การตรวจสอบการปลอมแปลงหมายเลข MAC ในเครือข่าย IEEE 802.11 โดยใช้เฟรม ACK

Detecting IEEE 802.11 MAC Address Spoofing using ACK frames

ชัญญมน ศรีคล้าย[1] และ **ประวิทย์ ชุมชู**[2]

[1]ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีมหานคร

[2]ภาควิชาวิศวกรรมโทรคมนาคม คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีมหานคร

140 ถนนเชื่อมสัมพันธ์ แขวงกระทุ่มราย เขตหนองจอก กรุงเทพฯ 10530

Email: project1_s@hotmail.com, prawit@mut.ac.th

Manuscript received June 1, 2010
Revised November 15, 2010

บทคัดย่อ

การตรวจสอบการปลอมหมายเลข MAC นั้นเป็นวิธีการที่เพิ่มการรักษาความมั่นคงของเครือข่ายไร้สาย IEEE 802.11 ขั้นพื้นฐาน วิธีการตรวจสอบการปลอมแปลงหมายเลข MAC ประกอบด้วย การตรวจสอบโดยใช้การตรวจสอบความผิดปกติของเลขลำดับของเฟรม การตรวจสอบความผิดปกติของความแรงของสัญญาณ และ การตรวจสอบความแตกต่างของสัญญาณ ข้อเสียของการตรวจสอบการปลอมแปลงหมายเลข MAC ดังกล่าว คือ ไม่สามารถให้ผลการตรวจสอบได้ถึง 100 เปอร์เซ็นต์ บทความนี้นำเสนอการตรวจสอบการปลอมแปลงหมายเลข MAC แบบใหม่โดยใช้ความแตกต่างของเฟรม ACK ของผู้ใช้งานถูกต้องและผู้ไม่ประสงค์ดี ผลการทดลองแสดงให้เห็นว่าวิธีการที่นำเสนอสามารถเพิ่มความถูกต้องในการตรวจสอบการปลอมแปลงหมายเลข MAC ได้มากกว่าการตรวจการปลอมแปลงด้วยวิธีการตรวจความผิดปกติของเลขลำดับของเฟรม

คำสำคัญ: ระบบไร้สาย, ความปลอดภัย, การตอบรับข้อมูล

ABSTRACT

Detection of IEEE 802.11 MAC address spoofing is very importance for improve security in IEEE 802.11 networks. The detection algorithms comprise of MAC Sequence number abnormal, signal strength analysis and transceiver fingerprint. In this paper, we propose to use the difference of ACK frames sent by the genuine station and attacker stations to detect MAC address spoofing. The experiment results show that the proposed algorithm works better than using MAC sequence number abnormal. The proposed algorithm provides 100% of corection if the number of monitor stations is high enough.

Keywords: *IEEE 802.11, Wireless, Security, MAC Address Spoofing, Sequence Number, Acknowledgement*

1 บทนำ

การใช้งานระบบเครือข่ายไร้สายในปัจจุบันกำลังเป็นที่นิยมมากขึ้น เพราะเนื่องจากความสะดวกและง่ายในการใช้งาน เครือข่ายไร้สายเป็นการส่งผ่านข้อมูลผ่านอากาศจึงง่ายต่อการขโมยข้อมูล ปลอมแปลงหรือโจมตีระบบ เป็นเหตุให้มีการพัฒนาระบบรักษาความมั่นคงปลอดภัยขึ้น การรักษาความมั่นคงปลอดภัยนี้มีหลายหลายวิธีที่ใช้งานกันโดยแพร่หลายอาทิเช่น การคัดกรอง

หมายเลข MAC (Media Access Control Address) การเข้ารหัส (Data Encryption) การพิสูจน์ตัวจริง (Authentication) เป็นต้น การคัดกรองหมายเลข MAC เป็นวิธีการพื้นฐานของการพิสูจน์ตัวจริงที่ใช้งานกันแพร่หลายเนื่องจากง่ายต่อการใช้งาน แต่การคัดกรองหมายเลข MAC นั้นสามารถปลอมแปลงได้ง่าย การตรวจสอบการปลอมแปลงหมายเลข MAC จึงเป็นงานวิจัยที่นักวิจัยได้นำเสนอมาแล้ว ซึ่งสามารถแบ่งออกได้ 3 แบบ คือ การตรวจสอบด้วยการตรวจสอบความผิดปกติของ ลำดับของเฟรม [1], [2] วิธีการตรวจการปลอมแปลงนี้ง่ายต่อการสร้างแต่มีข้อเสียคือ ผู้ไม่หวังดีสามารถลอกเลียนแบบลำดับของเฟรมได้ซึ่งทำให้วิธีนี้ไม่สามารถทำให้ถูกต้องได้ 100%

การตรวจการปลอมแปลงหมายเลขแม็คอีกวิธีคือ การตรวจสอบรูปแบบของสัญญาณที่ส่งของเครื่องรับส่ง (Transceiver Fingerprint) [3] วิธีนี้จะต้องสร้างเครื่องรับสัญญาณที่ระดับสื่อสารที่ 1 (physical layer) ซึ่งยากต่อการผลิตจริงและไม่สามารถใช้กับเครื่องรับส่งที่ผลิตจากบริษัทเดียวและรุ่นเดียวกัน

การตรวจสอบอีกวิธีคือ การตรวจสอบความแตกต่างของความแรงของสัญญาณ [4] – [7] ซึ่งมีความแตกต่างระหว่างสัญญาณที่ส่งโดยผู้ใช้งานปกติและผู้ไม่ประสงค์ดี เนื่องจากความแรงของสัญญาณจะมีค่าแบบสุ่มซึ่งจำเป็นต้องใช้หลักทางสถิติเพื่อใช้ในการตรวจสอบซึ่งทำให้เป็นไปได้ยากมากที่จะสามารถตรวจสอบให้มีความถูกต้อง 100% การเพิ่มความถูกต้องของการตรวจสอบของวิธีนี้สามารถกระทำได้โดยการเพิ่มจำนวนจุดตรวจสอบซึ่งทำให้ยากต่อการใช้งานจริง

