การเพิ่มความปลอดภัยให้กับโมไบล์ไอพีวีซิกส์ไบด์ดิ้งอัพเดท โดยวิธีเคอร์บิรอส

SECURE MOBILE IPv6 BINDING UPDATES USING KERBEROS

วโรดม วีระพันธ์

WARODOM WERAPUN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2548

ISBN 974-16-2051-4

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

การเพิ่มความปลอดภัยให้กับโมไบล์ไอพีวีซิกส์ไบด์ดิ้งอัพเดท โดยวิธีเคอร์บิรอส

SECURE MOBILE IPv6 BINDING UPDATES USING KERBEROS

T061240

วโรดม วีระพันธ์
WARODOM WERAPUN

หมู่.....
เลขทะเบียน 61240
วันเดือนปี 17 ก.ค. 2549
.b.....
.i.....

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์
บัณฑิตวิทยาลัย
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ.2548

ISBN 974-15-2051-4

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

SECURE MOBILE IPv6 BINDING UPDATES USING KERBEROS

WARODOM WERAPUN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
MASTER OF ENGINEERING IN COMPUTER ENGINEERING
SCHOOL OF GRADUATE STUDIES
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2005

ISBN 974-15-2051-4

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

COPYRIGHT 2005

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อวิทยานิพนธ์	การเพิ่มความปลอดภัยให้กับโมไบล์ไอพีวีซิกส์ไบด์ดิ้งอัพเดท โดยวิธีเคอร์บิรอส
นักศึกษา	นายวโรดม วีระพันธ์
รหัสนักศึกษา	45061030
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
พ.ศ.	2548
อาจารย์ผู้ควบคุมวิทยานิพนธ์	ผศ. อภิเนตร อูนากูล

บทคัดย่อ

สิ่งที่ท้าทายของการทำโมบิลิตี้ ในชั้นของไอพี คือ การอนุญาตให้โฮสต์นั้นสามารถใช้แอดเดรสเดิมอยู่ได้ โดยไม่มีการกระจายตารางเส้นทางการส่งข้อมูลแบบเฉพาะเจาะจง ไปยัง เราเตอร์หลาย ๆ ตัว หรือ มีการตัดการเชื่อมต่อสื่อสารในขณะนั้น โมไบล์ไอพีวีซิกส์ ออกแบบมาให้สามารถทำโมบิลิตี้ในชั้นไอพีได้ กล่าวคือ ตราบเท่าที่การเชื่อมต่อของทีซีพี ยังไม่ได้ตัดขาดการสื่อสาร แม้ว่าจะมีการเคลื่อนย้ายไอพีแอดเดรสไปแล้ว แต่การเชื่อมต่อสื่อสารนั้น ก็ยังคงอยู่และสามารถใช้งานได้ต่อเนื่องไป ไบด์ดิ้งอัพเดท คือ ข้อมูลที่ใช้บอกตำแหน่งที่อยู่ปัจจุบันของ โมไบล์โหนด และใช้ในการปรับปรุงเส้นทางการส่งข้อมูลให้มีประสิทธิภาพ เมื่อมีการย้ายเครือข่าย (Handoff) เกิดขึ้น กระบวนการย้ายเครือข่ายที่ใช้เวลานานนั้น มีผลกระทบโดยตรงต่อโปรแกรมที่เวลามีผลกระทบต่อการทำงาน งานวิจัยชิ้นนี้จึงได้นำเสนอ วิธีการประยุกต์ใช้วิธีเคอร์บิรอส เข้ากับกระบวนการทำไบด์ดิ้งอัพเดท เพื่อความปลอดภัยของข้อมูลไบด์ดิ้งอัพเดท และ สามารถทำงานได้มีประสิทธิภาพมากยิ่งขึ้น อีกทั้งยังมีความเข้ากันได้กับโพรโตคอลมาตรฐานที่ได้กำหนดไว้แล้วอีกด้วย ซึ่งกระบวนการลงทะเบียนก่อนล่วงหน้า จะประมวลผลก่อนที่โมไบล์โหนด จะตัดสินใจย้ายเครือข่ายเดิม ไปยังเครือข่ายใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Thesis Title	Secure Mobile IPv6 Binding Updates using Kerberos
Student	Warodom Werapun
Student ID.	45061030
Degree	Master of Engineering
Programme	Computer Engineering
Year	2005
Thesis Advisor	Asst. Prof. Apinetr Unakul

ABSTRACT

The challenge of mobility in IP layer allows host to retain theirs address without requiring routers to propagate specific routes or breaking current connection. Mobile IPv6 makes transparency of IP layer. In particular, as long as they remain idle, all open TCP connections survive a change in network and are ready for further use. Binding Updates (BUs) are used to tell current location of the Mobile Node for routing optimization purposed. High handoff latency directly affects Real-Time application. Therefore, this research was proposed to use Kerberos and Pre-Registration to secure Mobile IPv6 Binding Updates. The Pre-Registration was processed before Mobile Node was decided to handoff to another network for improve on the performances, and provide compatibility with a given standard protocol.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จได้ด้วยความกรุณาจากอาจารย์ที่ปรึกษา ผศ. อภิเนตร อูนากูลที่ให้ความช่วยเหลือ ให้คำชี้แนะช่วยแก้ไขปัญหาตลอดจนให้ความรู้และประสบการณ์ในการทำวิจัยที่ดีแก่ข้าพเจ้าเป็นอย่างยิ่ง

ขอขอบพระคุณกรรมการสอบวิทยานิพนธ์ทุกท่านที่ได้ กรุณาให้คำแนะนำในทุก ๆ เรื่อง ทั้งวิธีการแก้ปัญหาที่เกิดขึ้นในวิทยานิพนธ์ และมุมมองในเชิงวิศวกรรมอื่น ๆ ตลอดจนข้อชี้แนะจนในที่สุดทำให้วิทยานิพนธ์ฉบับนี้สำเร็จลงได้

ขอขอบคุณ บัณฑิตวิทยาลัยและบัณฑิตศึกษา สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ที่ให้การสนับสนุนการทำวิทยานิพนธ์นี้

สำหรับคุณงามความดีอันใดที่เกิดจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบให้กับบิดามารดา ซึ่งเป็นที่รักและเคารพยิ่ง ตลอดจนครูอาจารย์ที่เคารพทุกท่านที่ได้ประสิทธ์ประสาทวิชาความรู้และถ่ายทอดประสบการณ์ที่ดีให้แก่ข้าพเจ้า

วโรดม วีระพันธ์

สิงหาคม 2548

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

หน้า

บทคัดย่อภาษาไทย.....I

บทคัดย่อภาษาอังกฤษ.....II

กิตติกรรมประกาศ.....III

สารบัญ.....IV

สารบัญตาราง.....VIII

สารบัญรูป.....X

บทที่ 1 บทนำ.....1

1.1 ความเป็นมาและความสำคัญของปัญหา.....1

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา.....1

1.3 สมมุติฐานของการศึกษา.....2

1.4 ขอบเขตการวิจัย.....3

1.5 ประโยชน์ที่เกิดขึ้นจากงานวิจัย.....3

1.6 ขั้นตอนของการศึกษา.....3

1.7 รายละเอียดในแต่ละบท.....3

บทที่ 2 โมไบล์ไอพีวีซิกส์.....5

2.1 บทนำ.....5

2.2 ความจำเป็นของ Mobile IPv6.....5

2.3 การทำ Handoff.....6

2.3.1 ชนิดของการทำ Handoff.....7

2.3.1 Horizontal Handoff.....7

2.3.2 Vertical Handoff.....8

2.4 การทำงานของโมไบล์ไอพีวีซิกส์.....8

2.4.1 Move Detection.....9

2.4.2 Stateless and Stateful configuration.....10

2.4.3 Duplicate Address Detection.....11

2.4.4 Home Agent Registration.....11

2.4.5 Triangle Routing.....12

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

2.4.6 Routing Optimization.....12

บทที่ 3 ระบบความปลอดภัยของโมไบล์ไอพีวีซิกส์ไบด์ดิ้งอัพเดท.....14

3.1 บทนำ.....14

3.2 Home Agent Binding Updates.....14

3.3 ช่องโหว่การทำ Binding Updates.....16

3.4 ระบบความปลอดภัยของ Binding Updates.....16

3.4.1 Extend Certificate-based Binding Update Protocol.....16

3.4.2 Return Routability.....18

3.4.3 Return Routability with IPSec.....23

บทที่ 4 ระบบความปลอดภัยของโมไบล์ไอพีวีซิกส์ไบด์ดิ้งอัพเดทโดยวิธีเคอร์บิรอส.....25

4.1 บทนำ.....25

4.2 การเข้ารหัส.....25

4.2.1 Symmetric cryptography.....25

4.2.2 Public key cryptography.....26

4.3 Kerberos algorithm.....26

4.4 ความปลอดภัยของโมไบล์ไอพีวีซิกส์ไบด์ดิ้งอัพเดทโดยใช้ Kerberos.....27

4.4.1 Framework.....27

4.4.2 การทำงานของ Kerberos และ Pre-Registrations.....28

บทที่ 5 การวิเคราะห์ประสิทธิภาพและโมเดล.....31

5.1 บทนำ.....31

5.2 Handoff Performances.....31

5.2.1 Move Detection Time.....31

5.2.2 IPv6 Care-of Address Configuration Time.....32

5.2.3 Care-of Address Registration Time.....33

5.2.4 Route Optimization Time.....33

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

5.3 มาตรวัดประสิทธิภาพ.....33
5.4 แบบจำลองระบบคิว.....34

บทที่ 6 การทดลองและผลการทดลอง.....36
6.1 บทนำ.....36
6.2 ส่วนประกอบ JNS.....36
6.3 การทำงานของ JNS.....36
6.4 สภาพแวดล้อม.....37
6.5 ผลการทดลอง.....38
6.5.1 เมื่อกำหนด Operating point ของ utilization factor เป็น 70%.....38
6.5.1.1 การเชื่อมต่อ.....38
6.5.1.2 Handoff delay performance.....39
6.5.1.3 เพิ่มเวลารอคิว.....41
6.5.2 เมื่อทำการจำลองโดย เพิ่มจำนวน Mobile Node.....43
6.5.2.1 การเชื่อมต่อ.....43
6.5.2.2 ความยาวของคิว.....44
6.5.2.2.1 ในเครือข่ายที่มีการใช้งานไม่หนาแน่น.....44
6.5.2.2.2 ในเครือข่ายที่มีการใช้งานหนาแน่น.....45
6.5.2.3 Handoff delay performance.....45
6.5.2.3.1 ในเครือข่ายที่มีการใช้งานไม่หนาแน่น.....45
6.5.2.3.2 ในเครือข่ายที่มีการใช้งานหนาแน่น.....48
6.6 Velocity effect 50
6.7 Pre-Registrations Process delay.....51
6.7.1 ในเครือข่ายที่มีการใช้งานไม่หนาแน่น.....51
6.7.2 ในเครือข่ายที่มีการใช้งานหนาแน่น.....51

บทที่ 7 สรุปผลการทดลองและข้อเสนอแนะ.....53
7.1 บทนำ.....53

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

7.2 สรุปผลการทดลอง....53
7.3 ข้อเสนอแนะ....54

เอกสารอ้างอิง....55

ภาคผนวก....57
Return Routability Protocol Headers....58
Kerberos and Pre-Registrations Protocol Header....72
Java Network Simulator (JNS)....88
งานวิจัยที่ได้รับการตีพิมพ์....91

ประวัติผู้เขียน....103

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

ตารางที่ หน้า

5.1 แสดงความน่าจะเป็นที่มี packet อยู่ในคิว....35

6.1 Mobile IPv6 Handoff using ECBU....39

6.2 Mobile IPv6 Handoff using Return Routability....39

6.3 Mobile IPv6 Handoff using Kerberos and Pre-Register (KPR)....39

6.4 เปรียบเทียบเวลาในการ Handoff โดยใช้วิธีต่าง ๆ....40

6.5 เปรียบเทียบเวลาการ Handoff กับค่า Lantency สำหรับ Real-Time Application....41

6.6 Mobile IPv6 Handoff using ECBU เมื่อพิจารณาคิวร่วมด้วย....41

6.7 Mobile IPv6 Handoff using Return Routability เมื่อพิจารณาคิวร่วมด้วย....41

6.8 Mobile IPv6 Handoff using Kerberos and Pre-Register เมื่อพิจารณาคิวร่วมด้วย....42

6.9 เปรียบเทียบเวลาในการ Handoff โดยใช้วิธีต่าง ๆ เมื่อพิจารณาคิวร่วมด้วย....42

6.10 เปรียบเทียบเวลาการ Handoff กับค่า Lantency สำหรับ Real-Time Application เมื่อพิจารณาคิวร่วมด้วย....43

6.11 Mobile IPv6 Handoff using ECBU....46

6.12 Mobile IPv6 Handoff using Return Routability....46

6.13 Mobile IPv6 Handoff using Kerberos and Pre-Register (KPR)....46

6.14 เปรียบเทียบเวลาในการ Handoff โดยใช้วิธีต่าง ๆ....47

6.15 เปรียบเทียบเวลาการ Handoff กับค่า Lantency สำหรับ Real-Time Application....48

6.16 Mobile IPv6 Handoff using ECBU....48

6.17 Mobile IPv6 Handoff using Return Routability....48

6.18 Mobile IPv6 Handoff using Kerberos and Pre-Register....49

6.19 เปรียบเทียบเวลาในการ Handoff โดยใช้วิธีต่าง ๆ....49

6.20 เปรียบเทียบเวลาการ Handoff กับค่า Lantency สำหรับ Real-Time Application....50

6.21 เวลาที่ใช้ในการทำ Pre-Registration 1 hop ในเครือข่ายที่มีการใช้งานไม่หนาแน่น....51

6.22 เวลาที่ใช้ในการทำ Pre-Registration 1 hop ในเครือข่ายที่มีการใช้งานหนาแน่น....51

6.23 เวลาที่ใช้ในการทำ Pre-Registration เมื่อ Mobile Node มีการเคลื่อนที่ห่างจาก Home Agent ออกไป....52

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป

รูปที่ หน้า

2.1 การทำ Horizontal Handoff....7
2.2 การทำ Vertical Handoff....8
2.3 แผนผังการทำงาน Mobile IPv6....9
2.4 แสดงการลงทะเบียนกับ Home Agent....11
2.5 แสดงการ routing ข้อมูลเป็นรูปสามเหลี่ยมเมื่อมีการติดต่อระหว่าง Mobile node กับ Correspondent Node....12
2.6 แสดงการทำ Route Optimization เพื่อให้ส่งข้อมูลได้เร็วขึ้น....13
2.7 แสดงการทำงานของ Mobile IPv6 ทั้งระบบ....13
3.1 Binding update format....15
3.2 Binding Acknowledge format....15
3.3 Binding update de-registration format....15
3.4 Binding Acknowledge de-registration format....15
3.5 Extend Certificate-based Binding Update Protocol....17
3.6 Return Routability protocol....19
3.7 Home Test Init format....19
3.8 Care-of Test Init format....20
3.9 Home Test format....20
3.10 Care-of Test format....21
3.11 Binding Update to Correspondent Node format....22
3.12 Binding Acknowledge to Mobile Node format....23
3.13 Return Routability with IPSec protocol....24
4.1 Kerberos and Pre-Registrations Protocol Phase#1....27
4.2 Kerberos and Pre-Registrations Protocol Phase#2....27
6.1 การส่งข้อมูลที่ใช้ทำ Simulation ของ JNS....37
6.2 Mobile IPv6 Simulation Topology....38
6.3 กราฟแสดงการเปรียบเทียบการ Handoff โดยวิธีต่าง ๆ....40
6.4 กราฟแสดงการเปรียบเทียบการ Handoff โดยวิธีต่าง ๆ เมื่อเพิ่มเวลารอคิว....43
6.5 Mobile IPv6 Simulation Topology....44

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

Mobile IPv6 ก็คือ IPv6 ที่สามารถเคลื่อนที่จากเครือข่ายหนึ่ง ไปยังอีกเครือข่ายหนึ่งได้ ความสามารถในการทำ Mobility นั้น ส่วนมากมักจะใช้ร่วมกับเทคโนโลยีไร้สาย ซึ่งจุดที่น่าสนใจ คือ ถ้ามีการย้ายจากเครือข่ายเดิมไปยังเครือข่ายใหม่ ซึ่งหมายความว่า IP address เดิมที่ใช้ จะต้องถูกเปลี่ยนและเราเตอร์จะต้องบอกเส้นทางที่จะส่งข้อมูลให้ถูกต้อง เราจะมีการจัดการกับสิ่ง เหล่านี้ ได้อย่างไร กุญแจของความสำเร็จของ IP mobility คือ Home Agent ซึ่ง Home Agent ก็ คือ Router ที่ทำหน้าที่คอยดูแลแพ็คเก็จที่ถูกส่งมายัง home network ไปยัง foreign network [1, 3] Home Agent สามารถทราบที่อยู่ปัจจุบันของ Mobile Node ได้จาก Binding Updates โดย การทำ Home Agent Registration ในขณะเดียวกัน หาก Correspondent Node ต้องการติดต่อ กับ Mobile Node แน่นอนว่า Correspondent Node ไม่สามารถทราบที่อยู่ที่ Mobile Node ได้ เคลื่อนย้ายไป ดังนั้น Home Agent จึงคอยทำหน้าที่ส่งแพ็คเก็จต่อไปให้ Mobile Node ตามที่อยู่ ใหม่ที่ได้กำหนดไว้ใน Binding Updates [1, 2, 9] หาก Home Agent อยู่ไกลจาก Mobile Node และ Correspondent Node จะทำให้เกิด Overhead ที่ Border router ได้ ทาง Mobile IPv6 working group จึงได้นำเสนอวิธีการทำ Routing Optimization โดยให้ Mobile Node ส่ง Binding Updates ไปให้ Correspondent Node เพื่อบอกที่อยู่ปัจจุบันของ Mobile Node เอง แต่ Binding Updates สำหรับ ระบบของ Mobile IPv6 ยังมีส่วนที่ต้องวิจัย และปรับปรุงเพิ่มเติม ใน งานวิจัยนี้ได้เสนอการประยุกต์ใช้ วิธี Kerberos และ Pre-Registrations เพื่อให้การทำ Handoff มีประสิทธิภาพในการทำงานที่เร็วขึ้นและ คงไว้ซึ่งความปลอดภัย

ในอนาคตข้างหน้า Cellular devices หรือ อุปกรณ์ฝังตัวต่าง ๆ สนับสนุนการทำงานของ IPv6 และสามารถนำมาประยุกต์ใช้กับระบบ Voice over IPv6 เป็นต้น ซึ่งระบบเหล่านี้ต้องการ การส่งข้อมูลปริมาณมาก ๆ ได้อย่างรวดเร็ว และคงไว้ซึ่งความปลอดภัย

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

Mobile IPv6 working group นำเสนอวิธีการ Return Routability ซึ่งใช้ในการป้องกัน Binding Updates อย่างไรก็ดี วิธีการนี้ก็ยังให้ความปลอดภัยที่ยัง ไม่น่าพอใจ เพราะยังมีช่องโหว่ ในการโจมตีแบบ man-in the middle attack แม้ว่าจะมีการนำเสนอให้ใช้ IP Security (IPSec) [5, 6] ในการเพิ่มความสามารถในการป้องกันความปลอดภัย แต่มันก็ทำให้วิธี Return Routability

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

มีความซับซ้อนมากขึ้นเรื่อย ๆ และ หากพิจารณาถึงอุปกรณ์ขนาดเล็กในอนาคต ที่อาจจะมี IPv6 เป็นของตัวเอง ด้วยข้อจำกัดของแบนด์วิธ และความต้องการของโปรแกรมประเภท Real-Time Application ที่ใช้เวลาในการทำ Handoff อย่างรวดเร็ว ซึ่งในสภาพแวดล้อมเหล่านี้ จำเป็นต้องมีระบบที่เหมาะสม เพื่อเพิ่มความปลอดภัยและประสิทธิภาพให้กับ Binding Updates งานวิจัยชิ้นนี้จึงได้นำเสนอวิธีการ Secure Mobile IPv6 Binding Updates using Kerberos

1.3 สมมุติฐานของการศึกษา

1.3.1 จำนวนเซลล์ไซต์ในประเทศไทย มีประมาณ 500 ไซต์ โดยกำหนดสมมติฐานว่า มีการกระจายตัวของเซลล์ไซต์สม่ำเสมอ (uniform distribution) และมีลักษณะเป็นวงกลม

1.3.2 กำหนดให้ Mobile Node เคลื่อนที่ไปในแนวที่ออกห่างจาก Home Agent และ Correspondent Node ไปยัง Access Router ที่อยู่ใกล้เคียง ไปเรื่อย ๆ โดยที่ Access Router ที่อยู่ไกลที่สุด อยู่ห่างจาก Home Agent ไม่เกิน 11 hops

1.3.3 มีการกำหนดกุญแจที่ต้องมีการแลกเปลี่ยนแบบ out-of-band ที่จำเป็นต่อระบบระหว่าง Mobile Node <–> Home Agent, Mobile Node <–> Access Router, Home Agent <-> Access Router และ Home Agent <-> Correspondent Node

1.3.4 กำหนดให้แต่ละช่องทางการสื่อสารมีแบนด์วิธที่ 2 mbps ทุก ๆ ช่อง สัญญาณการสื่อสาร โดยช่องทางการสื่อสารที่เป็นสายหลัก จะมีแบนด์วิธสูงสุดไม่เกิน 2 mbps โดยอ้างอิงจากกรณีที่มีการทำ ReSerVation Protocol (RSVP) ซึ่งกำหนดให้มีการจองช่องสัญญาณไว้ที่ 2 mbps และ มีค่าความหน่วงเวลา 2 msec ซึ่งค่าความหน่วงของเวลานี้รวมไปถึงการคำนวนของซีพียูด้วย

1.3.5 กำหนด Access Router ทุก ๆ การสื่อสาร มีการซ้อนทับกันเป็นระยะทางเฉลี่ยไม่น้อยกว่า 250 เมตร

1.3.6 กำหนดชนิดการทำ Seamless handoff เป็น Vertical handoff และเป็นการ handoff ระหว่าง Access Router ที่อยู่คนละโดเมนกับ Home Agent ไปยัง Access Router ที่อยู่ติดกัน

1.3.7 กำหนดให้ Care-of address ที่ได้จากการทำ Stateless auto configuration ไม่ซ้ำกับไอพีของโหนดใด ๆ ในระบบเครือข่าย

1.3.8 กำหนดให้การส่งข้อมูลในแต่ละเส้นทางมีโอกาสผิดพลาดน้อยมาก

1.3.9 ใช้กับสภาพแวดล้อมที่ ไม่สามารถกำหนด Security Association pairs ระหว่าง Mobile Node และ Correspondent Node โดยตรงได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.4 ประโยชน์ที่เกิดขึ้นจากงานวิจัย

- เหมาะที่จะนำไปใช้กับ Real-Time Application โดยคงไว้ซึ่งระบบความปลอดภัย
- แก้ปัญหาเรื่องความปลอดภัย กรณี Man-in-the-middle attack ในวิธีการ Return Routability ที่ไม่ได้ใช้งานร่วมกับ IPSec
- ลดเวลาในการคำนวนการตรวจสอบ Binding Updates
- ใช้กุญแจในการเข้ารหัสที่สั้นกว่าวิธีที่นำเสนอมาแล้ว

1.5 ขอบเขตการวิจัย

ในระบบที่ได้นำเสนอไปนี้จะสนใจ ในส่วนที่เป็นการ Handoff ในชั้นไอพี โดยเปรียบเทียบประสิทธิภาพวิธีที่ได้นำเสนอ กับ วิธีที่เป็นมาตรฐานและวิธีที่มีผู้อื่นได้นำเสนองานวิจัยออกมาแล้ว ตามสมมุติฐานที่ได้กำหนดไว้

1.6 ขั้นตอนของการศึกษา

- ศึกษาทฤษฎีและวิธีการทำ Binding Updates จากงานวิจัยที่เคยมีผู้นำเสนอ
- ศึกษาทฤษฎี วิธีสร้างและการวัดค่า Handoff latency จากกลุ่มตัวอย่าง
- ทดลองวัดค่า Handoff latency ตามวิธีการที่นำเสนอ และเปรียบเทียบกับงานวิจัยที่เคยมีผู้นำเสนอมาแล้ว พร้อมทั้งวิเคราะห์ผล
- จัดทำเอกสารประกอบวิทยานิพนธ์

1.7 รายละเอียดในแต่ละบท

เพื่อศึกษา ทดลองถึงประสิทธิภาพของวิธีการนำเสนอ และเปรียบเทียบกับวิธีการที่มีอยู่เดิม รวมถึงวิเคราะห์ข้อดีข้อเสียต่างๆ วิทยานิพนธ์เล่มนี้แบ่งออกเป็น 7 บท ซึ่งประกอบด้วยเนื้อหาต่างๆ ดังนี้

1. บทที่ 1 กล่าวถึงความสำคัญและความเป็นมาของปัญหา จุดประสงค์ของการศึกษาและของเขตของงานวิจัย
2. บทที่ 2 กล่าวถึงโมไบล์ไอพีวีซิกส์
3. บทที่ 3 กล่าวถึงระบบความปลอดภัยของโมไบล์ไอพีวีซิกส์ไบด์ดิ้งอัพเดท
4. บทที่ 4 กล่าวถึงระบบความปลอดภัยของโมไบล์ไอพีวีซิกส์ไบด์ดิ้งอัพเดทโดยวิธีเคอร์บิรอส
5. บทที่ 5 กล่าวถึงการวิเคราะห์ประสิทธิภาพและโมเดล
6. บทที่ 6 กล่าวถึงการทดลองและผลการทดลอง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

7. บทที่ 7 สรุปผลการทดลองและข้อเสนอแนะ
8. เอกสารอ้างอิง
9. ภาคผนวกและงานวิจัยที่ได้รับการตีพิมพ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2
โมไบล์ไอพีวีซิกส์

2.1 บทนำ

ในปัจจุบันนี้ การเทคโนโลยีการสื่อสารแบบไร้สาย ได้เข้ามามีบทบาทกับชีวิตประจำวันของเรามากขึ้น โปรแกรมประยุกต์ต่าง ๆ ก็เพิ่มความสามารถในการติดต่อผ่านทางเครือข่ายเพิ่มมากขึ้น โปรแกรมที่ติดต่อผ่านทางเครือข่ายส่วนใหญ่ อ้างอิง การติดต่อสื่อสาร ผ่านทางโพรโตคอล IP ซึ่งเปรียบเสมือนกับที่อยู่ของบ้างหลังนั้น ถ้าโหนดที่ติดต่อกัน มีการเคลื่อนที่ไปยังเครือข่ายอื่นจากข้อกำหนดของ IP โหนดนั้น ๆ ก็จะต้องเปลี่ยน IP address ใหม่ตาม network prefix ของเครือข่ายนั้น ๆ ด้วยเหตุนี้เอง ทำให้การติดต่อสื่อสารผ่านทางเครือข่ายที่อ้างอิง IP address ต้องถูกตัดขาดไป

Mobile IPv6 [1,2,3] ก็คือ IP ที่สามารถเคลื่อนที่จากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่งได้ ความสามารถในการทำ Mobility นั้น จะใช้ร่วมกับเทคโนโลยีไร้สาย ซึ่งจุดที่น่าสนใจคือ ถ้ามีการย้ายจากเครือข่ายเดิมไปยังเครือข่ายใหม่ ซึ่งหมายความว่า host address จะต้องเปลี่ยน และ Router จะต้องบอกเส้นทางที่จะส่งข้อมูลให้ถูกต้อง โดยปกติ เมื่อมีการเปลี่ยนแปลงค่า IP address ส่วนมากจำเป็นต้องสิ้นสุดการติดต่อของ transport-layer หาก host นั้นมีการติดต่อกับ Domain Name Server (DNS) การเปลี่ยนแปลงข้อมูลใน DNS จึงจำเป็นด้วย ในทางกลับกันหากใช้วิธีการแก้ปัญหาโดยการกำหนด Routing แบบเฉพาะเจาะจงสำหรับที่อยู่ใหม่ของ Mobile node โดยใช้หลักการของ Longest matching ซึ่งจะต้องกระจาย Routing message ที่เฉพาะเจาะจงไปทั่วนั้น ก็ไม่สามารถทำได้ เพราะคาดว่าจะมี Mobile node ใน internet มากเกินไป ซึ่งจะต้องใช้การตาราง Routable ที่ใหญ่มาก มีการส่งข้อมูลของ Route table เพื่อปรับปรุง Router ต่าง ๆ ที่อยู่ระหว่าง Home Link และ Foreign Link การ Route ของเส้นทาง ซึ่งก็ใช้ bandwidth สูง และปัญหาเกี่ยวกับ Security ถ้ามีใครที่ลักลอบส่งข้อมูล Route table มาเพื่อให้ Mobile node ที่ย้ายไปไม่สามารถรับข้อมูลได้อีกต่อ เป็นต้น

2.2 ความจำเป็นของ Mobile IPv6

ถ้าการสื่อสารถูกกำหนดขึ้นโดยผู้ใช้และ ผู้ใช้สามารถหยุดการทำงานของโปรแกรมและเริ่มการทำงานใหม่ เมื่อมีการเปลี่ยนเครือข่ายได้ การย้ายเครือข่ายแบบ mobility (Vertical handoff) ก็อาจไม่มีความจำเป็นมาก การย้ายเครือข่ายแบบ nomadicity (Horizontal handoff) เพียงอย่างเดียวก็มีความจำเป็นและเพียงพอต่อการทำงาน ในทางกลับกัน หาก fix nodes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จำเป็นต้องมีการติดต่อกับ Mobile Node หรือ โปรแกรมที่จำเป็นต้องไม่เริ่มการทำงานใหม่เมื่อ Mobile Node เปลี่ยนเครือข่าย mobility จึงมีความจำเป็น การทำ nomadicity เพียงอย่างเดียว จึงไม่เพียงพอต่อการทำงาน

มีหลายเหตุผลที่อธิบายว่าทำไม mobility จึงน่าสนใจกว่า nomadicity ตัวอย่างเช่น

- โปรแกรมหลาย ๆ ชนิด มีการกำหนดการเชื่อมต่อฐานข้อมูล ให้ขึ้นตรงกับ IP address และไม่สนใจ hostname ซึ่งการเปลี่ยน IP address ทำให้การเชื่อมต่อถูกตัดขาดลง
- มีเหตุผลที่น่าเชื่อถือว่า ในอนาคต เครื่องแม่ขาย สามารถเคลื่อนย้ายเครือข่าย (mobility) ได้ ซึ่งก็มีความจำเป็นที่จะต้องกำหนดค่า IP address เดิม เพื่อให้เครื่องลูกข่าย สามารถเชื่อมต่อใช้งานได้
- โปรแกรมบางชนิด กำหนดระบบการอนุญาตใช้งานเครือข่าย ที่ให้ใช้งานในช่วงของ IP address ที่กำหนดเท่านั้น หากปราศจาก Mobile IP, nomadic node เมื่อเปลี่ยน Link ซึ่งจำเป็นต้องเปลี่ยน IP address ที่ไม่อยู่ในช่วงของระบบที่กำหนดในระบบการอนุญาตใช้งานในเครือข่าย ก็ไม่สามารถใช้งานเครือข่ายของโปรแกรมนั้น ๆ ได้
- กลไกรักษาความปลอดภัยบางประเภท กำหนดการให้สิทธิเข้าถึงข้อมูลของโหนด โดยขึ้นกับ IP address ของตัวเอง Mobile Node ที่สนับสนุนการทำงาน mobile IP ยังคงสามารถใช้งานระบบนี้ได้
- การดูแลจัดการ กลุ่มของ IP address ที่กำหนดให้ nomadic node ซึ่งกระจัดกระจาย ทำได้ลำบาก และในบางกรณีไม่สามารถกำหนดกลไกการทำงานตรงนี้ได้ เนื่องจากยังไม่ทราบ IP address ที่จะเปลี่ยนแปลง ในทางตรงข้าม mobile IP ไม่มีข้อจำกัดเกี่ยวกับปัญหาทางด้านนี้

2.3 การทำ Handoff

เมื่อ Mobile Node เปลี่ยนจุดการเชื่อมต่อระบบเครือข่าย หรือ จากเครือข่ายเดิมไปยังเครือข่ายใหม่ กระบวนการเช่นนี้เราจะเรียกว่า Handoff หรือ Handover โดยทั่วไปแล้ว นักวิจัยที่วิจัยเกี่ยวกับการออกแบบโพรโตคอลใน IP Layer (L3) มักจะเรียกกระบวนการนี้ว่า Handoff แต่นักวิจัยที่วิจัยเกี่ยวกับระบบการติดต่อสื่อสารใน Data Link layer (L2) มักจะเรียกกระบวนการนี้ว่า Handover ซึ่งในช่วงเวลาที่กระบวนการนี้ได้เกิดขึ้น ซึ่งแล้ว Mobile Node จะไม่สามารถติดต่อกับ Correspondent Node ที่ติดต่อกัน ก่อนที่เชื่อมต่อระบบเครือข่ายใหม่ได้ และจะมีช่วงเวลาหนึ่งที่ Mobile Node ไม่สามารถรับส่ง IPv6 packet เพื่อประมวลผลการทำงานของ application session ที่ยังทำงานอยู่ ในขณะที่ TCP Application ถูกออกแบบมาเพื่อแก้ปัญหา Packet ที่ไม่สามารถรับส่งได้ โดยการ รับส่งใหม่ซ้ำ ส่วนกรณีของ UDP application นั้นไม่สามารถที่เรียก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

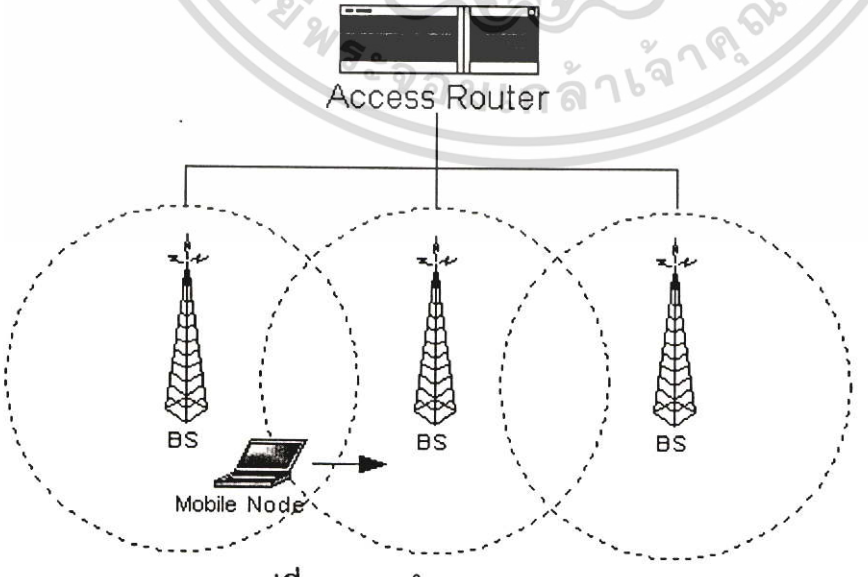
Packet ที่หายไปคืนมาได้ ยิ่งไปกว่านั้น ทั้ง TCP และ UDP application ที่ต้องส่ง Packet ให้ทันภายในช่วงเวลาที่จำกัด โปรแกรมประเภท Real-Time Applications ตัวอย่างเช่น VoIP และ audio/video applications ซึ่งช่วงเวลาที่ Packet สูญหายไปขณะที่ Mobile node ทำการ Handoff นั้นมีผลอย่างมาก Application เหล่านี้ เราเรียกว่า seamless handoff โดยคำว่า seamless ในที่นี้หมายถึง Packet สูญหายน้อยมาก และ มี Latency ที่ต่ำมาก [13]

