตรวจพบ	ได้

จากผลการทดลองในตารางที่ 11 แสดงให้เห็นว่าระบบสามารถตรวจจับและตอบโต้แอกเซสพอยต์เถื่อนที่มีการเปลี่ยนแปลงข้อมูลในหลายรูปแบบได้ครบทุกการทดลอง จากผลการทดลองสังเกตได้ว่าการเข้ารหัสข้อมูลของแอกเซสพอยต์เถื่อนไม่ส่งผลต่อการตรวจจับและตอบโต้ เพราะวิทยานิพนธ์นี้ได้เลือกเฟรมการจัดการที่ตามมาตรฐานกำหนดว่าไม่มีการเข้ารหัสเพื่อใช้ในการตรวจจับ และ เลือกเฟรมข้อมูลที่ใช่เพื่อระงับการสื่อสารก็ไม่ได้ทำการเข้ารหัสในเฮดเดอร์ทำให้สามารถระงับการสื่อสารได้ หรือแม้กระทั่งแอกเซสพอยต์ที่กำหนดค่าให้ซ่อนชื่อเครือข่ายไร้สาย (Hidden SSID) ระบบนี้ยังสามารถตรวจพบ และ ระงับการสื่อสารได้ ทั้งนี้เพราะการซ่อนชื่อเครือข่ายเป็นเพียงการไม่ส่งชื่อออกมาแต่แอกเซสพอยต์เถื่อนยังคงปล่อยบีคอนออกมาตามคาบเวลาอยู่ดี จากผลการทดลองทั้งหมดแสดงให้เห็นได้ว่าผลเป็นไปตาม ผลที่คาดว่าจะได้รับ

2. แอกเซสพอยต์เถื่อนชนิดที่ 2

แอกเซสพอยต์ชนิดนี้เกิดจากผู้บุกรุกที่อยู่ภายนอก ได้สร้างเครือข่ายขึ้นมาเพื่อหลอกให้พนักงานเชื่อมต่อ ในการทดลองนี้จึงกำหนดให้แอกเซสพอยเถื่อนไม่ได้เชื่อมในเครือข่ายดังแสดงในภาพที่ 32 และ ได้เปลี่ยนแปลงการกำหนดค่าแอกเซสพอยต์เถื่อนให้มีข้อมูลบางส่วน หรือทั้งหมดคล้ายกับแอกเซสพอยต์องค์กรดังที่แสดงในตารางหมายเลข 10 ซึ่งผลการทดลองได้แสดงตามตารางที่ 12



ภาพที่ 32 แอกเซสพอยต์เถื่อนชนิดที่ 2

ผลการทดลองนี้ได้แสดงให้เห็นถึง ระบบสามารถตรวจจับแอกเซสพอยต์เถื่อนที่ได้รับการตั้งค่าให้มีข้อมูลบางข้อมูลคล้ายกับแอกเซสพอยต์องค์กร โดยที่ข้อความ ปลอม หรือ ไม่ปลอม ในคอลัมน์ ชื่อเครือข่าย และ Wireless MAC หมายถึง มีข้อมูลตรงกับแอกเซสพอยต์ในองค์กร และ ไม่มีข้อมูลตรงกับแอกเซสพอยต์ในองค์กรตามลำดับ

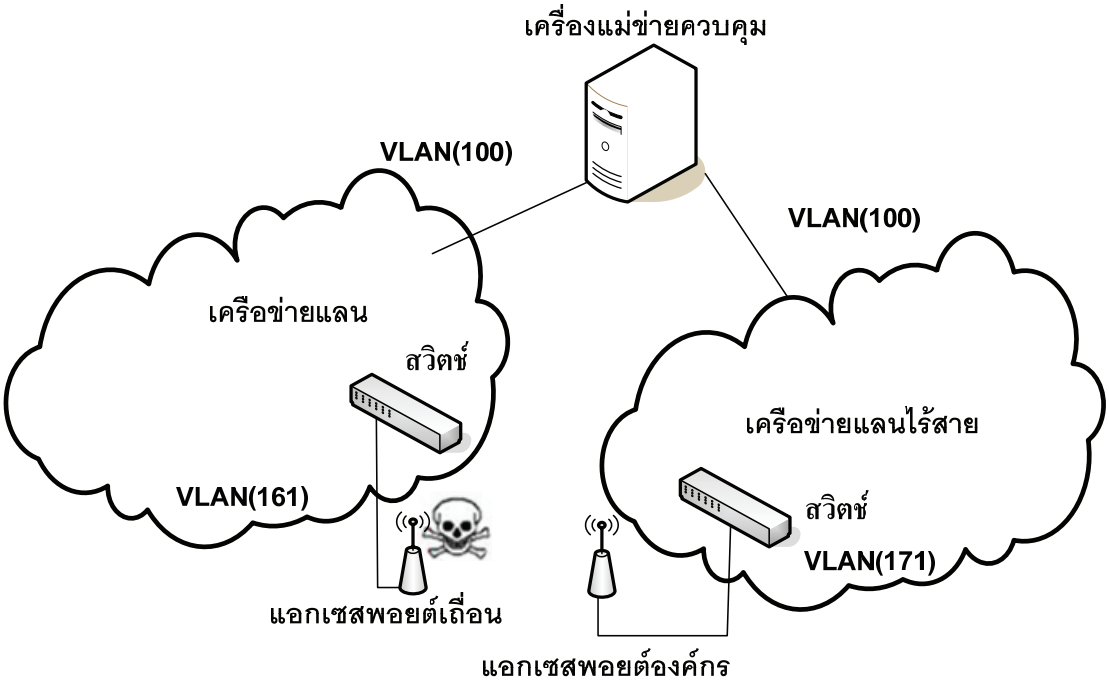
ตารางที่ 12 ผลการตรวจจับแอกเซสพอยต์เถื่อนชนิดที่ 2

ลำดับ	ชื่อเครือข่าย	Wireless MAC	เข้ารหัส	ผลตรวจพบ	ผลระงับ
1	ไม่ปลอม	ปลอม	ไม่	ตรวจพบ	ไม่ได้
2	ปลอม	ไม่ปลอม	ไม่	ตรวจพบ	ไม่ได้
3	ปลอม	ปลอม	ไม่	ตรวจพบ	ไม่ได้
4	ปลอม	ปลอม	เข้ารหัส	ตรวจพบ	ไม่ได้

จากตารางที่ 12 เป็นผลการทดลองความสามารถในการตรวจจับและตอบโต้แอกเซสพอยต์เถื่อนชนิดที่ 2 ด้วยการกำหนดให้แอกเซสพอยต์เถื่อนไม่ได้ทำการเชื่อมกับเครือข่ายองค์กร ในผลการทดลองลำดับที่ 1 ใช้การทดลองด้วยการเปลี่ยนค่าชื่อเครือข่ายแลนไร้สายให้ตรงกับแอกเซสพอยต์องค์กร เห็นได้ว่าระบบตรวจจับสามารถตรวจพบแอกเซสพอยต์เถื่อนได้ และ ที่น่าสนใจได้แก่ผลการทดลองลำดับที่ 3 และ 4 เพราะเป็นการทดลองด้วยการปลอมข้อมูล ชื่อเครือข่าย และหมายเลขอุปกรณ์เครือข่ายแลนไร้สายให้ตรงกับแอกเซสพอยต์องค์กร แอกเซสพอยต์เถื่อนที่กำหนดค่าในลักษณะนี้ไม่อาจตรวจจับได้โดยง่าย การเดินสำรวจของผู้ดูแลระบบ ไม่อาจแยกแยะว่าเครือข่ายแลนไร้สายนั้นเป็นแอกเซสพอยต์เถื่อนหรือแอกเซสพอยต์องค์กร แต่ผลจากการทดลองนี้แสดงให้เห็นว่าระบบสามารถตรวจพบแอกเซสพอยต์ที่มีการปลอมแปลงข้อมูลในลักษณะดังกล่าว ถึงแม้ว่าในการทดลองนี้จะไม่สามารถระงับการสื่อสารผ่านแอกเซสพอยต์เถื่อนนั้นได้ก็ตาม สาเหตุเพราะแอกเซสพอยต์เถื่อนดังกล่าวไม่ได้เชื่อมในเครือข่ายองค์กร