บทความนี้นำเสนอการการตรวจสอบการปลอมแปลงหมายเลข MAC โดยการวิเคราะห์ความแรงของสัญญาณที่ใช้ส่งเฟรมตอบกลับ (Acknowledgment Frame : ACK) และความแตกต่างของเฟรม ACK ในระดับชั้นสื่อสารที่ 1 ที่ส่งโดยสถานีผู้ไม่ประสงค์ดีและสถานีผู้ใช้งานปกติ ซึ่งวิธีการที่นำเสนอนี้จะมีประสิทธิภาพกว่าการใช้การวิเคราะห์ความแรงของสัญญาณที่ใช้ส่งเฟรมข้อมูล (DATA) เนื่องจากเฟรม ACK เป็นเฟรมตามมาตรฐานของเครือข่าย IEEE 802.11 ที่สถานีเครื่องเมื่อได้รับเฟรมต้องทำการส่งเฟรม ACK เพื่อแจ้งการได้รับ ในขณะที่เฟรมข้อมูลผู้ไม่ประสงค์ดีไม่จำเป็นต้องส่งถ้าไม่ต้องการใช้งานเครือข่าย วิธีการตรวจสอบการปลอมแปลงหมายเลข MAC ที่นำเสนอในส่วนของการตรวจสอบความแตกต่างของเฟรมของระดับชั้นสื่อสารที่ 1 ไม่จำเป็นต้องใช้หลักทางสถิติซึ่งสามารถทำให้ผลการตรวจการปลอมแปลงหมายเลข MAC ได้ 100% ซึ่งได้พิสูจน์ด้วยการทดลองจริง

2 การรักษาความมั่นคงของเครือข่ายไร้สาย IEEE 802.11

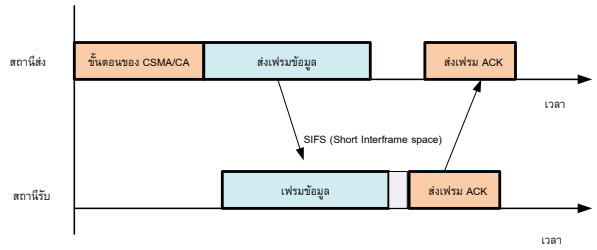
เครือข่ายไร้สาย IEEE 802.11 เป็นมาตรฐานที่มีใช้จริง (De facto Standard) ในเครือข่ายท้องถิ่นไร้สาย ปัจจุบันเครือข่ายไร้สายได้ใช้งานแพร่หลายไม่ว่าในธุรกิจขนาดเล็กหรือขนาดใหญ่ การสื่อสารในเครือข่ายไร้สายมีข้อมูลหลายประเภทเช่น ข้อมูลสื่อสารในชีวิตประจำวันทั่วไป ข้อมูลด้านการเงิน ข้อมูลทางการบริหารขององค์กร เป็นต้น ด้วยเหตุนี้เองระบบรักษาความมั่นคงของเครือข่ายไร้สาย IEEE 802.11 จึงมีความสำคัญมาก

2.1 ภาพรวมเครือข่ายไร้สาย IEEE 802.11

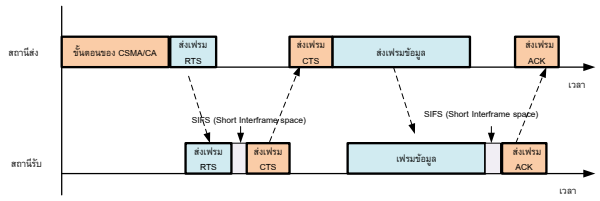
ปัจจุบันการเชื่อมต่อระบบอินเตอร์เน็ตที่ได้รับความนิยมก็คือระบบเครือข่ายไร้สาย IEEE 802.11 เพราะเนื่องจากการใช้งานที่สะดวก รวดเร็ว ให้พื้นที่บริการที่กว้าง อีกทั้งยังประหยัดค่าใช้จ่ายเพราะการติดตั้งสถานีแม่ข่าย (Access Point : AP) และมีการ์ดไร้สาย (Wireless Card) ติดตั้งที่เครื่องลูกข่ายเพียงแค่นี้ก็สามารถใช้งานระบบเครือข่ายได้แล้ว เครือข่ายไร้สาย IEEE 802.11 ได้ถูกนำมาใช้ในเครือข่ายหลายประเภท เช่น เชื่อมต่อเครือข่ายอินเตอร์เน็ต ระบบเครือข่ายสำหรับยานพาหนะ [2] เป็น

มาตรฐาน IEEE 802.11 มุ่งความสนใจไปที่ระดับชั้นสื่อสาร 2 ระดับชั้นของ ISO model คือ Physical Layer และ Data Link Layer ซึ่งรองรับโปรโตคอลในระดับชั้นสื่อสารที่ 3 ขึ้นไปสามารถใช้งานบนอุปกรณ์ที่ใช้งานตามมาตรฐาน IEEE 802.11 ได้ง่ายๆ เช่นเดียวกับใช้งานบน Ethernet มาตรฐาน IEEE 802.11 ได้รับการตีพิมพ์ครั้งแรกเมื่อปี พ.ศ.2540 โดย IEEE (The Institute of Electronics and Electrical Engineers) และเป็นเทคโนโลยีสำหรับ WLAN ที่นิยมใช้กันอย่างแพร่หลายมากที่สุด และตัวกำหนดมาตรฐานของชั้น Physical layer (PHY) ได้กำหนดให้อุปกรณ์มีความสามารถในการรับส่งข้อมูลด้วยความเร็ว 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 และ 54 Mbps โดยมีสื่อ 3 ประเภทให้เลือกใช้ได้แก่ คลื่นวิทยุที่ความถี่สาธารณะ 2.4 GHz, 5 GHz และอินฟราเรด (Infrared) (1 และ 2 Mbps เท่านั้น) และในส่วนของ

MAC Layer มาตรฐาน IEEE 802.11 ได้กำหนดให้มีกลไกการทำงานที่เรียกว่า CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) ซึ่งเป็นตัวกำหนดวิธีการทำงานของการสื่อสารภายใต้มาตรฐาน IEEE 802.11 มาตรฐาน IEEE 802.11 กำหนดรูปแบบของเฟรม 3 ประเภทคือ เฟรมข้อมูล (Data Frames) เฟรมควบคุม (Control Frames) และ เฟรมจัดการ (Management Frames) เฟรมข้อมูลใช้สำหรับให้บริการรับส่งข้อมูลของระดับชั้นสื่อสารที่สูงกว่า เฟรมควบคุมเป็นเฟรมที่ใช้สำหรับควบคุมการสื่อสารภายในเครือข่าย IEEE 802.11 ตัวอย่างเฟรม เช่น เฟรม ACK เฟรม RTS (Request to Send) เฟรม CTS (Request to Send Request to Send) เป็นต้น เฟรมจัดการเป็นเฟรมที่ใช้ในการจัดการเครือข่าย IEEE 802.11 ตัวอย่างเฟรม เช่น การเชื่อมต่อเครือข่าย (Association Frame) การพิสูจน์ตัวจริง(Authentication Frame) เป็นต้น