2.3.1 ชนิดของการ Handoff

มีงานวิจัยบางงาน กล่าวถึงการประเภทของการ Handoff สามารถแบ่งได้เป็น 2 ประเภท คือ hard และ soft handoff โดยที่ hard handoff หมายถึง เมื่อมีการ handoff เกิดขึ้น Mobile Node จะต้องตัดการเชื่อมต่อกับระบบเครือข่ายเก่า ก่อนที่จะเชื่อมต่อกับระบบเครือข่ายใหม่ ในทางกลับกัน soft handoff หมายถึง Mobile Node เชื่อมต่อกับระบบเครือข่ายอย่างน้อย 1 ช่องสื่อสาร ในกรณีนี้ จะเห็นได้ว่า ช่องสัญญาณการสื่อสารจะต้องมีการซ้อนทับระหว่างกัน ระหว่างที่มีการทำ handoff เกิดขึ้น และแน่นอนว่า Mobile Node จะต้องมี interface มากกว่า 1 interface เพื่อติดต่อสื่อสาร [9]

2.3.1.1 Horizontal Handoff

การทำ Horizontal Handoff คือการที่ Mobile node เปลี่ยนการเชื่อมต่อจาก Base station หนึ่งไปยัง Base station ถัดไปที่อยู่ติดกัน ซึ่งจะเห็นได้ว่าเป็นการเปลี่ยนระบบเครือข่ายใน Link Layer (L2) เท่านั้น ไม่มีผลต่อกระบวนการทำ Mobile IP Hand off ซึ่งในกรณีนี้ IPv6 layer ไม่จำเป็นต้องรับรู้ถึงการย้ายเครือข่ายระหว่าง Base station เลย

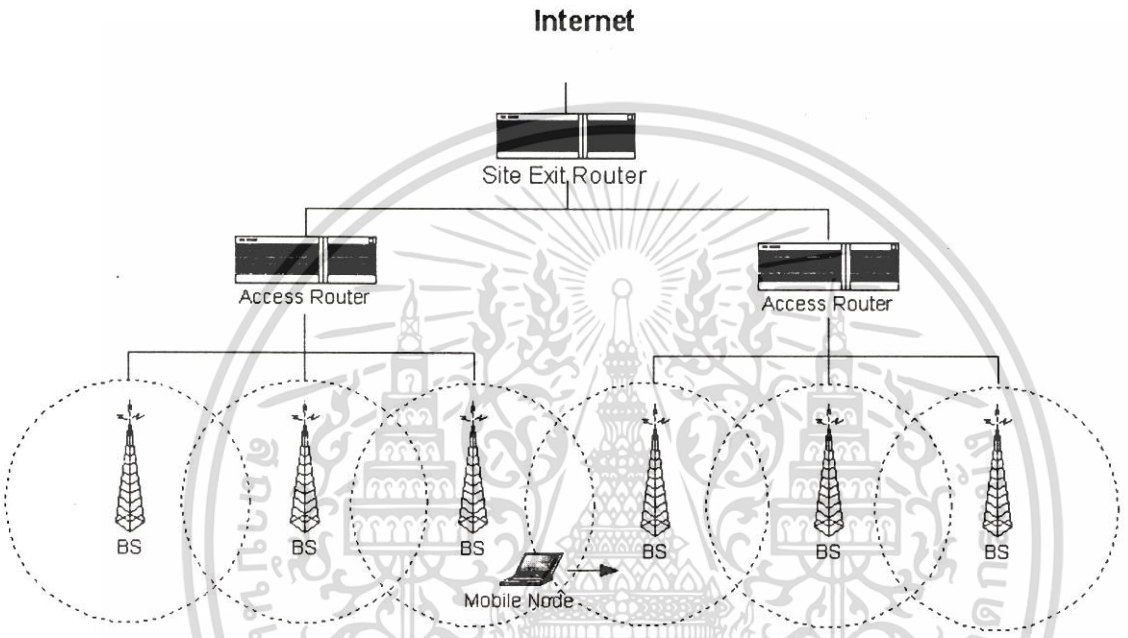


รูปที่ 2.1 การทำ Horizontal Handoff

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3.1.2 Vertical Handoff

Mobile node เปลี่ยนการเชื่อมต่อเครือข่ายจาก Base station ตัวเก่า ไปยัง Base station ตัวใหม่ โดยที่ Base station ตัวใหม่ นั้นอยู่คนละ domain กับ Base station ตัวเก่า กระบวนการ Handoff เช่นนี้ เรียกว่า Vertical Handoff หากต้องการให้ Application ที่ผูกติดกับ IPv6 address ตัวเดิม สามารถทำงานต่อไปได้โดยที่ไม่ติดขัด จะต้องมีกระบวนการทำ Mobile IPv6 Handoff ซึ่งจะได้อธิบายต่อไป

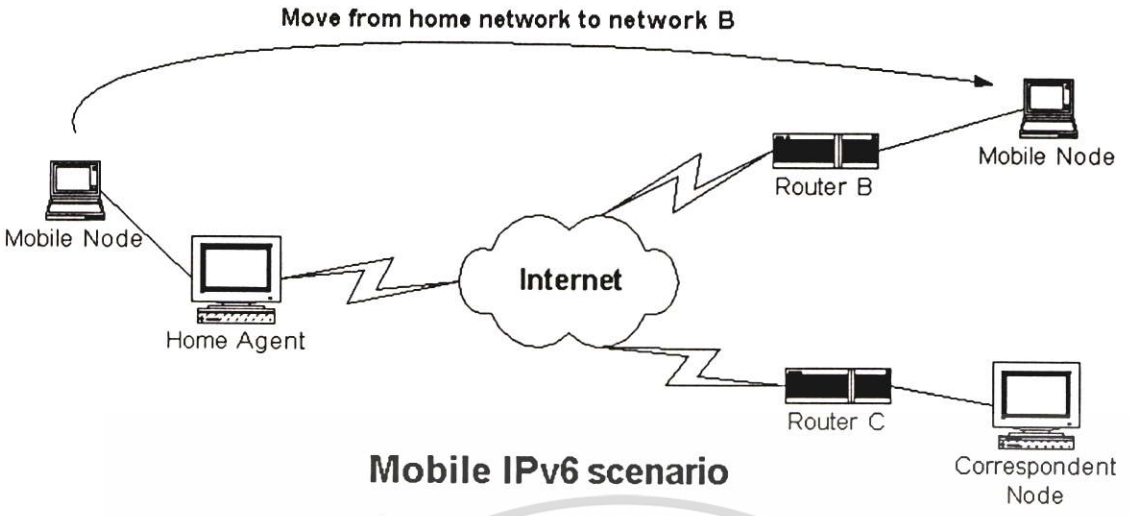


รูปที่ 2.2 การทำ Vertical Handoff

2.4 การทำงานของ Mobile IPv6

Mobile IPv6 จะประกอบไปด้วย Mobile Node หรือ โหนดที่สามารถเคลื่อนย้ายตัวเองไปยังที่ต่าง ๆ ได้ เมื่อ Mobile Node ย้ายที่อยู่ไป Home Agent ทำหน้าคอยส่งข้อมูลต่อไปให้ Mobile Node โดยจะคอยดักจับข้อมูลที่ Correspondent Node ส่งมาให้ Mobile Node ซึ่งจะเห็นได้ว่าการเชื่อมต่อกับอินเทอร์เน็ตซึ่งมีอยู่ด้วยกัน 3 เส้นทาง เริ่มต้น Mobile Node อยู่ที่ Home Network นั่นคือ อยู่ในเครือข่ายเดียวกันกับ Home Agent จากนั้น เมื่อ Mobile Node ย้ายจาก Home Network ไปยัง Foreign Network ซึ่งเป็นเครือข่ายที่เชื่อมต่อโดยตรงกับ Router B เราเรียกกระบวนการนี้ว่าเป็นการทำ Vertical Handoff ซึ่งเราจะเห็นว่า Mobile node ได้ย้ายจากที่อยู่เดิมไปแล้ว และถ้า Correspondent Node ต้องการจะติดต่อกับ Mobile node จะมีวิธีการขั้นตอนย่อย ๆ ดังต่อไปนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.3 แผนผังการทำงาน Mobile IPv6

2.4.1 Movement Detection

เป็นกลไกการทำงานที่ใช้ตรวจสอบว่า Mobile node ได้ย้ายออกไปจากเครือข่ายเดิมแล้ว ซึ่งวิธีการตรวจสอบนั้น แบ่งย่อย ได้เป็น 2 วิธีคือ

- ตรวจสอบจาก ICMP packet lifetime

ใช้ค่า Lifetime ใน ICMP Router Advertisement โดยปกติแล้ว Agent จะทำการ broadcast ICMP Router Advertisement message ซึ่งจะมี ข้อมูลของ maximum registration lifetime โดยที่ Mobile node จะบันทึกค่า lifetime สำหรับแต่ละ message ที่ Agent Advertise มาให้ โดยค่านี้จะบอก Mobile Node ว่าภายในช่วงเวลาเท่าไร ที่ Mobile Node ควรจะได้รับ Advertisement message อีกครั้ง จาก Agent เดิม ซึ่ง Agent จะคอยส่ง message นี้มาเพื่อ ปรับปรุงค่า lifetime อยู่เรื่อย ๆ ถ้า lifetime หมดอายุเมื่อไรก็แสดงว่ามันได้ย้ายเครือข่ายไปแล้ว อย่างไรก็ดี Advertisement อาจจะสูญหายระหว่างส่งได้ โดยเฉพาะการส่งข้อมูลใน ระบบเครือข่ายที่มีความผิดพลาดสูง และ เครือข่ายไร้สาย ดังนั้น โดยส่วนมากแล้ว Agent จะส่ง Advertisement เร็วกว่าค่า Lifetime ที่กำหนดไว้ใน Router Advertisement ประมาณ 3 เท่า ซึ่งแนะนำโดย [15]

- ตรวจสอบจาก Network prefix ใน Router Advertisement message

Agent advertisement จะมีข้อมูลของ network prefix ซึ่ง Mobile node สามารถนำค่า prefix ที่มีอยู่เดิมเปรียบเทียบกับค่า prefix ใหม่ ถ้าพบว่ามีการเปลี่ยนแปลงก็สันนิษฐานได้ว่ามีการย้าย network ไปแล้ว เมื่อ Mobile node สามารถตรวจสอบได้ว่าตัวเอง ย้ายจาก Link หนึ่งไปยัง Link อันใหม่ (Foreign

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Network) Mobile Node จะหา Router ใหม่ จากนั้นก็จัดการกำหนด IP address ใหม่ ที่อยู่ใน Network เดียวกันกับ Foreign Network

หากระบบเครือข่ายมี Agent มากกว่า 1 Agent ทำให้ Mobile node ได้รับ Agent advertisement มากกว่า 1 message ดังนั้น Mobile Node ก็ตรวจสอบว่าหากตัวเองยังคงได้รับ advertisement เดิมอยู่ ก็แสดงว่า ยังไม่ได้ย้ายไปยังเครือข่ายใหม่

2.4.2 Stateless and Stateful configuration

Stateless Autoconfiguration

stateless address autoconfiguration [2] คือการกำหนด IP address แบบอัตโนมัติให้กับตัวมันเอง ดังนี้

- host ต้องกำหนด link-local address ก่อน โดยใช้ link-local prefix (FE80) กับ MAC address
- ทำกระบวนการ Duplicate Address Detection (DAD)
- หลังจากกำหนด link-local address แล้ว host ต้องหาว่ามี router อยู่ใน local network หรือเปล่า ซึ่งทำได้สองวิธีคือ รอรับ Router Advertisement ซึ่ง Router จะส่งออกมาเป็นระยะๆ หรือไม่ host ก็ส่ง Router Solicitation message ไปยัง all-router multicast address (FF02::2) เพื่อให้ Router ส่ง Advertisement ตอบกลับมา ขั้นตอนนี้จะทำให้รู้ว่ามี router อยู่ใน network หรือเปล่า และ node ไหนบ้างที่เป็น router
- ถ้ามี Router อยู่ใน network, host ก็จะได้ Router Advertisement message ซึ่งประกอบด้วย global unicast prefix ของ network สำหรับกำหนดเป็น global unicast address ของ host พร้อมกับได้ local-link address ของ Default Router

Stateful Autoconfiguration

stateful address autoconfiguration คือการกำหนด IP address แบบอัตโนมัติให้กับตัวมันเอง โดยใช้บริการของ DHCP Server ซึ่ง server เป็นคนแจก IP มาให้เครื่องลูกข่ายที่ร้องขอใช้บริการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

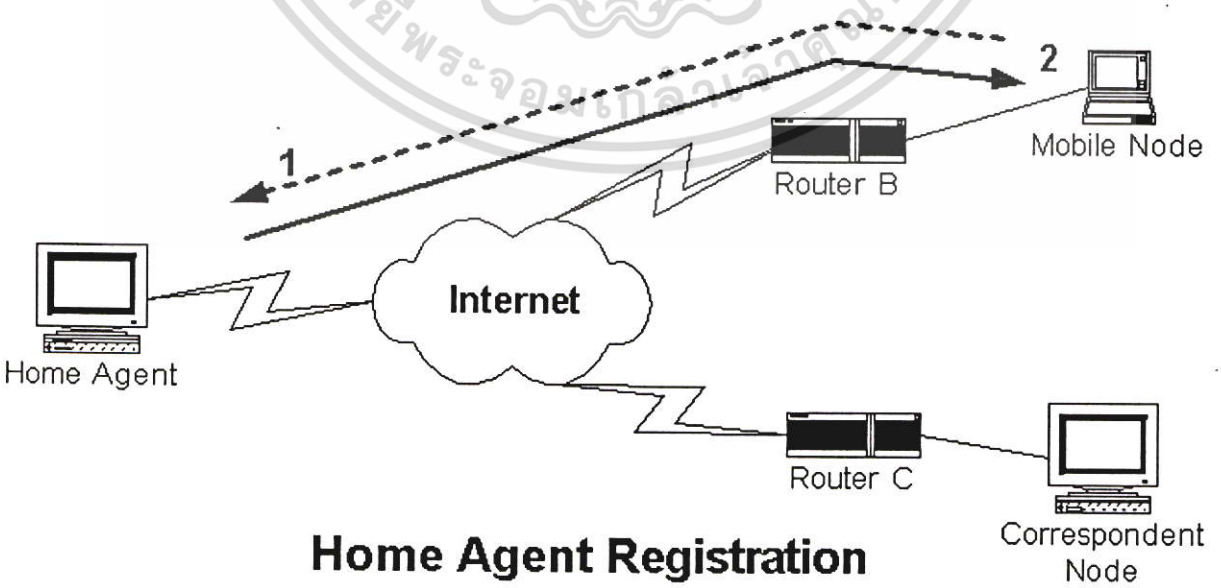
2.4.3 Duplicate Address Detection

เมื่อมีการกำหนด IPv6 address ให้กับ interface ของ node ใด ๆ node นั้นจะต้องทำกระบวนการ Duplicate Address Detection (DAD) เพื่อให้มั่นใจว่า address ที่ได้มาจะไม่ซ้ำกับ node ใด ๆ ใน Link นี้ วิธีการทำ DAD คือ node จะต้องใช้ IPv6 address ที่สร้างขึ้นมาใหม่ (CoA) ส่ง Neighbor Solicitation message (NS) ไปยัง node-solicited multicast address โดย แล้วรอ node อื่น ๆ ส่ง Neighbor Acknowledgement message (NA) กลับมา ถ้ามี node อื่นที่ใช้ address เดียวกัน มันก็จะรู้ว่า link-local address ชน กรณีนี้ node ก็จะต้องกำหนด IPv6 address ขึ้นมาใหม่ แต่ถ้าไม่ชน link-local address ที่สร้างไว้ ก็จะเอาไปใช้งานต่อได้

2.4.4 Home Agent Registration

หลังจากที่ Mobile node ได้ย้ายไปยัง Foreign Network และจัดการ Configuration ตัวเองเป็นที่เรียบร้อยแล้ว มันก็จะต้องติดต่อกับ Home agent เพื่อบอกตำแหน่งที่อยู่ใหม่ของตัวมันเอง และให้ Home agent สามารถ Route ข้อมูลที่จะส่งมาที่อยู่เดิม ให้ส่งไปยังที่อยู่ใหม่ได้ ซึ่ง Mobile node จะต้องติดต่อกับ Home agent ดังนี้

1. Mobile Node ส่ง packet Binding Updates (เส้นเบอร์ 1)
2. Home Agent ทำการ register binding อันนี้เพื่อทราบว่า Mobile node อยู่ที่ไหน
3. Home Agent ส่ง Bind Acknowledgement packet ตอบกลับไป (เส้นเบอร์ 2)

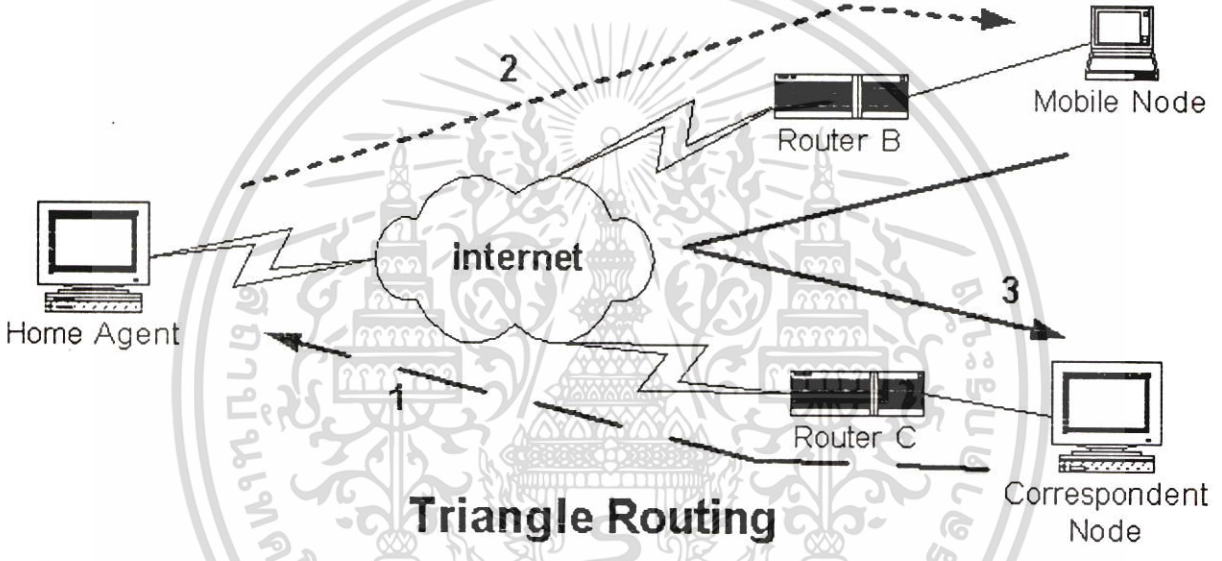


รูปที่ 2.4 แสดงการลงทะเบียนกับ Home Agent

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.4.5 Triangle Routing

ถ้า Mobile node ย้ายที่อยู่ไปยัง Foreign Network แล้วข้อมูลที่ Correspondent Node จะส่งไปหา Mobile node, Correspondent Node จะต้องส่งไปยัง Home address ก่อน (เส้นเบอร์ 1) Home agent จะมาคอยดักจับ packet ที่ส่งให้ Mobile node โดยทำเป็น tunnel ไปหา packet ที่ส่งไปจะเป็นลักษณะของ IP encapsulation ใน IP อีกครั้งหนึ่ง (เส้นเบอร์ 2) เมื่อไปถึงปลายทางก็จะทำการถอด packet ออกมาอีกทีหนึ่ง จากนั้นถ้า Mobile node ต้องการจะส่งข้อมูลกลับไปหา Correspondent Node ก็สามารถส่ง packet ไปหาได้โดยตรง (เส้นเบอร์ 3)



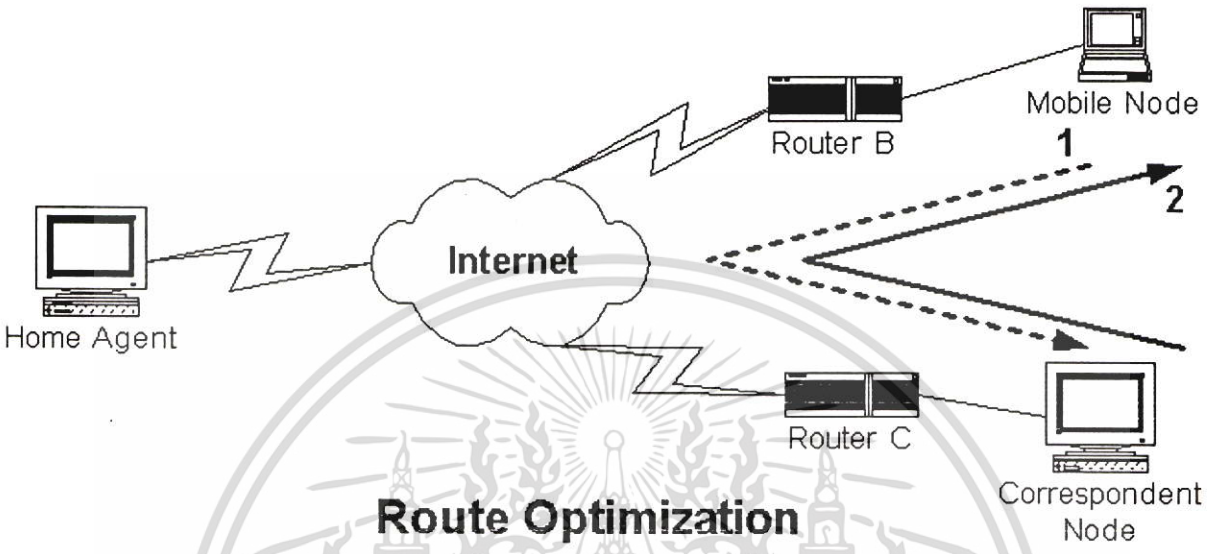
รูปที่ 2.5 แสดงการ routing ข้อมูลเป็นรูปสามเหลี่ยมเมื่อมีการติดต่อ ระหว่าง Mobile node กับ Correspondent Node

2.4.6 Routing Optimization

Mobile Node ส่ง Binding Updates ไปให้ Correspondent node เพื่อทำ Routing Optimization โดย Correspondent Node จะนำข้อมูลใน Binding Updates มาตรวจสอบกับ Binding cache ของตนเอง ถ้าข้อมูลที่อยู่ใน Binding cache ไม่ตรงกับข้อมูลใน Binding Updates แสดงว่า Mobile Node ย้ายไปอยู่ที่ใหม่ ซึ่ง Correspondent Node จะต้อง Register Care-of address สำหรับที่อยู่ใหม่ของ Mobile Node ลงใน Binding cache และส่ง Binding Acknowledge ตอบกลับมาให้ Mobile node เพื่อบอกให้ Mobile Node ทราบว่า Correspondent Node พร้อมที่ส่งข้อมูลไปหา Mobile Node โดยตรงแล้ว หลังจากนั้น Correspondent Node สามารถที่จะส่ง packet ไปยัง Mobile

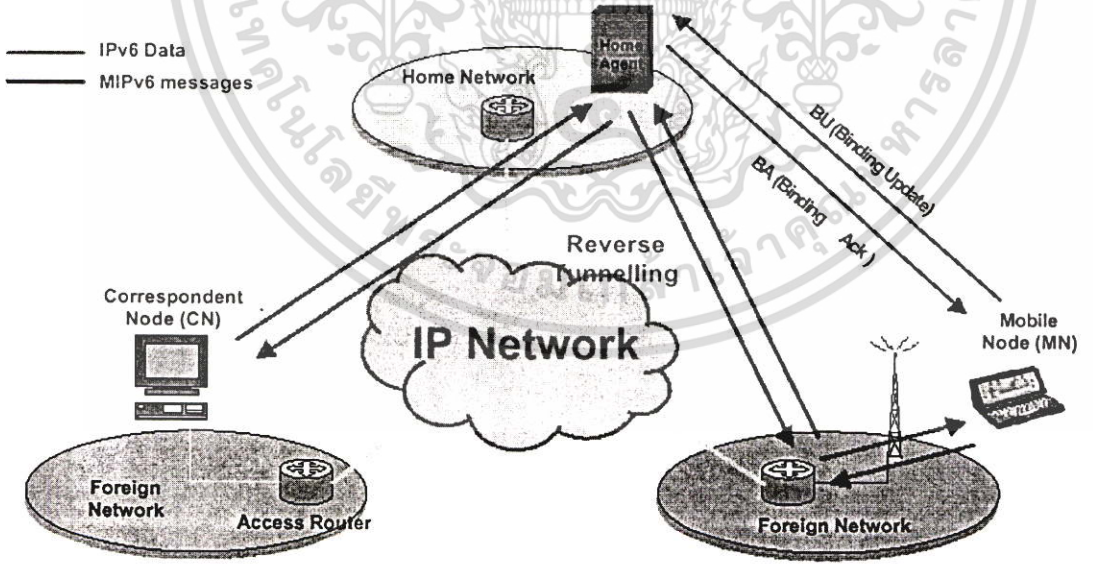
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Node โดยใช้ routing header ซึ่งส่งตรงไปยัง care-of address และต่อไปยัง home address โดยตรง ลดการส่งข้อมูลแบบ Triangle Routing แต่ถ้า Binding cache ไม่มีข้อมูล



รูปที่ 2.6 แสดงการทำ Route Optimization เพื่อให้ส่งข้อมูลได้เร็วขึ้น

การทำงานของ Mobile IPv6 สามารถสรุปได้ดังรูปข้างล่างนี้



รูปที่ 2.7 แสดงการทำงานของ Mobile IPv6 ทั้งระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3
ระบบความปลอดภัยของโมไบล์ไอพีวีซิกส์ไบด์ดิ้งอัพเดท

3.1 บทนำ

Mobile IPv6 ได้ถูกพัฒนามาเพื่อให้ อุปกรณ์ IP ต่าง ๆ สามารถเคลื่อนย้าย ไปยังที่อื่น ๆ ต่างระบบเครือข่ายกัน โดยที่การเชื่อมต่อการสื่อสารเดิม ไม่ถูกตัดขาด ซึ่งเทคโนโลยีนี้ ได้ถูกนำมาใช้งานอย่างแพร่หลาย กระบวนการทำงานนี้ ใช้ Binding Updates ซึ่งเป็น message ที่ใช้ในการบอกที่อยู่ปัจจุบันของ Mobile Node จากนั้น Mobile node สามารถทำ Routing Optimization โดยใช้ข้อมูลจาก Binding Updates ซึ่งสามารถลด Overhead ที่เกิดขึ้น ทำให้การส่งข้อมูลทำได้อย่างมีประสิทธิภาพ ดังจะเห็นได้ว่า Binding Updates นั้นมีความสำคัญมาก หากมีผู้ไม่หวังดี พยายามปลอม Binding Updates เพื่อวัตถุประสงค์ใด ๆ ของผู้ไม่หวังดีเอง เช่น แก้ไข Care-of address ใน Binding Updates ของ Mobile Node ซึ่งทำให้ Mobile Node ไม่สามารถติดต่อสื่อสารกับ Correspondent Node ได้ และหากมองในอีกแง่หนึ่งคือ หากกระบวนการย้ายเครือข่าย (Handoff) ที่มีค่า Latency สูงนั้น มีผลกระทบโดยตรงต่อโปรแกรมประเภท Real-Time Application ที่เวลามีผลกระทบต่อการทำงาน เป็นอย่างมาก

3.2 Home Agent Binding Updates

Mobile Node ส่ง Binding Updates เพื่อบอกให้ Home Agent ทราบที่อยู่ปัจจุบันของ Mobile Node เพื่อให้ Node อื่น ๆ ที่จะติดต่อ Mobile Node สามารถส่งข้อมูล ไปยัง Home Address ของ Mobile Node โดย Home Agent จะคอยดักจับข้อมูลแล้ว ส่งต่อไปยัง ที่อยู่ปัจจุบันของ Mobile Node ต่อไป ข้อมูลของ Binding Updates มีดังนี้

IPv6 header
- Source Address = Care-of Address
- Destination Address = Home Agent

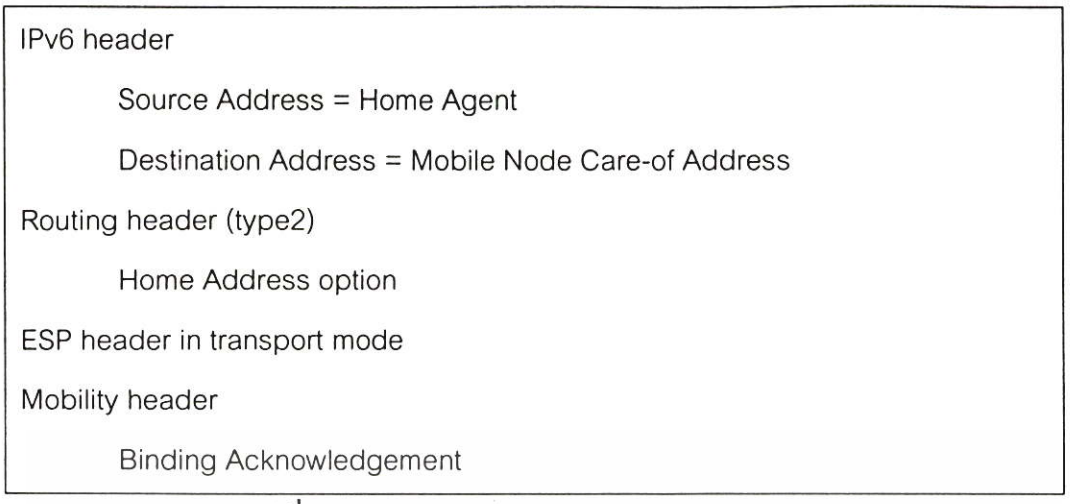
Destination Options header
- Home Address option

ESP header in transport mode

Mobility header
- Binding Update: Alternate Care-of Address option

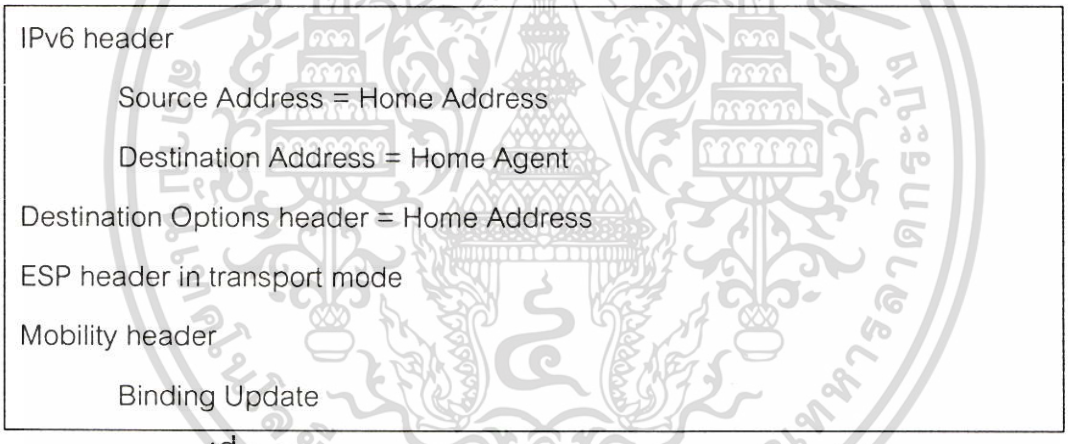
รูปที่ 3.1 Binding Updates format

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

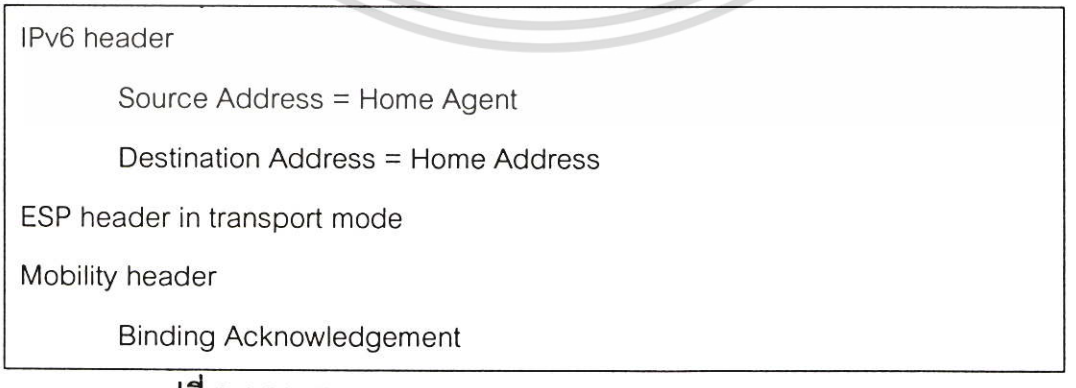


รูปที่ 3.2 Binding Acknowledge format

เมื่อ Mobile Node ย้ายเครือข่ายกลับมายัง Home Network แล้ว Mobile Node จะต้องทำการ de-registration Binding Updates ซึ่งข้อมูลที่กำหนดใน Binding Updates และ Binding Acknowledge มีดังนี้



รูปที่ 3.3 Binding Updates de-registration format



รูปที่ 3.4 Binding Acknowledge de-registration format

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3 ช่องโหว่ของ Binding update

ผู้โจมตีสามารถโจมตี เหยื่อ ที่ใช้ Original Binding Updates ได้ดังนี้

1. เปลี่ยนข้อมูลที่ Mobile Node ส่ง Binding Updates ไปให้ Home Agent โดยแก้ข้อมูลใน Binding Updates จาก IP address ปัจจุบันของ Mobile Node เองเป็นของ ผู้โจมตี เพื่อให้ Home Agent tunneling packet มายัง ผู้โจมตี เอง ทำให้ ผู้โจมตี สามารถอ่านข้อมูลของ Mobile Node ได้
2. เปลี่ยนข้อมูลที่ Mobile Node ส่ง Binding Updates ไปให้ Home Agent โดยแก้ข้อมูลใน Binding Updates จาก IP address ปัจจุบันของ Mobile Node เองเป็นของ ผู้ถูกโจมตี ในลักษณะ ของ Distributed Denial of Services (DDoS)
3. เปลี่ยนข้อมูลที่ Mobile Node ส่ง Binding Updates ไปให้ Home Agent โดยแก้ข้อมูลใน Binding Updates จาก IP address ปัจจุบันของ Mobile Node เองเป็นของ node อื่น ๆ เพื่อให้ Mobile Node ไม่สามารถรับข้อมูลจาก Home Agent ได้
4. เปลี่ยนข้อมูลที่ Home Agent tunneling packet ไปยัง Correspondent Node ให้ tunneling packet มาที่ ผู้โจมตี เอง ทำให้ ผู้โจมตี สามารถอ่านข้อมูลของ Mobile Node ได้
5. เปลี่ยนข้อมูลที่ Mobile Node ส่ง Binding Updates ไปให้ Correspondent Node จากตำแหน่งปัจจุบันของ Mobile Node เองเป็นของ ผู้โจมตี เพื่อให้ Home Agent tunneling packet มายัง ผู้โจมตี เอง ทำให้ ผู้โจมตี สามารถอ่านข้อมูลของ Mobile Node ได้
6. เปลี่ยนข้อมูลที่ Mobile Node ส่ง Binding Updates ไปให้ Correspondent Node โดยแก้ข้อมูลใน Binding Updates จาก IP address ปัจจุบันของ Mobile Node เองเป็นของ ผู้ถูกโจมตี ในลักษณะ ของ DDoS
7. แม้ว่า packet นั้นจะมีการ sign แล้ว แต่ ผู้โจมตี อาจจะ copy เอา header packet ในเส้นทางการสื่อสารระหว่าง node นั้นมา เพื่อใช้ส่งด้วยตัวเองในภายหลัง ซึ่งสามารถแก้ไขโดยการกำหนด cookie