3. แอกเซสพอยต์เถื่อนชนิดที่ 3

แอกเซสพอยต์เถื่อนชนิดที่ 3 มีรูปแบบการเชื่อมต่อเหมือนกับแอกเซสพอยต์เถื่อนชนิดที่ 1 แต่มีความแตกต่างจากแอกเซสพอยต์ชนิดที่ 1 ตรงที่แอกเซสพอยต์เถื่อนดังกล่าวได้ทำการดัดแปลงให้มีข้อมูลบางส่วนหรือทั้งหมดคล้ายกับแอกเซสพอยต์องค์กร ดังแสดงในภาพที่ 33



ภาพที่ 33 แอกเซสพอยต์เถื่อนชนิดที่ 3

จากผลการทดลองแสดงในตารางที่ 13 ได้ทำการทดลองเลือกตัวอย่างการตั้งค่าแอกเซสพอยต์เถื่อนที่พบบ่อยจำนวน 4 การทดลอง จากผลการทดลองแสดงให้เห็นว่า ระบบสามารถตรวจพบแอกเซสพอยต์เถื่อน ได้ในทุกการทดลอง ถึงแม้ว่าว่าแอกเซสพอยต์นั้นได้ทำการเข้ารหัสข้อมูลแล้วก็ตามเพราะวิธีการที่เลือกใช้ในการค้นหาแอกเซสพอยต์เถื่อนได้เลือกรูปแบบเฟรมการจัดการซึ่งเป็นรูปแบบเฟรมที่ได้รับทำการเข้ารหัสข้อมูล และในการทดลองได้แสดงให้เห็นว่าสามารถระงับการสื่อสารได้ โดยที่การเข้ารหัสข้อมูลไม่ได้ส่งผลต่อการระงับการเชื่อมต่อ

ตารางที่ 13 ผลการตรวจจับแอกเซสพอยต์เถื่อนชนิดที่ 3

ลำดับ	ชื่อเครือข่าย	Wireless MAC	เข้ารหัส	ผลตรวจพบ	ผลระงับ
1	ปลอม	ไม่ปลอม	ไม่	ตรวจพบ	ได้
2	ปลอม	ปลอม	ไม่	ตรวจพบ	ได้
3	ปลอม	ปลอม	เข้ารหัส	ตรวจพบ	ได้
4	ไม่ปลอม	ปลอม	ไม่	ตรวจพบ	ได้

4. แอกเซสพอยต์เถื่อนชนิดที่ 4

แอกเซสพอยต์เถื่อนชนิดนี้บางครั้งไม่ได้รับการจัดกลุ่มให้เป็นแอกเซสพอยต์เถื่อน แต่วิทยานิพนธ์นี้ได้จัดให้อยู่ในกลุ่มแอกเซสพอยต์เถื่อนเพราะการส่งสัญญาณจากแอกเซสพอยต์อื่นที่ไม่ได้ใช้นโยบายเดียวกัน ถือเป็นการรบกวนสัญญาณได้ รูปแบบการเชื่อมต่อของแอกเซสพอยต์เถื่อนชนิดนี้คล้ายกับการเชื่อมต่อในภาพที่ 32 แต่แตกต่างตรงที่แอกเซสพอยต์ดังกล่าวไม่ได้รับการปรับแต่งให้มีข้อมูลคล้ายแอกเซสพอยต์องค์กร

ในตารางที่ 14 ได้แสดงผลการทดลองการตรวจจับแอกเซสพอยต์ชนิดที่ 4 ซึ่งเป็นแอกเซสพอยต์ที่อยู่ภายนอก และไม่มีข้อมูลใด ๆ ที่คล้ายกับแอกเซสพอยต์ในองค์กร และ ไม่ได้เชื่อมกับเครือข่ายภายในองค์กร ถึงแม้แอกเซสพอยต์ในกลุ่มนี้บางครั้งไม่ได้จัดให้อยู่ในกลุ่มแอกเซสพอยต์เถื่อน แต่สำหรับระบบตรวจจับแอกเซสพอยต์ไม่สามารถละเลยแอกเซสพอยต์ที่มีลักษณะเช่นนี้ได้ เพราะเป็นแอกเซสพอยต์ที่ไม่ได้ดำเนินการตามนโยบายขององค์กร และ ส่งสัญญาณควบคุม และในด้านความปลอดภัยอาจเป็นแอกเซสพอยต์ที่พนักงานเชื่อมต่อและส่งข้อมูลความลับผ่านเครือข่ายภายนอกโดยไม่ได้ตั้งใจ

ตารางที่ 14 ผลการตรวจจับแอกเซสพอยต์เถื่อนชนิดที่ 4

ลำดับ	ชื่อเครือข่าย	Wireless MAC	เข้ารหัส	ผลตรวจพบ	ผลระงับ
1	ไม่ปลอม	ไม่ปลอม	ไม่	ตรวจพบ	ไม่ได้
2	ไม่ปลอม	ไม่ปลอม	เข้ารหัส	ตรวจพบ	ไม่ได้

การทดลองที่ 2

การทดลองนี้มีวัตถุประสงค์เพื่อ ทดสอบเวลาการทำงานทั้งหมดของระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน ซึ่งได้รวมถึงการศึกษาช่วงเวลาที่คงที่ของอุปกรณ์ และ ช่วงเวลาใดที่สามารถปรับเปลี่ยนได้ โดยเริ่มตั้งแต่การสั่งงานให้แอกเซสพอยต์เปลี่ยนโหมดให้ดักฟังข้อมูล จนกระทั้งแอกเซสพอยต์กลับมาให้บริการปกติ การทดลองนี้ใช้วิธีการดักจับข้อมูลที่เครื่องแม่ข่ายตั้งแต่เริ่มส่งคำสั่งออกไปควบคุมแอกเซสพอยต์จนกระทั่งแอกเซสพอยต์คืนสู่สถานะปกติ ตารางที่ 15 ได้แสดงถึงตัวแปรแอกเซสพอยต์ที่ใช้ในการทดลอง

การทดลองนี้ได้กำหนดให้เครื่องแม่ข่ายควบคุมส่งคำสั่งให้แอกเซสพอยต์ดักจับข้อมูลช่องสัญญาณละ 1 วินาที รวมทั้งสิ้น 11 ช่องสัญญาณ ผลการทดลองได้แสดงไว้ดังภาพที่ 34 จากการทดลองทำให้ทราบเวลาที่ระบบใช้เพื่อทำการตรวจจับและระงับการสื่อสาร ในการทดลองได้ทดสอบกับแอกเซสพอยต์จำนวน 3 เครื่อง ซึ่งได้ให้ผลการทดลองที่ใกล้เคียงกัน

ตารางที่ 15 ตัวแปรแอกเซสพอยต์องค์กร

Order	ตัวแปร	ข้อมูล
1	ยี่ห้อ	ซิสโก้
2	โมเดล	Aironet
3	รุ่น	1121
4	เฟิร์มแวร์	12.3(8)JA
5	CH Sniff	1 วินาที
6	จำนวนช่องสัญญาณ	11 ช่อง

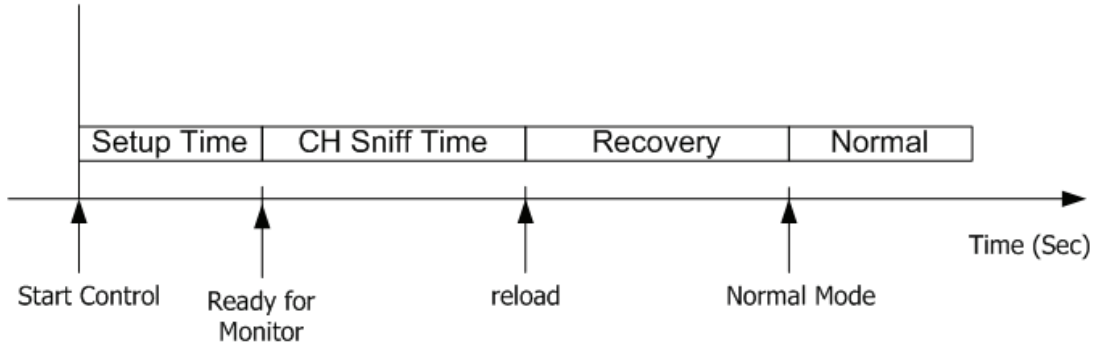
ภาพที่ 34 ได้แสดงถึงแผนภาพเวลาการทำงานของระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อนโดยเริ่มตั้งแต่เครื่องแม่ข่ายควบคุมส่งคำสั่งไปยังแอกเซสพอยต์เพื่อทำการเปลี่ยนสถานะให้เป็นอุปกรณ์ดักจับข้อมูลจนกระทั้งแอกเซสพอยต์พร้อมกับการดักจับ(Setup Time) หลังจากนั้นแอกเซสพอยต์จึงเริ่มจับข้อมูลและส่งกลับมายังเครื่องแม่ข่ายควบคุมโดยเริ่มดักจับข้อมูลทั้งหมด 11 ช่องสัญญาณโดยได้กำหนดให้ดักจับช่องสัญญาณละ 1 วินาที (CH Sniff Time) หลังจากดักจับข้อมูลเสร็จสิ้นครบทุกช่องสัญญาณ หลังจากนั้นเครื่องแม่ข่ายควบคุมจะสั่งงานให้แอกเซสพอยต์คืนสู่สถานะปกติ(Recovery)