รูปที่ 1 *รูปการส่งเฟรมแบบพื้นฐาน*



รูปที่ 2 *รูปการส่งเฟรมแบบที่ใช้ RTS และ CTS*

หลังจากที่สถานีเชื่อมต่อเครือข่ายได้ทำการเชื่อมต่อเรียบร้อยแล้วแต่ละสถานีสามารถรับส่งข้อมูล วิธีการส่งข้อมูลแบ่งออกเป็น 2 แบบ คือการสื่อสารแบบพื้นฐาน ดังรูปที่ 1 และ การสื่อสารแบบที่ใช้ RTS และ CTS ดังรูปที่ 2 การสื่อแบบพื้นฐานประกอบด้วยขั้นตอนตามหลักการของ CSMA/CA ซึ่งประกอบด้วยการตรวจสอบคลื่นพาห์และเวลาสุ่มเพื่อแข่งขันการส่งข้อมูล เมื่อสถานีที่ต้องการส่งชนะการแข่งขันก็จะทำการส่งเฟรมข้อมูล เมื่อเฟรมข้อมูลได้รับโดยเครื่องรับเครื่องรับก็จะทำการส่งเฟรม ACK เพื่อตอบกลับการได้รับเฟรม ก่อนที่จะส่งเฟรม ACK สถานีรับต้องรอด้วยเวลาคงที่ (SIFS) ซึ่งมีค่าเท่ากับ 10 ไมโครวินาที สำหรับมาตรฐาน IEEE 802.11b ส่วนการสื่อแบบที่ใช้เฟรม RTS และ CTS จะคล้ายกับการสื่อสารแบบพื้นฐานต่างกันที่ก่อนจะส่งเฟรมข้อมูลสถานีส่งต้องส่งเฟรม RTS ไปยังสถานีรับเพื่อตรวจสอบความพร้อมของเครื่องรับถ้าเครื่องรับพร้อมก็จะส่งเฟรม CTS ให้กับเครื่องส่ง

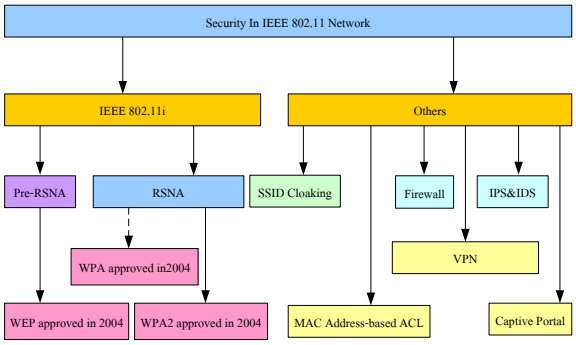
2.2 การรักษาความมั่นคงปลอดภัยของเครือข่าย WLAN

ปัญหาอย่างหนึ่งที่ต้องคำนึงเป็นอย่างมากคือ การรักษาความปลอดภัยของเครือข่ายและข้อมูลที่ใช้สื่อสาร ในปัจจุบันการใช้งานเครือข่ายไร้สายยังไม่ได้จัดการกับเครือข่ายไร้สาย IEEE 802.11 ให้ถูกต้องซึ่งอาจส่งผลให้เกิดการโจรกรรมข้อมูล จากปัญหานี้เองแนวทางในการการใช้งานระบบการรักษาความปลอดภัยที่ดีนั้นสามารถแก้ได้

การรักษาความมั่นคงของเครือข่ายไร้สายสามารถแบ่งออกเป็น 2 แบบแสดงดังรูปที่ 3 ซึ่งประกอบด้วย IEEE 802.11i และอื่นๆ การรักษาความมั่นคงด้วย IEEE 802.11i นั้นประกอบด้วย Pre-RSNA (Robust Security Network Association) และ RSNA ส่วนการรักษาความมั่นคงอื่น ๆ เช่น การปกปิด SSID (SSID Cloaking) การคัดกรองหมายเลข MAC (MAC Addressed-based ACL (Access control list) การใช้งาน VPN (Virtual Private Network) ไฟร์วอลล์ (Firewall) การป้องกันการใช้งานด้วย user และ password (Captive Portal) และ IPS (intrusion protection systems)/IDS (intrusion detection systems) การรักษาความมั่นคงด้วย Pre-RSNA เป็นมาตรฐาน WEP การรักษาความมั่นคงด้วย RSNA นั้นประกอบด้วย WPA (Wi-Fi Protected Access) และ WPA2

การวิเคราะห์ระบบรักษาความมั่นคงของมาตรฐาน IEEE 802.11 ได้นำเสนอในงานวิจัย [8] และ [9] ในบทความนี้จะกล่าวถึงพื้นฐานของการคัดกรองหมายเลข MAC (Medium Access Control) ซึ่งเป็นพื้นฐานของการพิสูจน์ตัวจริงของเครือข่ายไร้สาย IEEE 802.11

การคัดกรองหมายเลข MAC เป็นวิธีการตรวจสอบเบื้องต้นที่ใช้ในการอนุญาตหรือไม่อนุญาตใช้งานเครือข่ายไร้สาย IEEE 802.11 การคัดกรองหมายเลข MAC สามารถกำหนดที่แอคเซสพอยต์ซึ่งในปัจจุบันสามารถใช้งานกับแอคเซสพอยต์ทุกตัว แต่อย่างไรถ้าผู้ไม่ประสงค์ดีต้องการปลอมแปลงหมายเลข MAC เพื่อเข้าใช้งานเครือข่ายก็สามารถทำได้โดยง่ายซึ่งจะอธิบายในหัวข้อต่อไป



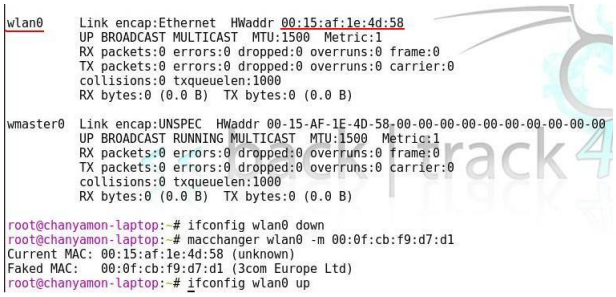
รูปที่ 3 *ระบบรักษาความปลอดภัยของ IEEE 802.11*

2.3 การปลอมแปลงหมายเลข MAC

หมายเลข MAC เป็นหมายเลขที่เป็นค่าเฉพาะของแต่ละอุปกรณ์เชื่อมต่อเครือข่ายซึ่งเป็นค่าที่ออกโดยผู้ผลิตซึ่งจะมีค่าไม่ซ้ำกันเลย แต่ก็สามารถปลอมแปลงได้ง่ายเพียงมีหมายเลข MAC ที่ต้องการจะเปลี่ยนโดยใช้คำสั่งในระบบปฏิบัติการ Linux ดังนี้

#ifconfig wlan0 hw ether 00:0f:cb:f9:d7:d1

เมื่อ ifconfig เป็นชุดคำสั่งที่มีไว้จัดการเกี่ยวกับอุปกรณ์เครือข่ายของระบบปฏิบัติการ Linux wlan0 จะเป็นชื่อของอุปกรณ์ที่ต้องการปลอมแปลง 00:0f:cb:f9:d7:d1 คือชุดหมายเลข MAC ที่ต้องการปลอมแปลง ตัวอย่างการผลปลอมแปลงแสดงดังรูปที่ 4 นอกจากการใช้ ifconfig ในระบบปฏิบัติการ Linux สามารถใช้งานโปรแกรม Macchanger [9] ในการปลอมแปลงหมายเลข MAC