3.4 ระบบความปลอดภัยของ Binding updates

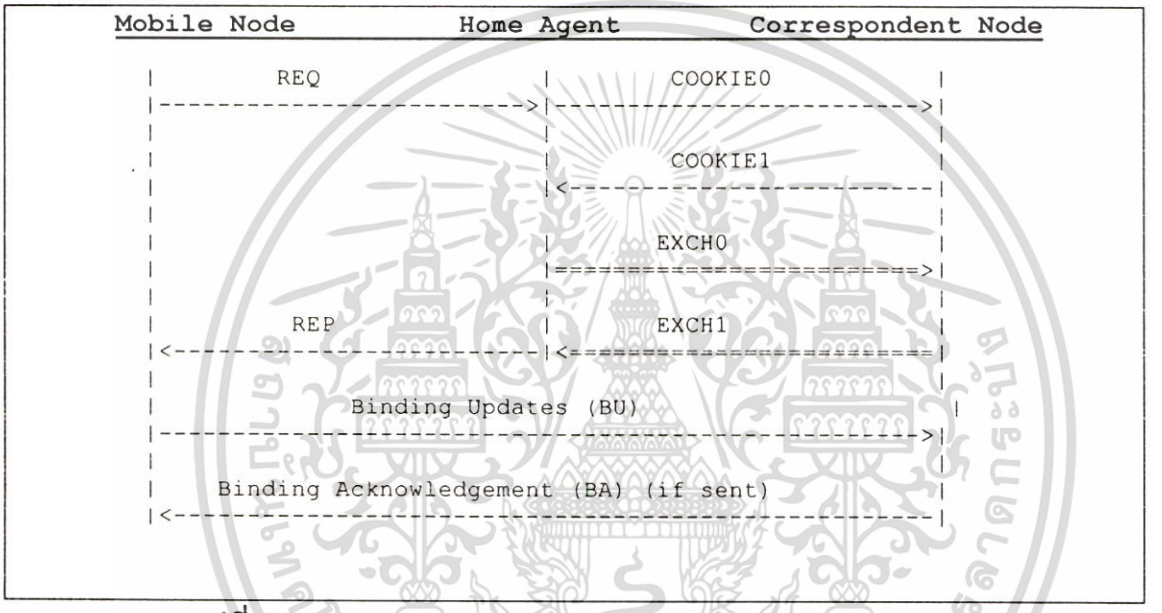
3.4.1 Extend Certificate-based Binding Updates Protocol (ECBU) [7,8]

ในการทำงานของการทำ Handoff Protocol เริ่มแรกสุด ยังไม่ได้มีการเข้ารหัสเพื่อความปลอดภัยใด ๆ ทั้งสิ้นทำให้การส่ง Binding Updates มีโอกาสที่จะถูกโจมตีตามช่องโหว่ที่ได้กล่าวมา นักวิจัยจึงได้เสนอวิธีการเพิ่มความปลอดภัยให้กับ Mobile IPv6 Binding Updates โดยวิธี ECBU

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

สำหรับวิธีนี้ Mobile Node จะส่ง REQ ไปยัง Home Agent เพื่อร้องขอ secret key ที่ใช้สำหรับการทำ Binding Updates เมื่อ Home Agent ได้รับ REQ ก็จะส่ง COOKIE0 ไปให้ Correspondent Node จากนั้น Correspondent Node สร้าง Nonce และ COOKIE1 ตอบกลับมาให้ Home Agent การส่ง COOKIE เพื่อป้องกัน Attacker ที่สามารถปลอม IP ส่ง REQ มาเพื่อ Distributed Denial of Services (DDoS) เมื่อ Home Agent ได้รับ COOKIE1 จาก Correspondent Node แล้ว Home Agent ก็ส่ง EXCH0 ไปให้ Correspondent Node และ Correspondent Node ก็จะตอบ EXCH1 กลับมาให้ Home Agent แล้ว Home Agent ก็ส่งต่อไปยัง Mobile Node



รูปที่ 3.5 Extend Certificate-based Binding Updates Protocol

REQ = {Src=HoA, Des=HA, $e(k_{HA},HoA,CoA,CN,N_0)$ }

COOKIE0 = {Src=HoA, Des=CN, C_0}

COOKIE1 = {Src=CN, Des=HoA, C_0, C_1, N_1}

EXCH0 = {Src=HoA, Des=CN, C_0, C_1, N_1, N_2, g^x, TS, SIG_H, $Cert_H$}

EXCH1 = {Src=CN, Des=HoA, C_0, C_1, g^y, SIG_{CN}, $Cert_{CN}$}

REP = {Src =CN, Des=CoA, $e(k_{HA},N_0, k_{BU}, k_{HA\text{-}next})$ }

การทำงานของ $e(k_{HA},N_0, k_{BU}, k_{HA\text{-}next})$ จะใช้ k_{HA} เป็นกุญแจในการเข้ารหัส N_0, k_{BU}, $k_{HA\text{-}next}$

prf(k,m) คือ keyed pseudo random function เป็นการนำ secket k และ message m มาทำ hashing ตามหลักการเข้ารหัส เพื่อสร้างเป็น authentication message

$e(k_{HA},m)$ คือ การเข้ารหัส message m ด้วย secret key k_{HA}

k_{HA} คือ session key สำหรับ IPSec ที่ได้กำหนดกันไว้ก่อนล่วงหน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

61240

N_0 มีเพื่อไว้ตอบ Mobile Node กลับมาว่าข้อมูลที่ส่งมาจาก Home Agent นั้นเป็นของ Home Agent จริง ๆ

k_{BU} มีไว้เพื่อใช้เข้ารหัส เมื่อทำ Binding update

$k_{BU} = prf((g^x)^y \mid N_1 \mid N_2)$

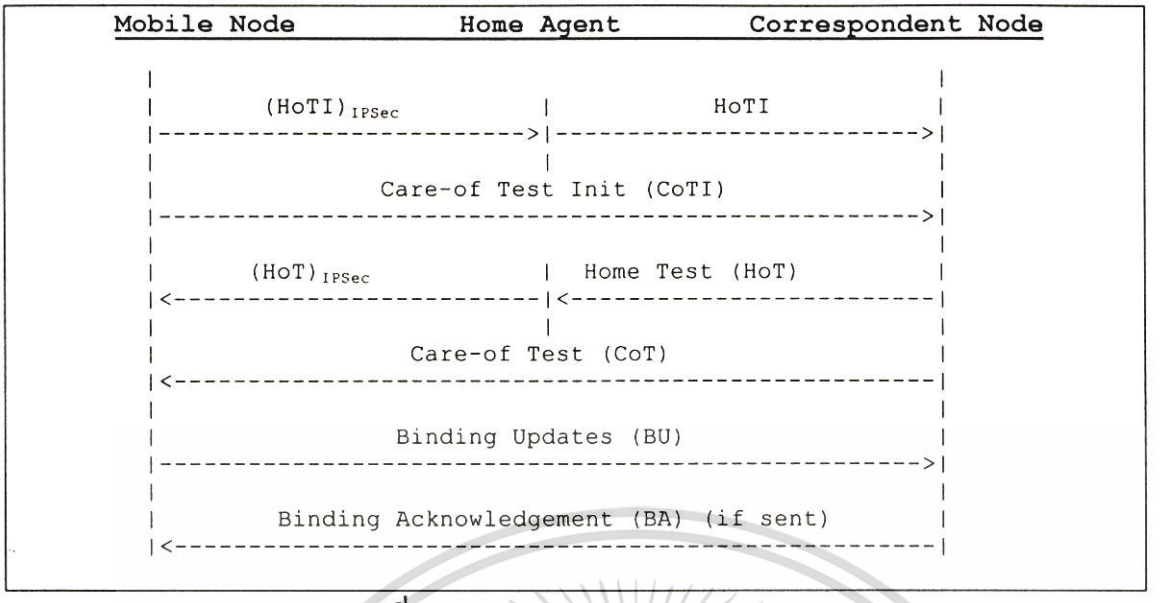
$k_{HA\text{-}next}$ มีไว้เพื่อให้ Mobile Node ติดต่อกับ Home Agent ใน session ต่อไป สามารถคำนวนได้จาก $k_{HA\text{-}next} = prf((g^x)^y \mid N_0 \mid N_1)$

Secret key ที่ใช้ใน ECBU นั้น สร้างจากวิธีการของ Diffie-Hellman [17] เนื่องจากวิธีการของ Diffie-Hellman มีปัญหาเกี่ยวกับ Man-in-the middle attack ดังนั้นใน EXCH0,1 จึงส่ง Certificate แนบไปด้วย Certificated-based ที่แนบไปนั้นสร้างมาจาก public key ของ Mobile Node ที่ส่งไปให้ Trust certificate server เพื่อออก Certificated มาให้ โดย Correspondent Node จะใช้ public key ของ Trust certificate server ในการตรวจสอบ public key ของ Mobile Node ซึ่งการใช้ certificated ในลักษณะนี้ เป็นการเข้ารหัสแบบ public key แบบ Rivest Shamir Adleman (RSA) [18] ทำให้ใช้เวลาในการคำนวนที่นานกว่า การเข้ารหัสที่เป็นแบบ secret key และยังใช้กุญแจที่ยาวกว่าในความปลอดภัยที่เท่ากันอีกด้วย

3.4.2 Return Routability [1,5]

Return Routability (RR) เป็นวิธีการพื้นฐานที่กลุ่มคณะทำงาน Mobile IPv6 นำเสนอ และใช้ในการตรวจสอบการทำ Handoff ว่าเป็นข้อมูลที่ส่งมาจากโหนดนั้นจริง ๆ ซึ่งวิธีนี้ Binding Updates ที่ส่งให้ Correspondent Node นั้น ไม่จำเป็นต้องมีการกำหนด Security Associations (SA) ระหว่าง Mobile Node กับ Correspondent Node ในการเชื่อมต่อระหว่าง Mobile Node และ Home Agent ทาง Mobile IPv6 working group แนะนำให้ใช้ IPSec [5] ในการควบคุม แต่ระหว่าง Correspondent Node กับ Mobile Node หรือ Home Agent นั้น เป็นการส่งข้อมูลแบบไม่ได้มีการป้องกัน ซึ่งถ้าผู้ไม่หวังดี แอบขโมยข้อมูลระหว่างการเชื่อมต่อของ Correspondent Node กับ Mobile Node และ Correspondent Node กับ Home Agent ผู้ไม่หวังดีก็มีโอกาสสามารถปลอม Binding Updates ได้สำเร็จ ข้อได้เปรียบของวิธีนี้คือ ผู้ไม่หวังดีที่ อยู่บนเส้นทางการติดต่อสื่อสาร ระหว่าง Home Agentกับ Correspondent Node และ Mobile Node กับ Correspondent Node เพียงเส้นทางใดทางหนึ่ง จะไม่สามารถปลอม Binding Updates ได้ การป้องกัน Binding Updates วิธีนี้จะใช้ Binding Management Key (K_{bm}) ที่สร้างมาจากกระบวนการ RR ซึ่งมีการทำงานดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.6 Return Routability protocol

Home Test Init (HoTI) และ Care of Test Init (CoTI) message ถูกส่งออกมาพร้อม ๆ กัน เพื่อใช้ในการสร้าง K_{bm} ดังนี้

Home Test Init

Mobile Node ส่ง HoTI ซึ่งมี Home address และ Home Init Cookie ไปให้ Correspondent Node ผ่านทาง Home Agent เพื่อที่รับ Home keygen token ซึ่งข้อมูลของ HoTI มีดังนี้

IPv6 header

Source Address = Mobile Node CoA

Destination Address = Correspondent

ESP header in tunnel mode

IPv6 header

Source Address = Home Address

Destination Address = Correspondent

Mobility header

Home Test Init

+ home init cookie

รูปที่ 3.7 Home Test Init format

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Care-of Test Init

Mobile Node ส่ง CoTI ซึ่งมี Care-of address และ Care-of init Cookie ไปให้ Correspondent Node โดยไม่ผ่านทาง Home Agent เพื่อที่รับ Care of keygen token ตอบกลับมา ข้อมูลของ CoTI มีดังนี้

IPv6 header

Source Address = Mobile Node CoA

Destination Address = Correspondent

Mobility header

Care-of Test Init

+ care-of init cookie

รูปที่ 3.8 Care-of Test Init format

Home Test

Home Test (HoT) ถูกส่งออกมาจาก Correspondent Node หลังจากที่ได้รับ HoTI ที่ส่งมาจาก Mobile Node โดย HoT จะส่งผ่านทาง Home Agent แล้ว Home Agent ก็จะส่งต่อกลับไปให้ Mobile Node ซึ่งหมายความว่า Mobile Node ทำได้ลงทะเบียน Care-of address ใหม่ กับ Home Agent เสร็จเรียบร้อย ก่อนที่จะมีการทำ Return Routability ข้อมูลของ HoT มีดังนี้

IPv6 header

Source Address = Correspondent

Destination Address = Home address

Mobility header

Home Test

+ home init cookie

+ home keygen token

+ home nonce index

รูปที่ 3.9 Home Test format

home init cookie มีไว้สำหรับตรวจสอบ HoT ที่ส่งไปให้นั้น สอดคล้องกับ HoTI ที่ส่งมาก่อน เพื่อให้แน่ใจว่า ผู้ที่ไม่ได้รับ HoTI นั้นไม่สามารถปลอมแปลง HoT ได้ เมื่อ Correspondent Node ส่ง HoT ไปให้ Mobile Node แล้ว Correspondent Node ก็จะสร้าง home keygen token โดยเลือกมาเฉพาะ 64 bits แรก ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Home keygen token := First(64, HMAC_SHA1 (K_{cn}, (home address | nonce | 0))) (3.1)

HMAC_SHA1 หมายถึง การทำ Message Digest ด้วย SHA1 Algorithm โดยใช้ (home address | nonce | 0) เป็นข้อมูล K_{cn} เป็นกุญแจที่ใช้ในการทำ Message Digest, nonce สร้างจาก Random number generator ที่มีคุณสมบัติการสุ่มตัวเลขที่ดี และ เลข 0 ที่อยู่ท้ายสุด ใช้บอกว่า keygen token นี้ สร้างเป็น home keygen token ซึ่ง home keygen token มีไว้สำหรับสร้าง K_{bm} เพื่อใช้ในการทำ Binding Updates

Home nonce index มีไว้สำหรับเก็บที่อยู่ของ nonce ที่ใช้สร้าง home keygen token ที่สร้างขึ้นมาให้ขณะนั้น

Care-of Test

Care-of Test (CoT) ถูกส่งออกมาจาก Correspondent Node หลังจากที่ได้รับ CoTI ที่ส่งมาจาก Mobile Node โดย CoT จะไม่ส่งผ่านทาง Home Agent ข้อมูลของ CoT มีดังนี้

iPv6 header
- Source Address = Correspondent
- Destination Address = Care-of address

Mobility header
- Care-of Test
  - + care-of init cookie
  - + care-of keygen token
  - + care-of nonce index

รูปที่ 3.10 Care-of Test format

care-of init cookie มีไว้สำหรับตรวจสอบ CoT ที่ส่งไปให้นั้น สอดคล้องกับ CoTI ที่ส่งมาก่อน เพื่อให้แน่ใจว่า ผู้ที่ไม่ได้รับ CoTI นั้นไม่สามารถปลอมแปลง CoT ได้ เมื่อ Correspondent Node ส่ง CoT ไปให้ Mobile Node แล้ว Correspondent Node ก็จะสร้าง care-of keygen token โดยเลือกมาเฉพาะ 64 bits แรก ดังนี้

Care-of keygen token := First(64, HMAC_SHA1 (K_{cn}, (care-of address | nonce | 1))) (3.2)

HMAC_SHA1 หมายถึง การทำ Message Digest ด้วย SHA1 Algorithm โดยใช้ (care-of address | nonce | 1) เป็นข้อมูล K_{cn} เป็นกุญแจที่ใช้ในการทำ Message Digest, nonce สร้างจาก Random number generator ที่มีคุณสมบัติการสุ่มตัวเลขที่ดี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

และ เลข 1 ที่อยู่ท้ายสุด ใช้บอกว่า keygen token นี้ สร้างเป็น care-of keygen token ซึ่ง care-of keygen token มีไว้สำหรับสร้าง K_{bm} เพื่อใช้ในการทำ Binding Updates

Care-of nonce index มีไว้สำหรับเก็บที่อยู่ของ nonce ที่ใช้สร้าง home keygen token ที่สร้างขึ้นมาให้ขณะนั้น

เมื่อ Mobile Node ได้รับ HoT และ CoT หมายความว่ากระบวนการทำ RR ได้เสร็จสิ้นสมบูรณ์ หลังจากนั้น ทั้ง Mobile Node และ Correspondent Node สามารถสร้าง K_{bm} ได้ดังนี้

$$K_{bm} = \text{SHA1 (home keygen token | care-of keygen token)} \quad (3.3)$$

Binding Updates

หลังจากที่ Mobile Node สร้าง K_{bm} เสร็จเรียบร้อยแล้ว Mobile Node สามารถสร้าง Binding Updates โดยใช้ K_{bm} เป็นกุญแจในการเข้ารหัสเพื่อเพิ่มความปลอดภัย ซึ่ง Correspondent Node ก็สามารถตรวจสอบ Binding Updates ด้วย K_{bm} ได้เช่นกัน ข้อมูลของ Binding Updates มีดังนี้

IPv6 header
- Source Address = Care-of address
- Destination Address = Correspondent

Destination Options header = Home Address

Mobility header
- Binding Update
  - + sequence number
  - + home nonce index
  - + care-of nonce index
  - + First(96, BU, HMAC_SHA1(K_{bm}, (care-of address | correspondent | BU)))

รูปที่ 3.11 Binding Updates to Correspondent Node format

Binding Updates เก็บค่า nonce index ไว้เพื่อให้ Correspondent Node สามารถใช้ nonce index ในการดึงค่า nonce ที่เก็บไว้ เพื่อคำนวน K_{bm} และตรวจสอบ Binding Updates ใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Binding Acknowledgement

ใช้สำหรับตอบกลับ Binding Updates เพื่อให้ Mobile Node รู้ว่า Correspondent Node ทำ Routing Optimization เสร็จเรียบร้อยแล้ว ข้อมูลของ Binding Updates มีดังนี้

IPv6 header

Source Address = Correspondent

Destination Address = Care-of address

Mobility header

Binding Acknowledgement

+ sequence number

+ First(96, BU, HMAC_SHA1(K_{bm}, (care-of address | correspondent | BA)))

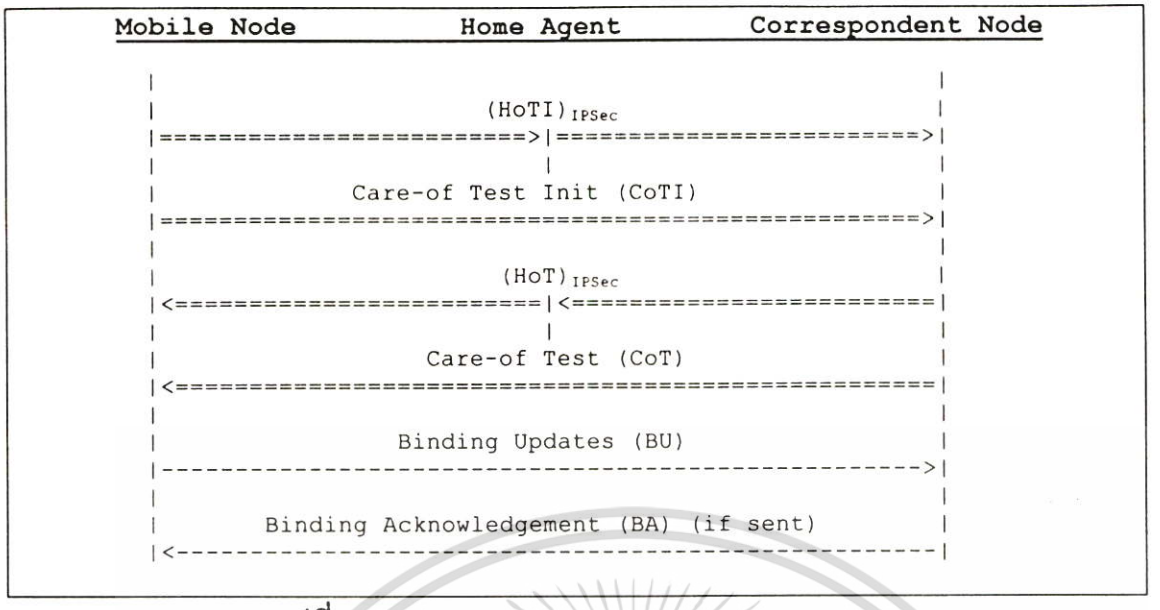
รูปที่ 3.12 Binding Acknowledge to Mobile Node format

ปัจจุบัน การทำ Route Optimization ใน Implement version [16] ของ Mobile IP ไม่ได้มีการใช้ เข้ารหัสใด ๆ ซึ่งอาจเกิดปัญหาที่กล่าวมาข้างต้น กลุ่ม Mobile IP working group ก็ได้เสนอให้ใช้ วิธี Return Routability [1] เพื่อพิสูจน์ว่าผู้ส่งอยู่ที่ตำแหน่งนั้นจริง ๆ แต่โอกาสเกิดปัญหา ในข้อ 3-6 ก็ยังมีอยู่ เพราะ วิธีการของ Return Routability นั้น มีการเข้ารหัสเพียงเส้นทางการติดต่อระหว่าง Mobile Node กับ Home Agent เท่านั้น

3.4.3 Return Routability with IPSec [6]

จากจุดอ่อนของวิธีการ Return Routability ทำให้มีการนำเสนอการใช้ IPSec [5] เพิ่มเติมในเส้นทางระหว่าง Home Agent กับ Correspondent Node [6] เพื่อเพิ่มความปลอดภัยให้กับข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.13 Return Routability with IPSec protocol

วิธีการก็เหมือนกับการทำ Return Routability ที่ได้กล่าวมาแล้ว แต่มีการใช้ IPSec ป้องกันข้อมูลที่ส่งระหว่าง Home Agent กับ Correspondent Node เพิ่มขึ้น หลังจากใช้ IPSec เพิ่มความปลอดภัยแล้ว แต่ก็ยังมีปัญหาในเรื่องเวลาในการทำ Handoff ที่ใช้สำหรับ Real-Time Application ที่มีความต้องการของ Latency ที่มีค่าต่ำ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4
ระบบความปลอดภัยของโมไบล์ไอพีวีซิกส์ไบด์ดิ้งอัพเดทโดยวิธีเคอร์บิรอส

4.1 บทนำ

ในปัจจุบัน การพัฒนา Mobile IPv6 Binding Updates ยังไม่เสร็จสมบูรณ์ และต้องการการพัฒนาปรับปรุงมากขึ้น ดังจะเห็นได้จากงานวิจัย ที่ออกมาสนับสนุนระบบนี้ เนื่องจาก Mobile IPv6 เป็นโปรโตคอลที่ค่อนข้างใหม่ วิธีการต่าง ๆ ที่นำเสนอนั้น ส่วนมากจะใช้การเข้ารหัสแบบ Diffie-Hellman [17] และ Public key แบบเก่า อย่างเช่น RSA [18] ในการเพิ่มความปลอดภัยให้กับ Binding Update สำหรับวิธีการของ Diffie-Hellman นั้นมีข้อดีคือ สามารถสร้าง Key ที่ใช้ในการเข้ารหัสได้โดยที่ไม่จำเป็นต้อง แจกจ่าย key กันก่อนล่วงหน้า แต่วิธีนี้ ไม่สามารถ Sign ข้อความที่ต้องการส่งได้ ทำให้ไม่สามารถตรวจสอบผู้ส่งข้อมูลได้จริง เมื่อเปลี่ยนมาใช้ วิธีแบบ Public Key Cryptography (PKC) จำพวก RSA ทำให้สามารถ Sign ข้อความที่ต้องการส่งเพื่อยืนยันตัวผู้ส่งได้ แต่ก็มีข้อเสียคือ ในระบบของ Mobile จะมีข้อจำกัดหลาย ๆ ด้าน ไม่ว่าจะเป็นแบนด์วิธ, พลังงาน การใช้ PKC แบบ RSA นั้นจะต้องมีการ Obtain certificated [7] และ ใช้ Key length ที่มีขนาดมากกว่า หรือเท่ากับ 1024 bit ขึ้นไป จึงจะมีความในระดับที่ยอมรับได้ ซึ่งการส่งข้อมูลที่มีปริมาณมากในระบบ Mobile IPv6 นั้นอาจจะไม่เหมาะสม ซึ่งในอนาคตอุปกรณ์ที่สามารถเคลื่อนย้ายไปยังเครือข่ายต่าง ๆ จะมีอยู่มากมาย และมีแนวโน้มที่จะใช้งานเกี่ยวกับด้าน voice over iP และ video conference มากขึ้นตามมาตรฐานอินเทอร์เน็ต อย่างไรก็ตาม กระบวนการเคลื่อนย้ายของอุปกรณ์ IP ที่ย้ายไปยังเครือข่ายอื่น ๆ ทำงานล่าช้า และยังไม่เพียงพอต่อการทำงานสำหรับ Real-Time Application

4.2 การเข้ารหัส

4.2.1 Symmetric cryptography

การเข้ารหัสแบบ Symmetric เป็นการเข้ารหัสแบบใช้ key เดียว นั่นคือ การเข้ารหัสกับการถอดรหัสใช้ key เดียวกัน ทำให้ง่ายแก่การใช้งานและการสร้างระบบ แต่ปัญหาที่เกิดขึ้นคือ หากใช้การเข้ารหัสแบบนี้ ในการติดต่อกันแต่ละคน ก็จะมีปัญหาในการจัดเก็บ key ที่ใช้ติดต่อ เช่น ติดต่อกัน n user ก็ต้องใช้ key ทั้งหมด Cn,2 key และปัญหาใหญ่อีกอย่างก็คือ จะรับส่ง key กันอย่างไรให้ปลอดภัย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.2.2 Public key cryptography

ปัญหานี้ แก้ไขโดยการเสนอการเข้ารหัสแบบไม่สมมาตร (Asymmetric cryptography) โดยใช้ กุญแจคู่ ซึ่งมีกุญแจที่ใช้ในการเข้ารหัสและถอดรหัสคนละอันกัน หรือที่รู้จักกันในชื่อที่ว่า Public Key Cryptography การเข้ารหัสด้วยวิธีนี้ สามารถแก้ปัญหาต่าง ๆ ที่เกิดขึ้นจาก การเข้ารหัสแบบกุญแจเดียวได้ เพราะ private key ที่ใช้ในการถอดรหัส หรือการ sign ไม่จำเป็นต้องส่งไปยังเครือข่าย จึงสามารถมั่นใจได้ว่า ไม่ถูกใครดักจับหรือแก้ไขเปลี่ยนแปลงได้

แต่ก็ยังมีปัญหาเกิดขึ้นจาก การใช้ public key นั่นก็คือ public key ที่ใช้ในการเข้ารหัส อาจจะถูกแก้ไขได้ จึงมีการเสนอให้ใช้ certificated เพื่อตรวจสอบว่า public key ที่ใช้นั้นเป็นของผู้ใช้คนนั้นจริง ๆ และ certificated สร้างจาก certificated authority ซึ่งสืบทอดกันมาเป็นลำดับชั้น ทำให้มั่นใจว่า public key ที่ใช้เป็นของจริง ไม่ถูกแก้ไขใด ๆ ทั้งสิ้น ดูเหมือนว่า PKC ที่ใช้อยู่ มีความปลอดภัย เพราะว่า private key ก็ไม่ต้องส่ง public key ก็สามารถตรวจสอบได้ว่า เป็นของจริง ไม่ได้ถูกแก้ไขใด ๆ แต่ปัญหาใหญ่ของ PKC คือ ต้องมีการแลกเปลี่ยน message และต้องใช้เวลาในการประมวลผลมากกว่าแบบ Symmetric cryptography

4.3 Kerberos algorithm

Kerberos Distribution Center (KDC) [4] จึงถูกพัฒนา ขึ้นมาเพื่อแก้ไขปัญหาเกี่ยวกับการเข้ารหัสจากวิธีที่ได้กล่าวมาแล้ว โดยใช้วิธีการสร้าง session key ขึ้นมา เมื่อมีการร้องขอข้อมูลจากผู้ใช้ และส่ง session key ไปให้ผู้ใช้ โดยใช้กุญแจที่ได้มีการตกลงกับผู้ใช้ไว้ เป็นกุญแจในการเข้ารหัส session key

วิธีการแก้ปัญหาต่าง ๆ เกี่ยวกับ Binding Updates ที่ถูกนำเสนอขึ้นมานั้น เหมาะสมกับการใช้งานในกรณีทั่ว ๆ ไป แต่หากมองในอีกสภาพแวดล้อมหนึ่ง ซึ่งสามารถกำหนด pre-shared key ให้กับ node ต่าง ๆ ได้บางส่วน แต่มีข้อจำกัดในด้านแบนด์วิธ และความสามารถในการคำนวน ซึ่งใน Mobile IPv6 มี Home Agent ที่เป็นส่วนสำคัญในการทำงาน และ Mobile Node จำเป็นที่จะต้องติดต่อกับ Home Agent เสมอเมื่อมีการเปลี่ยนเครือข่าย จากจุดนี้ทำให้การประยุกต์ใช้ KDC เข้ากับ Home Agent นั้นเป็นไปได้ โดยที่ Home Agent จะสร้างกุญแจและรับส่งกุญแจกันล่วงหน้าก่อนกับ Node ที่จะติดต่อสื่อสารกัน ก่อนที่จะมีการย้ายเครือข่ายกันจริง ๆ และโดยส่วนมาก Home Agent จะเป็นอุปกรณ์ที่อยู่ใน fix network และ มีความสามารถในการประมวลผลได้สูงอยู่แล้ว การประยุกต์ใช้ระบบ Kerberos จึงเป็นวิธีการที่เหมาะสม ทำให้

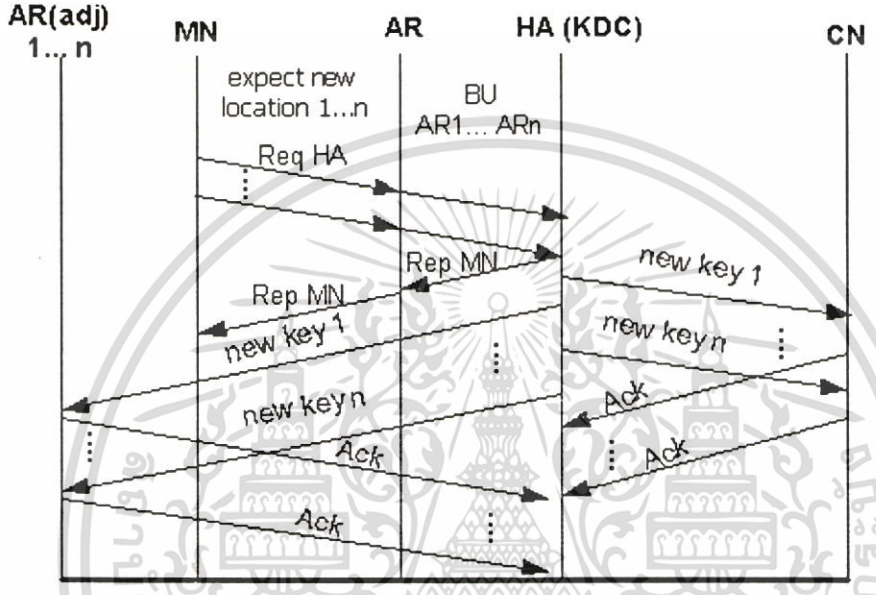
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Handoff Latency มีค่าน้อยลง และยังคงไว้ซึ่งความปลอดภัยของข้อมูล Binding update และสามารถทำงานเข้ากันได้กับโพรโตคอลมาตรฐานที่ได้กำหนดไว้แล้วอีกด้วย

4.4 ความปลอดภัยของโมไบล์ไอพีวีซิกส์ไบด์ดิ้งอัพเดทโดยใช้ Kerberos

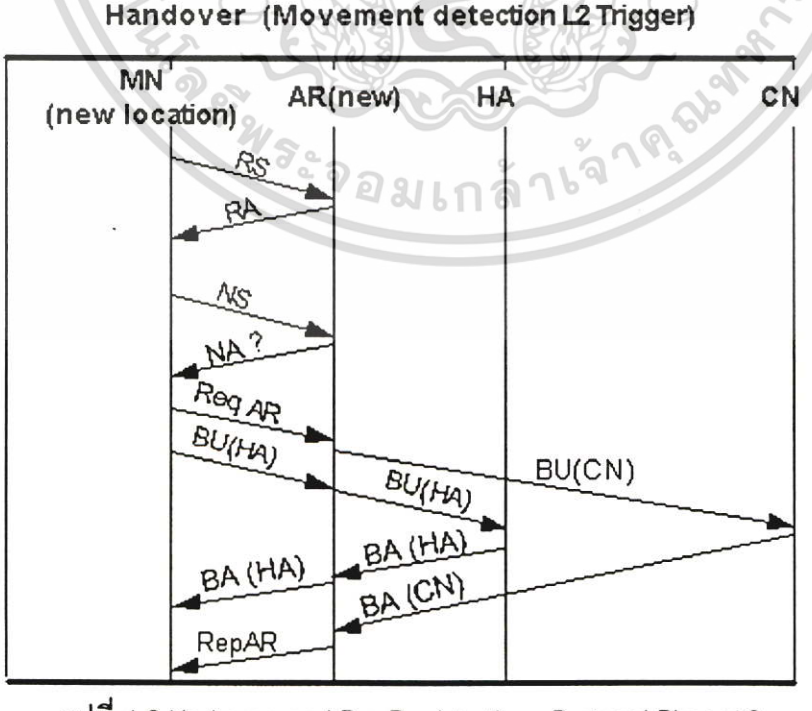
4.4.1 Framework

Phase#1



รูปที่ 4.1 Kerberos and Pre-Registrations Protocol Phase#1

Phase #2



รูปที่ 4.2 Kerberos and Pre-Registrations Protocol Phase#2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$BU = \{ Src=CoA, Des=HA, HoA, Seq\#, LT_{BU}, MAC_{BU}\}$

$BA = \{ Src=CN, Des=CoA, HoA, Seq\#, LT_{BU}, MAC_{BU}\}$

$MAC_{BU} = prf(K_{MN}, HoA|CoA|Seq\#, LTbu)$

$(m)_k$ คือ การเข้ารหัส message m ด้วย secret key k

prf(k,m) คือ key pseudo random function เป็นการใช้ secret key k และ message m สร้าง random output โดยการทำ Hashing เพื่อใช้ในการทำ Authentication

4.4.2 การทำงานของ Kerberos and Pre-Registration

จะแบ่งออกเป็น 2 phase ด้วยกันคือ

Phase #1

1. ก่อนที่ Mobile Node จะย้ายเครือข่าย Mobile Node จะต้องร้องขอ session key จาก Home Agent โดย Mobile Node ส่ง ReqHA ไปให้ Home Agent เพื่อร้องขอ session key สำหรับติดต่อกับ Correspondent Node โดยที่ session key ที่ส่งไปร้องขอนั้น จะมีข้อมูลของ Adjacent Access Router ที่ Mobile Node คาดหวังว่าจะเคลื่อนย้ายไป การส่ง ReqHA จะใช้ Authentication Header ของ IPSec เป็นการพิสูจน์ตัวตนที่แท้จริง เพื่อป้องกันการปลอมคำสั่ง ใน message นี้จะกำหนด Type ของ Destination options header เป็น 13 เพื่อบอกให้ Home Agent รู้ว่า Mobile Node ต้องการ session key ที่จะติดต่อกับ Correspondent Node
2. เมื่อ Home Agent ได้รับ ReqHA แล้ว Home Agent ก็จะตอบ RepMN ไปให้ Mobile Node เพื่อบอกให้ Mobile Node รู้ว่า Home Agent ได้รับ ReqHA มาจาก Mobile Node แล้ว การส่ง ReqHA จะใช้ Authentication Header ของ IPSec เป็นการพิสูจน์ตัวตนที่แท้จริง เพื่อป้องกันการปลอมคำสั่ง และใน message นี้จะกำหนด Type ของ Destination options header เป็น 11 เพื่อบอกให้ Mobile Node รู้ว่า Home Agent รับสร้างการร้องขอ session key ของ Mobile Node แล้ว
3. จากนั้น Home Agent ก็จะสร้าง session key ขึ้นมา แล้วส่ง session key ไปให้ Adjacent Access Router และ Correspondent Node ตามที่ Mobile Node ร้องขอมาทั้งหมด โดยเข้ารหัส session key ที่สร้างขึ้นมาด้วย IPSec ตาม Security Association (SA) ที่กำหนดไว้ของ Adjacent Access Router และ Correspondent Node ตามลำดับ ใน message นี้จะกำหนด Type ของ Destination option header เป็น 12 เพื่อบอกให้ Adjacent Access Router และ Correspondent Node เก็บ session key ที่ Home