ในการทดลองนี้ได้เลือกใช้วิธีส่งคำสั่งจากเครื่องแม่ข่ายควบคุม ด้วย ICMP-request ไปยังแอกเซสพอยต์องค์กร และปรับปรุงให้การส่ง ICMP-request มีความเร็วสูงที่สุด เพื่อให้ช่วงระยะเวลาในการวัดมีความแม่นยำกว่าการส่งด้วย ICMP-request ในแบบปกติ ในการทดลองนี้มีเป้าหมายเพื่อตรวจสอบความคงอยู่ของแอกเซสพอยต์ โดยตั้งสมมติฐานหาแอกเซสพอยต์ไม่สามารถตอบกลับ (ICMP-response) หมายถึงแอกเซสพอยต์นั้นไม่พร้อมใช้งาน ตารางที่ 16 แสดงถึงค่าตัวแปรในการตั้งค่าสำหรับ ping [http://en.wikipedia.org/Ping] เวลาที่ใช้ในการรายงานการไม่ตอบกลับข้อมูลแต่ละชุดใช้เป็นค่าเวลาบ่งชี้ความละเอียดของคาบเวลาในการทดลอง

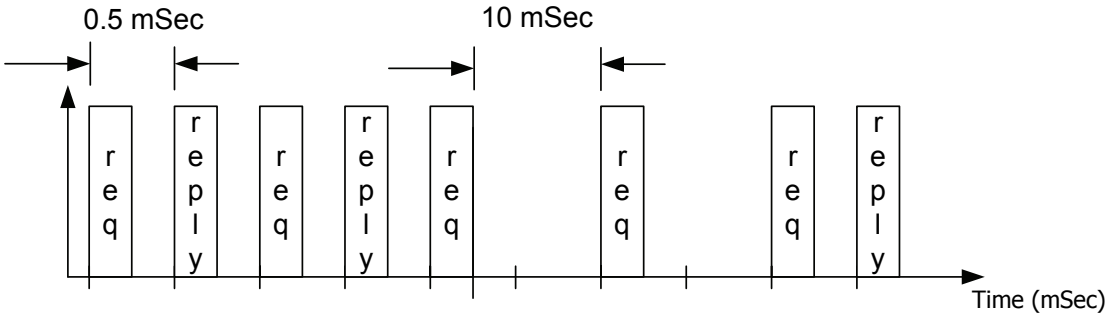
ภาพที่ 35 ได้แสดงถึงตัวอย่างของข้อมูลการทดสอบด้วย ping เพื่ออธิบายให้เกิดความเข้าใจในการทดลอง มาตรวัดที่แสดงในภาพไม่ได้อ้างอิงตามสเกลเพราะระยะห่างของข้อมูลแตกต่างมากเกินไป ภาพที่แสดงจึงเป็นการสรุปให้เห็นการทำงาน

ตารางที่ 16 ตัวแปรการทดสอบ ping

ตัวแปรในการทดลอง	พารามิเตอร์
คำสั่ง	ping -A 172.16.19.151
เวลาตอบกลับสั้นที่สุด	0.5 mSec
เวลาที่ใช้ในการรายงานการไม่ตอบกลับ	10 mSec



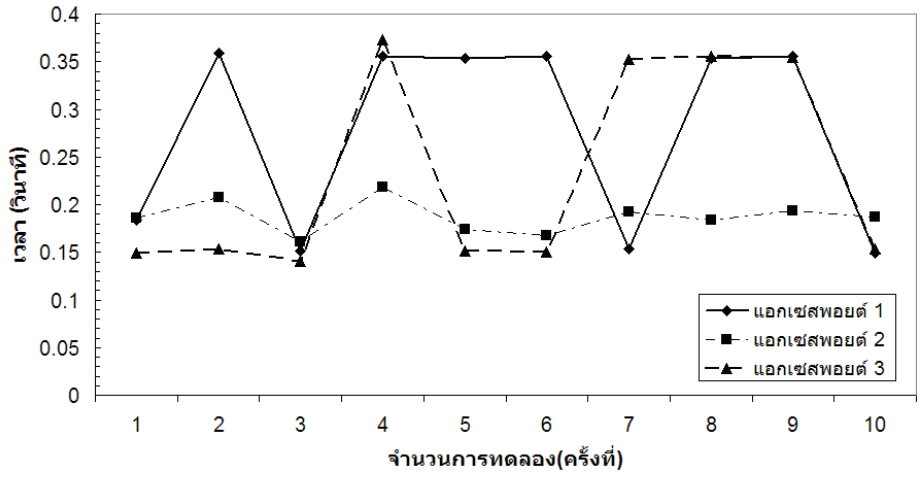
ภาพที่ 34 แผนภาพเวลาการทำงานของระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน



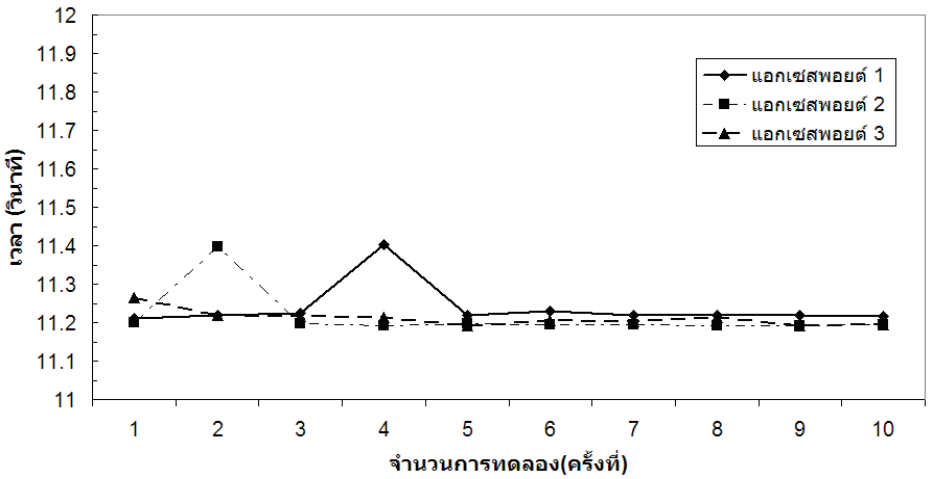
ภาพที่ 35 การเดินทางของข้อมูล ping

จากภาพที่ 35 เมื่อแอกเซสพอยต์อยู่ระหว่างการคืนสู่สถานะปกติ แอกเซสพอยต์นั้นจะไม่ตอบกลับข้อมูลที่โปรแกรม ping ส่งไปสอบถาม ทำให้เกิดช่วงเวลาที่ข้อมูลเงียบหายไป เป็นเวลา 10mSec ก่อนที่โปรแกรม ping จะส่งข้อมูลอีกครั้ง

ภาพที่ 36 แสดงถึงช่วงเวลาในการส่งคำสั่งควบคุมแอกเซสพอยต์จนกระทั่งแอกเซสพอยต์พร้อมส่งข้อมูลที่ได้จากการดักจับ วิธีในการทดสอบเริ่มจากการใช้โปรแกรม WireShark ดักจับข้อมูล SYN ของทีซีพี(TCP) ซึ่งเป็นชุดคำสั่งแรกที่ส่งออกจากเครื่องแม่ข่ายควบคุมแล้วเริ่มจับเวลาจนกระทั่งแอกเซสพอยต์ส่งข้อมูลที่ได้จากเครือข่ายไร้สายกลับมายังเครื่องแม่ข่ายควบคุม