รูปที่ 4 *แสดงการเปลี่ยนหมายเลข MAC เป็น 00:0f:cb:f9:d7:d1*

ส่วนการปลอมแปลงหมายเลข MAC ของระบบปฏิบัติการ Windows สามารถใช้ซอฟท์แวร์เช่นโปรแกรม MAC Makeup [10] เป็นต้น

จุดมุ่งหมายของการปลอมแปลงหมายเลข MAC ของผู้ไม่ประสงค์ดีคือ เพื่อใช้งานเครือข่ายไร้สาย IEEE และเพื่อโจมตีเครือข่ายไม่ให้สามารถใช้งานได้ การตรวจสอบหมายเลขแมคจึงมีความจำเป็นที่ต้องทำได้ถูกต้องเพื่อแก้ปัญหาดังกล่าวข้างต้น

3 การตรวจสอบการปลอมแปลงหมายเลขแมค

การตรวจสอบการปลอมแปลงหมายเลข MAC โดยทั่วไปนั้นประกอบด้วย 3 วิธีซึ่งจะอธิบายในหัวข้อนี้

3.1 การตรวจสอบโดยการวิเคราะห์เลขลำดับของเฟรม (Sequence-Number Analysis)

วิธีการนี้เป็นการตรวจสอบโดยการนำเลขลำดับของเฟรม (Sequence Number: SN) [1] มาทำการหาความแตกต่าง (Gap) ระหว่างค่าเลขลำดับของเฟรมปัจจุบันกับเลขลำดับของเฟรมก่อนหน้าที่มีหมายเลข MAC ต้นทางเดียวกัน ซึ่งสามารถวิเคราะห์ได้ดังสมการ (1)

$$Gap = SN_{(i)} - SN_{(i-1)} \bmod 4096 \qquad (1)$$

โดยที่ Gap คือ ระยะห่างระหว่างลำดับของเฟรม

$SN_{(i)}$ คือ เลขลำดับของเฟรมปัจจุบัน

$SN_{(i-1)}$ คือเลขลำดับของเฟรมก่อนหน้า

ซึ่งจากสมการค่าของ Gap = 2 [2] หากเฟรมใดที่มีระยะห่างมากกว่าระดับอ้างอิงเช่น 2 ก็สามารถระบุได้ว่าเฟรมดังกล่าวมีการปลอมแปลงเกิดขึ้น Gou และ Chiueh [2] ได้พัฒนาต่อจากงานวิจัยของ Wright [1] โดยการเพิ่มวิธีการยืนยันว่าหมายเลขที่กำลังตรวจจับเป็นของผู้ใช้งานปกติ ข้อเสียของการตรวจสอบโดยการใช้เลขลำดับคือ ผู้ไม่ประสงค์ดีสามารถปลอมหมายเลขให้ต่อเนื่องกับเลขลำดับของผู้ใช้งานปกติได้ รวมถึงถ้าผู้ไม่ประส่งดีส่งแต่เฟรมความคุม (Control Frame) ไม่ส่งเฟรมข้อมูลก็ไม่สามารถใช้การตรวจสอบด้วยวิธีนี้ได้เนื่องจากเฟรมควบคุมไม่มีลำดับของเฟรม

3.2 การตรวจสอบคุณลักษณะการส่งสัญญาณของเครื่องส่ง (Transceiver Fingerprint)

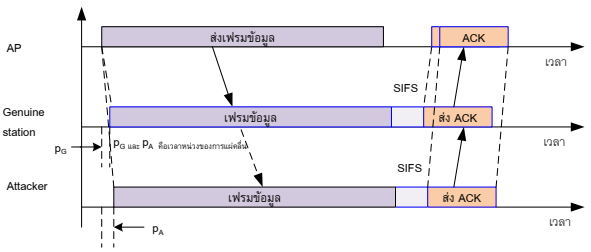
การตรวจสอบโดยใช้คุณลักษณะของเครื่องส่งสัญญาณเป็นตัวตรวจสอบ ซึ่งหากว่าเครื่องตรวจสอบสัญญาณมีลักษณะที่เปลี่ยนแปลงไปจากลักษณะที่ถูกส่งออกมาของเครื่องผู้ใช้งานปกติก็ถือว่ามีการปลอมแปลง งานวิจัยที่ใช้วิธีนี้เช่น งานวิจัยของ Hall และ คณะ [3] เป็นต้น

3.3 การตรวจสอบระดับความแรงของสัญญาณ (Receive Signal-Strength (RSS) Analysis)[6]-[8]

การตรวจสอบวิธีนี้เป็นการตรวจสอบค่าความแรงที่รับได้ ซึ่งระดับของสัญญาณจะขึ้นอยู่กับระยะทางของเครื่องส่งและเครื่องรับ ตัวอย่างเช่น ถ้าระยะห่างของเครื่องใช้งานปกติถึงเครื่องตรวจจับ มีระยะทางที่น้อยกว่าเครื่องปลอมแปลง เครื่องตรวจจับจะตรวจจับความแรงของสัญญาณของเครื่องใช้งานปกติได้แรงกว่าของเครื่องปลอมแปลง แต่ทั้งนี้ก็ยังขึ้นอยู่กับสภาพแวดล้อม ว่ามีสิ่งกีดขวาง หรือตัวรบกวนของสัญญาณหรือไม่ ด้วยเหตุนี้การตรวจสอบการปลอมแปลงหมายเลขแมคด้วยวิธีนี้จึงต้องใช้หลักการทางสถิติในการแยกแยะความแตกต่างนี้ ดังเช่น Modory [5] ใช้ SSFA (Short Term Fourier Transform) Fari and Cheriton [4] ใช้การหามัธยฐาน (median) ของความแรงจากจุดที่ทำการตรวจสอบหลายๆ จุด Chen และ คณะ [6] ใช้การกระจาย แบบเกาส์เซียน (Gausian Distribution) ในการวิเคราะห์ Sheng และคณะ [7] ใช้การกระจายแบบ Gaussian Mixture ตรวจสอบการปลอมแปลง