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Agent สร้างขึ้นมาเพื่อใช้ติดต่อกับ Mobile Node หลังจากที่ Mobile Node มีการย้ายเครือข่าย

4. เมื่อ Adjacent Access Router และ Correspondent Node ได้รับ Session Key ที่ Home Agent สร้างมาให้ Adjacent Access Router และ Correspondent Node ก็จะตอบ Acknowledge กลับไปหา Home Agent ซึ่ง Adjacent Access Router และ Correspondent Node จะต้องเก็บ session key ไว้กับคู่กับ Adj Access Router ที่คิดว่าจะย้ายเครือข่ายไป เพื่อที่จะรู้ได้ว่า session key นี้เป็นของ Mobile Node ไหน การส่งตอบ Acknowledge จะใช้ Authentication Header ของ IPSec เป็นการพิสูจน์ตัวตนที่แท้จริง เพื่อป้องกันการปลอมคำสั่ง และใน message นี้จะกำหนด Type ของ Destination options header เป็น 11 เพื่อบอกให้ Home Agent รู้ว่า Adjacent Access Router และ Correspondent Node ได้รับ Session Key ที่ Home Agent สร้างมาให้แล้ว

Phase #2

1. จากนั้น เมื่อ Mobile Node ย้ายเครือข่าย Mobile Node ก็ค้นหา Access Router ใหม่ที่จะใช้งาน และ กำหนดค่า Care of Address ตามกระบวนการมาตรฐานของ Mobile IPv6
2. หลังจากที่ Mobile Node ได้รับการเชื่อมต่อกับเครือข่ายใหม่ Mobile Node ส่ง Binding Update ไปให้ Home Agent พร้อมกับส่ง ReqAR ไปยัง Access Router เพื่อให้ Access Router ส่ง Binding Update ที่เข้ารหัสจาก key ที่ Home Agent ได้สร้างขึ้นมา ไปให้ Correspondent Node การส่ง ReqAR จะใช้ Authentication Header ของ IPSec เป็นการพิสูจน์ตัวตนที่แท้จริง เพื่อป้องกันการปลอมคำสั่ง และใน message นี้จะกำหนด Type ของ Destination options header เป็น 14 เพื่อบอกให้ Access Router ส่ง Binding Update โดยเข้ารหัสด้วย Session Key ที่ Home Agent สร้างมาให้แล้วไปให้ Correspondent Node
3. Access Router ส่ง Binding Update ไปยัง Correspondent Node ใน message นี้จะกำหนด Type ของ Destination options header เป็น 15 เพื่อบอกให้ Correspondent Node รู้ว่าข้อมูลที่แนบมาเป็น Home address และ Care of Address ของ Mobile Node ตามลำดับ
4. จากนั้น Correspondent Node รับข้อมูล Binding Update ที่ Access Router ส่งมา Correspondent Node ถอดรหัส session key ด้วย secret key ของ Correspondent Node ที่ Home Agent เคยส่งมาให้ โดยตรวจสอบจาก HoA และ CoA ที่ส่งมาด้วย ว่าตรงกับ session key ที่มีอยู่อันไหน แล้วส่ง Binding Acknowledgement กลับไปให้

เอกสารนี้สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Mobile Node ผ่านทาง Access Router ใน message นี้จะกำหนด Type ของ Destination options header เป็น 15 เพื่อบอกให้ Access Router รู้ว่าข้อมูลที่แนบมาเป็น Home address และ Care of Address ของ Mobile Node ตามลำดับ

5. Access Router ส่ง Binding Acknowledge ไปให้ Mobile Node ตามมาตรฐาน Mobile IPv6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5
การวิเคราะห์ประสิทธิภาพและโมเดล

5.1 บทนำ

ในบทนี้จะกล่าวถึงการวิเคราะห์เวลาที่ใช้ในการทำ Handoff โดยแยกย่อยละเอียดว่า ในการทำ Handoff นั้นประกอบไปด้วยเวลาอะไรบ้าง เช่น การตรวจสอบการซ้ำซ้อนของ IPv6 address, การ registration Binding Updates และ ตัวแปรหลัก ๆ ที่ผลต่อเวลา และมีการ Model คิวในระบบ เพื่อที่จะนำไปทำเป็น Simulation

5.2 Handoff performance

จากที่ได้กล่าวมาแล้ว เกี่ยวกับการทำงานของ Mobile IPv6 ที่อ้างอิงพื้นฐานฟังก์ชันการทำงานของ IPv6 ซึ่งวิเคราะห์เกี่ยวกับ delay time ในการทำงานของกระบวนการต่าง ๆ มีดังนี้

- Movement detection time (t_d) เป็นเวลาที่ Mobile Node ใช้ในการค้นหาและเชื่อมต่อการสื่อสารใหม่เมื่อ Mobile Node ย้ายเครือข่ายจากจุดเชื่อมต่อเก่า ไปยังจุดเชื่อมต่อใหม่ ตัวอย่างเช่นการค้นหา Link ใหม่ บน Link Router
- IP Care-of address configuration time (t_a) เป็นเวลาที่ใช้ในการกำหนด IPv6 address ใหม่ เวลานี้รวมถึงกระบวนการทำการตรวจสอบ address ที่ซ้ำกันด้วย
- Binding registration time (t_r) เป็นเวลาที่ Mobile Node register Care-of address ที่สร้างขึ้นมาใหม่ กับ Home Agent โดยการส่ง Binding update เพื่อบอกที่อยู่ใหม่ให้กับ Home Agent และ รอการตอบ Binding Acknowledge กลับของ Home Agent มายัง Mobile Node
- Route optimization time (t_o) เป็นเวลาหลังจากที่ Mobile Node register Care-of address ที่สร้างขึ้นมาใหม่ กับ Correspondent Node ซึ่งกระบวนการนี้รวมถึงกระบวนการทำ Return Routability ซึ่งจะต้องเกิดขึ้นก่อนที่ Mobile node จะส่ง Binding update ไปยัง Correspondent Node

$$T_{HANDOFF} = T_d + T_a + T_r + T_o \quad (5.1)$$

5.2.1 Move Detection Time

Movement detection time (t_d) แบ่งออก เป็น latency 2 ช่วงเวลาด้วยกันคือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Link switching delay (T_{l2}) คือเวลาที่ Mobile Node ใช้ในการตรวจสอบ การย้ายเครือข่ายไปใช้Base station หรือ Access point ใหม่ ในระดับ Layer 2
- Link local IPv6 address configuration delay (T_{ll}) คือเวลาที่ Mobile Node ใช้ในการ กำหนด Link local IPv6 address เมื่อได้รับ neighbour advertisement จาก solicited nodes multicast address

Movement detection time (t_d) สามารถสรุปได้เป็น

$$t_d = T_{l2} + T_{ll} \quad (5.2)$$

5.2.2 IPv6 Care-of Address Configuration Time

Care-of address configuration time (t_a) เป็นที่ใช้ในการรับ Router Advertisement การสร้าง Care-of address ขึ้นมาใหม่ รวมไปถึงเวลาการตรวจสอบความซ้ำซ้อนของ Care-of address ที่ได้สร้างขึ้นมาใหม่อีกด้วย สามารถสรุปได้เป็น

$$t_a = T_{RtAdv} + T_{AddrConfig} + T_{DAD} \quad (5.3)$$

$T_{AddrConfig}$ เป็นเวลาที่ Mobile Node ใช้ในการ กำหนด IPv6 address ซึ่งแบ่งแยกได้เป็น 2 วิธีคือ ใช้เป็น stateless auto configuration หรือ stateful auto configuration ในที่นี้จะมองไปถึงวิธี stateless auto configuration โดย Mobile Node นำ Router Prefix ที่ได้จาก Router Advertisement มารวมกับ MAC address ที่เข้ารหัสแบบ EUI-64 เพื่อสร้างเป็น Care-of address IPv6 ใหม่ ที่จะใช้ในการเชื่อมต่อกับเครือข่ายใหม่ต่อไป ซึ่งเวลาที่ใช้ใน กระบวนการทำ stateless auto configuration นั้น ขึ้นอยู่กับความเร็วของ หน่วยประมวลผลกลาง ของ Mobile Node และ เมื่อมาเทียบกับ เวลารวมของ t_a แล้ว ถือว่า มีผลต่อเวลาโดยรวมน้อยมาก

T_{DAD} เป็นเวลาที่ใช้ในการตรวจสอบความซ้ำซ้อนของ Tentative IPv6 address ที่ Mobile Node สร้างขึ้นมาใหม่โดยกระบวนการ stateless auto configuration ซึ่งเวลาในการทำ DAD คือ เวลาที่ Mobile Node ส่ง Neighbor Solicitation message ไปยัง node-solicited multicast address และ เวลาที่รอ node อื่น ๆ ส่ง Neighbor Acknowledgement message (NA) กลับมา โดยทั่วไปแล้ว เวลาที่ Mobile Node รอ Node อื่น ๆ ส่ง NA ตอบกลับมา จะใช้เวลาประมาณ 500 msec แต่อย่างไรก็ดี เราสามารถกำหนดช่วงเวลาการรอตรงนี้ ให้มีค่าน้อยลง ซึ่งในการทดลองได้กำหนดให้ใช้ค่าเวลาที่รอ 50 msec [16] เพื่อให้การทำ Care-of address configuration time มีค่าน้อย ทำให้ทำงานได้เร็วขึ้น เมื่อไม่มี Node ใด ๆ ตอบมา Tentative IPv6 address นั้นก็สามารถกำหนดเป็น Care-of address และ นำไปใช้งานได้เลย แต่หากมี node ใด ๆ

เอกสารนี้มีลิขสิทธิ์ ห้ามนำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

อย่างน้อย 1 node ส่ง NA ตอบกลับไปยัง Mobile Node ว่า Tentative IPv6 address นั้น ไม่สามารถใช้งานได้ และต้องกลับไปเริ่มต้นกระบวนการนี้ใหม่ทั้งหมด

Latency send conservative = Max (RTT_HA, RTT_RR) + RTT_RO (5.4)

RTT = Round Trip Time

5.2.3 Care-of Address Registration Time

Care-of address Registration Time (t_r) เป็นเวลาที่ใช้ในสำหรับการส่งข้อมูล Mobile Node Care-of address ไปยัง Home Agent ของมันเอง ซึ่งสามารถสรุป เวลาในการทำงานดังนี้

$$t_r = RTT_{MN\text{-}HA} + BU_{proc} + BA_{proc} \quad (5.5)$$

5.2.4 Route Optimization Time

Route optimization time (t_o) เป็นเวลาที่เกิดขึ้นระหว่างที่ Mobile Node Registration Binding Update กับ Correspondent Node ซึ่งสามารถแบ่งย่อยได้เป็น 2 กรณี คือ

- $t_o = RTT_{MN\text{-}CN} + BU_{proc} + BA_{proc}$ (ถ้า Binding Update ไม่มีการ Authenticated)
- $t_o = T_{HoT\text{-}CoT} + (RTT_{MN\text{-}CN} + BU_{proc} + BA_{proc})$ (ถ้า Binding Update มีการ Authenticated โดย Return Routability)

หาก Binding Update ไม่มีการ Authenticate เวลา Route optimization (t_o) คือ เวลาที่ใช้ในการส่ง Binding Update ระหว่าง Mobile Node กับ Correspondent Node โดยที่ความเร็วในการประมวลผล Binding Update และ Binding Acknowledgement มีผล Route Trip Time ไม่มากนัก ถ้าเป็นกรณี ที่ Binding Update มีการ Authenticate โดยวิธี Return Routability Mobile Node จะต้อง ส่ง Home Test Init (HoTI) กับ Care of Test Init (CoTI) และรอรับ Home Test (HoT) กับ Care of Test (CoT) ก่อนที่จะส่ง Binding Update

5.3 มาตรวัดประสิทธิภาพ

- Velocity

$$V = S/T \quad (5.6)$$

- Packet transmission time

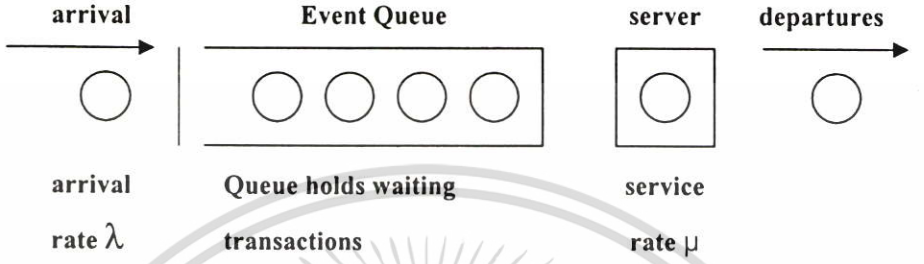
$$T_{hop} = (\text{Packet size} * 8) / \text{Bandwidth} + \text{delay time} \quad (5.7)$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Average end-to-end handoff delay of data packets

$$= \text{sum}(t_d + t_a + t_r + t_o) \quad (5.8)$$

5.4 แบบจำลองระบบคิว (M/M/1) [20]



รูปที่ 5.1 Queuing model M/M/1

โดยทั่วไปแล้ว ความหนาแน่นของการให้บริการ utilization factor (ρ) ของการใช้ระบบเครือข่ายไร้สายที่คุ้มค่า และมีประสิทธิภาพจะอยู่ที่ประมาณ 70% ในสภาพแวดล้อมที่ได้ทดสอบได้กำหนดแบนด์วิธ 2 mbps/ 2 msec [11] มีลักษณะการแจกแจงแบบเอกซโพเนนเชียล ซึ่งนำมาคำนวนหาค่า services rate (μ) ได้เป็น

μ = (Average packet size * 8 / Bandwidth + delay) msec/ packet

μ = (100 * 8 / 2000 + 2) msec/ packet

μ = 0.416 packet/msec

เราสามารถคำนวนหา arrival rate (λ) ได้เป็น

$\lambda = \rho * \mu = 70\% * 0.417$

$\lambda = 0.7 * 0.417$

$= 0.291$ packet/msec

ความน่าจะเป็นที่ไม่มี packet ในระบบเลย (P_0) มีค่าเป็น $1 - \rho = 1 - 0.7 = 0.300$

ความน่าจะเป็นที่จะมี 1 packet ในระบบ (P_1) มีค่าเป็น $P_0 \rho^1 = 0.3 (0.7) = 0.210$

ความน่าจะเป็นที่จะมี 2 packet ในระบบ (P_2) มีค่าเป็น $P_0 \rho^2 = 0.3 (0.7^2) = 0.147$

ความน่าจะเป็นที่จะมี 3 packet ในระบบ (P_3) มีค่าเป็น $P_0 \rho^3 = 0.3 (0.7^3) = 0.103$

ความน่าจะเป็นที่จะมี 4 packet ในระบบ (P_4) มีค่าเป็น $P_0 \rho^4 = 0.3 (0.7^4) = 0.072$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 5.1 แสดงความน่าจะเป็นที่มี packet อยู่ในคิว

จำนวน Packet	**ความน่าจะเป็น**	**ความน่าจะเป็นสะสม**
0	1 - 0.7 = 0.300	0.300
1	0.300 (0.7) =0.210	0.510
2	0.300 (0.7^2) = 0.147	0.657
3	0.300 (0.7^3) = 0.103	0.769
4	0.300 (0.7^4) = 0.072	0.832

จะเห็นได้ว่า ความน่าจะเป็นที่จะมี packet ในระบบไม่เกิน 4 packet มีค่าเป็น 0.832

ค่าเฉลี่ยของ packet ทั้งหมดในระบบการให้บริการคำนวนได้จาก

$$L_s = \lambda / (\mu-\lambda) = \rho / (1-\rho) = 0.7 / (1-0.7) = 2.333$$

นั่นคือโดยเฉลี่ยแล้ว จะมี packet 2.333 packet ในระบบ

สำหรับค่าเฉลี่ยของลูกค้าที่คอยในแถวคอยเพื่อรอรับบริการจะคำนวนได้จาก

$$L_q = \lambda^2 / (\mu(\mu-\lambda)) = L_s - \rho = 2.333 - 0.700 = 1.633$$

นั่นคือ โดยเฉลี่ยแล้วในระบบการให้บริการจะมี packet ที่ต้องคอยเพื่อรับบริการจำนวน 1.633 packet

สำหรับเวลาเฉลี่ยที่แต่ละ packet ต้องใช้ในระบบนับจากเริ่มเข้ามาในระบบจนกระทั่งได้รับบริการจนเสร็จแล้วมีค่าเป็น

$$W_s = 1/(\mu - \lambda) = L_s / \lambda = 2.333/0.291 = 8.017 \text{ msec}$$

สำหรับเวลาเฉลี่ยที่แต่ละ packet ต้องใช้ในการคอยเพื่อรับบริการ (ไม่นับเวลารับบริการ) นับจากเริ่มเข้ามาในระบบจนกระทั่งเริ่มได้รับบริการจะมีค่าเป็น

$$W_q = \lambda / (\mu(\mu-\lambda)) = L_q / \lambda = 1.633/0.291 = 7.593$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 6
การทดลองและผลการทดลอง

6.1 บทนำ

Java Network Simulator (JNS) [19] เป็น โปรแกรม simulator ที่สร้างขึ้นมาแบบ NS-2 [21] แต่ พัฒนาโดยใช้ ภาษาจาวา simulator ตัวนี้ เหมาะสำหรับนักวิจัยที่ไม่ชำนาญภาษา C++ และ Object TCL, JNS อนุญาตให้นักวิจัยจำลองการทำงานของโพรโตคอลในสภาพแวดล้อมที่สามารถกำหนดได้โดยใช้ภาษาจาวา หลังจากนั้น JNS ก็จะสร้าง Trace ที่สามารถดูการเคลื่อนไหว ได้ด้วยโปรแกรม NAM [21] หรือ Javis [19] งานวิจัยนี้ ได้ใช้โปรแกรม JNS เป็นตัวจำลองการทำงานของ Mobile IPv6 โดยเขียนส่วน กระบวนการทำ Mobile IPv6 Handoff เพิ่มเข้ามาทำงานกับ IPHandler Layer และมีการจัด Queue ภายในตัว Simulator ที่มีการทำงานเป็นแบบ Thread ในการทดลองนี้จะ Simulation Mobile IPv6 โดยประยุกต์ใช้ security scheme แบบต่าง ๆ แล้วหาค่า end-to-end handoff delay time ที่ใช้ในการส่งข้อมูล

6.2 ส่วนประกอบของ JNS

JNS ประกอบไปด้วย Package ย่อย ๆ ดังนี้

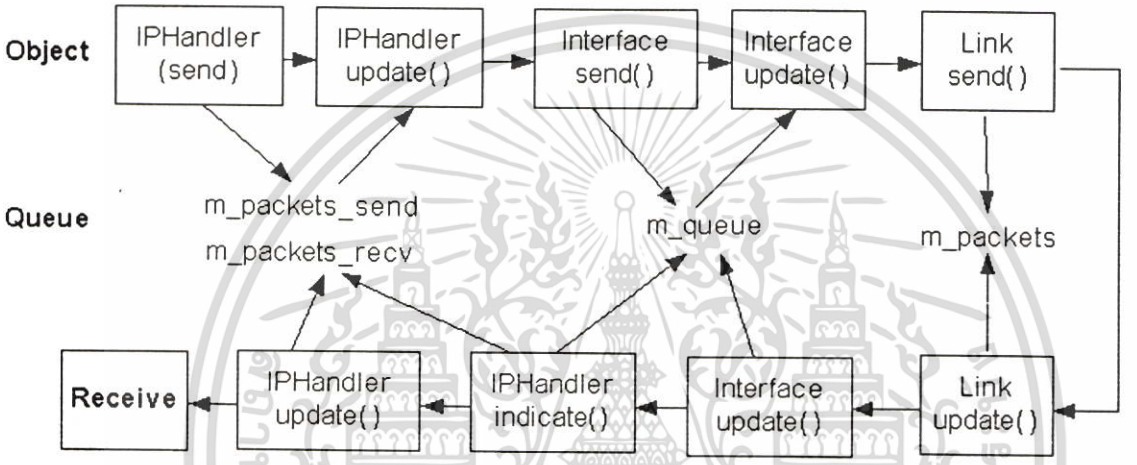
- jns.element เป็น network components ต่าง เช่น node, network interface, network link
- jns.agent ประกอบด้วย interface ที่ใช้สำหรับ agents ซึ่งเราสามารถพัฒนาโพรโตคอลใหม่ โดยการ implement interface ขึ้นมา
- jns.trace ไว้สำหรับ เขียนผลลัพธ์การทำงานทุก ๆ สิ่งที่ต้องการให้แสดงผลใน NAM หรือ Javis ลงใน File
- jns.command จำลองการทำงานของงานที่จะต้องทำโดยใส่ไว้ใน Priority Queue ของ Simulator
- jns.util เป็นข้อมูลประกอบสำหรับการทำ Simulation เช่น IPAddr, Queue, Preference

6.3 การทำงานของ JNS

Simulator เป็น object ที่ implements มาจาก class Runnable โดยจะถูกเรียกจาก Configuration script ที่ใช้กำหนดการทำงาน เริ่มการทำงานโดยการเรียก method run() ใน Simulator class ซึ่งมี Priority queue ในการเก็บ Command object ที่มี element object เป็น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

attribute ซึ่ง element object กำหนดการทำงานของ method execute() เอาไว้ command object เปรียบเสมือน job ที่เราต้องการจะใช้ในการจำลองการส่ง packet ในแต่ละรูปแบบ ลงไปในเครือข่าย ตัว Simulator จะเรียก command object ที่เก็บใน Priority queue เข้ามาทำงานเมื่อถึงเวลาที่กำหนดไว้ โดยเวลาของแต่ละ command object จะเป็นตัวกำหนด Priority เมื่อ element object ของ command ทำงาน มันก็จะ execute() โดยส่ง packet เป็นลำดับขั้น โดยส่งจาก IPHandler – Interface – Link – Interface – IPHandler ในระหว่างที่มีการส่ง packet ระหว่าง layer ก็จะมี Queue ไว้สำหรับพักข้อมูลชั่วคราว ก่อนที่จะถูกส่งไปยัง Layer ถัดไป



รูปที่ 6.1 การส่งข้อมูลที่ใช้ทำ Simulation ของ JNS

IPHandler เป็นตัวสร้าง และรับ IP Packet แล้วส่งต่อไปยัง SimplexInterface เอาไปเก็บไว้ใน queue เพื่อรอถาม Link ว่า พร้อมที่จะส่งข้อมูลหรือไม่ หากพร้อมจะส่งข้อมูล SimplexInterface ก็จะส่งข้อมูลต่อไปยัง Link หลังจากนั้น Link ก็จะคำนวน เวลาในการส่งข้อมูลโดยใช้สูตร (packet size * 8)/(bandwidth) + propagation delay เมื่อ Packet ไปถึงปลายทาง มันก็จะเรียก method indicated() เพื่อให้ อ่าน Packet มาจาก Link ผ่านยัง Interface และ IPHandler เป็นลำดับขั้น โดยที่มีการเขียนบันทึกลง Trace file สำหรับทุก ๆ เหตุการณ์

6.4 สภาพแวดล้อม

- กำหนดจำนวนเซลล์ไซต์ ใน กรุงเทพมหานคร มีอยู่ประมาณ 500 ไซต์
- กำหนดให้ Mobile Node เคลื่อนที่ออกจาก Home Agent ไปยัง Access Router ที่อยู่ใกล้เคียง ไปเรื่อย ๆ โดยที่ Access Router ที่อยู่ไกลจาก HA สูงสุด ไม่เกิน 10 hops
- ระยะทางเฉลี่ยระหว่าง Mobile Node กับ Home Agent 6 hops

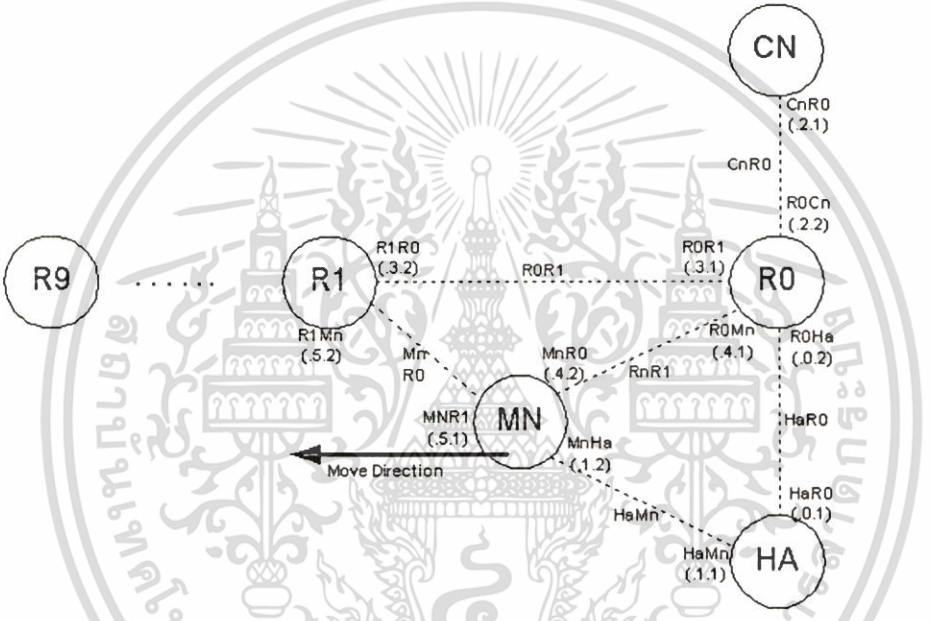
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Home Agent ตั้งอยู่บริเวณศูนย์กลางของสถานที่ให้บริการทั้งหมด
- Correspondent Node อยู่ห่างกับ Home Agent 2 hops
- แบนด์วิธที่ใช้ในการติดต่อสื่อสาร ในแต่ละช่องทางการสื่อสารมีค่าไม่เกิน 2 mbps [11]
- Delay time ในช่องการสื่อสารที่ใช้ในการติดต่อสื่อสาร และ ประมวลผล มีค่าไม่เกิน 2 msec [11]

6.5 ผลการทดลอง

6.5.1 เมื่อกำหนด Operating point ของ utilization factor เป็น 70%

6.5.1.1 การเชื่อมต่อ



รูปที่ 6.2 Mobile IPv6 Simulation Topology

6.5.1.2 Handoff Delay performance

ทดลองกำหนดจำลองการทำงานตามสภาพแวดล้อมที่ได้กล่าวมา เพื่อหาค่า delay time ในการทำ Handoff

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.5.1.2.1 Mobile IPv6 Handoff using ECBU

ตารางที่ 6.1 Mobile IPv6 Handoff using ECBU

	PacketSize	Hop	Time
L2 Handoff			45
RS	68	1	2.272
RA	84	1	2.336
NS	68	1	2.272
NA ?	84	1	50
BU(ha)	80	2	4.64
BA(ha)	104	2	4.832
Req(mn-ha)	68	2	4.544
Ck0	64	2	4.512
Ck1	64	2	4.512
Exch0	128	2	5.024
Exch1	128	2	5.024
Rep(ha-mn)	128	2	5.024
BU(cn)	92	2	4.736
BA(cn)	92	2	4.736
Sum			149.464

6.5.1.2.2 Mobile IPv6 Handoff using Return Routability (RR)

ตารางที่ 6.2 Mobile IPv6 Handoff using Return Routability

	PacketSize	Hop	Time
L2 Handoff			45
RS	68	1	2.272
RA	84	1	2.336
NS	68	1	2.272
NA ?	84	1	50
BU(ha)	80	2	4.64
BA(ha)	104	2	4.832
HoTI(mn-ha-cn)	84	4	9.344
HoT(mn-ha-cn)	92	4	9.472
BU(cn)	92	2	4.736
BA(cn)	92	2	4.736
Sum			139.64

6.5.1.2.3 Mobile IPv6 Handoff using Kerberos and Pre-Register (KPR)

ตารางที่ 6.3 Mobile IPv6 Handoff using Kerberos and Pre-Register (KPR)

	PacketSize	Hop	Time
L2 Handoff			45
RS	68	1	2.272
RA	84	1	2.336
NS	68	1	2.272
NA ?	84	1	50
BU(cn)	100	2	4.8
BA(cn)	100	2	4.8
Sum			111.48

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

วิเคราะห์ผลการทำงาน

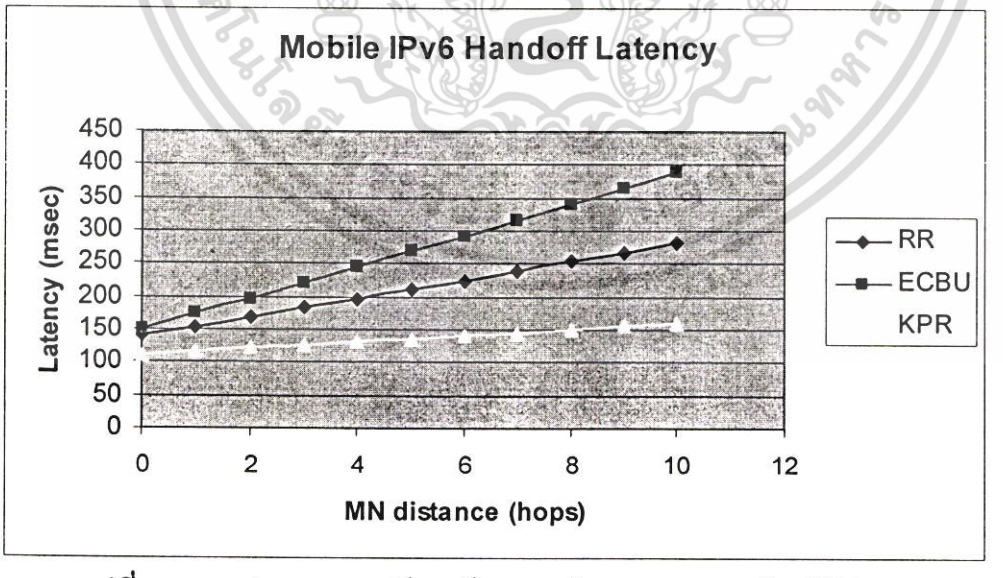
ตารางที่ 6.4 เปรียบเทียบเวลาในการ Handoff โดยใช้วิธีต่าง ๆ

Add Range MN->R				Speed Up	
Hop	RR	ECBU	KPR	RR vs KPR	ECBU vs KPR
0	139.64	149.464	111.48	25.26%	34.07%
1	153.816	173.256	116.28	32.28%	49.00%
2	167.992	197.048	121.08	38.74%	62.74%
3	182.168	220.84	125.88	44.72%	75.44%
4	196.344	244.632	130.68	50.25%	87.20%
5	210.52	268.424	135.48	55.39%	98.13%
6	224.696	292.216	140.28	60.18%	108.31%
7	238.872	316.008	145.08	64.65%	117.82%
8	253.048	339.8	149.88	68.83%	126.71%
9	267.224	363.592	154.68	72.76%	135.06%
10	281.4	387.384	159.48	76.45%	142.90%

เมื่อ Hop = 0 หมายถึง Path ระหว่าง MN กับ HA ห่างกัน 2 hop

Hop = 1 หมายถึง Path ระหว่าง MN กับ HA ห่างกัน 3 hop โดยเพิ่มขึ้นตามลำดับ

ในระยะทาง ที่ Mobile Node ห่างกับ Home Agent 5 hop พบว่าค่า Handoff delay time ลดถึง 55.39% เมื่อเทียบกับวิธี RR และ ลดลง 98.13% เมื่อเทียบกับวิธี ECBU ซึ่งจะเห็นได้ว่า ยิ่ง Mobile Node เคลื่อนที่ออกห่างจาก Home Agent หรือ Correspondent Node มากเท่าไร วิธี KPR ใช้เวลาในการทำ Hand off น้อยวิธีอื่น ๆ



รูปที่ 6.3 กราฟแสดงการเปรียบเทียบเวลาในการ Handoff โดยวิธีต่าง ๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แสดง IP application latency [13] สำหรับ Real-Time Application ซึ่งแบ่งได้ออกเป็นช่วงเวลาดังนี้

ตารางที่ 6.5 เปรียบเทียบเวลาการ Handoff กับค่า Lantency สำหรับ Real-Time Application

ECBU	Hop 0	Hop 1 - 6	Hop > 6	-
RR	Hop 0	Hop > 0	-	-
KRP	Hop 0 - 8	Hop > 8	-	-

6.5.1.3 เพิ่มเวลาในการรอคิว

6.5.1.3.1 Mobile IPv6 Handoff using ECBU

ตารางที่ 6.6 Mobile IPv6 Handoff using ECBU เมื่อพิจารณาคิวร่วมด้วย

	PacketSize	Hop	Time
L2 Handoff			45
RS	68	1	9.865
RA	84	1	9.929
NS	68	1	9.865
NA ?	84	1	50
BU(ha)	80	2	19.826
BA(ha)	104	2	20.018
Req(mn-ha)	68	2	19.73
Ck0	64	2	19.698
Ck1	64	2	19.698
Exch0	128	2	20.21
Exch1	128	2	20.21
Rep(ha-mn)	128	2	20.21
BU(cn)	92	2	19.922
BA(cn)	92	2	19.922
Sum			324.103

6.5.1.3.2 Mobile IPv6 Handoff using Return Routability

ตารางที่ 6.7 Mobile IPv6 Handoff using Return Routability เมื่อพิจารณาคิวร่วมด้วย

L2 Handoff	PacketSize	Hop	Queue
RS	68	1	45
RA	84	1	9.865
NS	68	1	9.929
NA ?	84	1	9.865
BU(ha)	80	2	50
BA(ha)	104	2	19.826
HoTI(mn-ha-cn)	84	4	20.018
HoT(mn-ha-cn)	92	4	39.716

เอกสารนี้ใช้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

BU(cn)	92	2	39.844
BA(cn)	92	2	19.922
Sum			283.907

6.5.1.3.3 Mobile IPv6 Handoff using Kerberos and Pre-Register

ตารางที่ 6.8 Mobile IPv6 Handoff using Kerberos and Pre-Register เมื่อพิจารณาคิวร่วมด้วย

	PacketSize	Hop	Time
L2 Handoff			45
RS	68	1	9.865
RA	84	1	9.929
NS	68	1	9.865
NA ?	84	1	50
BU(cn) | BU(ha) (parallel)	100	2	19.986
BA(cn) | BA (ha) (parallel)	100	2	19.986
Sum			164.631

วิเคราะห์ผลการทำงาน

ตารางที่ 6.9 เปรียบเทียบเวลาในการ Handoff โดยใช้วิธีต่าง ๆ เมื่อพิจารณาคิวร่วมด้วย