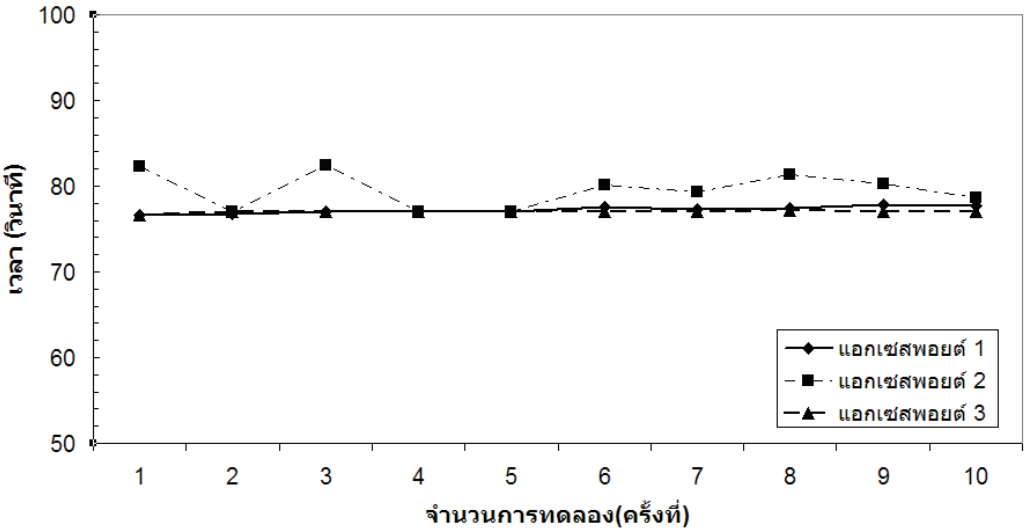


ภาพที่ 36 เวลาตั้งค่าให้แอกเซสพอยต์องค์กรเปลี่ยนสถานะเพื่อตรวจจับแอกเซสพอยต์เถื่อน

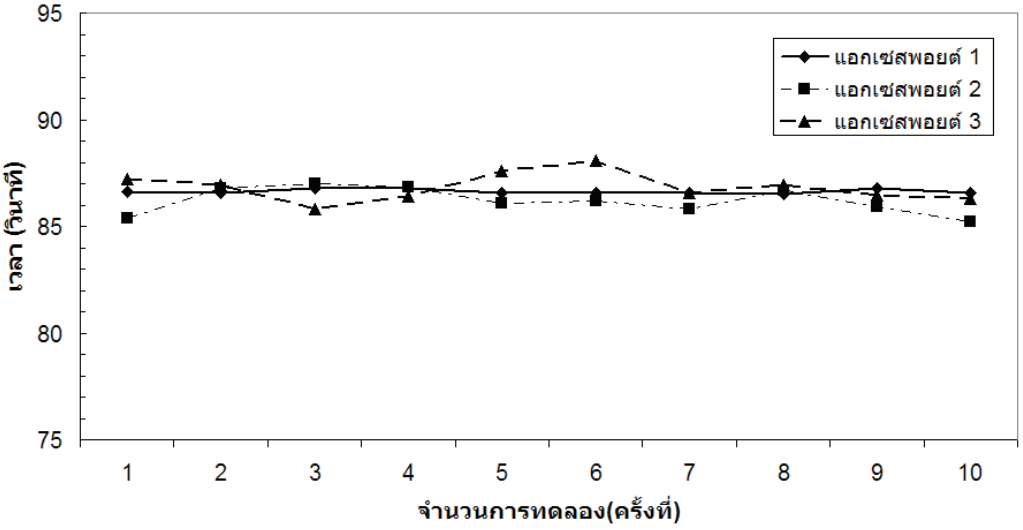


ภาพที่ 37 เวลาในการดักฟังข้อมูลครบ 11 ช่องสัญญาณ

ภาพที่ 37 แสดงถึง ช่วงเวลาในการดักจับข้อมูลโดยที่กำหนดให้เครื่องแม่ข่ายควบคุมควบคุมให้แอกเซสพอยต์ดักฟังข้อมูลตามตัวแปรที่กำหนดในตารางหมายเลข 15 จากภาพที่ 37 เห็นได้ว่าเครื่องแม่ข่ายควบคุมใช้เวลาในการดักฟังข้อมูลประมาณ 11 วินาที ในการจับข้อมูล 11 ช่องสัญญาณ และ ภาพที่ 38 แสดงถึงช่วงเวลาที่แอกเซสพอยต์คืนสู่สถานะปกติ ซึ่งแอกเซสพอยต์ที่ใช้ในการทดลองจำนวน 3 เครื่อง เป็นแอกเซสพอยต์ที่อยู่ในรุ่นเดียวกันจึงใช้เวลาในคืนสู่สถานะปกติใกล้เคียงกัน โดยใช้เวลาประมาณ 77.925 $\pm$ 0.01

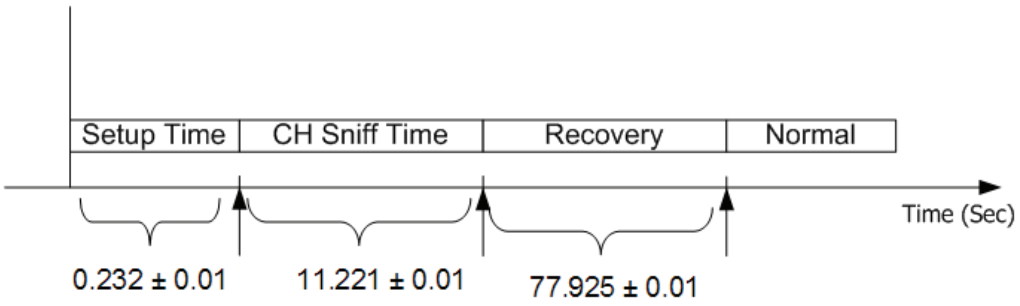


ภาพที่ 38 เวลาที่แอกเซสพอยต์คืนสู่สถานะปกติ



ภาพที่ 39 เวลาการทำงานรวมของระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน

ภาพที่ 39 และ ภาพที่ 40 แสดงถึงเวลารวมในการทำงานของระบบ สำหรับภาพที่ 39 เกิดจากทดลองวัดเวลาตั้งแต่เครื่องแม่ข่ายควบคุมส่งคำสั่งไปควบคุมแอกเซสพอยต์จนกระทั้งแอกเซสพอยต์กลับสู่สถานะปกติ (ตอบรับ ICMP-request) สำหรับ ภาพที่ 40 เกิดจากการนำผลการทดลองจากภาพที่ 36 , 37 และ 38 มาเขียนให้อยู่ในรูปแบบแผนภาพเวลา



ภาพที่ 40 แผนภาพเวลาการทำงานรวม

สรุปการทำงานโดยเฉลี่ยของแอกเซสพอยต์ 1 เครื่องใช่เวลาในการทำงานเท่ากับ 89.378 ± 0.01 วินาที ผลของการทดลองจะถูกนำไปใช้ในการวิเคราะห์เพื่อหาจำนวนครั้งที่เหมาะสมในการดักฟังข้อมูลในแต่ละวันซึ่งจะกล่าวในหัวข้อ การวิเคราะห์ช่วงเวลาในการตรวจจับที่เหมาะสม

การทดลองที่ 3

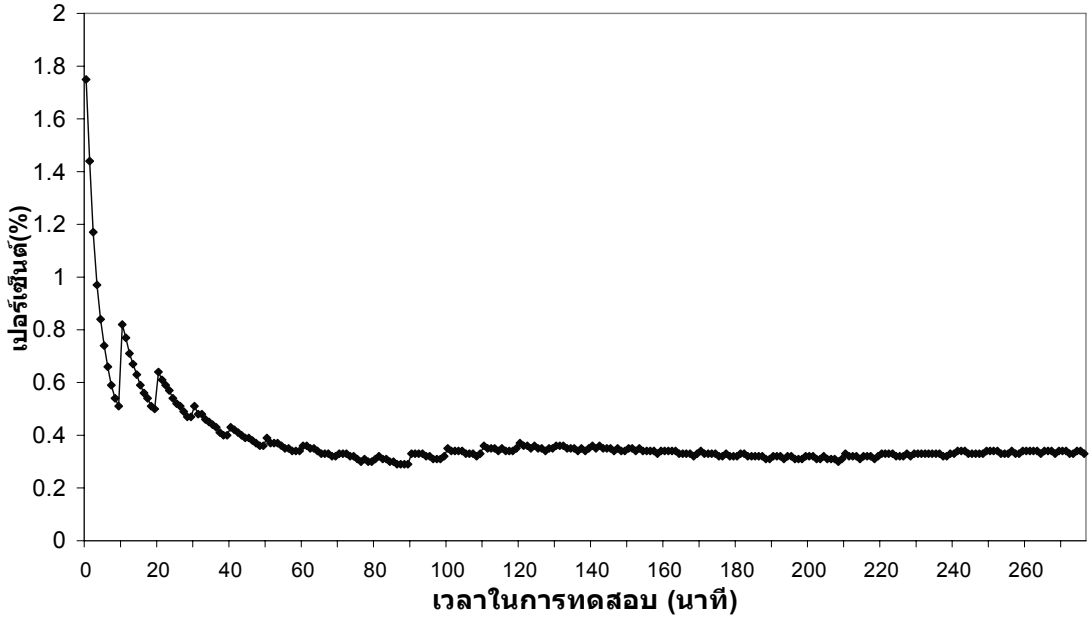
การทดลองนี้มีวัตถุประสงค์เพื่อทดสอบประสิทธิภาพการทำงานของเครื่องแม่ข่ายโดยเปรียบเทียบระหว่าง ก่อนการติดตั้งซอฟต์แวร์ และ หลังจากที่ซอฟต์แวร์กำลังทำงาน เพื่อใช้ในการพิจารณาการเลือกเครื่องข่ายเพื่อนำมาใช้กับระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน

1. เปรียบเทียบประสิทธิภาพการใช้งานหน่วยประมวลผล

ภาพที่ 41 แสดงถึง ผลต่างของปริมาณการใช้หน่วยประผลเมื่อเครื่องแม่ข่ายไม่ได้ติดตั้งซอฟต์แวร์ กับ ปริมาณการใช้หน่วยประมวลผลเมื่อซอฟต์แวร์กำลังทำงาน จากกราฟได้แสดงผลความแตกต่างของการใช้หน่วยประมวลผล จากกราฟเห็นได้ว่า หลังจากทดลองนำซอฟต์แวร์ไปทำงานที่เครื่องแม่ข่าย มีการเปลี่ยนแปลงน้อยมาก

2. เปรียบเทียบประสิทธิภาพการใช้เนื้อที่เก็บข้อมูล

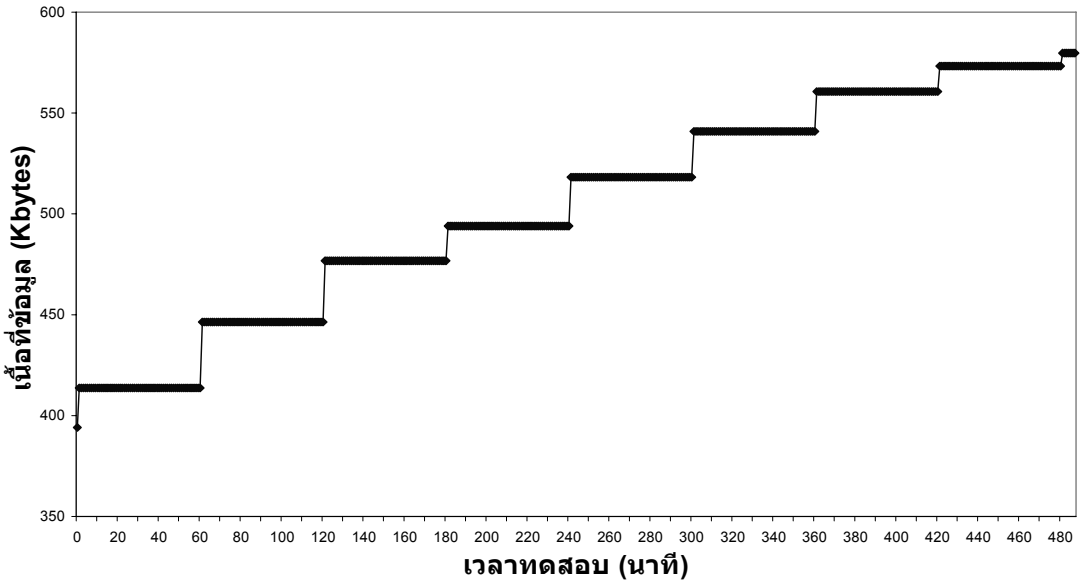
ในการทดลองนี้มีวัตถุประสงค์เพื่อทดสอบการใช้งานเนื้อที่ข้อมูล การทดลองนี้เป็นการทดสอบแอกเซสพอยต์เพียงเครื่องเดียวด้วยการทดลองสั่งงานให้ระบบทำการตรวจจับและตอบโต้แอกเซสพอยต์ทำงานทุก 1 ชั่วโมง และตรวจสอบเนื้อที่ทุก 1 นาที จากภาพที่ 42 สังเกตได้ว่าข้อมูลได้มีการปรับขนาดเพิ่มขึ้นทุกชั่วโมง ซึ่งข้อมูลจะเพิ่มทุกครั้งที่มีการสั่งงานให้ตรวจจับ แต่การปรับขนาดมีขนาดลดลงเรื่อย ๆ ทั้งนี้เกิดจากข้อมูลที่ได้รับการบันทึกไว้แล้ว จะไม่ได้รับการเพิ่มข้อมูลอีกครั้ง สำหรับข้อมูลที่เพิ่มขึ้นนั้นโดยมากเกิดจากข้อมูลการสื่อสารของสถานีลูก



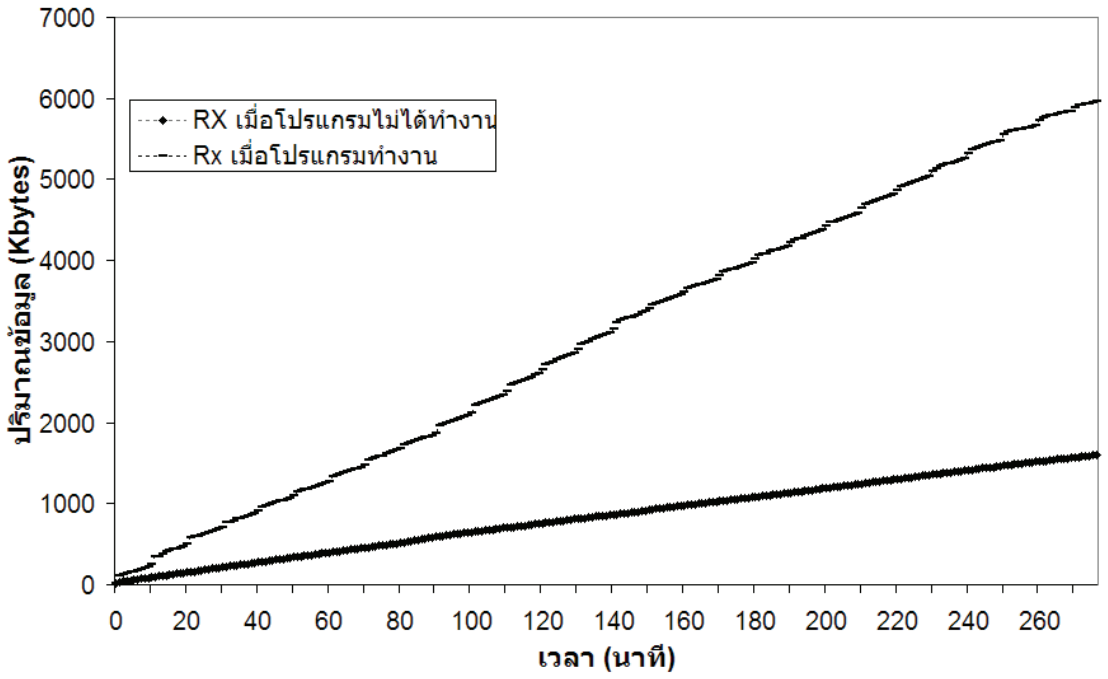
ภาพที่ 41 ผลต่างของการว่างงานซีพียูระหว่างไม่มีโปรแกรมกับมีโปรแกรมตรวจจับกำลังทำงาน

3. เปรียบเทียบประสิทธิภาพการใช้ทรัพยากรเครือข่าย

การทดลองนี้มีวัตถุประสงค์เพื่อทดสอบการทำงานของเครือข่าย เพื่อให้ทราบถึงปริมาณข้อมูลที่ส่งผ่านเครือข่ายมาสู่แอกเซสพอยต์ ในการทดลองนี้ได้ทดลองกับระบบที่ทำงานจริง ด้วยการอ่านข้อมูลทุก 1 นาที และ สั่งงานให้ระบบตรวจจับทำงานทุก 10 นาที จากภาพที่ 43 สังเกตได้ว่าข้อมูลที่ส่งมาสู่เครื่องแม่ข่าย มีปริมาณน้อยเนื่องจากได้ควบคุมแอกเซสพอยต์ให้ตัดข้อมูลส่วนที่ไม่จำเป็นออกไปก่อนส่งมายังเครื่องแม่ข่ายควบคุม ดังนั้นขนาดข้อมูลที่ส่งผ่านเครือข่ายแลนมายังเครื่องแม่ข่ายจึงมีเพียงข้อมูลที่มีความจำเป็นในการใช้วิเคราะห์เพื่อค้นหาแอกเซสพอยต์เถื่อน