4 การตรวจสอบโดยใช้ความแตกต่างของเฟรม ACK (Acknowledgement Frame) ที่นำเสนอ

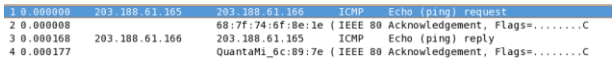
การทำงานของเฟรมตอบกลับจะเกิดขึ้นเมื่อเครื่องรับได้รับเฟรมข้อมูลเรียบร้อยแล้ว เพื่อเป็นการยืนยันว่าได้รับข้อมูลเสร็จสิ้น เครื่องรับจะทำการส่งเฟรมตอบกลับไปให้เครื่องส่งเพื่อแจ้งให้เครื่องส่งทราบ ซึ่งระยะเวลาในการตอบกลับจะมีค่าเท่ากับ SIFS ดังนั้นถ้าหากเกิดการปลอมแปลงหมายเลข MAC ขึ้น เฟรมตอบกลับก็จะถูกส่งมาจากเครื่องรับที่มีหมายเลข MAC เดียวกันเกินกว่าหนึ่งครั้งในระยะเวลาที่ใกล้เคียงกัน หรืออาจจะไม่ได้รับการตอบกลับเลย เพราะเนื่องจากเกิดการชนกันของเฟรมตอบกลับ ตัวอย่างดังรูปที่ 5 เมื่อแอคเซสพอยต์ส่งเฟรมข้อมูลที่มีหมายเลขปลายทางเป็นหมายเลข MAC เป็น 00:17:C4:6C:89:7E ซึ่งเป็นหมายเลข MAC ของคอมพิวเตอร์ของผู้ใช้งานปกติและผู้ไม่ประสงค์ดี เมื่อคอมพิวเตอร์ทั้ง 2 ได้รับเฟรมก็รอด้วยเวลา SIFS ที่มีค่าเท่ากับ 10 ไมโครวินาทีก่อนที่จะส่ง ACK กลับไปยังแอคเซสพอยต์ เวลาที่ได้รับเฟรม ACK ของแอคเซสพอยต์ไม่พอดีกันขึ้นอยู่กับระห่างระหว่างแอคเซสพอยต์และคอมพิวเตอร์ซึ่งเป็นเวลาหน่วงของการแผ่คลื่นวิทยุ (pG, pA) ตัวอย่างการคำนวณเช่น ถ้าคอมพิวเตอร์ของผู้ใช้งานปกติห่างจากแอคเซสพอยต์เท่ากับ 50 เมตรซึ่งสามารถคำนวณเวลาหน่วงได้ดังนี้ $pA=50/(3x10^8) = 0.16$ ไมโครวินาที ถ้าคอมพิวเตอร์ของผู้ไม่ประสงค์ดีใกล้กว่าคอมพิวเตอร์ของผู้ใช้งานปกติ แอคแซสพอยต์ก็จะรับเฟรม ACK ของคอมพิวเตอร์ผู้ไม่ประสงค์ดีเนื่องจากมีความแรงมากกว่า แต่ถ้าระยะห่างใกล้เคียงกันมากเฟรม ACK จะเกิดการสูญหายเนื่องจากเฟรม ACK ทั้ง 2 รบกวนกันเอง



รูปที่ 5 *ตัวอย่างการส่งเฟรม ACK เมื่อมีการปลอมแปลงหมายเลข MAC*

4.1 การตรวจสอบการปลอมหมายเลขแมคโดยใช้ระดับความแรงของสัญญาณของเฟรมและเฟรมข้อมูล

ซึ่งสามารถดูระดับของสัญญาณได้ดังรูปที่ 6 ซึ่งเป็นระดับสัญญาณที่ไม่มีการปลอมแปลง จะเห็นได้ว่าความแรงของสัญญาณมีความแตกต่างเพียงเล็กน้อย แต่หากเกิดการปลอมแปลงขึ้นระดับความแรงของสัญญาณก็จะเปลี่ยนแปลงตามรูปที่ 7 ซึ่งจะเห็นได้ชัดเจนว่าระดับความแรงของสัญญาณมีความแตกต่างกันอย่างเห็นได้ชัด



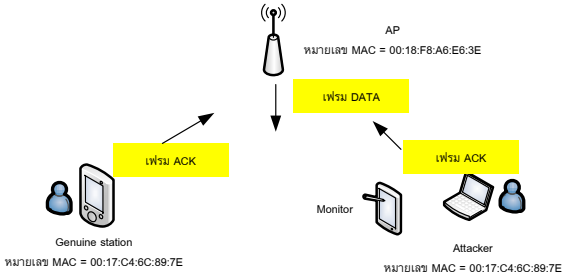
RSSI ของเฟรม 1 = -49 dBm
RSSI ของเฟรม 2 = -49 dBm
RSSI ของเฟรม 3 = -53 dBm
RSSI ของเฟรม 4 = -50 dBm

รูปที่ 6 *ตัวอย่างการส่งเฟรม ACK เมื่อไม่มีการปลอมแปลงหมายเลข MAC*

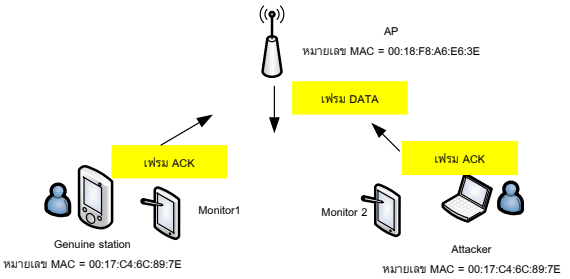
RSSI ของเฟรม 1 = -46 dBm
RSSI ของเฟรม 2 = -23 dBm
RSSI ของเฟรม 3 = -52 dBm
RSSI ของเฟรม 4 = -49 dBm

รูปที่ 7 *ตัวอย่างการส่งเฟรม ACK เมื่อมีการปลอมแปลงหมายเลข MAC*

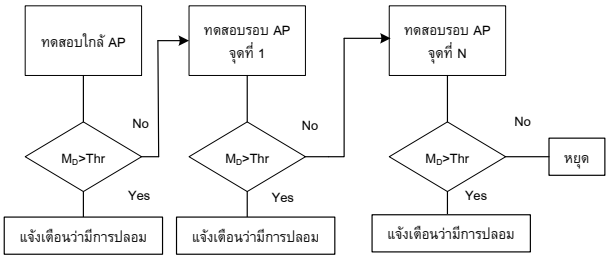
4.2 การตรวจสอบการปลอมแปลงหมายเลขแม็คโดยใช้การตรวจสอบความแตกต่างของส่วน PLCP ของเฟรมตอบกลับ



รูปที่ 8 *ตัวอย่างโครงสร้างการทดลองตรวจสอบความผิดปกติโดยใช้ความแตกต่างของความแรงของสัญญาณ*



รูปที่ 9 *ตัวอย่างโครงสร้างการทดลองตรวจสอบความผิดปกติโดยใช้ความแตกต่างของระดับชั้นสื่อสารที่ 1 ของเฟรม ACK*