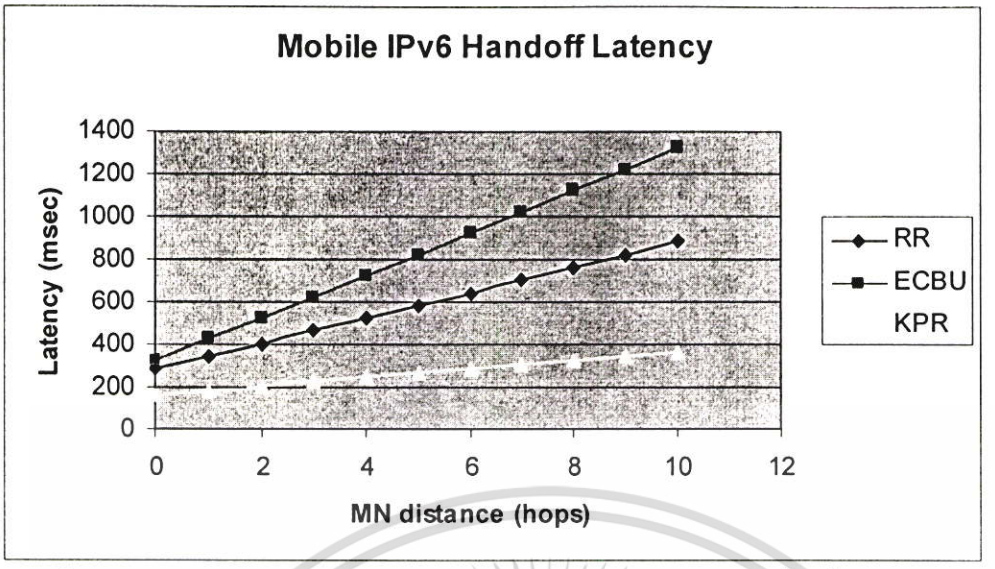
Add Range MN->R [With Queue]				Speed Up	
Hop	RR	ECBU	KPR	RR vs KPR	ECBU vs KPR
0	283.907	324.103	164.631	72.45%	96.87%
1	343.641	423.825	184.617	86.14%	129.57%
2	403.375	523.547	204.603	97.15%	155.88%
3	463.109	623.269	224.589	106.20%	177.52%
4	522.843	722.991	244.575	113.78%	195.61%
5	582.577	822.713	264.561	120.21%	210.97%
6	642.311	922.435	284.547	125.73%	224.18%
7	702.045	1022.157	304.533	130.53%	235.65%
8	761.779	1121.879	324.519	134.74%	245.71%
9	821.513	1221.601	344.505	138.46%	254.60%
10	881.247	1321.323	364.491	141.77%	262.51%

เมื่อ Hop = 0 หมายถึง Path ระหว่าง MN กับ HA ห่างกัน 2 Hop

Hop = 1 หมายถึง Path ระหว่าง MN กับ HA ห่างกัน 3 Hop โดยเพิ่มขึ้นตามลำดับ

จากรูปที่ 6.3 จะเห็นได้ว่า ในระยะทาง ที่ Mobile Node ห่างกับ Home Agent 5 hop พบว่าค่า Handoff delay time ลดถึง 120.21% เมื่อเทียบกับวิธี RR และ ลดลง 210.97% เมื่อเทียบกับวิธี ECBU ซึ่งจะเห็นได้ว่า ยิ่ง Mobile Node เคลื่อนที่ออกห่างจาก Home Agent หรือ Correspondent Node มากเท่าไร วิธี KPR ใช้เวลาในการทำ Hand off น้อยวิธีอื่น ๆ มากขึ้นกว่าเดิม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 6.4 กราฟแสดงการเปรียบเทียบการ Handoff โดยวิธีต่าง ๆ เมื่อเพิ่มเวลารอคิว

แสดง IP application latency สำหรับ Real Time Application ซึ่งแบ่งได้ออกเป็นช่วงเวลาดังนี้

ตารางที่ 6.10 เปรียบเทียบเวลาการ Handoff กับค่า Lantency สำหรับ Real-Time Application เมื่อพิจารณาคิวร่วมด้วย

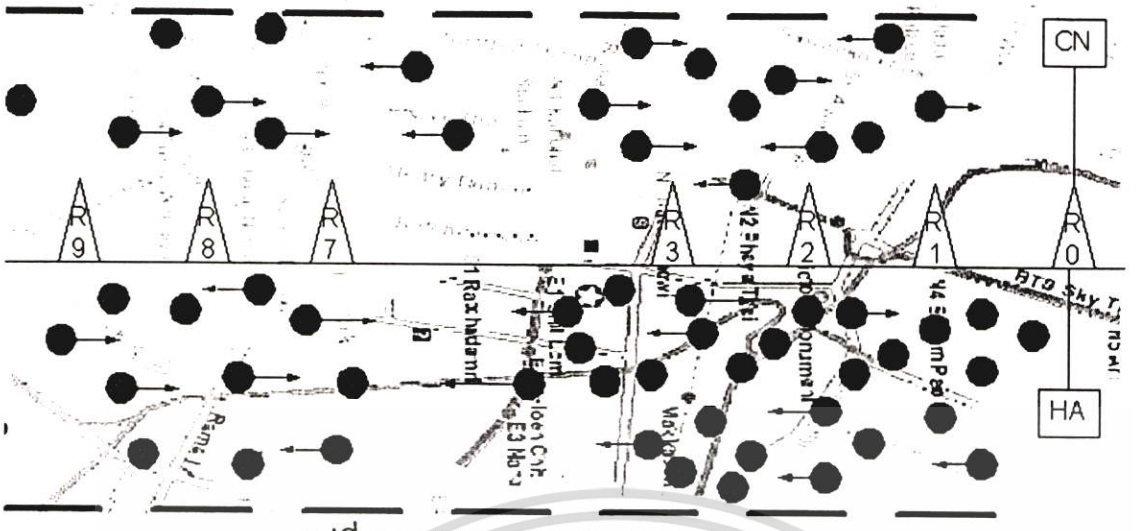
ECBU	-	-	Hop 0 - 1	Hop > 1
RR	-	Hop 0	Hop 1 - 2	Hop > 2
KRP	Hop 0	Hop 1 - 4	Hop 5 - 6	Hop > 6

6.5.2 เมื่อทำการจำลองโดย เพิ่มจำนวน Mobile Node

6.5.2.1 การเชื่อมต่อ

กำหนดสภาพแวดล้อม เป็นลักษณะการจำลองการทำงานของ Mobile Node ที่เคลื่อนที่อยู่บนถนนทางด่วน ซึ่งมีการเคลื่อนที่ ที่มีลักษณะเป็นเส้นตรง ใช้เวลาในการจำลอง 2000 วินาที โดยกำหนดเวลาการเริ่มเคลื่อนที่และหยุด เป็นการสุ่มแบบ Uniform และ มีการกำหนดค่าแบนด์วิธ ให้มีค่าอยู่ในช่วง 0 – 2 mbps.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



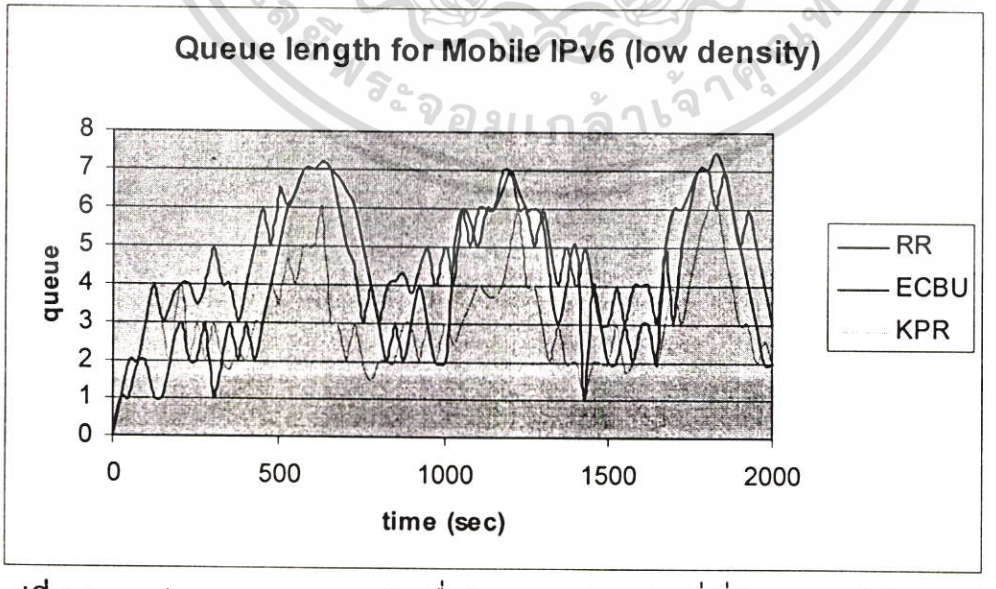
รูปที่ 6.5 Mobile IPv6 Simulation Topology

สร้าง Topology โดยการกำหนด MN รอบ ๆ R1, R2, R3 จำนวน 100 โหนด และ รอบ ๆ R7, R8, R9 จำนวน 50 โหนด โดยที่สุ่มให้ Mobile Node แต่ละตัว มีการ ให้ส่งข้อมูล 32 kbps รวมกับ ข้อมูลที่ใช้ในการทำ Handoff

6.5.2.2 ความยาวของคิว

6.5.2.2.1 ในเครือข่ายที่มีการใช้งานไม่หนาแน่น

ในการจำลองครั้งนี้ ได้วัดค่าความยาวของคิว ระหว่างการติดต่อสื่อสารของ R7 กับ R8 และ R1 กับ R2 โดยแบ่ง การจำลองออกเป็น 2 ส่วน คือ ทดลองในสภาพแวดล้อมที่มีการจราจรที่ไม่หนาแน่น กับ ทดลองในสภาพแวดล้อมที่มีการจราจรหนาแน่น

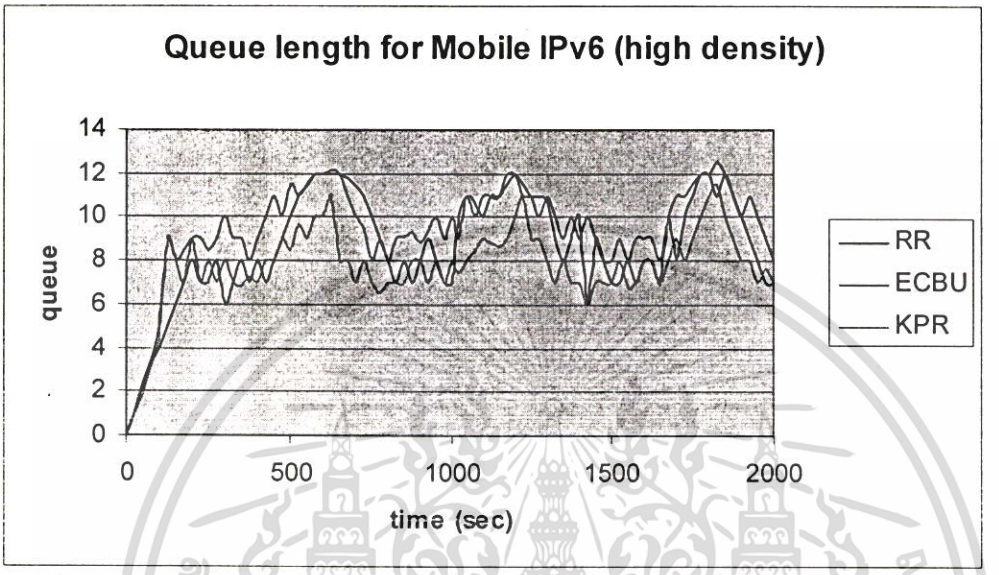


รูปที่ 6.6 กราฟแสดงความยาวของคิวเมื่อจำลองการทำงานในที่ ที่มีการจราจรไม่หนาแน่น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ได้มีการโมเดล จำลองเลียนแบบ การใช้งานในชีวิตประจำวัน กล่าวคือ ช่วงเวลาประมาณ เริ่มทำงาน ช่วงเวลาพักเที่ยง และ ช่วงหลังเลิกงาน จะมีการใช้งานระบบเครือข่ายมาก ทำให้มีคิวที่ค่อนข้างสูงกว่าช่วงเวลาปกติ

6.5.2.2.2 **ในเครือข่ายที่มีการใช้งานหนาแน่น**



รูปที่ 6.7 กราฟแสดงความยาวของคิว เมื่อจำลองการทำงานในที่ ที่มีการจราจรหนาแน่น

วิเคราะห์ผลการทดลอง

ค่าเฉลี่ยของคิว สำหรับกรณีของเครือข่ายที่มีการใช้งานไม่หนาแน่น มีค่าประมาณ 4 packets และ เครือข่ายที่มีการใช้งานหนาแน่น มีค่าประมาณ 6 packets หลังจากทดลอง จำลองการทำงานทั้ง 3 วิธีเพื่อพิจารณาถึง ความยาวของคิว แล้ว พบว่าคิวที่เกิดขึ้นนั้น ไม่ได้แตกต่างกันมากนัก ทั้งนี้ เนื่องจากวิธีการ KPR จำเป็นต้องมีการส่งข้อมูลไปก่อนที่จะเริ่มทำ Handoff จริง ๆ จึงทำให้ค่าความยาวของคิวที่เกิดขึ้น ไม่ได้มีความแตกต่างกับวิธีอื่น ๆ มากนัก

6.5.2.3 Handoff delay performance

ทดลองกำหนดจำลองการทำงานตามสภาพแวดล้อมที่ได้กล่าวมา เพื่อหาค่า delay time ในการทำ Handoff

6.5.2.3.1 **ในเครือข่ายที่มีการใช้งานไม่หนาแน่น**

6.5.2.3.1.1 Mobile IPv6 Handoff using ECBU

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 6.11 Mobile IPv6 Handoff using ECBU

	PacketSize	Hop	Time
L2 Handoff			45.00
RS	68	1	11.92
RA	84	1	11.98
NS	68	1	11.92
NA ?	84	1	50.00
BU(ha)	80	2	23.94
BA(ha)	104	2	24.13
Req(mn-ha)	68	2	23.84
Ck0	64	2	23.81
Ck1	64	2	23.81
Exch0	128	2	24.32
Exch1	128	2	24.32
Rep(ha-mn)	128	2	24.32
BU(cn)	92	2	24.04
BA(cn)	92	2	24.04
Sum			371.46

6.5.2.3.1.2 Mobile IPv6 Handoff using Return Routability (RR)

ตารางที่ 6.12 Mobile IPv6 Handoff using Return Routability

	PacketSize	Hop	Time
L2 Handoff			45.00
RS	68	1	11.92
RA	84	1	11.98
NS	68	1	11.92
NA ?	84	1	50.00
BU(ha)	80	2	23.94
BA(ha)	104	2	24.13
HoTI(mn-ha-cn)	84	4	47.95
HoT(mn-ha-cn)	92	4	48.08
BU(cn)	92	2	24.04
BA(cn)	92	2	24.04
Sum			323.02

6.5.2.3.1.3 Mobile IPv6 Handoff using Kerberos and Pre-Register (KPR)

ตารางที่ 6.13 Mobile IPv6 Handoff using Kerberos and Pre-Register (KPR)

	PacketSize	Hop	Time
L2 Handoff			45.00
RS	68	1	11.92
RA	84	1	11.98
NS	68	1	11.92
NA ?	84	1	50.00
BU(cn)	100	2	24.10
BA(cn)	100	2	24.10
Sum			179.04

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

วิเคราะห์ผลการทำงาน

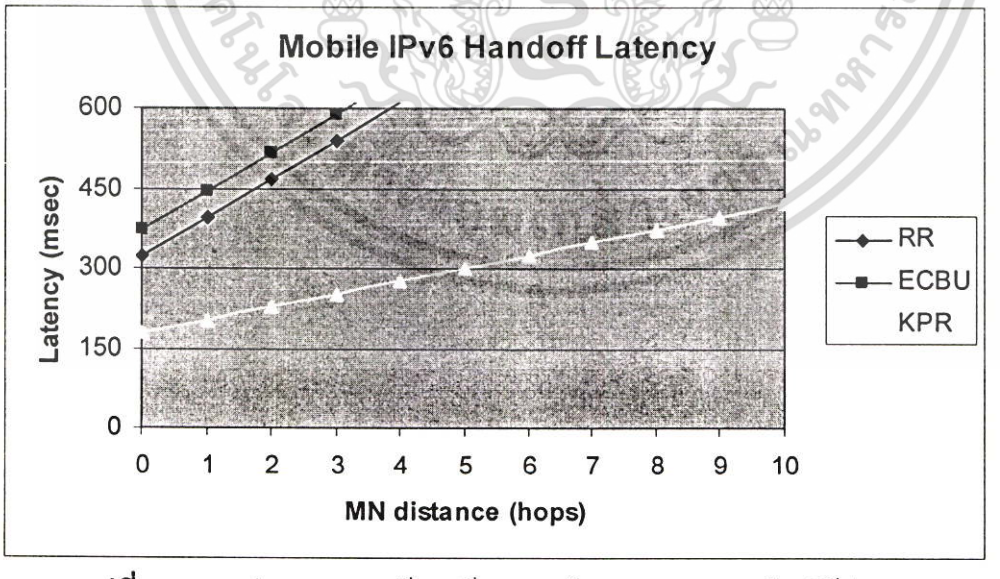
ตารางที่ 6.14 เปรียบเทียบเวลาในการ Handoff โดยใช้วิธีต่าง ๆ

Add Range MN->R				Speed Up	
Hop	RR	ECBU	KPR	RR vs KPR	ECBU vs KPR
0	323.02	371.46	179.04	80.42%	107.47%
1	395.11	443.62	203.14	94.50%	118.38%
2	467.20	515.79	227.25	105.59%	126.97%
3	539.29	587.96	251.35	114.55%	133.92%
4	611.38	660.132	275.46	121.95%	139.65%
5	683.46	732.30	299.56	128.15%	144.46%
6	755.55	804.46	323.66	133.44%	148.55%
7	827.64	876.63	347.77	137.98%	152.07%
8	899.73	948.80	371.87	141.94%	155.14%
9	971.82	1020.97	395.98	145.42%	157.83%
10	1043.90	1093.14	420.08	148.50%	160.22%

เมื่อ Hop = 0 หมายถึง Path ระหว่าง MN กับ HA ห่างกัน 2 hop

Hop = 1 หมายถึง Path ระหว่าง MN กับ HA ห่างกัน 3 hop โดยเพิ่มขึ้นตามลำดับ

ในระยะทาง ที่ Mobile Node ห่างกับ Home Agent 5 hop พบว่าค่า Handoff delay time ลดถึง 128.15% เมื่อเทียบกับวิธี RR และ ลดลง 144.46% เมื่อเทียบกับวิธี ECBU ซึ่งจะเห็นได้ว่า ยิ่ง Mobile Node เคลื่อนที่ออกห่างจาก Home Agent หรือ Correspondent Node มากเท่าไร วิธี KPR ใช้เวลาในการทำ Hand off น้อยวิธีอื่น ๆ



รูปที่ 6.8 กราฟแสดงการเปรียบเทียบเวลาในการ Handoff โดยวิธีต่าง ๆ

แสดง IP application latency [13] สำหรับ Real-Time Application ซึ่งแบ่งได้ออกเป็นช่วงเวลาดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 6.15 เปรียบเทียบเวลาการ Handoff กับค่า Lantency สำหรับ Real-Time Application

Delay 0 → Excellent 150 → Good 300 → Poor 450 → Unacceptable (msec)

ECBU	-	-	Hop 0 - 1	Hop > 1
RR	-	-	Hop 0 - 1	Hop > 1
KRP	-	Hop 0 - 5	Hop 6 - 10	Hop > 10

6.5.2.3.2 ในเครือข่ายที่มีการใช้งานหนาแน่น

6.5.2.3.2.1 Mobile IPv6 Handoff using ECBU

ตารางที่ 6.16 Mobile IPv6 Handoff using ECBU

	PacketSize	Hop	Time
L2 Handoff			45.00
RS	68	1	16.84
RA	84	1	16.90
NS	68	1	16.84
NA ?	84	1	50.00
BU(ha)	80	2	33.78
BA(ha)	104	2	33.97
Req(mn-ha)	68	2	33.68
Ck0	64	2	33.65
Ck1	64	2	33.65
Exch0	128	2	34.16
Exch1	128	2	34.16
Rep(ha-mn)	128	2	34.16
BU(cn)	92	2	33.87
BA(cn)	92	2	33.87
Sum			484.59

6.5.2.3.2.2 Mobile IPv6 Handoff using Return Routability

ตารางที่ 6.17 Mobile IPv6 Handoff using Return Routability

	PacketSize	Hop	Queue
L2 Handofff			45.00
RS	68	1	16.843
RA	84	1	16.90
NS	68	1	16.84
NA ?	84	1	50.00
BU(ha)	80	2	33.78
BA(ha)	104	2	33.97
HoTI(mn-ha-cn)	84	4	67.62
HoT(mn-ha-cn)	92	4	67.75
BU(cn)	92	2	33.87
BA(cn)	92	2	33.87
Sum			416.48

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.5.2.3.2.3 Mobile IPv6 Handoff using Kerberos and Pre-Register

ตารางที่ 6.18 Mobile IPv6 Handoff using Kerberos and Pre-Register

	PacketSize	Hop	Time
L2 Handoff			45.00
RS	68	1	16.84
RA	84	1	16.90
NS	68	1	16.84
NA ?	84	1	50.00
BU(cn) | BU(ha) (parallel)	100	2	33.94
BA(cn) | BA (ha) (parallel)	100	2	33.94
Sum			213.47

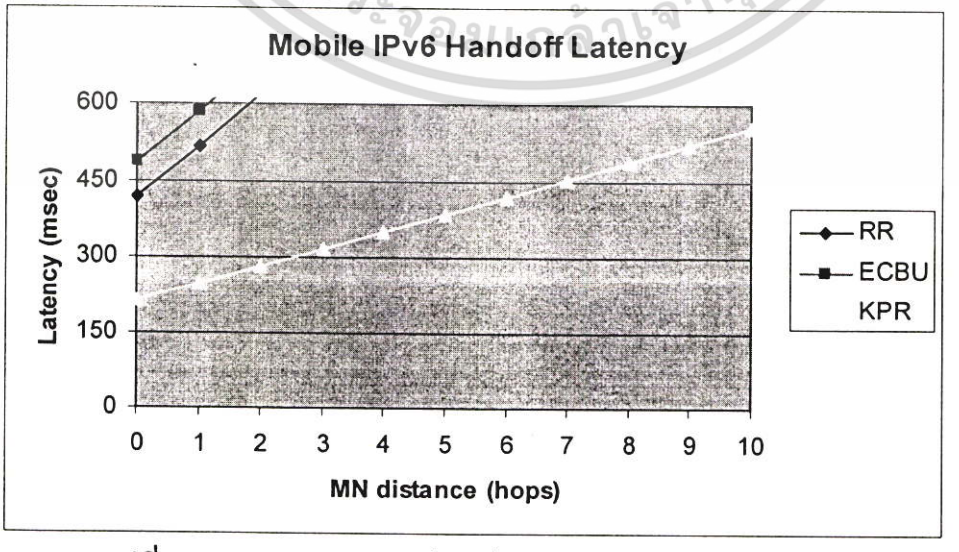
วิเคราะห์ผลการทำงาน

ตารางที่ 6.19 เปรียบเทียบเวลาในการ Handoff โดยใช้วิธีต่าง ๆ

Add Range MN->R				Speed Up	
Hop	RR	ECBU	KPR	RR vs KPR	ECBU vs KPR
0	416.48	484.59	213.47	95.10%	127.00%
1	518.09	586.27	247.47	109.40%	136.96%
2	619.69	687.96	281.36	120.25%	144.51%
3	721.29	789.64	315.30	128.76%	150.44%
4	822.89	891.32	349.24	135.62%	155.21%
5	924.49	993.00	383.18	141.27%	159.14%
6	1026.10	1094.68	417.12	145.99%	162.43%
7	1127.70	1196.37	451.07	150.01%	165.23%
8	1229.30	1298.05	485.01	153.46%	167.63%
9	1330.90	1399.73	518.95	156.46%	169.72%
10	1432.50	1501.41	552.89	159.09%	171.55%

เมื่อ Hop = 0 หมายถึง Path ระหว่าง MN กับ HA ห่างกัน 2 Hop

Hop = 1 หมายถึง Path ระหว่าง MN กับ HA ห่างกัน 3 Hop โดยเพิ่มขึ้นตามลำดับ



รูปที่ 6.9 กราฟแสดงการเปรียบเทียบการ Handoff โดยวิธีต่าง ๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในระยะทาง ที่ Mobile Node ห่างกับ Home Agent 5 hop พบว่าค่า Handoff delay time ลดถึง 141.27% เมื่อเทียบกับวิธี RR และ ลดลง 159.14% เมื่อเทียบกับวิธี ECBU ซึ่งจะเห็นได้ว่า ยิ่ง Mobile Node เคลื่อนที่ออกห่างจาก Home Agent หรือ Correspondent Node มากเท่าไร วิธี KPR ใช้เวลาในการทำ Hand off น้อยวิธีอื่น ๆ มากขึ้นกว่าเดิม

แสดง IP application latency สำหรับ Real Time Application ซึ่งแบ่งได้ออกเป็นช่วงเวลาดังนี้

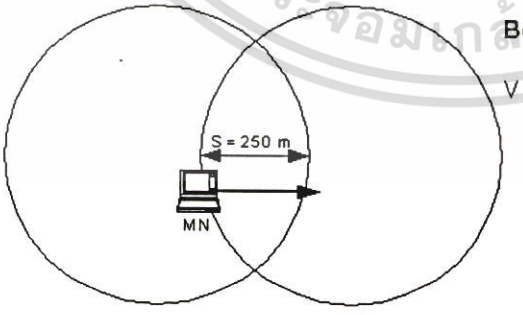
ตารางที่ 6.20 เปรียบเทียบเวลาการ Handoff กับค่า Lantency สำหรับ Real-Time Application

Delay 0 Excellent 150 Good 300 Poor 450 Unacceptable (msec)

ECBU	-	-	-	Hop > 0
RR	-	-	Hop 0	Hop > 0
KRP	-	Hop 0 - 2	Hop 3 - 6	Hop > 6

6.6 Velocity effect

เมื่อกำหนดระยะในการซ้อนทับของ Base station เป็น 250 เมตร สามารถคำนวนหาความเร็วสูงสุดในการเคลื่อนที่ของ Mobile Node ความเร็วสูงสุดในการเคลื่อนที่ภายในช่วงเวลา Handoff สามารถแบ่งเป็นกรณี ต่าง ๆ ดังนี้

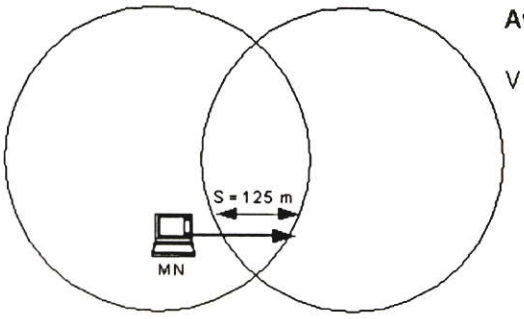


Best case:

V = S/T
= 250 m/ 383.19 ms
= 250 * 1000 / (383.19) m/s
= 652.417 m/s
= 652.417 * (60*60/1000) km/hr
= 2,348.70 km/hr

รูปที่ 6.10 คำนวนค่าความเร็วกรณีที่ระยะทาง Base station ที่ซ้อนทับ 250 เมตร

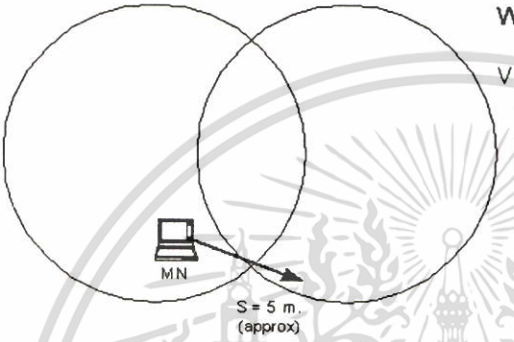
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



Average case:

V = S/T
= 125 m/ 383.19 ms
= 125 * 1000 / (383.19) m/s
= 326.21 m/s
= 326.21 * (60*60/1000) km/hr
= 1,174.35 km/hr

รูปที่ 6.11 คำนวนค่าความเร็วกรณีที่ระยะทาง Base station **ที่ซ้อนทับ** 125 เมตร



Worst case:

V = S/T
= 5 m / (383.19) ms
= 5 * 1000 / (383.19) m/s
= 13.01 m/s
= 13.01 * (60*60/1000) km/hr
= 46.97 km/hr

รูปที่ 6.12 คำนวนค่าความเร็วกรณีที่ระยะทาง Base station **ที่ซ้อนทับ** 5 เมตร

ภายในเวลาการทำ Handoff ต่าง ๆ นั่น หาก Mobile Node เคลื่อนที่ด้วยความเร็วที่มากกว่า ระยะทาง / เวลาในการทำ Handoff เสร็จสิ้น Mobile Node ก็จะสูญเสียการเชื่อมต่อในขณะนั้นไป

6.7 Pre-Registration Process delay

6.7.1 ในเครือข่ายที่มีการใช้งานไม่หนาแน่น

ตารางที่ 6.21 เวลาที่ใช้ในการทำ Pre-Registration 1 hop **ในเครือข่ายที่มีการใช้งานหนาแน่น**

	PacketSize	Hop	Time
ReqHA	68	2	23.84
SendKey	84	3	35.96
AckKey	68	3	35.77
			95.58

6.7.2 ในเครือข่ายที่มีการใช้งานหนาแน่น

ตารางที่ 6.22 เวลาที่ใช้ในการทำ Pre-Registration 1 hop **ในเครือข่ายที่มีการใช้งานหนาแน่น**

	PacketSize	Hop	Time
ReqHA	68	2	33.68
SendKey	84	3	50.72
AckKey	68	3	50.52
			134.93

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 6.23 เวลาที่ใช้ในการทำ Pre-Registration

เมื่อ Mobile Node มีการเคลื่อนที่ห่างจาก Home Agent ออกไป

Hop	KPR (low density)	KPR (high density)
0	95.58	134.93
1	131.4	185.52
2	167.25	236.12
3	203.09	286.71
4	238.92	337.30
5	274.76	387.90
6	310.60	438.49
7	346.43	489.08
8	382.27	539.68
9	418.10	590.27
10	453.94	640.86

วิเคราะห์ผลการทดลอง

วิธี Kerberos และ Pre-Registration ไม่สามารถใช้กับ การ Handoff ในกรณีที่เปลี่ยน Base station ไป แล้วเปลี่ยน Base station ย้อนกลับมาที่เดิมภายในช่วงเวลาก่อนที่จะทำกระบวนการ Pre-Registration เสร็จสิ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 7
สรุปผลการทดลองและข้อเสนอแนะ

7.1 บทนำ

เมื่อ Mobile Node ย้ายเครือข่าย การทำ Handoff สำหรับ Mobile IPv6 ที่นักวิจัยกลุ่ม Mobile IPv6 ได้นำเสนอไว้นั้น ทางกลุ่มทำงาน ได้พยายามนำเสนอวิธีที่ใช้ได้ครอบคลุมในหลาย ๆ กรณีมากที่สุด แต่ไม่ได้ดีที่สุดสำหรับกรณีที่ใช้งานในบางกรณี เช่น ใช้งานร่วมกับโปรแกรมประเภท Real-Time Application วิทยานิพนธ์นี้จึงนำเสนอทางเลือกอีกทางหนึ่ง ในการทำ Handoff ที่มี latency ต่ำ และคงไว้ซึ่งความปลอดภัย โดยการแก้ไข ปรับปรุงโพรโตคอล และยังออกแบบให้สามารถใช้งานร่วมกับโพรโตคอลที่เป็นมาตรฐานที่มีอยู่แล้วได้อีกด้วย

7.2 สรุปผลการทดลอง

มาตรฐานกระบวนการทำ Mobile IPv6 Handoff กำหนดไว้จะต้องทำการทดสอบ home address กับ Care-of address ก่อนที่จะมีการลงทะเบียน Care-of address ใน binding cache ของ Correspondent Node เพื่อสร้างกุญแจที่ใช้ในการเข้ารหัสข้อมูลที่จะส่งต่อไป ซึ่งกระบวนการนี้ ก่อให้เกิด latency ที่สูงขึ้น และมีผลกระทบกับ โปรแกรมประเภท Real-Time Application ที่ทำงานโดย IP based ดังนั้น เพื่อให้การทำงาน สามารถทำต่อไปได้โดยไม่ติดขัด วิทยานิพนธ์นี้จึงได้นำกระบวนการทำ Mobile IPv6 Handoff ที่มีกำหนดเป็นมาตรฐานมาปรับปรุง โดยยกเลิกการทดสอบ home address กับ Care-of address และแก้ไขให้ทำการรับส่งกุญแจให้เรียบร้อยก่อนที่จะมีการย้ายระบบเครือข่ายจริง ๆ โดยใช้ แนวคิดของ Kerberos นั่นคือ ให้ Home Agent เปรียบเสมือนศูนย์กลางในการสร้างกุญแจที่ใช้ในการติดต่อสื่อสารในช่วงเวลานั้น ๆ และให้มีการแลกเปลี่ยนกุญแจกันก่อนที่จะมีการย้ายระบบเครือข่ายจริง ๆ เพื่อเพิ่มระดับความปลอดภัยในการติดต่อสื่อสารให้มากขึ้น และแก้ปัญหาการเก็บกุญแจจำนวนมาก ๆ อีกด้วย ซึ่งการทำ handoff โดยใช้วิธี Kerberos และ Pre-registrations นั้น จากผลการทดลองพบว่า เกิด handoff delay time น้อยที่สุด เมื่อเทียบกับวิธีการอื่น ๆ

เมื่อเปรียบเทียบข้อดีข้อเสีย พบว่าวิธี ECBU มีข้อดีคือ ไม่จำเป็นต้องมีการกำหนด Pre-Shared Key ระหว่าง Home Agent กับ Correspondent Node ก่อน ล่วงหน้า เพราะ การส่ง packet ติดต่อกันระหว่าง Home Agent กับ Correspondent Node นั้น ใช้วิธีการสร้าง Secret Key แบบ Diffie-Hellman [17] โดยแนบ Certificated ต่อท้ายไปด้วย แต่มีข้อเสียคือ ใช้เวลาใน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การ ตรวจสอบผู้ใช้นานกว่าใช้วิธีการติดต่อแบบ Secret และต้องจัดการเกี่ยวกับ Certificated management อีกด้วย

วิธีที่ทาง Mobile IPv6 working group กำหนดคือ Return Routability มี ข้อดี คือ เป็นวิธีมาตรฐาน มีความซับซ้อนน้อยกว่าวิธีการอื่น ๆ ครอบคลุมกับการใช้งานในหลาย ๆ กรณี แต่มีข้อเสียคือ ใช้เวลาในการทำ Handoff นานกว่าที่วิธีที่ได้นำเสนอ

วิธีที่ได้นำเสนอคือ Kerberos and Pre-Registration มี ข้อดีคือ ใช้เวลาในการ Handoff น้อยกว่า วิธีการอื่น ๆ เหมาะสำหรับ Real-Time Application แต่มีข้อเสียคือ มีความยุ่งยากซับซ้อนกว่าวิธีอื่น ๆ และมีข้อจำกัด คือ ต้องมีการกำหนดกุญแจที่ต้องมีการแลกเปลี่ยนแบบ out-of-band ที่จำเป็นต่อระบบ ระหว่าง Mobile Node <–> Home Agent, Mobile Node <–> Access Router, Home Agent <-> Access Router และ Home Agent <-> Correspondent Node ซึ่งอาจจะไม่เหมาะกับสภาพแวดล้อมอื่น ๆ

7.3 ข้อเสนอแนะ

วิทยานิพนธ์นี้ นำเสนอ การทำ Handoff ที่มี latency ต่ำ และคงไว้ซึ่งความปลอดภัย โดยประยุกต์ Kerberos and Pre-Registration หาก พิจารณาที่ latency ของการทำ Handoff จะประกอบไปด้วย เวลาการทำงานในหลาย ๆ ส่วน คือ เวลาในการประมวลผล packet, เวลาในการตรวจสอบย้ายระบบเครือข่าย , เวลาในการค้นหา Access Router และ เวลาในการส่งข้อมูล Binding Update ในหัวข้อวิจัยเกี่ยวกับเวลาในการประมวลผล packet นั้นอาจจะไม่มีความน่าสนใจมากนัก เนื่องจากว่าในปัจจุบันนี้ ความเร็วของหน่วยประมวลได้พัฒนาไปอย่างรวดเร็ว ส่วนในเรื่อง เวลาในการตรวจสอบการย้ายเครือข่ายและ ค้นหา Access Router นั้น น่าสนใจและอาจพัฒนาให้ดีขึ้นได้ เช่น โมเดลเวลาในการรอรับ Router Advertisement จาก Access Router ให้มีความฉลาดและ เหมาะกับสภาพแวดล้อมนั้น ๆ