ภาพที่ 42 ขนาดการใช้งานเนื้อที่สำหรับเก็บข้อมูล



ภาพที่ 43 ปริมาณการใช้ทรัพยากรเครือข่าย

การวิเคราะห์ช่วงเวลาในการตรวจจับที่เหมาะสม

ระบบตรวจจับและตอบโต้แอกเซสพอยต์นี้เป็นระบบที่สั่งงานแอกเซสพอยต์ให้เปลี่ยนสถานะชั่วขณะเป็นอุปกรณ์ดักจับข้อมูลไร้สาย เมื่อรับข้อมูลเสร็จสิ้นจึงคืนสภาวะเป็นปกติ ข้อจำกัดของการใช้งานแอกเซสพอยต์ในลักษณะนี้เกิดจากในขณะที่แอกเซสพอยต์อยู่ระหว่างดักจับข้อมูลทำให้ไม่สามารถให้บริการเครือข่ายแลนไร้สายได้ เวลาที่ใช้ในการตรวจจับจึงส่งกระทบแก่บริการ ดังนั้นจำนวนครั้งในการเปลี่ยนสถานะของแอกเซสพอยต์ควรเลือกให้เหมาะสมกับองค์กร สำหรับภาพที่ 44 ช่วยให้ผู้ดูแลระบบสามารถเลือกช่วงเวลาในการดับจับข้อมูลให้เหมาะสมกับความต้องการ โดยภาพที่ 44 แสดงความสัมพันธ์ระหว่างค่าสภาพพร้อมใช้งาน อธิบายได้ด้วยสมการต่อไปนี้ โดยกำหนดให้

μ หมายถึง เวลารวมที่ใช้ในการทำงานของระบบตรวจจับแอกเซสพอยต์เถื่อนหน่วยเป็นวินาที

$A_T(n)$ หมายถึง ค่าสภาพพร้อมใช้งาน

n หมายถึง ช่วงรอบเวลาในการเปลี่ยนสถานะ หน่วยเป็นจำนวนครั้ง

$$A_T(n) = \frac{n-\mu}{n} \tag{1}$$

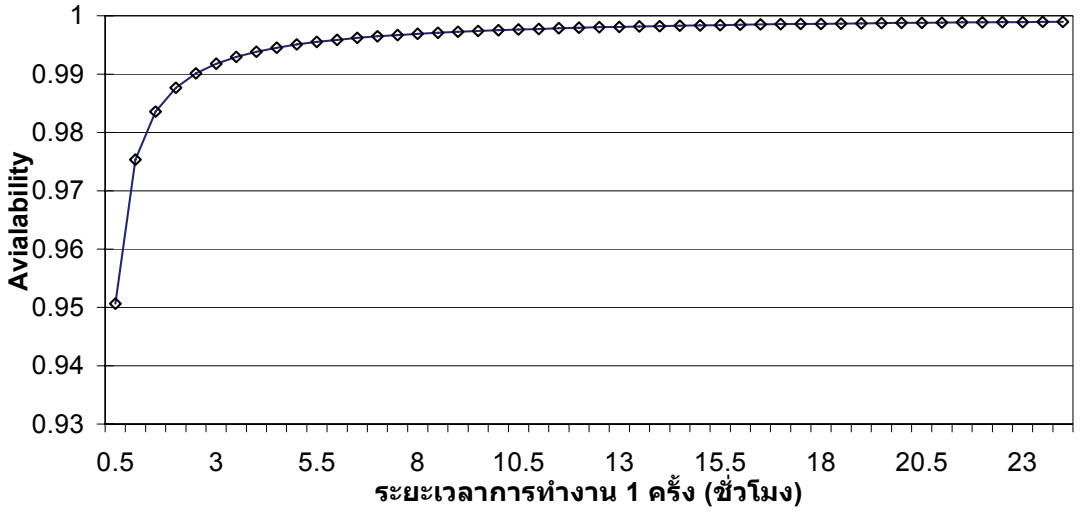
แทนค่าคงที่ซึ่งได้จากการทดลอง 2 ค่าเฉลี่ยในการทำงานของระบบเท่ากับ 89.378 $\pm$0.01 ทำให้ได้สมการ (2)

$$A_T(n) = \frac{n-89.378}{n} \tag{2}$$

เมื่อนำสมการที่ 2 แทนค่า n ทำให้ความสัมพันธ์ดังแสดงในภาพที่ 44 ซึ่งเป็นความสัมพันธ์ระหว่างค่าสภาพพร้อมใช้งานกับจำนวนรอบที่ต้องการดักจับข้อมูล

จากกราฟภาพที่ 44 ได้แสดงให้เห็นถึงความสัมพันธ์ของอัตราการเปลี่ยนสถานะของแอกเซสพอยต์ในหนึ่งวันเปรียบเทียบกับค่าความพร้อมใช้งาน ซึ่งผลของกราฟนี้นิยมนำไปใช้อ้างอิงถึงความพร้อมใช้ของการให้บริการซึ่งเรียกว่า SLA (Service Lavel Agreement) การเปลี่ยนแปลง

ระยะเวลาในการทำงานของระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน จะส่งผลต่อค่าความพร้อมใช้งานของแอกเซสพอยต์นั้น ๆ



ภาพที่ 44 ความสัมพันธ์ระหว่างค่าสภาพพร้อมใช้งานกับจำนวนรอบที่ต้องการดักจับข้อมูล

สรุปและข้อเสนอแนะ

สรุป

ระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน เป็นระบบที่มีความจำเป็นสำหรับองค์กรที่ต้องการสื่อสารอย่างปลอดภัย ไม่เว้นแม้กระทั้งองค์กรที่ไม่มีเครือข่ายแลนไร้สายใช้งาน เพราะแอกเซสพอยต์นั้นเป็นอุปกรณ์ที่มีราคาถูกทำให้บุคคลทั่วไปสามารถซื้อและติดตั้งได้เองโดยง่าย รวมถึงแอกเซสพอยต์สามารถทำงานร่วมกับเครือข่ายแลนมีสายได้โดยไม่ต้องปรับแต่งใด ๆ เพียงนำสายแลนเชื่อมกับแอกเซสพอยต์ ก็ทำให้เครือข่ายแลนไร้สายสื่อสารกับเครือข่ายแลนมีสายได้ทันที เนื่องจากความสะดวกเหล่านี้ทำให้พนักงานที่ไม่ได้ตระหนักถึงความเสียหายที่เกิดจากแอกเซสพอยต์เถื่อนนำแอกเซสพอยต์มาติดตั้งด้วยตนเองโดยที่ผู้ดูแลเครือข่ายไม่ล่วงรู้ ซึ่งอาจเป็นสาเหตุให้ผู้บุกรุกเข้าโจมตีเครือข่ายได้ง่าย นอกจากนี้แอกเซสพอยต์เถื่อนยังเกิดขึ้นจากผู้ที่ประสงค์ร้ายมีเจตนาโจมตีเครือข่ายด้วยการปรับปรุงแอกเซสพอยต์ให้มีข้อมูลบางประการเพื่อใช้หลอกล่อให้เป้าหมายสื่อสารผ่านเครือข่ายตนเอง รวมถึงผู้บุกแอบนำแอกเซสพอยต์มาติดตั้งในจุดแลนที่ลับตาคนแล้วปลอมแปลงข้อมูลให้คล้ายกับแอกเซสพอยต์ขององค์กรเพื่อป้องกันการล่วงรู้ของผู้ดูแลเครือข่าย ด้วยวิธีการเหล่านี้นำมาซึ่งภัยที่ส่งผลร้ายต่อองค์กรทั้งสิ้น ตารางที่ 17 ได้แสดงถึงการสรุปความสามารถของระบบตรวจจับและตอบโต้แอกเซสพอยต์เถื่อน