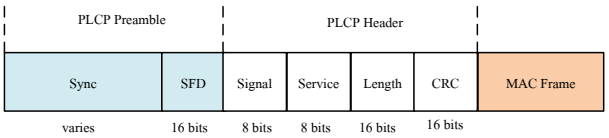


รูปที่ 10 *หลักการตรวจสอบการปลอมโดยใช้ความแตกต่างของความแรงสัญญาณที่นำเสนอ*

ตัวอย่างการทดลองเมื่อมีการปลอมหมายเลข MAC และไม่มีการปลอมหมายเลข MAC แสดงดังรูปที่ 8 และรูปที่ 9 ตามลำดับ จากรูปแสดงให้เห็นว่าถ้าตำแหน่งคอมพิวเตอร์ที่ใช้ตรวจจับ (Monitor) อยู่ใกล้กับคอมพิวเตอร์ของผู้ไม่ประสงค์ดีก็จะได้รับความแตกต่างของความแรงของเฟรม DATA และ เฟรม ACK ดังเช่น 46 dBm และ 23 dBm จากความแตกต่างนี้จึงนำมาใช้ในการตรวจสอบการปลอมแปลงหมายเลข MAC ซึ่งขั้นตอนการตรวจสอบแสดงดังรูปที่ 10 เมื่อ Thr เป็นระดับอ้างอิงที่กำหนดโดยผู้ดูแลระบบ เมื่อ M_D สามารถคำนวณได้ดังสมการที่ 2 เมื่อ $RSSI_{DATA}(i)$ เป็นความแรงของสัญญาณของเฟรมข้อมูลที่ส่งโดยสถานีผู้ใช้งานปกติของเฟรมที่ i และ $RSSI_{ACK}(i)$ เป็นความแรงของเฟรม ACK ที่ส่งโดยสถานีผู้ใช้ปกติและสถานีผู้ไม่ประสงค์ดี

$$M_D = \left| \frac{1}{N} \sum_{i=1}^{N} (RSSI_{DATA}(i) - RSSI_{ACK}(i)) \right| \qquad (2)$$

นอกจากการตรวจสอบด้วยการใช้ค่าเฉลี่ยของความแตกต่างของความแรงของเฟรมข้อมูลที่ส่งจากสถานีที่ถูกต้องและความแรงของเฟรม ACK ที่ส่งโดยสถานีที่ไม่ประสงค์ดียังสามารถตรวจสอบด้วยการตรวจสอบรูปแบบของเฟรม ACK ในระดับชั้นสื่อสารที่ 1 ซึ่งรูปแบบของเฟรม ACK ของโปรโตคอลในระดับชั้นสื่อสารที่ 1 ที่ส่งโดยสถานีของผู้ใช้งานปกติและสถานีของผู้ไม่ประสงค์ดี รูปแบบของเฟรมสื่อสารในระดับชั้นสื่อสารที่ 1 แสดงดังรูปที่ 11 จากรูปเฟรมของระดับชั้นสื่อสารที่ 1 ประกอบด้วยส่วนนำของ PLCP (Physical Layer Convergence Procedur Preamble) และ ส่วนหัวของ PLCP (PLCP header) ข้อมูลที่ความแตกต่างระหว่างสถานีผู้ใช้ปกติและสถานีผู้ไม่ประสงค์คือส่วนหัวของ PLCP ซึ่งประกอบด้วยฟิลด์สำคัญต่อไปนี้



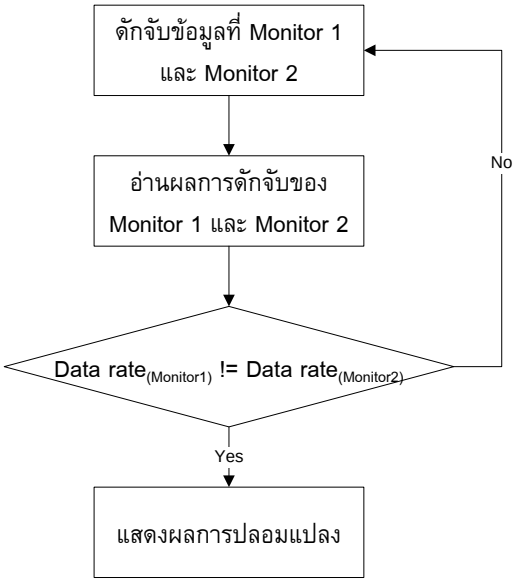
รูปที่ 11 *รูปแบบของเฟรมในระดับชั้นสื่อสารที่ 1 ตามมาตรฐาน IEEE 802.11b และ IEEE 802.11g*

1 ฟิลด์ Signal มีขนาด 8 บิตใช้ระบุชนิดของการผสมสัญญาณ (Modulation) และอัตราการส่งข้อมูลโดยมีค่าดังนี้คือ 0x0A สำหรับการส่งที่อัตราเร็ว 1 Mbps และ 0x14 สำหรับการส่งที่อัตราเร็ว 2 Mbps อัตราเร็วที่สามารถสื่อสารได้คือ 1 Mbps 2 Mbps 5.5 Mbps และ 11 Mbps สำหรับมาตรฐาน IEEE 802.11b ส่วนมาตรฐาน IEEE 802.11g สามารถสื่อสารได้ที่ความเร็ว 6 Mbps 9 Mbps 12 Mbps 18 Mbps 24 Mbps 46 Mbps 48 และ 54 Mbps อัตราส่งเฟรมข้อมูลแต่ละระดับใช้การผสมสัญญาณที่ต่างกันด้วยการเปลี่ยนอัตราเร็วของการส่งของเฟรมข้อมูลตามมาตรฐานแล้วสามารถเปลี่ยนได้ทุกเฟรมซึ่งขึ้นอยู่กับสภาพแวดล้อมและวิธีการของการปรับอัตราเร็วการส่งเฟรมของบริษัทผู้ผลิตอุปกรณ์เชื่อมต่อเครือข่ายไร้สาย

2 ฟิลด์ Service มีขนาด 8 บิตเป็นฟิลด์ที่สงวนไว้ใช้ในอนาคต

3 ฟิลด์ Length มีขนาด 16 บิตใช้บรรจุเวลาที่ใช้ในการส่งเฟรมโดยมีหน่วยเป็นมิลลิวินาที

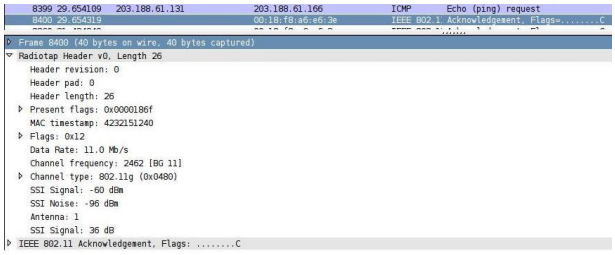
4 ฟิลด์ CRC มีขนาด 16 บิตใช้ในการบรรจุค่าตรวจสอบความถูกต้องที่ได้จากการนำส่วนหัว PLCP มาคำนวณตามมาตรฐานของ ITU-T CRC-16 ซึ่งจากเขตข้อมูลเหล่านำมาวิเคราะห์ดังรูปที่ 12