เรื่องการควบคุมความผิดพลาดในการส่งข้อมูล เพราะในระบบเครือข่ายไร้สาย โอกาสที่ข้อมูลจะสูญหายหรือผิดพลาดนั้น เกิดขึ้นได้มากกว่า ระบบเครือข่ายแบบใช้สาย

เรื่องการตัดสินใจ Handoff ของ Mobile Node ซึ่งอาจจะพิจารณาจากปัจจัยต่าง ๆ เช่น ระยะทาง, ความแรงของสัญญาณ และ งานที่ Base station กับกำลังประมวลผลอยู่ในช่วงเวลานั้น เป็นต้น หากมองในสภาพแวดล้อมที่มีระบบจราจรหนาแน่น และมีผู้ใช้งานระบบเครือข่ายเป็นจำนวนมาก เรื่องความน่าจะเป็นในการ Handoff แล้ว ไม่สามารถติดต่อระบบเครือข่ายได้ ก็เป็นจุดที่น่าสนใจ โดยนำมาประยุกต์ใช้กับงานวิจัยที่ได้ทำมา เพื่อให้ได้ผลการทดลองที่ถูกต้องมากยิ่งขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เอกสารอ้างอิง

[1] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6, RFC 3775", June 2004

[2] W. Simpson, "IPng Mobility Considerations, RFC 1688", August 1994

[3] F. Teraoka, "Options for Mobility Support in IPv6", January 1996

[4] J. Kohl, C. Neuman, "The Kerberos Network Authentication Service", September 1993

[5] J. Arkko, F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents, RFC 3776", June 2004

[6] F. Dupont, "Using IPsec between Mobile and Correspondent IPv6 Nodes", IETF draft, work in progress

[7] Feng BAO, Robert DENG, Jianying ZHOU, "Certificate-based Binding Update Protocol (CBU)", IETF draft, work in progress

[8] Ying QIU, Jianying ZHOU, Feng BAO, "Protect All Traffic Channels in Mobile IPv6 Network", WCNC 2004 IEEE

[9] D. Solomon, Mobile IP The Internet Unplugged, Prentice Hall, New Jersey, 1998

[10] J. Postel, "Internet Protocol", RFC 791, September 1981

[11] T. Schmidt, M. Wahlisch, "Performance Analysis of Multicast Mobility in a Hierarchical Mobile IP Proxy Environment", TERENA Networking Conference Rhodes, 2004

[12] T. Schmidt, M. Wahisch, "Roaming Real-Time Applications – Mobility Services in IPv6 Networks, Proceedings TERENA Networking Conference Zagreb, 2003

[13] A. Percy, "Understanding Latency in IP Telephony", Feb 1999

[14] "One-way transmission time", ITU-T Recommendation G.114, May 2000

[15] T. Narten, E. Nordmark and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6), RFC 2461", Dec 1998

[16] Linux Mobile IPv6, http://www.mipl.mediapoli.com/

[17] W. Diffie, M. E. Hellman, "New directions in cryptography", IEE Trans, 1976, pp.644-654

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

[18] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, vol. 21, pp. 120-126, Feb 1978

[19] E. Vollset, "Java network simulator", http://jns.sourceforge.net/

[20] J. Blommers, "Practical Planning for Network Growth", Hewlett Packard, Prentice Hall PTR Upper Saddle River, New Jersey 07458, 1996

[21] NS-2 Network Simulator, http://www.isi.edu/nsnam/ns/

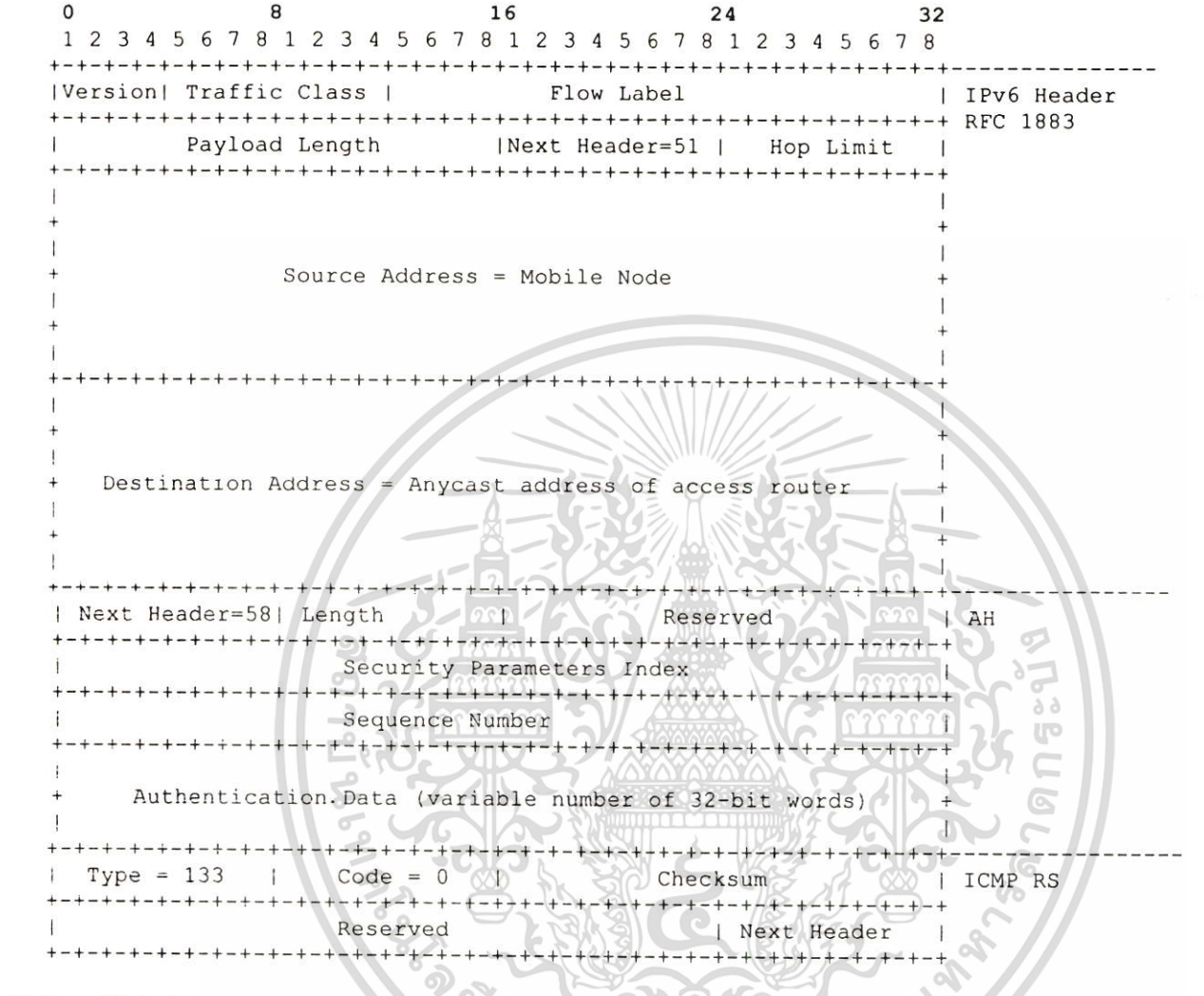
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Return Routability Protocol Header

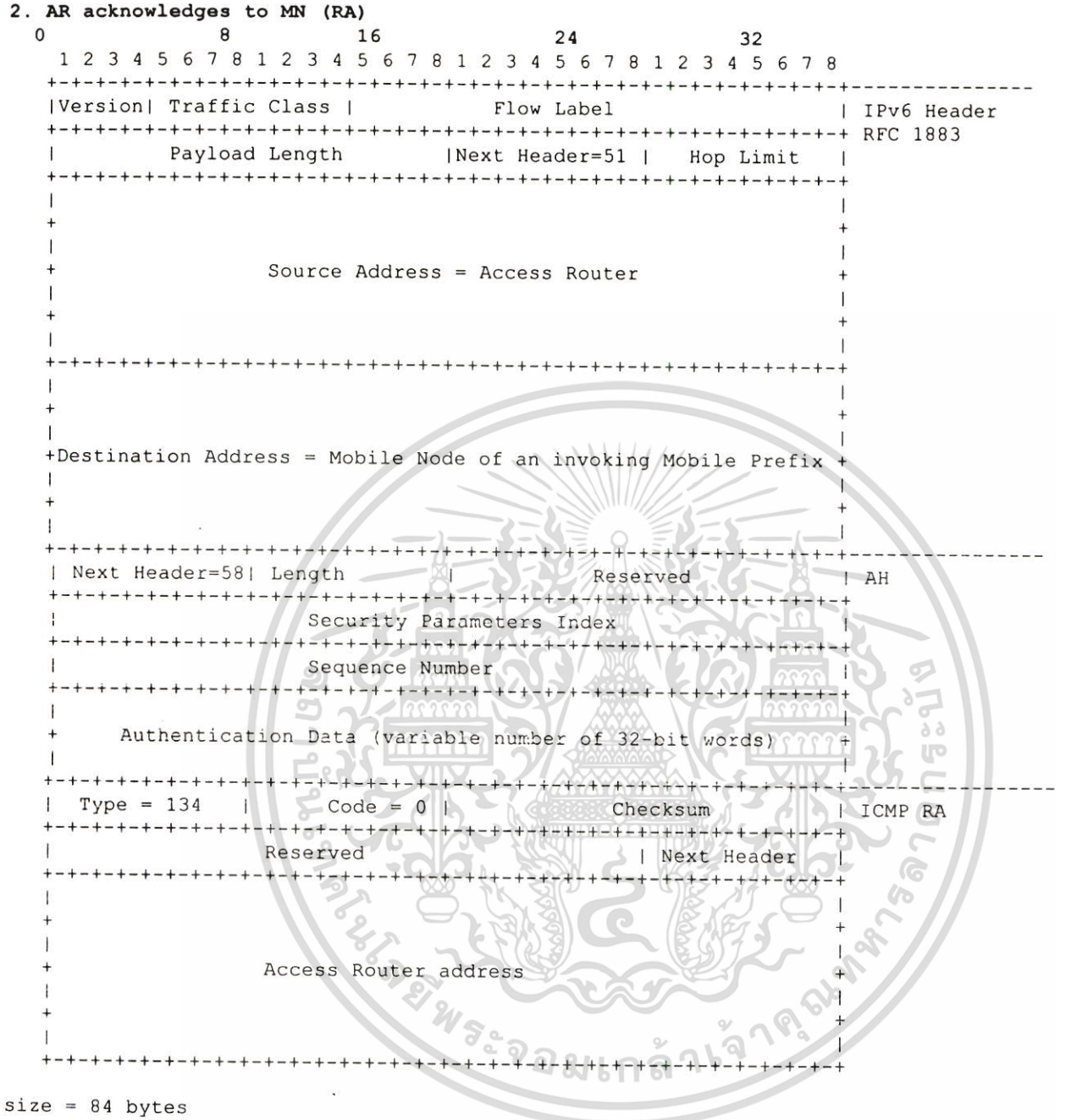
1. MN sends RS to AR



size = 68 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

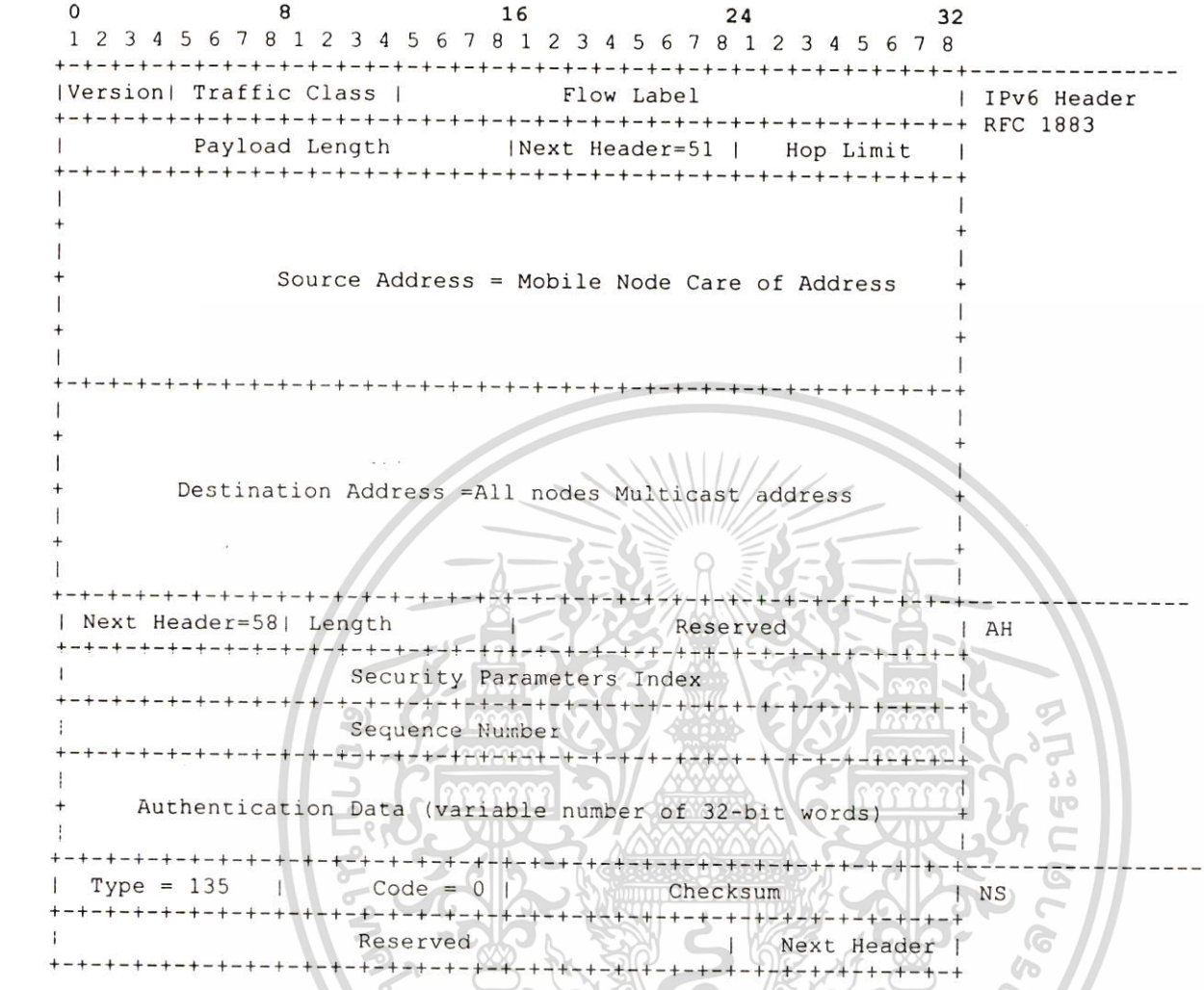
2. AR acknowledges to MN (RA)



size = 84 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. MN sends NS to all nodes



size =68 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4. AR acknowledges to MN (NA) (if duplicate)

size =84 bytes

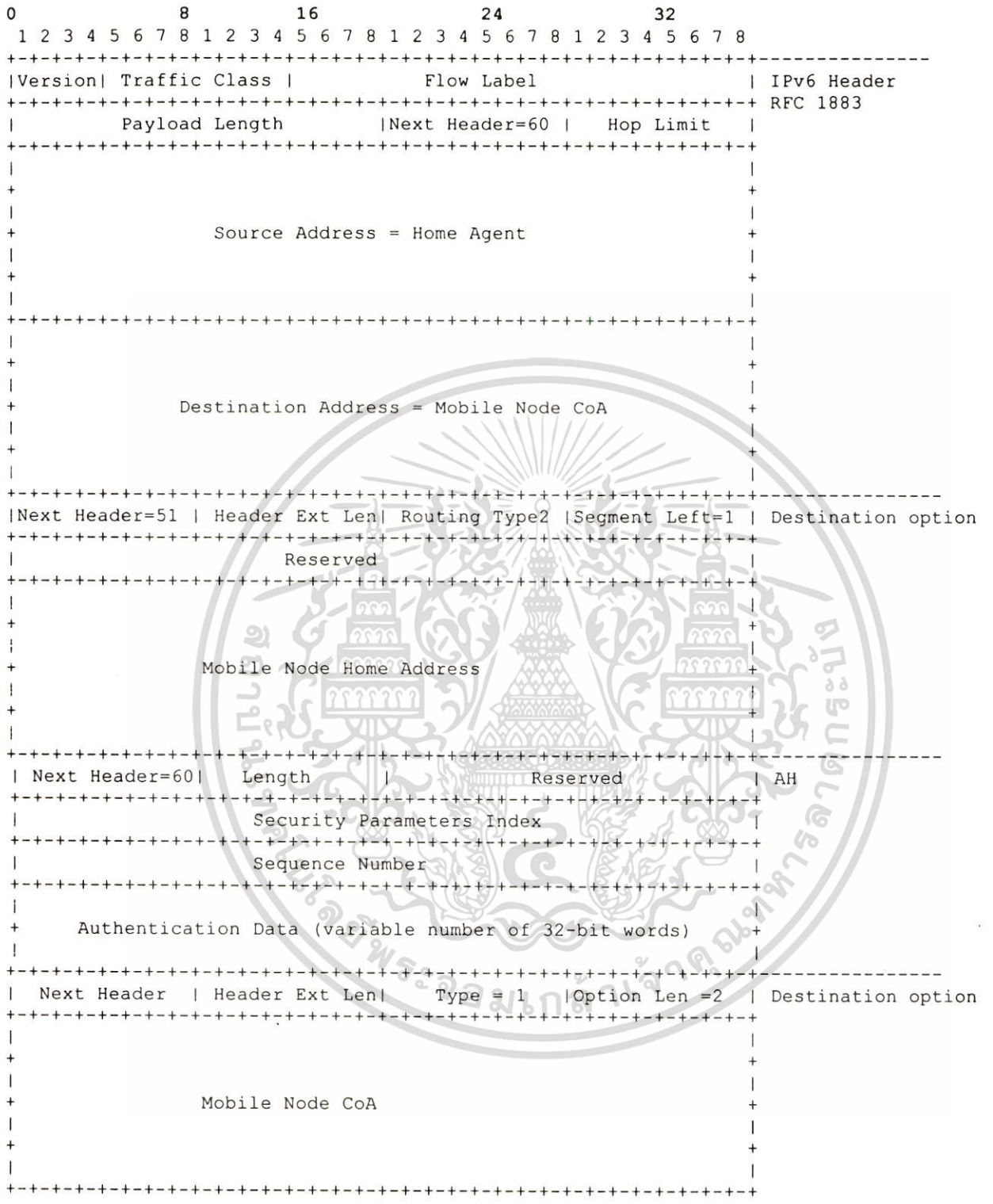
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5. MN sends BU to HA

size = 80 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

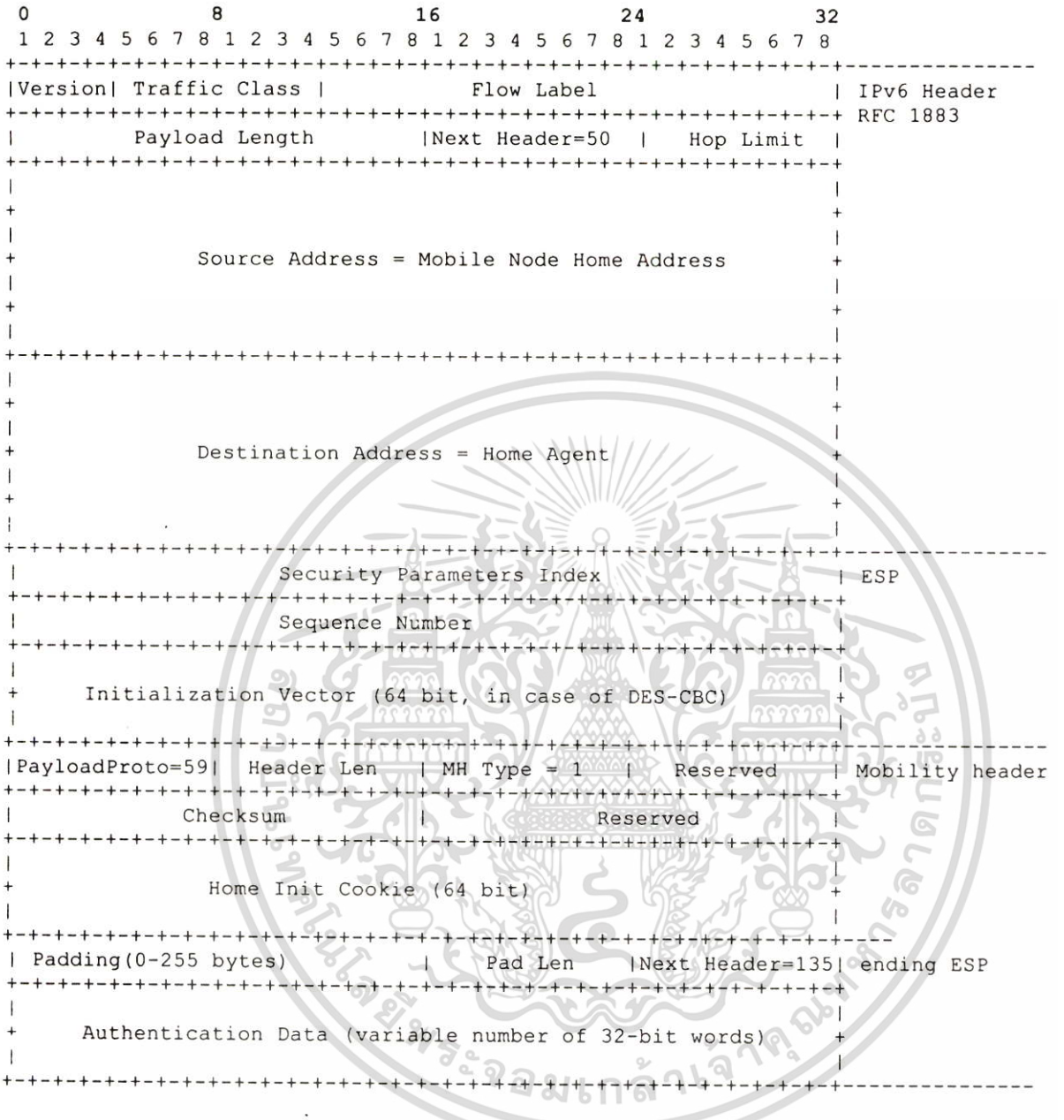
6. HA acknowledges BA to MN



size = 104 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

7. MN send HoTI to HA



size = 84 byte

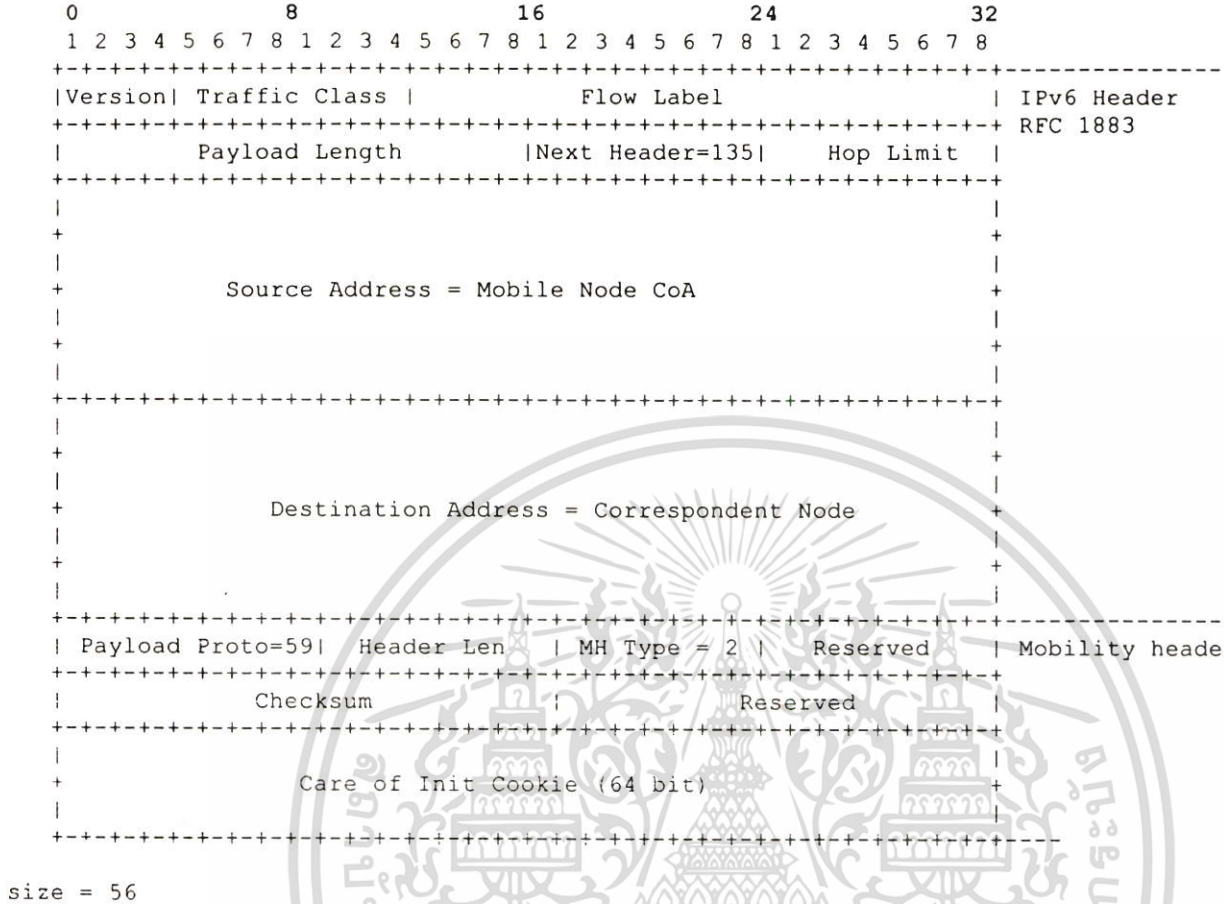
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

8. HA forward HoTI to CN

size = 84

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

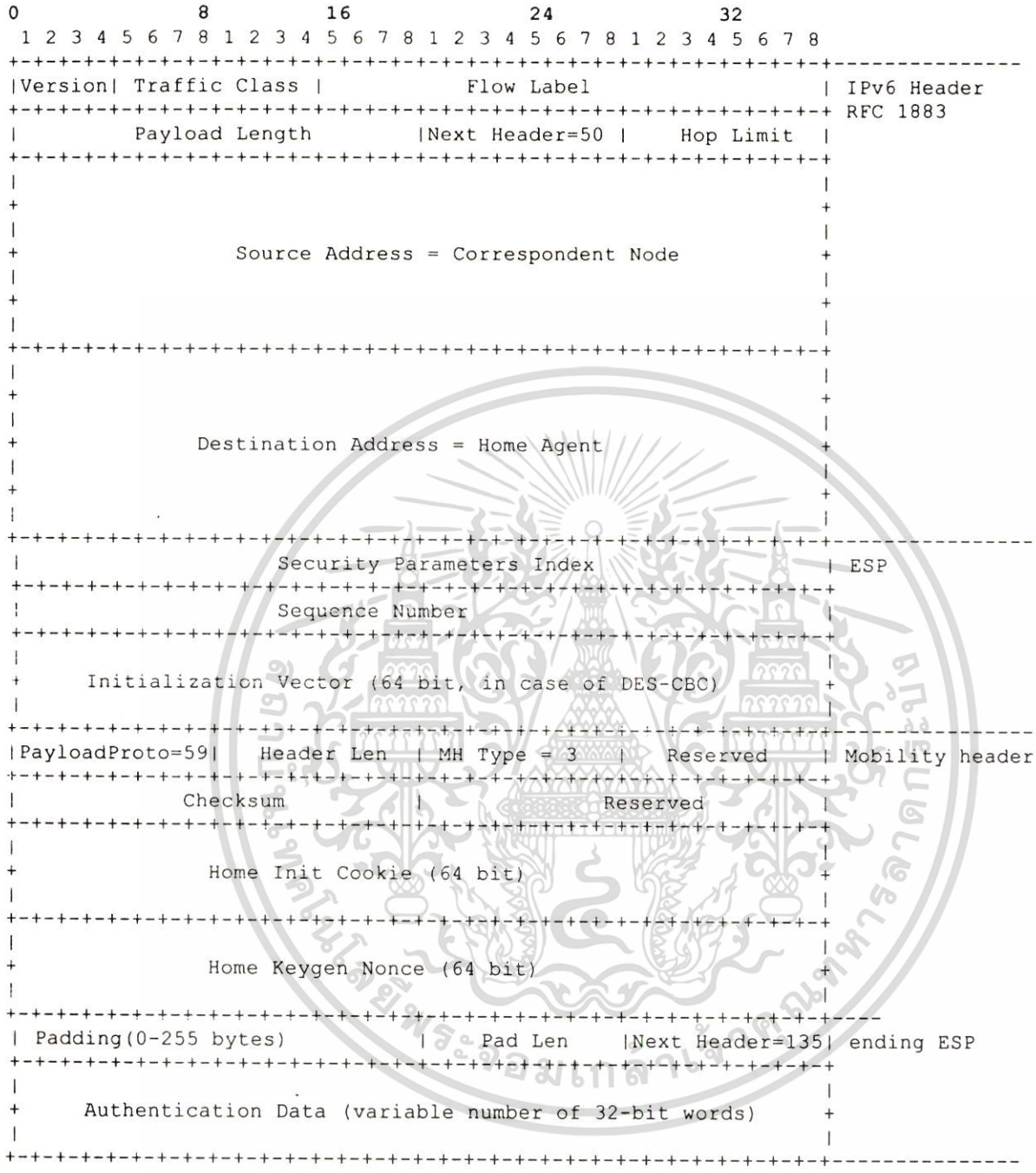
9. MN send CoTI to CN



size = 56

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

10. CN acknowledge HoT to HA



size = 92 byte

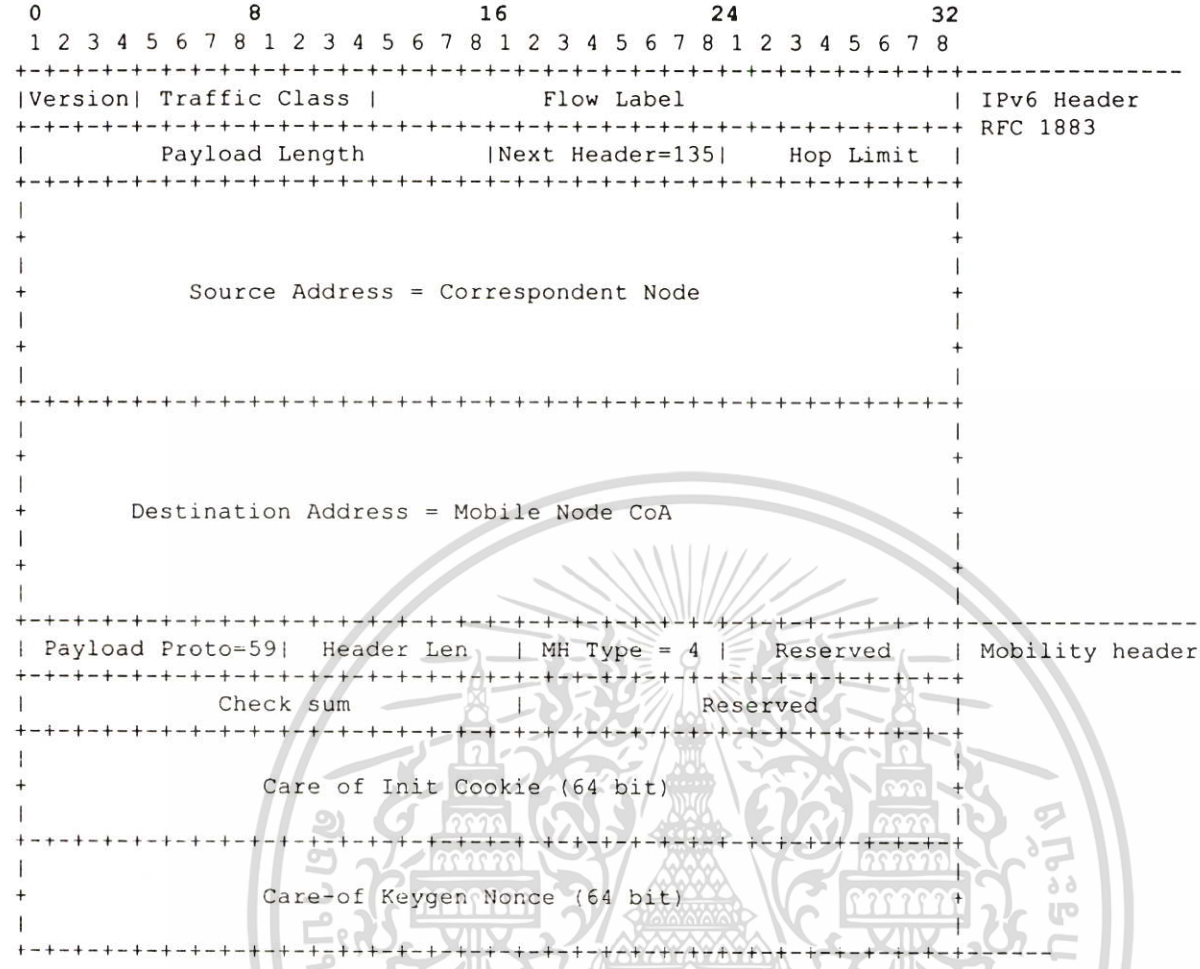
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

11. HA forward HoT to MN

size = 92 byte

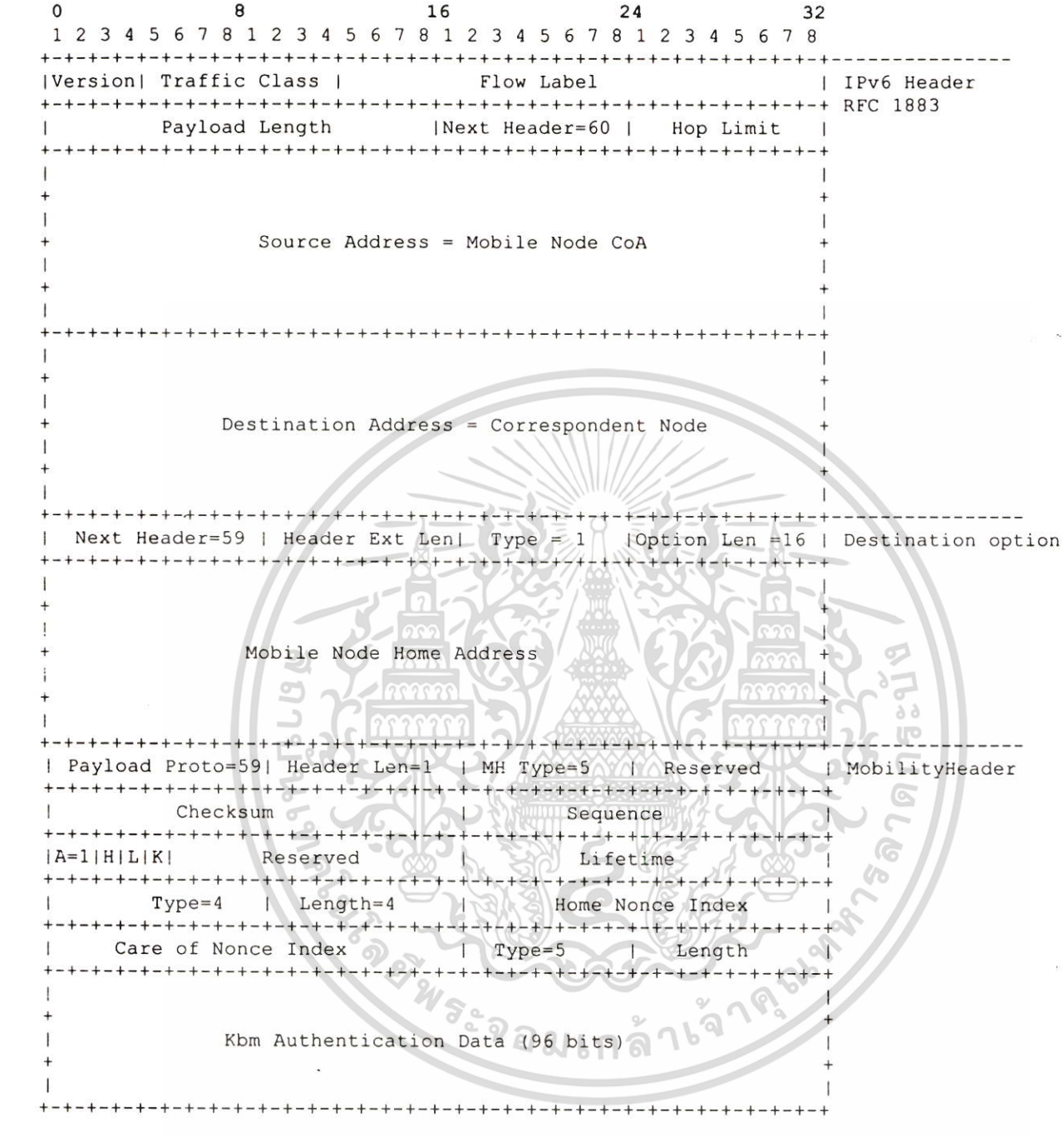
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