ข้อเสนอแนะ

วิทยานิพนธ์นี้ได้เสนอวิธีตรวจจับ และ ตอบโต้แอกเซสพอยต์เถื่อนซึ่งมีความสามารถตรวจพบแอกเซสพอยต์ในทุกการทดสอบ แต่จากการทดลองแสดงให้เห็นว่าไม่สามารถระงับการสื่อสารของแอกเซสพอยต์เถื่อนที่อยู่ภายนอกองค์กร หรือ ระงับการสื่อสารของแอกเซสพอยต์ที่ทำงานใน Layer-3 ซึ่งใช้ความสามารถการทำ NAT (Network Address Translation) ได้ แนวทางการระงับการสื่อสารในแบบอัตโนมัติสามารถทำได้หลายวิธีซึ่งวิธีที่น่าศึกษาได้แก่การติดตั้งอุปกรณ์เซนเซอร์ที่ราคาถูก เช่น แอกเซสพอยต์ที่สามารถดัดแปลงให้สามารถติดตั้งระบบปฏิบัติการลินุกซ์เพื่อทำการควบคุมให้แอกเซสพอยต์จำลองเป็นสถานีลูกเพื่อทดสอบส่งข้อมูลผ่านแอกเซสพอยต์ Layer-3 เพื่อใช้ตรวจสอบการเชื่อมกับแอกเซสพอยต์ในองค์กร หรือ แม้กระทั้งการเลือกอุปกรณ์เซนเซอร์ที่มีความสามารถในการส่งข้อมูลระงับการเชื่อมต่อ (De-authentication) ไปยังแอกเซสพอยต์เถื่อน เพื่อระงับการสื่อสารของเครื่องลูกข่ายไม่ให้เชื่อมต่อกับแอกเซสพอยต์เถื่อนในกรณีที่แอกเซสพอยต์เถื่อนนั้นไม่ได้เชื่อมกับเครือข่ายองค์กร

งานวิจัยนี้เลือกวิธีการเก็บข้อมูลลงฐานข้อมูล ทำให้ในอนาคตสามารถพัฒนาต่อยอดจากข้อมูลที่ได้รับจากแอกเซสพอยต์ได้ง่าย เช่น การค้นหาพิกัดของแอกเซสพอยต์ โดยใช้ค่าความแรงของสัญญาณที่แอกเซสพอยต์แต่ละตัวได้รับ หรือ การนำข้อมูลที่ได้ไปวิเคราะห์เพื่อค้นหาพฤติกรรมการบุกรุกเครือข่าย

เอกสารและสิ่งอ้างอิง

Adya, Atul, Bahl Paramvir, Chandra Ranveer and Qiu Lili. 2004. Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks, pp. 30-44. **International Conference on Mobile Computing and Networking 10th**, Philadelphia.

Bahl, Paramvir, Chandra Ranveer, Padhye Jitendra, Ravindranath Lenin, Singh Manpreet, Wolman Alec and Zill Brian. 2006. Enhancing the security of corporate Wi-Fi networks using DAIR, pp. 1-14. **International Conference on Mobile Systems, Applications and Services 4th,** Uppsala.

Beyah, Raheem, Kangude Shantanu, Yu George, Strickland Brian and Copeland John. 2004. Rogue access point detection using temporal traffic characteristics, pp. 2271-2275. **Global Telecommunications Conference 47th**, Dallas.

Borisov, Nikita, Goldberg Ian and Wagner David. 2001. Intercepting mobile communications: the insecurity of 802.11, pp. 180-189. **International Conference on Mobile Computing and Networking 7th,** New York.

Chad, D., Mano, Blaich Andrew, Liao Qi, Jiang Yingxim, Cieslak A. David, Salyers C. David and Striegel Aaron. 2008. RIPPS: rogue identifying packet payload slicer detecting unauthorized wireless hosts through network traffic conditioning. **ACM Trans. Inf. Syst. Secur** 11(2):1-23.

Libes, Don. 2006. **Tool for automating interactive application expect - expect - home page**. Available Source: http://expect.nist.gov, February 4, 2009.

Lyon, Gordon. 1997. **Nmap - Wikipedia, the free encyclopedia**. Available Source: http://en.wikipedia.org/wiki/Nmap, March 22, 2009.

Ma, Liran, Teymorian Y. Amin, Cheng Xiuzhen. 2007. Passive listening and intrusion management in commodity Wi-Fi networks, pp. 327-331. **Global Telecommunications Conference 50th**, North West Washington.

Sachin, Shetty, Song Min and Ma Liran. 2007. Rogue access point detection by analyzing network traffic characteristics, pp. 1-7. **Military Communications Conference 39th**, Orlando.

Scarfone, Karen, Dicoi Derrick, Sexton Matthew and Tibbs Cyrus. 2008. **Guide to securing legacy IEEE 802.11 wireless networks**. Available Source: http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf, March 22, 2009.

Srilasak, Songrit, Wongthavarawat Kitti, PhonPhoem Anan. 2008. Integrated wireless rogue access point detection and counterattack system, pp. 326-331. **Information Security and Assurance 1st,** Busan.

Watkins, Lanier, Beyah Raheem and Corbett Cherita. 2007. A passive approach to rogue access point detection, pp. 355-360. **Global Telecommunications Conference 50th.** North West Washington.

Wei, Wei, Suh Kyoungwon, Wang Bing, Gu Yu, Kurose Jim and Towsley Don. 2007. Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-pairs, pp. 365-378. **ACM SIGCOMM Conference on internet Measurement 7th**. New York.

Wilson, Piers. 2003. Rogue Servers. **Network security** 10(8):16-18.

Yin, Hongda, Chen Guanling and Wang Jie. 2007. Detecting protected layer-3 rogue APs, pp. 449-458. **Broadband Communications Networks and Systems 4th**. North Carolina.

ภาคผนวก

ตัวอย่างชุดคำสั่งควบคุมอุปกรณ์

1. ชุดคำสั่งสำหรับควบคุมแอกเซสพอยต์ซิสโก้ รุ่น AP1121

```
#!/usr/bin/expect -f
#\
exec tclsh "$0" ${1+"$@"}
package require Expect
package require mysqltcl

set rds "/etc/rds.conf"

set force_conservative 0  ;
if {$force_conservative} {
        set send_slow {1 .1}
        proc send {ignore arg} {
                sleep .1
                exp_send -s -- $arg
        }
}

proc readconfig {fname attribute} {
        if {[file exists $fname]} {
            set fd [open $fname r]
        } else {
            puts "Can't find $fname or perms are bad"
            exit
        }

        while {![eof $fd]} {
            set data [gets $fd]
            if {[string index $data 0] == "#" || \
                    [string index $data 0] == " " || \
                    [string index $data 0] == ""} {
                continue
            }
        if {[lindex $data 0] == "$attribute" } {return [lindex
$data 1]}
        }
        catch {close $fd}
        return
}


if { $argc !=1 } {
 puts "Using :"
 puts "./scan-telnet.exp <ip>"
 puts "Example: ./scan-telnet.exp 192.168.1.1"
} else {
set ap_ip [lindex $argv 0]

set username [readconfig $rds "sql_username"]
set password [readconfig $rds "sql_password"]
set server [readconfig $rds "sql_server"]
set database [readconfig $rds "sql_database"]


set db [mysqlconnect -h $server -u $username -password
$password]
```

```
54  mysqluse $db ryg
55  set user [mysqlsel $db "SELECT user FROM authorize_ap WHERE ip
    = '$ap_ip'" -list]
56  set password [mysqlsel $db "SELECT password FROM authorize_ap
    WHERE ip = '$ap_ip'" -list]
57  set rics [mysqlsel $db "SELECT value FROM setting WHERE
    attribute = 'rics_ip'" -list]
58  set duration [mysqlsel $db "SELECT value FROM setting WHERE
    attribute = 'duration'" -list]
59  set truncate [mysqlsel $db "SELECT value FROM setting WHERE
    attribute = 'truncate'" -list]
60
61  set timeout -1
62  spawn telnet $ap_ip
63  match_max 100000
64  expect -exact "Username: "
65  send -- "$user\r"
66  expect -exact "Password: "
67  send -- "$password\r"
68  set timeout $duration
69  expect -exact "#"
70  send -- "conf t"
71  expect -exact "conf t"
72  send -- "\r"
73  expect -exact "(config)#"
74  send -- "int dot11Radio 0"
75  expect -exact "int dot11Radio 0"
76  send -- "\r"
77  expect -exact "(config-if)#"
78  send -- "no mbssid"
79  expect -exact "no mbssid"
80  send -- "\r"
81  send -- "channel 1"
82  expect -exact "channel 1"
83  send -- "\r"
84  expect -exact "(config-if)#"
85  send -- "station-role scanner"
86  expect -exact "station-role scanner"
87  send -- "\r"
88  expect -exact "(config-if)#"
89  send -- "monitor frames endpoint ip address $rics port 5222
    truncate $truncate"
90  expect -exact "monitor frames endpoint ip address $rics port
    5222 truncate $truncate"
91  send -- "\r"
92  expect -exact "(config-if)#"
93  expect timeout
94
95  send -- "channel 2"
96  expect -exact "channel 2"
97  send -- "\r"
98  expect "(config-if)#"
99  expect timeout
100
101 send -- "channel 3"
102 expect -exact "channel 3"
103 send -- "\r"
104 expect "(config-if)#"
105 expect timeout
```

```
106
107 send -- "channel 4"
108 expect -exact "channel 4"
109 send -- "\r"
110 expect "(config-if)#"
111 expect timeout
112
113 send -- "channel 5"
114 expect -exact "channel 5"
115 send -- "\r"
116 expect "(config-if)#"
117 expect timeout
118
119 send -- "channel 6"
120 expect -exact "channel 6"
121 send -- "\r"
122 expect "(config-if)#"
123 expect timeout
124
125 send -- "channel 7"
126 expect -exact "channel 7"
127 send -- "\r"
128 expect "(config-if)#"
129 expect timeout
130
131 send -- "channel 8"
132 expect -exact "channel 8"
133 send -- "\r"
134 expect "(config-if)#"
135 expect timeout
136
137 send -- "channel 9"
138 expect -exact "channel 9"
139 send -- "\r"
140 expect "(config-if)#"
141 expect timeout
142
143 send -- "channel 10"
144 expect -exact "channel 10"
145 send -- "\r"
146 expect "(config-if)#"
147 expect timeout
148
149 send -- "channel 11"
150 expect -exact "channel 11"
151 send -- "\r"
152 expect timeout
153
154 expect -exact "(config-if)#"
155 send -- "exit\r"
156 expect -exact "(config)#"
157 send -- "exit\r"
158 expect -exact "#"
159
160 send -- "reload\r"
161 expect -exact "reload\r
162 \r
163 System configuration has been modified. Save? \[yes/no\]: "
164 send -- "no\r"
```

```
165  expect -exact "no\r
166  Proceed with reload? \[confirm\]"
167  send -- "\r"
168
169  #send -- "exit\r"
170  expect eof
171  mysqlclose $db
172  }
```