รูปที่ 12 *แสดงหลักการตรวจสอบการปลอมแปลงที่นำเสนอโดยใช้ความแตกต่างของระดับสัญญาณในชั้นที่ 1 ที่นำเสนอ*

ตัวอย่างของความแตกต่างของเฟรม ACK แสดงดังรูปที่ 13 และ รูปที่ 14 จากรูปเป็นเฟรม ACK ที่ส่งโดยสถานีผู้ใช้ปกติและสถานีผู้ไม่ประสงค์ดีเพื่อตอบการรับเฟรมข้อมูลเดียวเดียว เฟรม ACK จะมีข้อมูลของระดับชั้นสื่อสารที่ 2 ที่เหมือนกันแต่ข้อมูลของเฟรมในระดับชั้นสื่อสารที่ 1 มีโอกาสที่เหมือนกันน้อยมาก จากเงื่อนไขนี้เองสามารถนำมาใช้ในการตรวจสอบการปลอมแปลงหมายเลข MAC ที่ทำให้มีความถูกต้องใกล้เคียง 100 เปอร์เซ็นต์และยากต่อการปลอมแปลงข้อมูลสื่อสารในระดับชั้นสื่อสารที่ 1 เนื่องจากข้อมูลเฟรมในระดับชั้นสื่อสารที่ 1 จะสามารถเปลี่ยนได้ทุกครั้งที่ส่งเฟรมขึ้นอยู่กับสภาพแวดล้อมและวิธีการออกแบบของแต่ละบริษัทที่ผลิตอุปกรณ์เชื่อมต่อเครือข่ายไร้สาย

รูปที่ 13 *ตัวอย่างเฟรม ACK ที่มาจากสถานีปกติ*



รูปที่ 14 *ตัวอย่างเฟรม ACK ที่มาจากสถานีผู้ไม้ประสงค์ดี*

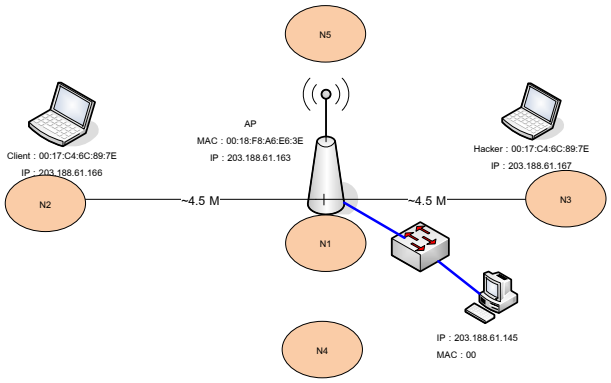
5 โครงสร้างการทดลองและผลการทดลอง

เพื่อพิสูจน์แนวความคิดที่นำเสนอในบทความนี้จะเป็นการนำเสนอการทดลองและผลการทดลอง

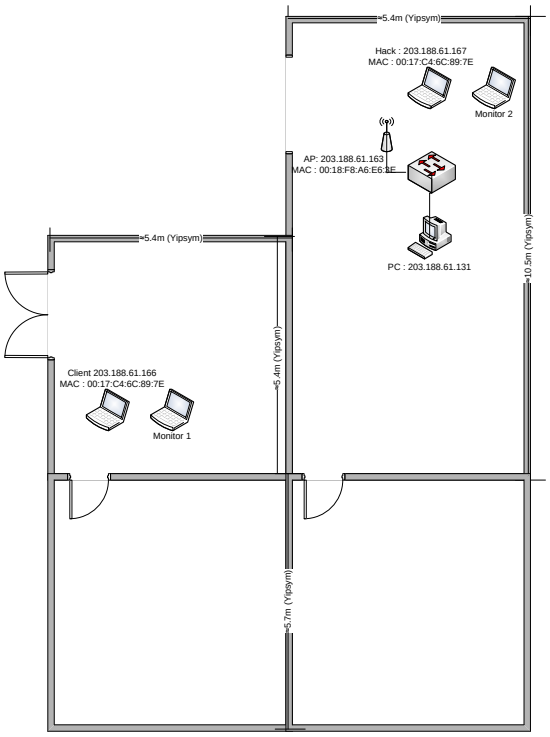
5.1 โครงสร้างของการทดลอง

โครงสร้างการทดลองการตรวจสอบความผิดปกติโดยใช้ความแตกต่างของความแรงสัญญาณ ซึ่งประกอบด้วย AP 1 เครื่อง คอมพิวเตอร์ผู้ไม่ประส่งดี 1 เครื่อง คอมพิวเตอร์ผู้ใช้งานปกติ 1 เครื่อง คอมพิวเตอร์สำหรับการตรวจสอบ 1 เครื่อง และคอมพิวเตอร์สำหรับการส่งเฟรมไปยังคอมพิวเตอร์ใช้งานปกติ 1 เครื่อง หมายเลข IP และหมายเลข MAC ของอุปกรณ์แสดงรูปที่ 15

โครงสร้างการทดลองการตรวจสอบความผิดปกติโดยตรวจสอบความแตกต่างของระดับชั้นสื่อสารที่ 1 ของเฟรม ACK ซึ่งประกอบด้วย AP 1 เครื่อง คอมพิวเตอร์สำหรับการตรวจจับจำนวน 2 เครื่อง เครื่องผู้ไม่ประสงค์ดี 1 เครื่อง และเครื่องผู้ใช้งานปกติ 1 เครื่อง ซึ่งมีโครงสร้างการทดลองและการกำหนดค่าต่างๆ แสดงดังรูปที่ 16



รูปที่ 15 *แสดงโครงสร้างของอุปกรณ์ในการทดลองโดยใช้ความแตกต่างของความแรงสัญญาณ*



รูปที่ 16 *แสดงโครงสร้างของอุปกรณ์ในการทดลองโดยใช้ความผิดปกติของระดับชั้นสื่อสารที่ 1*

5.2 ผลการทดลอง

ผลการทดลองของการตรวจด้วยความผิดปกติของความแตกต่างของความแรงสัญญาณดังตารางที่ 1 จากผลที่ได้จะเห็นได้ว่าการตรวจสอบด้วยวิธีนี้เมื่อใช้ค่าระดับอ้างอิง (Thr) ที่แตกต่างกันไป ค่าเปอร์เซ็นต์ของการตรวจพบจะลดลงเมื่อมีค่าของ Thr ที่มากขึ้นและค่าของการตรวจสอบที่ไม่มีการปลอมแปลงก็จะลดลงเช่นกัน นั่นคือเมื่อค่า Thr = 0 dB, 3 dB, 10 dB และ 20 dB ค่าความถูกต้องในการตรวจสอบจะมีค่าเท่ากับ 100% ทุกค่าอ้างอิง มีความผิดพลาดในการตรวจสอบในกรณีที่มีการปลอมแปลงแต่ตรวจไม่พบเป็น 0% และความผิดพลาดในการตรวจสอบในกรณีที่ไม่มีการปลอมแปลงแต่ตรวจพบการปลอมแปลงเป็น 100% ที่ค่าอ้างอิงเท่ากับ 0 dB และที่ค่าอ้างอิงที่ 3 dB เป็น 20% ส่วนในค่าอ้างอิงที่ 10 dB และ 20 dB จะเป็น 0% ซึ่งจะเห็นได้ว่าการเลือกค่าอ้างอิงที่เหมาะสมต้องมีค่าประมาณไม่เกิน 20 dB เพราะเนื่องจากการทดลองค่าความแตกต่างของระดับความแรงสัญญาณ จะมีค่าที่สูงมากกว่า 20 dB แต่ที่ระดับค่าอ้างอิงที่ น้อยกว่า 20 dB ยังมีโอกาสเกิดขึ้นได้ในกรณีที่ไม่เกิดการปลอมแปลง เป็นค่าอ้างอิงที่สูงกว่า