12. CN acknowledge CoT to MN



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

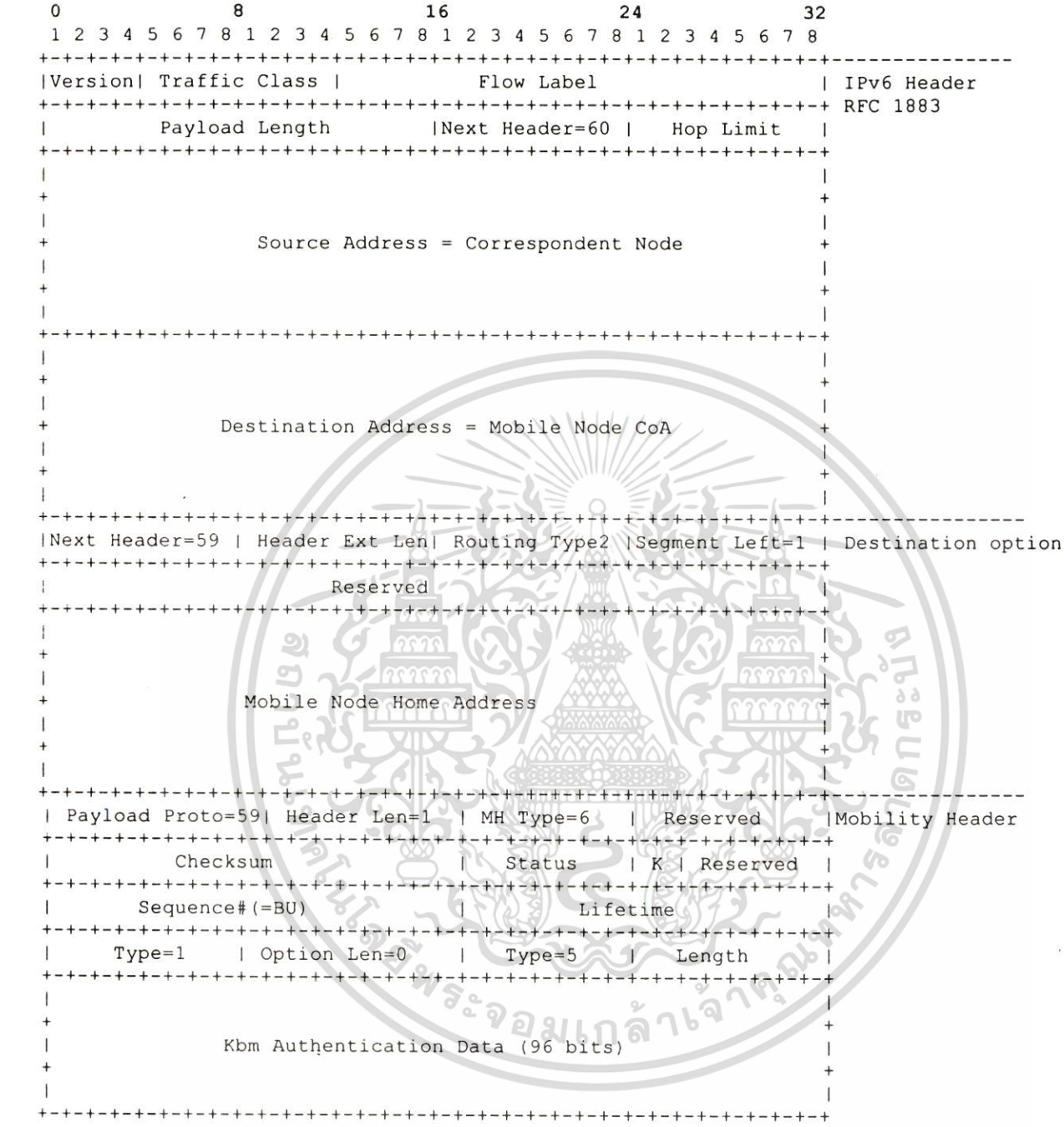
14. MN send BU to CN



size = 92 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

15. CN sends BA to MN



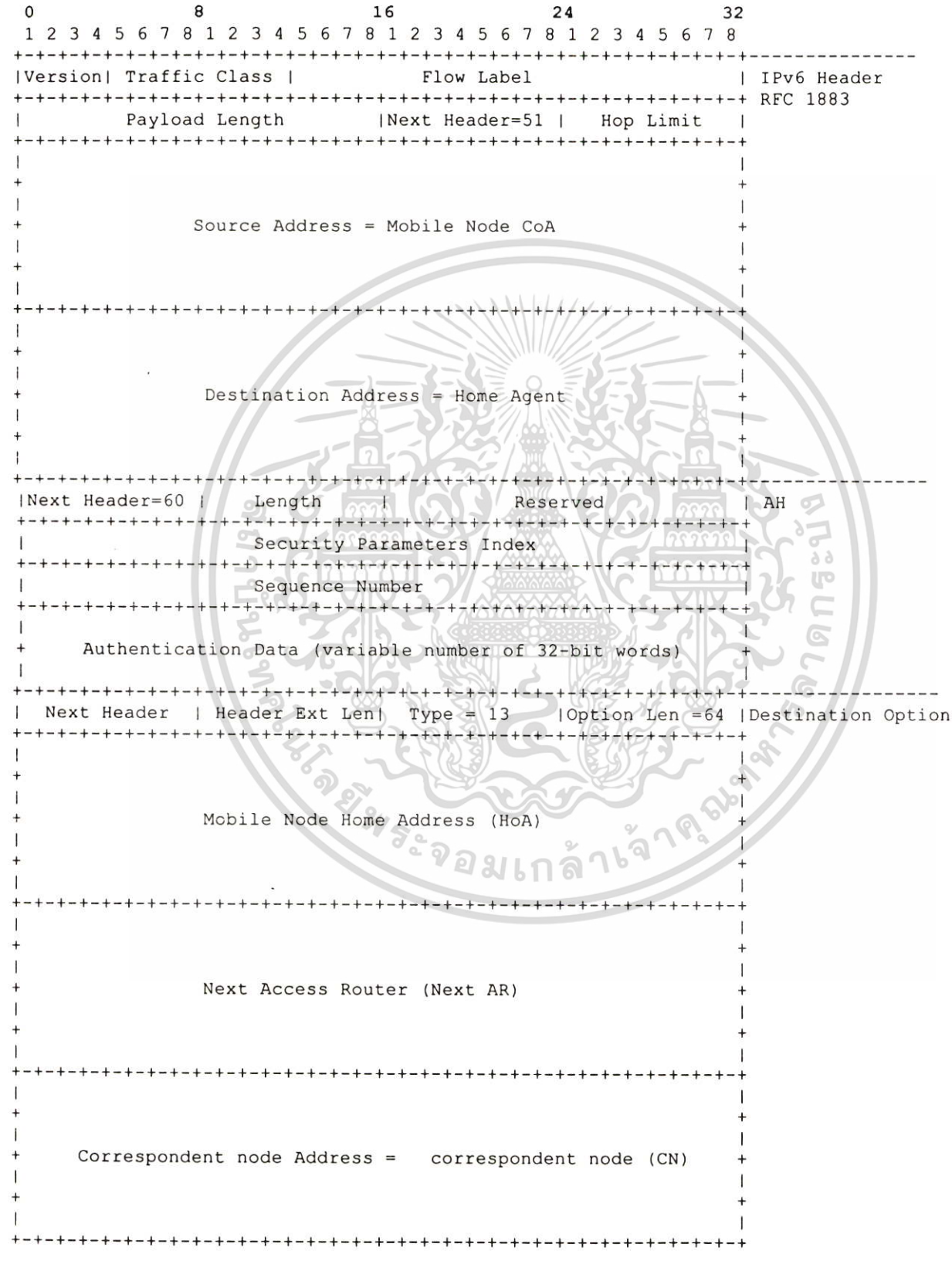
size = 92 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Kerberos and Pre-Registrations Protocol Header

hase #1

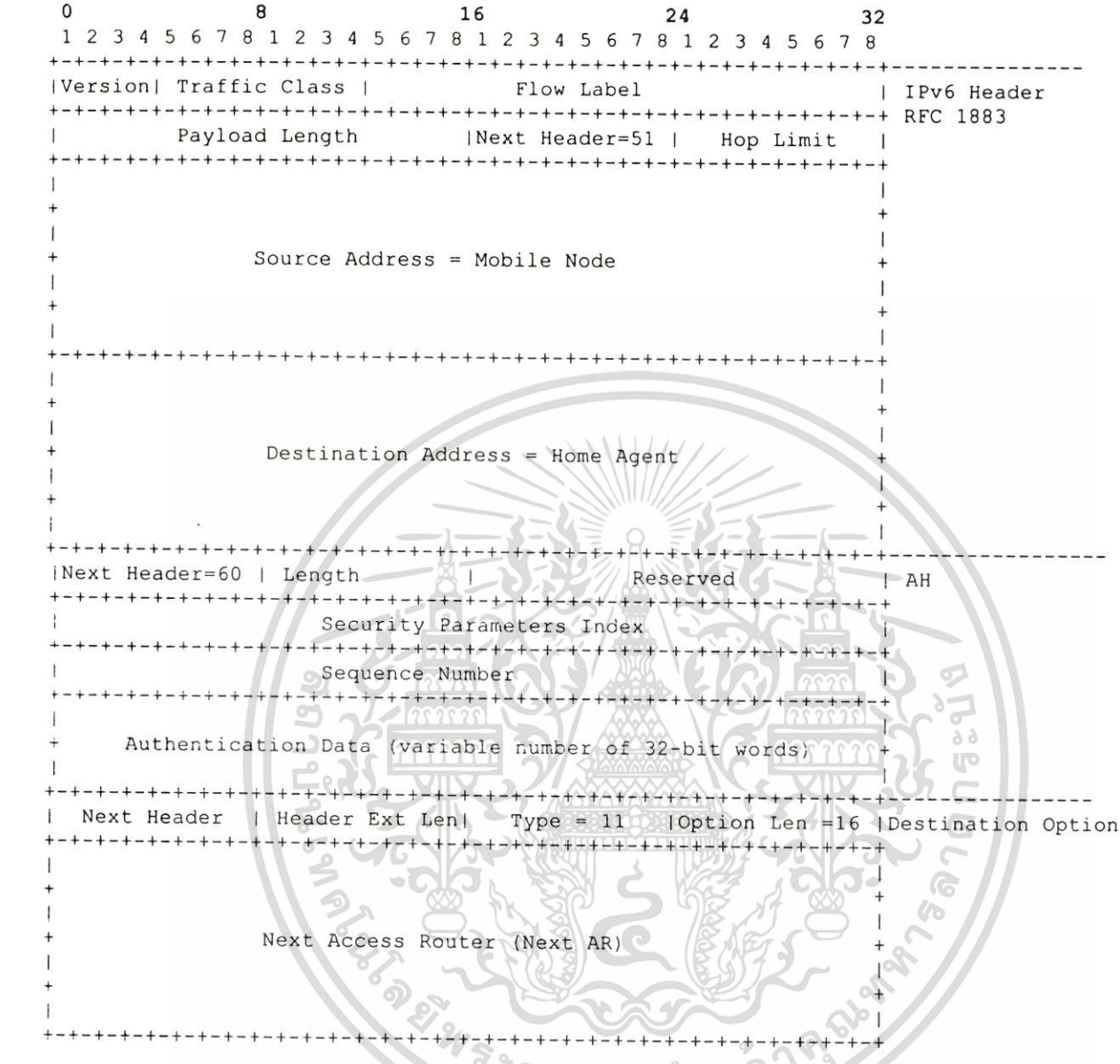
MN requests session key from HA (ReqHA)



size = 112 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

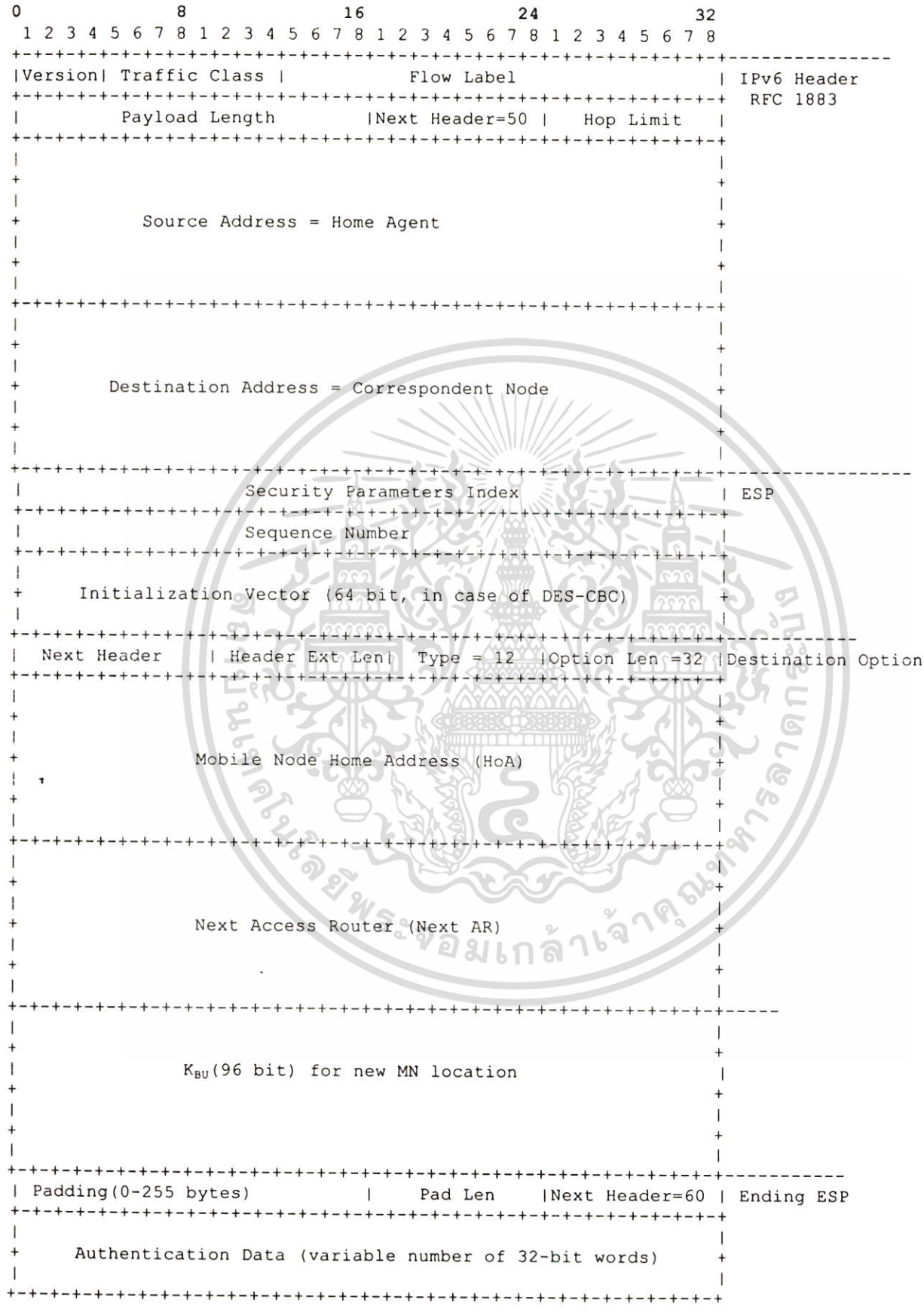
HA acknowledges to MN (RepMN)



size = 80 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

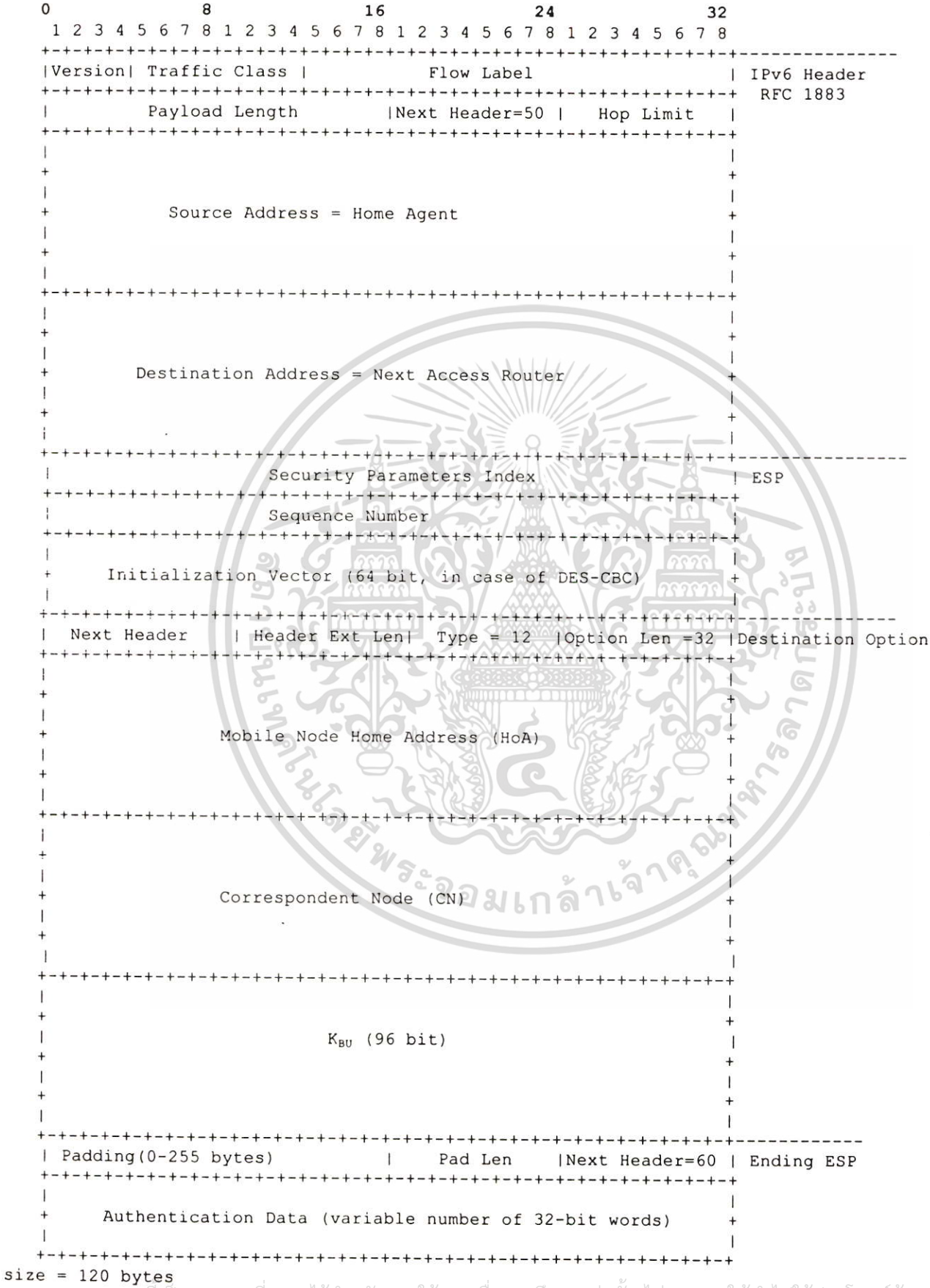
HA sends session key to CN



size = 120 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

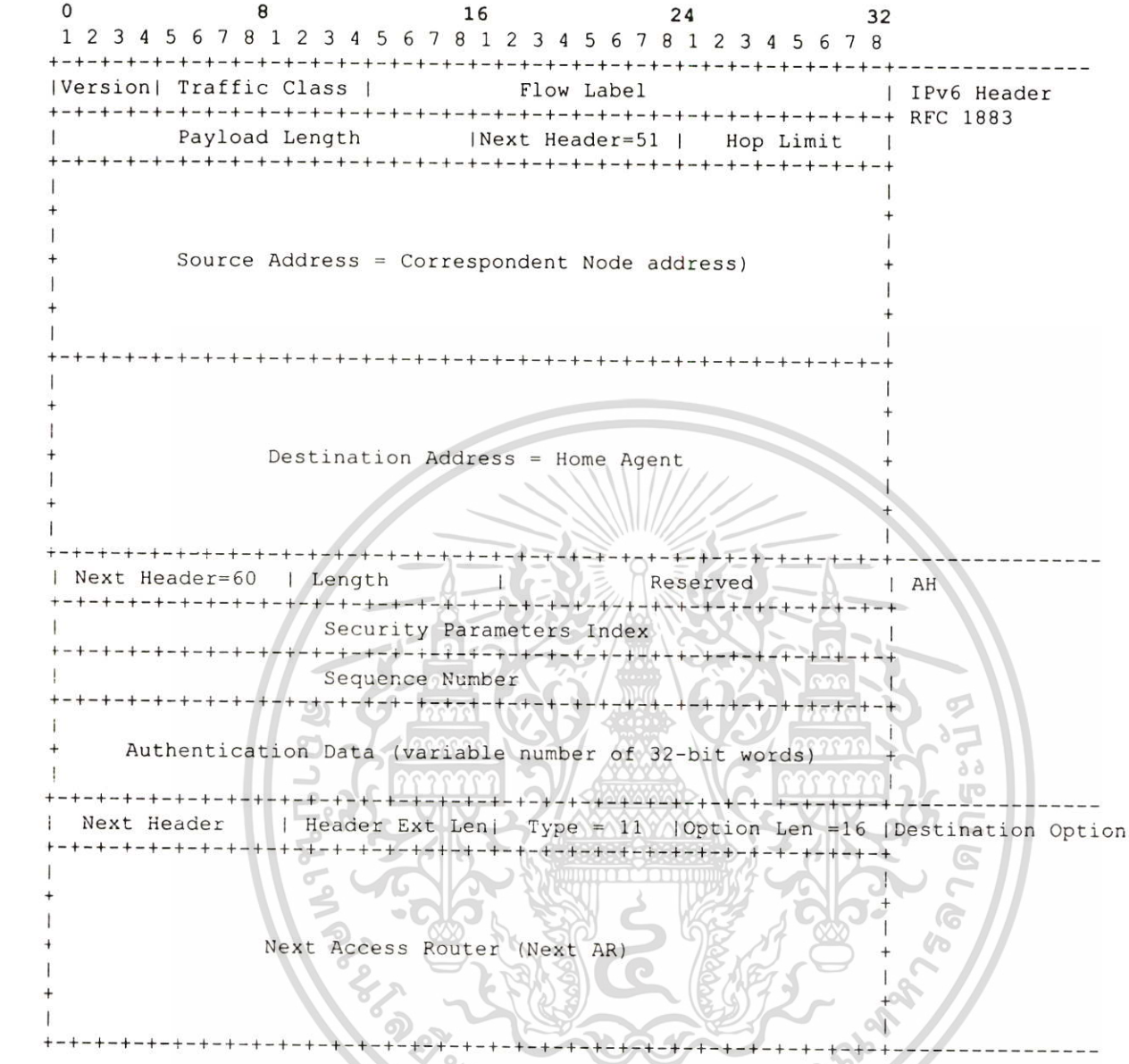
HA sends session key to ARs



size = 120 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

CN acknowledges to HA



size = 80 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

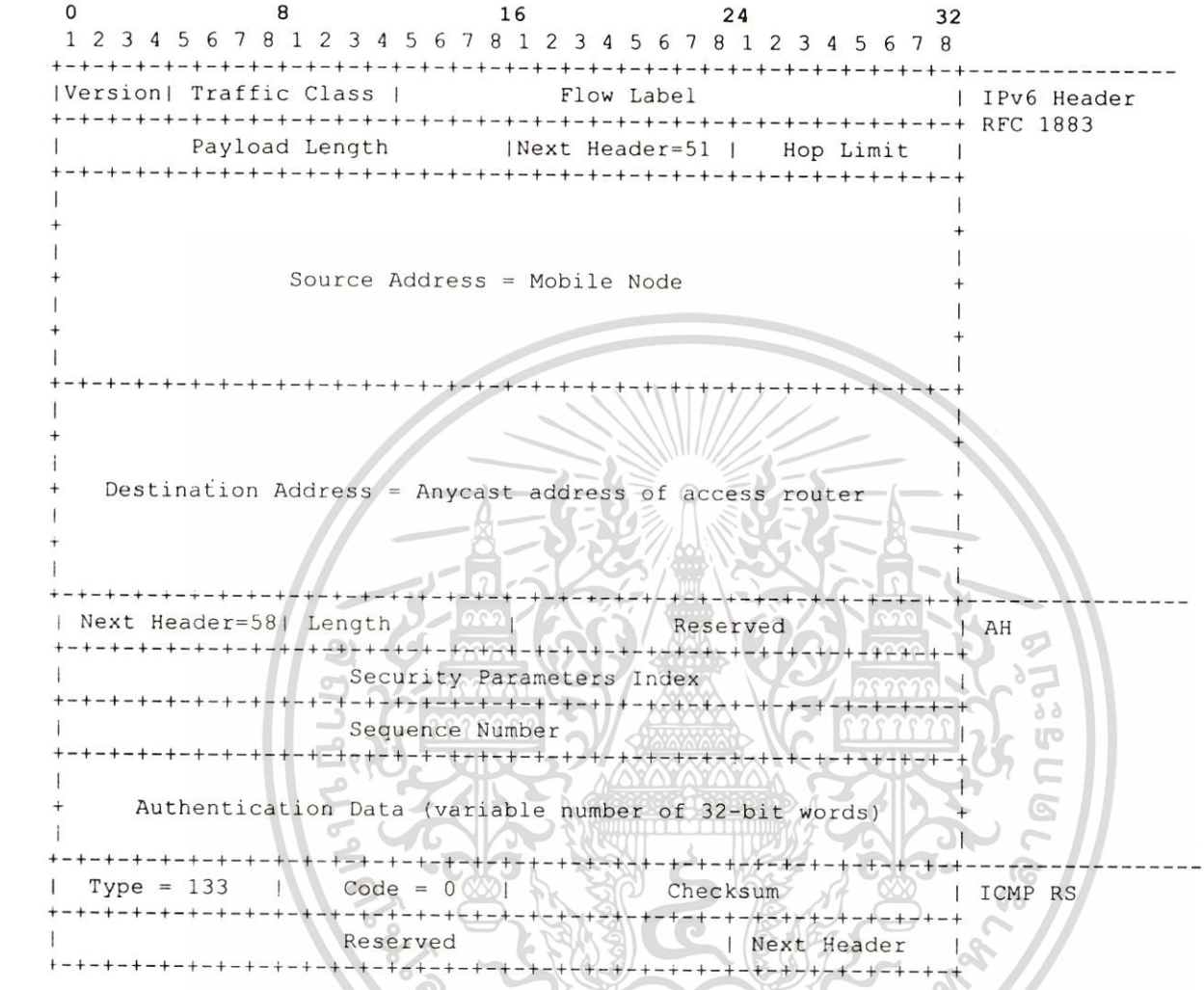
ARs acknowledges to HA

size = 64 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Phase #2 (Handoff)

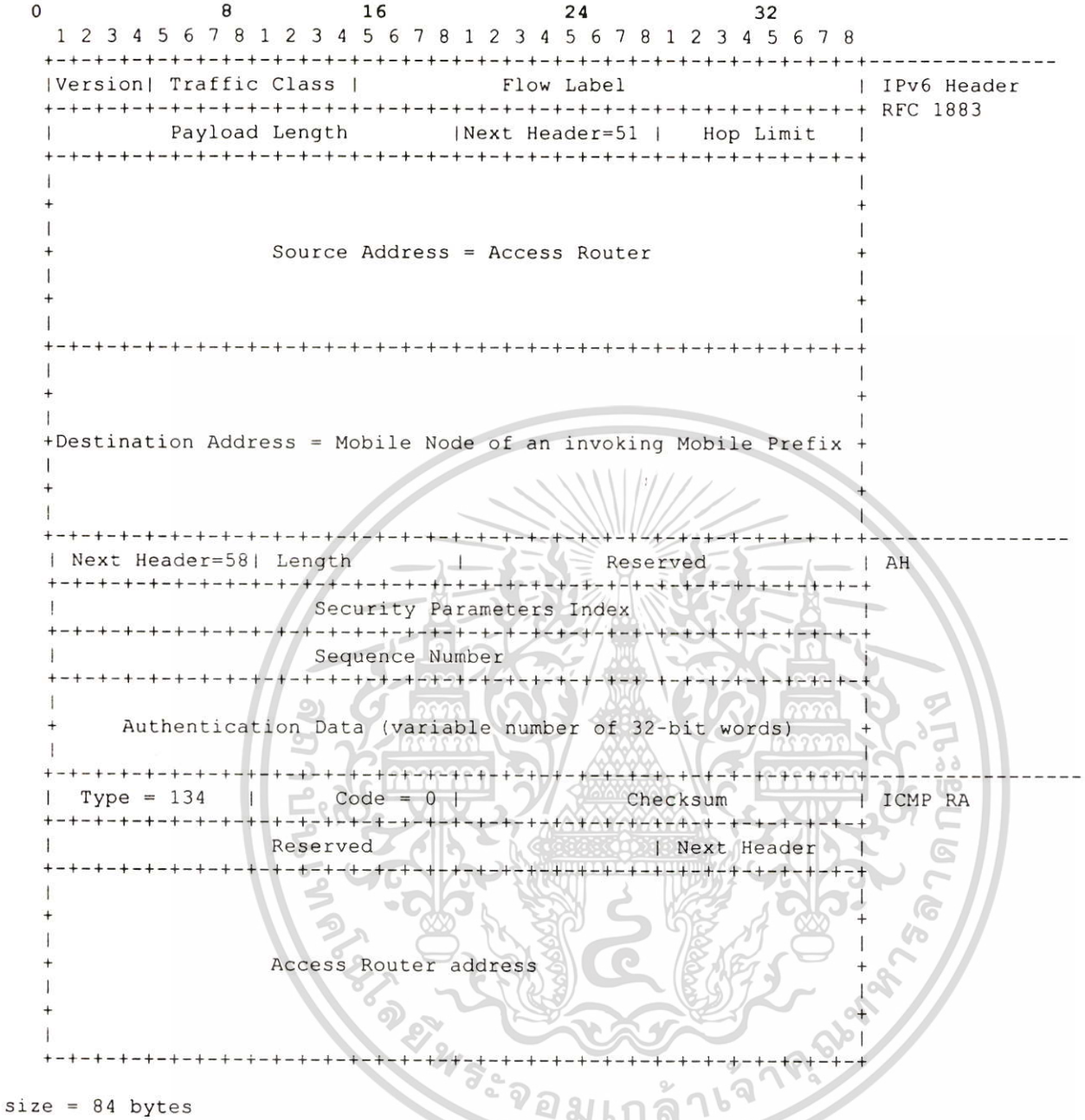
1. MN sends RS to AR



size = 68 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

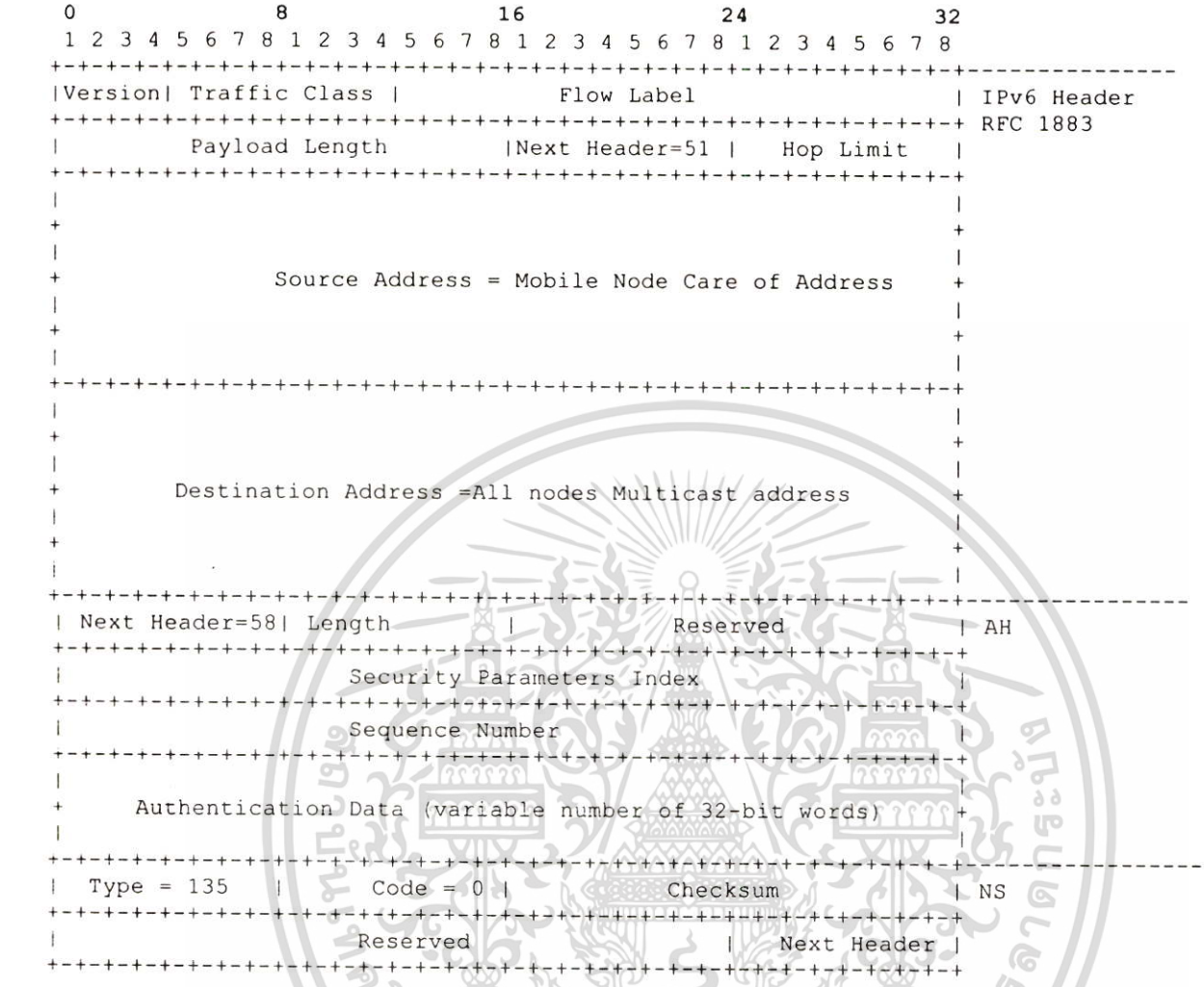
2. AR acknowledges to MN (RA)