2. ชุดคำสั่งสำหรับสอบถามตำแหน่งการเชื่อมต่อของสวิตช์ SMC รุ่น 6726AL2

```
 1  #!/bin/sh
 2
 3  ip=$1
 4  mac=$2
 5  community=$3
 6
 7  #community=public
 8  #community=research-monitor
 9  #Alliend
10  #OID = 1.3.6.1.2.1.3.1.1.2.8.1
11  first=`snmpwalk -v 1 -Os $ip -c $community
12  .1.3.6.1.2.1.17.4.3.1.1 | grep "$mac" | cut -d= -f 1 | cut -d.
    -f 7-`
13  if [ -n "$first" ]; then
14  Bridge=`snmpwalk -v 1 -Os $ip -c $community
    .1.3.6.1.2.1.17.4.3.1.2.$first | cut -d" " -f4`
15  ifIndex=`snmpwalk -v 1 -Os $ip -c $community
    .1.3.6.1.2.1.17.1.4.1.2.$Bridge | cut -d" " -f4`
16  ifName=`snmpwalk -v 1 -Os $ip -c $community
    .1.3.6.1.2.1.31.1.1.1.1.$ifIndex | cut -d" " -f4`
17  echo $equipo" "`echo $mac | tr -s " " ":"`" "$ip" "$ifName
18  fi
```

3. ชุดคำสั่งสำหรับควบคุมสวิตช์

3.1 สวิตช์ SMC รุ่น 6726AL2

```
 1  #!/bin/sh
 2  #\
 3  exec tclsh "$0" ${1+"$@"}
 4  package require Expect
 5  package require mysqltcl
 6
 7  set force_conservative 0
 8  if {$force_conservative} {
 9        set send_slow {1 .1}
10        proc send {ignore arg} {
11              sleep .1
12              exp_send -s -- $arg
13        }
```

```
14  }
15
16  proc readconfig {fname attribute} {
17          if {[file exists $fname]} {
18              set fd [open $fname r]
19          } else {
20              puts "Can't find $fname or perms are bad"
21              exit
22          }
23
24          while {![eof $fd]} {
25              set data [gets $fd]
26              if {[string index $data 0] == "#" || \
27                      [string index $data 0] == " " || \
28                      [string index $data 0] == ""} {
29                  continue
30              }
31          if {[lindex $data 0] == "$attribute" } {return [lindex
    $data 1]}
32          }
33          catch {close $fd}
34          return
35  }
36
37  if { $argc !=0 } {
38   puts "Using :"
39   puts "./deny-smc.exp"
40   puts "Example: ./deny-smc.exp"
41  } else {
42
43  set rds "/etc/rds.conf"
44  set username [readconfig $rds "sql_username"]
45  set password [readconfig $rds "sql_password"]
46  set server [readconfig $rds "sql_server"]
47  set database [readconfig $rds "sql_database"]
48
49  set db [mysqlconnect -h $server -u $username -password $password]
    mysqluse $db ryg
50  set switch_ip [mysqlsel $db "SELECT DISTINCT switch FROM roguelv2
    WHERE investigate = '0'" -list]
51  set rogue_port [mysqlsel $db "SELECT DISTINCT port FROM roguelv2
    WHERE investigate = '0' AND switch ='$switch_ip'" -list]
52  set quarantine_vlan [mysqlsel $db "SELECT value FROM `default`
    WHERE attribute = 'vlan_quarantine'" -list]
53  set current_vlan [mysqlsel $db "SELECT current_vlan FROM vlan
    WHERE switch ='$switch_ip' AND port ='$rogue_port' AND tag ='0'"
54  -list]

55  set sw_user [mysqlsel $db "SELECT user FROM switch WHERE ip =
    '$switch_ip'" -list]
56  set sw_password [mysqlsel $db "SELECT password FROM switch WHERE
    ip = '$switch_ip'" -list]

57  set timeout -1
58  spawn telnet $switch_ip
59  match_max 100000
60  expect -exact "Username: "
61  send -- "$sw_user\r"
62  expect -exact "Password: "
```

```
63  send -- "$sw_password\r"
64  expect -exact "#"
65  send -- "conf\r"
66  expect -exact "(config)#"
67  send -- "int eth 1/$rogue_port\r"
68  expect -exact "(config-if)#"
69  send -- "switchport allowed vlan add $quarantine_vlan untagged"
70  expect -exact "switchport allowed vlan add $quarantine_vlan
    untagged"
71  send -- "\r"
72  expect -exact "(config-if)#"
73  send -- "switchport native vlan $quarantine_vlan"
74  expect -exact "switchport native vlan $quarantine_vlan"
75  send -- "\r"
76  expect -exact "(config-if)#"
77  send -- "switchport allowed vlan remove $current_vlan"
78  expect -exact "switchport allowed vlan remove $current_vlan"
79  send -- "\r"
80  expect -exact "(config-if)#"
81  send -- "exit\r"
82  expect -exact "(config)#"
83  send -- "exit\r"
84  expect -exact "#"
85  send -- "exit\r"
86  send -- "exit\r"
87
88  mysqlsel $db "UPDATE roguelv2 SET investigate='1' WHERE
    switch='$switch_ip' AND port='$rogue_port'" -list
89  mysqlsel $db "UPDATE vlan SET previous_vlan='$current_vlan' WHERE
    switch='$switch_ip' AND port='$rogue_port'" -list
90  mysqlsel $db "UPDATE vlan SET current_vlan='$quarantine_vlan'
    WHERE switch='$switch_ip' AND port='$rogue_port'" -list

91  expect eof
92  }
```

ประวัติการศึกษา และการทำงาน

ชื่อ –นามสกุล	นายทรงฤทธิ์ ศรีลาศักดิ์
วัน เดือน ปี ที่เกิด	15 พฤษภาคม 2522
สถานที่เกิด	นครพนม
ประวัติการศึกษา	ปริญญาวิศวกรรมศาสตรบัณฑิต(วิศวกรรมคอมพิวเตอร์) มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
ตำแหน่งหน้าที่การงานปัจจุบัน	วิศวกร1
สถานที่ทำงานปัจจุบัน	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