ส่วนในตารางที่ 2 เป็นการเปรียบเทียบความแตกต่างของการตรวจสอบโดยใช้ความแตกต่างของเลขลำดับซึ่งจะเห็นได้ว่าสามารถตรวจสอบพบการปลอมแปลงได้น้อยกว่าการตรวจสอบโดยใช้ความแตกต่างของระดับชั้นสื่อสารที่ 1 ของเฟรมตอบกลับ

ตารางที่ 1 *เปอร์เซ็นต์ความถูกต้องการสื่อสาร*

ระดับอ้างอิง (dB)	ตรวจสอบพบการปลอมแปลง (Spoof Detect)	มีการปลอมแปลงแต่ตรวจไม่พบ (False Negative)	ไม่มีการปลอมแปลงแต่ตรวจพบ (False Positive)
0	100	0	100
3	100	0	20
10	100	0	0
20	100	0	0

ตารางที่ 2 *ผลการทดลองโดยใช้การตรวจสอบความผิดปกติโดยการตรวจสอบความผิดปกติของหมายเลขลำดับ [5]*

วิธีการตรวจสอบ	ตรวจสอบพบการปลอมแปลง (Spoof Detect)	มีการปลอมแปลงแต่ตรวจไม่พบ (False Negative)	ไม่มีการปลอมแปลงแต่ตรวจพบ (False Positive)
ความแตกต่างของเลขลำดับ	85.77	14.23	36.69
ความแตกต่างของระดับชั้นสื่อสารที่ 1 ของเฟรม ACK	100	0	0

6 สรุปและงานวิจัยที่จะทำในอนาคต

บทความนี้ได้นำเสนอวิธีการในการตรวจสอบการปลอมแปลงหมายเลขแม็คโดยใช้ความแตกต่างของเฟรมตอบกลับ ซึ่งผลที่ได้แสดงให้เห็นว่าการตรวจสอบโดยวิธีการดังกล่าวสามารถตรวจพบการปลอมแปลงได้สูงถึง 100% และตรวจไม่พบความผิดพลาดในการตรวจสอบเลย ในขณะที่การตรวจสอบโดยใช้เลขลำดับสามารถตรวจสอบพบการปลอมแปลงได้เพียง 85.77% แต่ก็ยังเกิดการผิดพลาดในการตรวจสอบ ซึ่งจากผลการทดลองดังกล่าว

สามารถสรุปได้ว่า วิธีการที่นำเสนอสามารถเพิ่มประสิทธิภาพในการตรวจสอบการปลอมแปลงหมายเลขแม็คได้สูงกว่าการตรวจสอบโดยใช้ความแตกต่างของเลขลำดับ

เอกสารอ้างอิง

[1] J. Wright, "Detecting wireless LAN MAC address spoofing," 2003, technical document. [Online]. Available: http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf

[2] F. Guo and T. cker Chiueh, "Sequence number-based MAC address spoof detection," *in Proceedings of the 8th International Symposium on Recent Advances in Intrusion Detection*, Seattle, WA, USA, Sept. 2005.

[3] Hall, M. Bareau, and E. Kranakis, "Using transceiverprints for anomaly based intrusion detection," *in Proceedings of 3rd IASTED*,CIIT, Nov. 2004, pp. 22–24.

[4] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using singalprints," *in Proceedings of WiSe'06: ACM Workshop on Wireless Security*, Sept. 2006, pp. 43–52.

[5] D. C. Madory, "*New methods of spoof detection in 802.11b wireless networks*" Hanover, NH: M. Eng. Thesis, Dartmouth College, 2006.

[6] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," *in SECON'07: Proceedings of the 4th Annual IEEE Conference on Sensor*, Mesh and Ad Hoc Communications and Networks, June 2007.

[7] Y. Sheng, G. Chen, K. Tan, U. Deshpande, B. Vance, C. McDonald,H. Yin, T. Henderson, D. Kotz, A. Campbell, and J. Wright, "Securing 802.11 wireless networks through fine-grained measurements," *Submitted to IEEE Wireless Communications Magazine*.

[8] Changhua He and John C Mitchell, "Security analysis and improvements for IEEE 802.11i (2005)", *In Proceedings of the 12th Annual Network and Distributed System Security Symposium*, 2005.

[9] http://linux.die.net/man/1/macchanger

[10] www.gorlani.com/publicprj/macmakeup/macmaeup.asp.

[11] ธนทรรศน์ แซ่ลิ้ม และ ประวิทย์ ชุมชู "การวิเคราะห์กลไกรักษาความปลอดภัยและผลกระทบต่อประสิทธิภาพของเครือข่ายไร้สาย", IEEE 802.11, Engineering Transactions, Vol. 12, No. 1, pp. 1-8, 2552

[12] ธนทรรศน์ แซ่ลิ้ม และ ประวิทย์ ชุมชู "ระบบเครือข่ายเคลื่อนที่สำหรับยาพาหนะ," Engineering Transactions, Vol. 9, No. 2, pp. 12-21, 2549

ชัญญมน ศรีคล้าย นักศึกษาระดับปริญญาโท สาขาวิศวกรรมศาสตร์ไฟฟ้า สาขาย่อย วิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีมหานคร จบการศึกษาระดับปริญญาตรี ในสาขาวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีมหานคร

ประวิทย์ ชุมชู เป็นอาจารย์ประจำภาควิชาวิศวกรรมโทรคมนาคม มหาวิทยาลัยเทคโนโลยีมหานคร จบการศึกษาระดับปริญญาตรีจากมหาวิทยาลัยธรรมศาสตร์ในสาขาวิศวกรรมไฟฟ้า ระดับปริญญาโทจากมหาวิทยาลัยเทคโนโลยีมหานคร ระดับปริญญาเอกจากมหาวิทยาลัยนิวเซาท์เวลล์ สนใจงานวิจัยด้าน Digital Signal Processing for telecommunication systems, mobile computing และ Networking.