size = 84 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. MN sends NS to all nodes



size =68 bytes

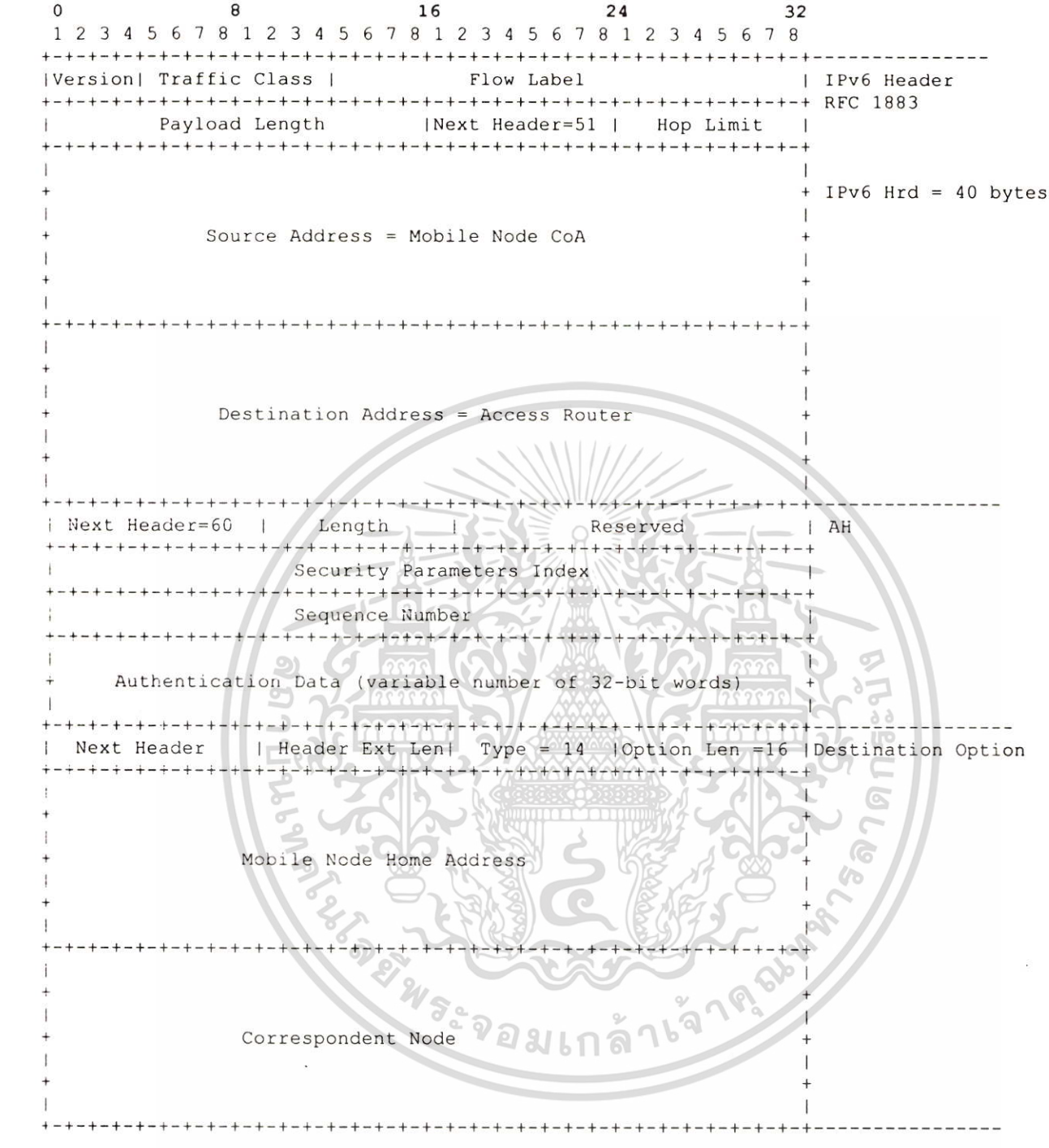
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4. AR acknowledges to MN (NA) (if duplicated)

size = 84 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

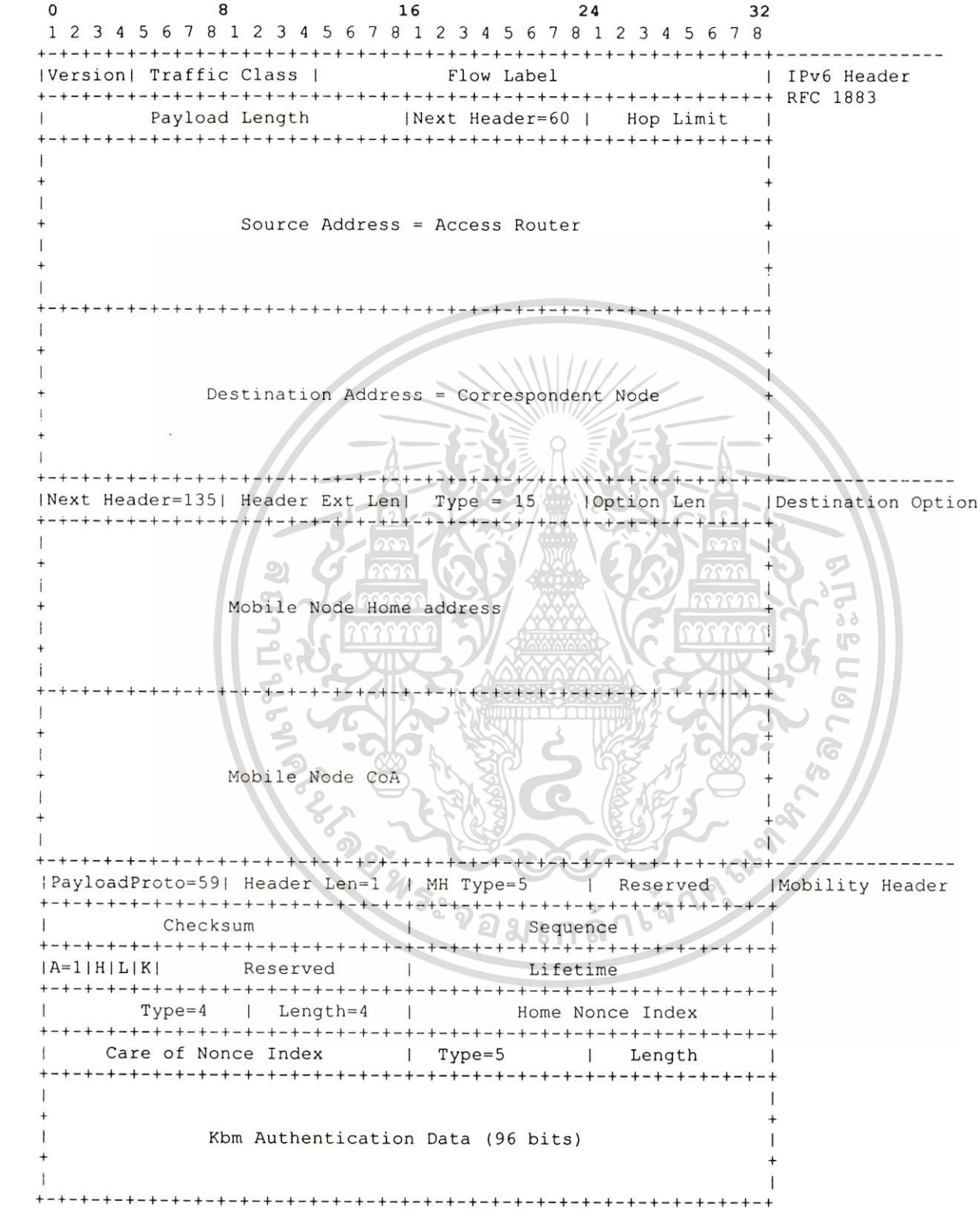
5. MN requests AR to forward the pre-registration BU to CN



size =96 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

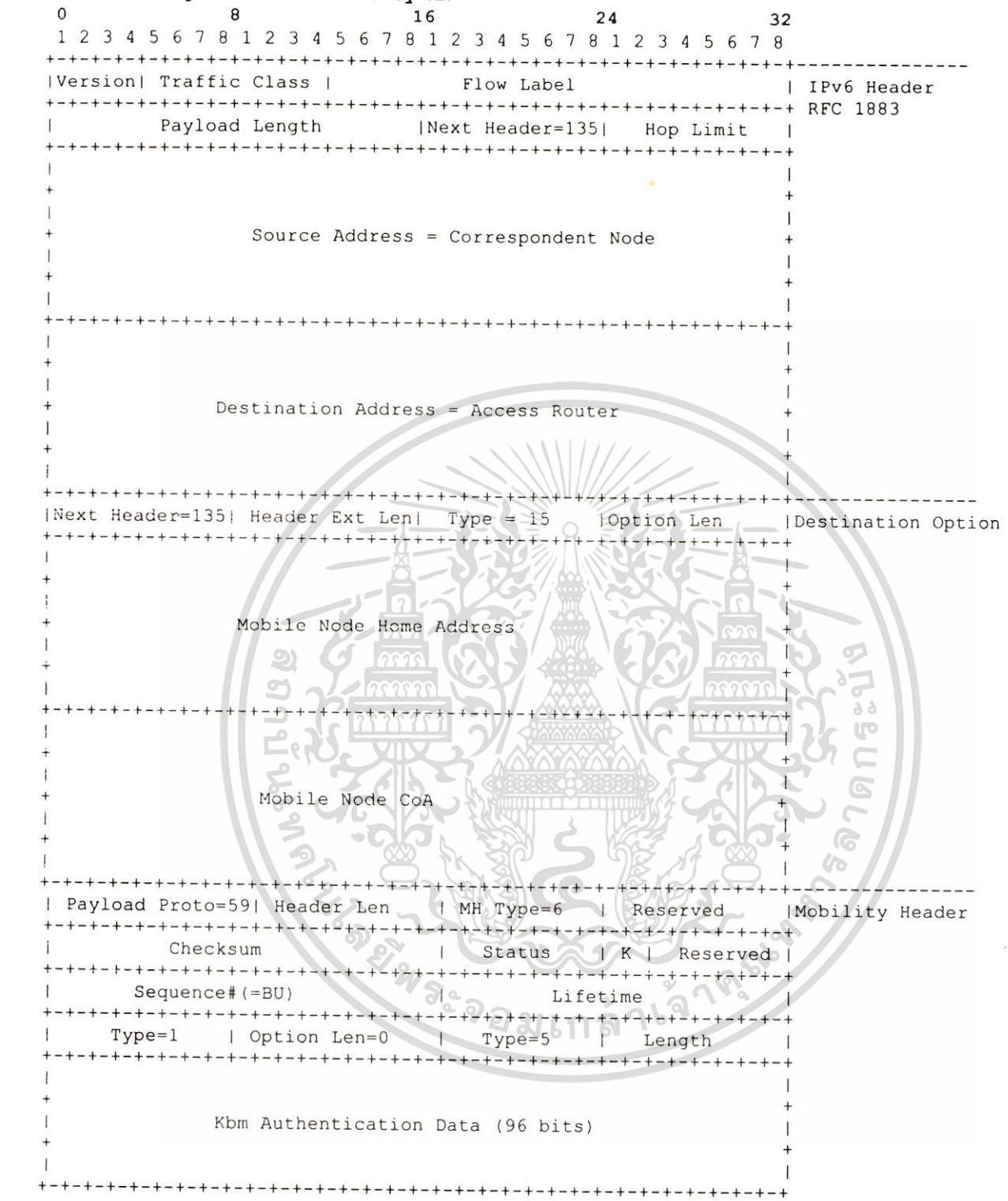
6. AR sends BU to CN



size = 108 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

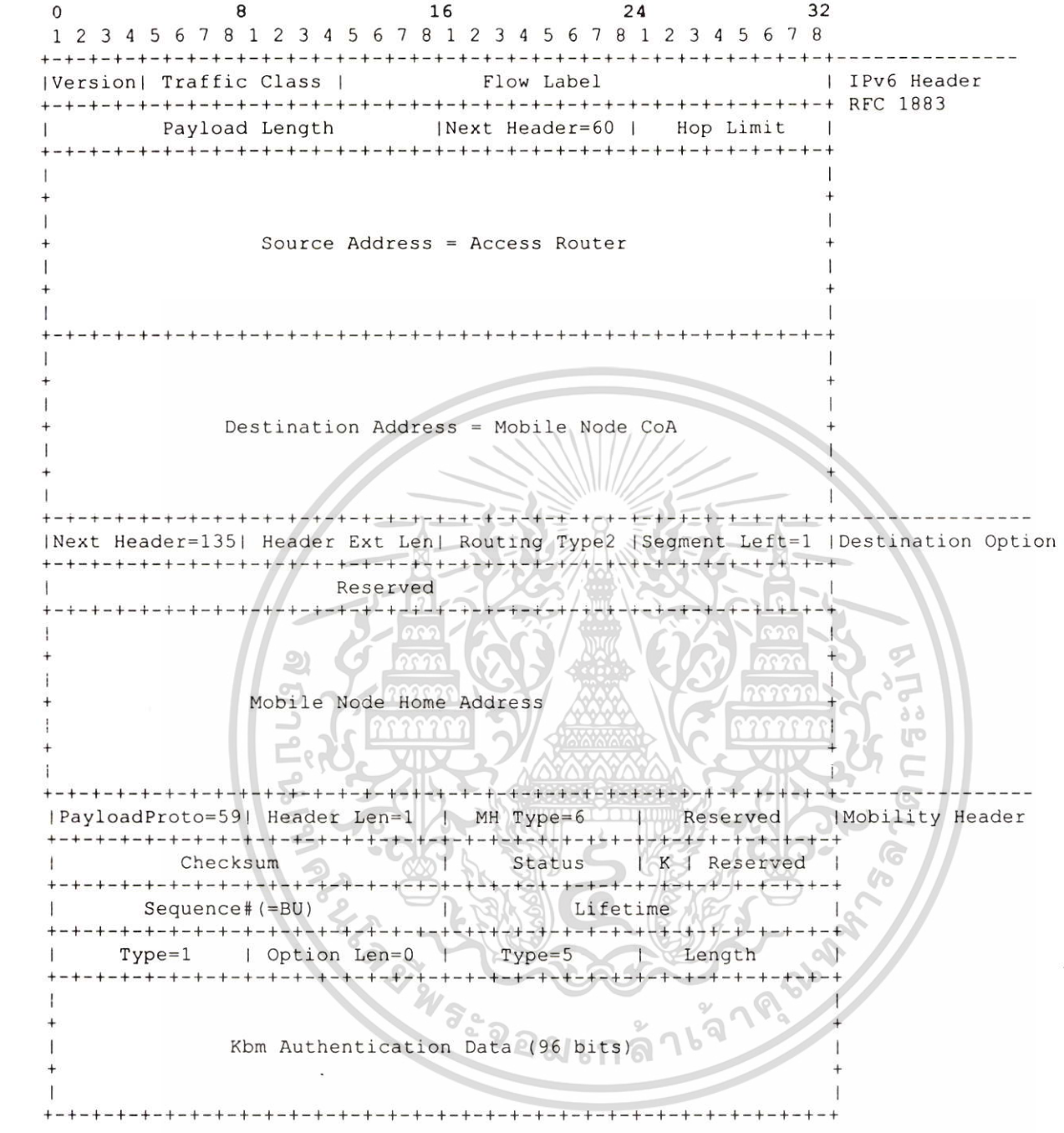
7. CN acknowledges to MN forward by AR



size = 104 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

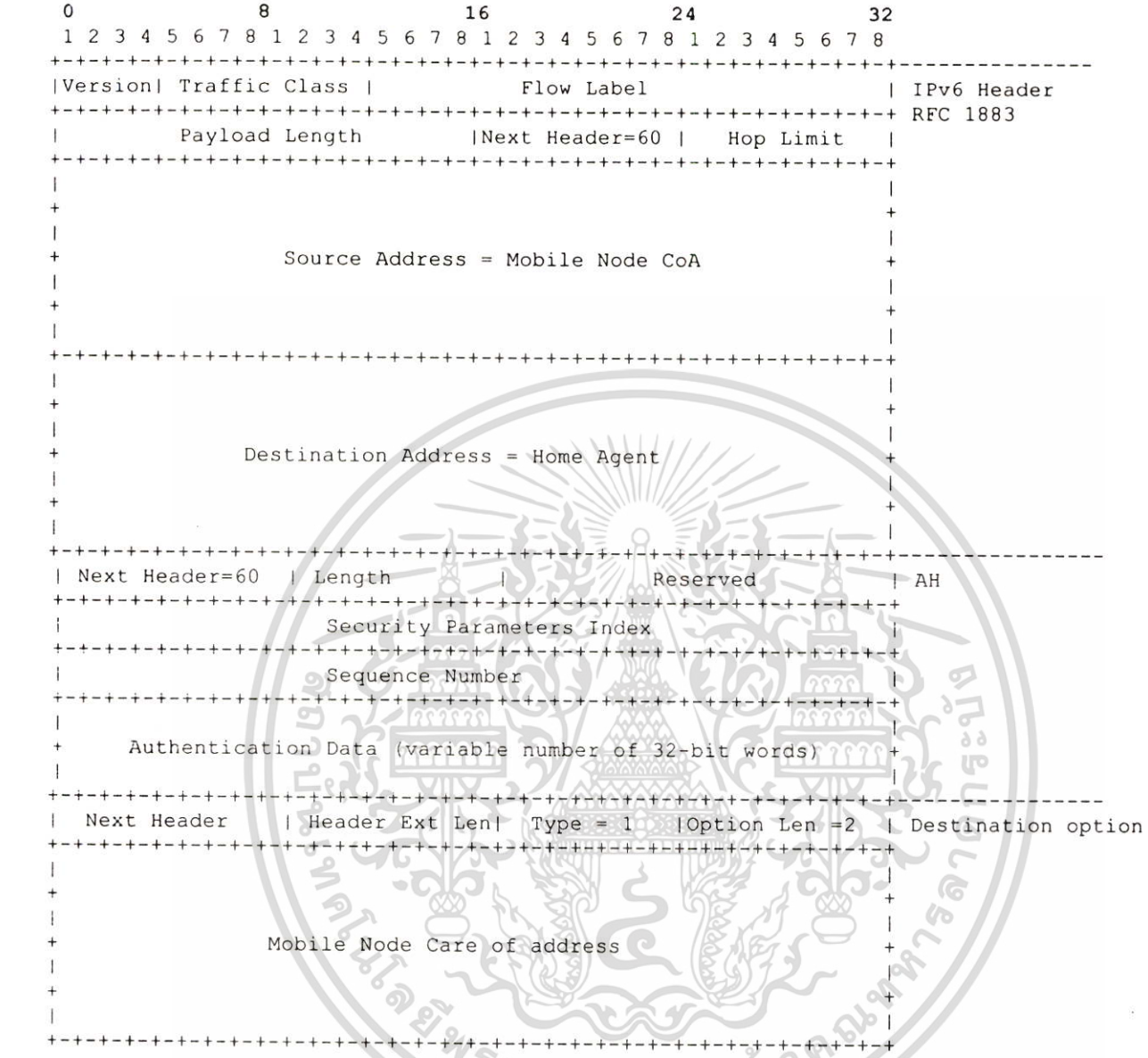
8. AR sends BA to MN



size = 92 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

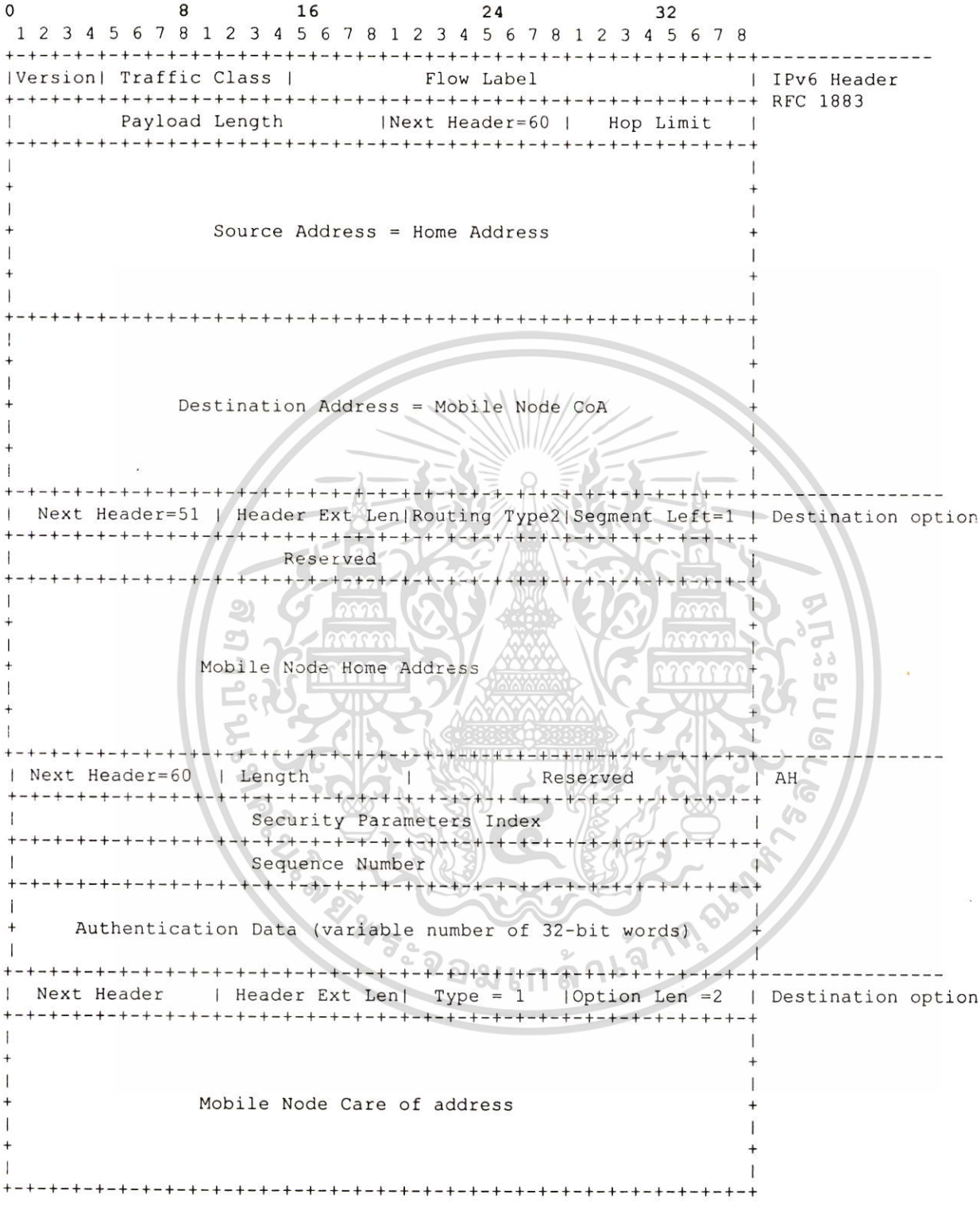
9. MN sends BU to HA



size = 80 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

10. HA acknowledges to MN

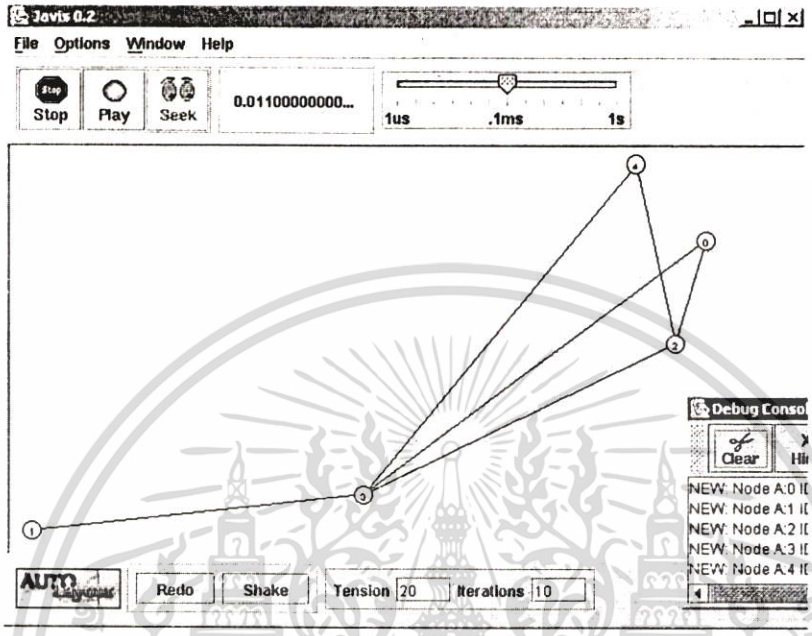


size = 104 bytes

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Java Network Simulation (JNS)

- Javis Animation Example

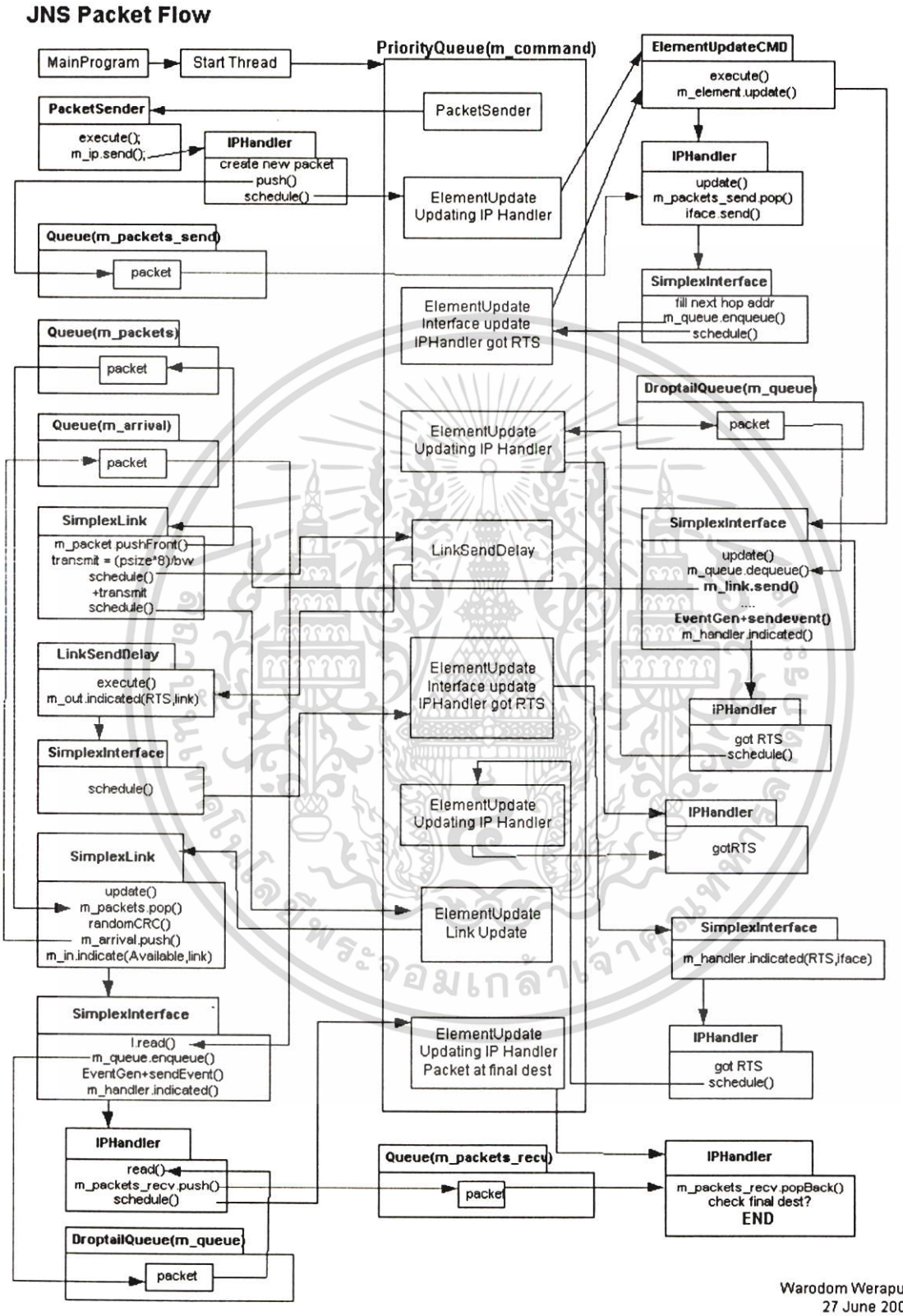


- Java Network Simulation log

```
# Trace file generated by JNS Version 1.7.
n -t * -a 0 -s 0 -S UP -v circle -c black
n -t * -a 1 -s 1 -S UP -v circle -c black
n -t * -a 2 -s 2 -S UP -v circle -c black
n -t * -a 3 -s 3 -S UP -v circle -c black
n -t * -a 4 -s 4 -S UP -v circle -c black
l -t * -s 3 -d 0 -S UP -r 10000000 -D 0.0020
l -t * -s 2 -d 0 -S UP -r 10000000 -D 0.0020
l -t * -s 3 -d 2 -S UP -r 10000000 -D 0.0020
l -t * -s 4 -d 2 -S UP -r 10000000 -D 0.0020
l -t * -s 4 -d 3 -S UP -r 10000000 -D 0.0020
l -t * -s 3 -d 1 -S UP -r 10000000 -D 0.0020
+ -t 0.0 -s 2 -d 4 -i 0 -e 72 -p udp -a 0  -c 0
- -t 0.0 -s 2 -d 4 -i 0 -e 72 -p udp -a 0  -c 0
h -t 0.0 -s 2 -d 4 -i 0 -e 72 -p udp -a 0  -c 0
+ -t 0.0020576 -s 2 -d 4 -i 0 -e 72 -p udp -a 0  -c 0
- -t 0.0020576 -s 2 -d 4 -i 0 -e 72 -p udp -a 0  -c 0
r -t 0.0020576 -s 2 -d 4 -i 0 -e 72 -p udp -a 0  -c 0
+ -t 0.0020576 -s 4 -d 2 -i 0 -e 72 -p udp -a 0  -c 0
- -t 0.0020576 -s 4 -d 2 -i 0 -e 72 -p udp -a 0  -c 0
h -t 0.0020576 -s 4 -d 2 -i 0 -e 72 -p udp -a 0  -c 0
+ -t 0.0041152 -s 4 -d 2 -i 0 -e 72 -p udp -a 0  -c 0
- -t 0.0041152 -s 4 -d 2 -i 0 -e 72 -p udp -a 0  -c 0
r -t 0.0041152 -s 4 -d 2 -i 0 -e 72 -p udp -a 0  -c 0
+ -t 0.0041152 -s 2 -d 4 -i 1 -e 72 -p udp -a 0  -c 0
- -t 0.0041152 -s 2 -d 4 -i 1 -e 72 -p udp -a 0  -c 0
h -t 0.0041152 -s 2 -d 4 -i 1 -e 72 -p udp -a 0  -c 0
```

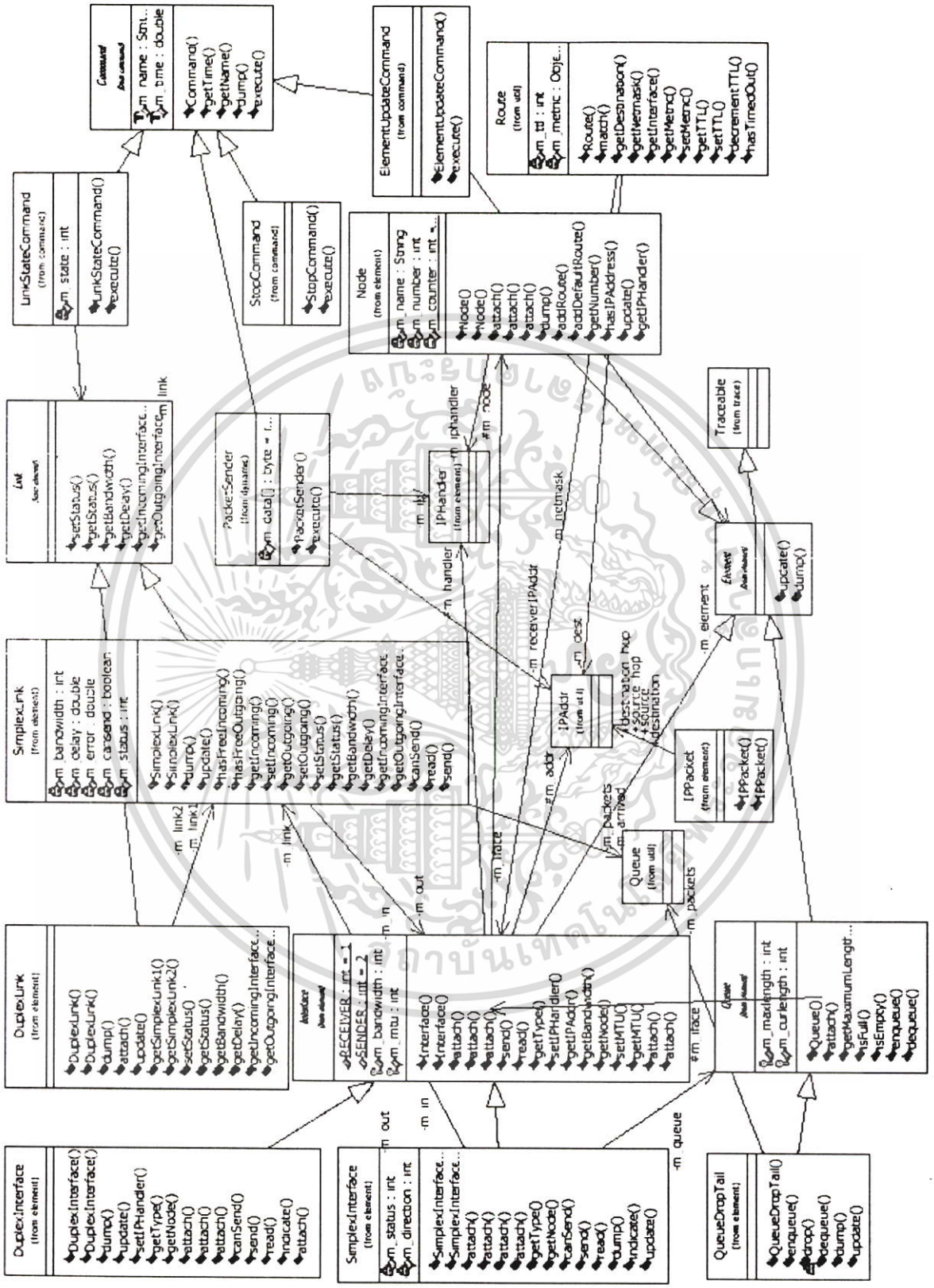
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Java Network Simulation Packet Flow



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Java Network Simulator Class Diagram



งานวิจัยที่ได้รับการตีพิมพ์

- W. Werapun, A. Unakul, An Experimental Mobile IPv6 for Linux Testbed System, "The Seventh National Computer Science and Engineering Conference, NCSEC 2003", Oct 2003
- W. Werapun, A. Unakul, Secure Mobile IPv6 Binding Updates with Identity-based Signature, "Information and Computer Engineering Postgraduate Workshop 2003", Jan 2004
- W. Werapun, A. Unakul, An Experimental Mobile IPv6 Simulation using NS-2 Mobiwan, "NS-2 Network Simulation Workshop 2004", Nov 2004

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

NCSEC2003

The 7th National Computer Science and Engineering Conference

October 28-30, 2003

Chonburi, THAILAND

Organized by :

Department of Computer Science,

Faculty of Science,

Burapha University

ISBN : 974-382-604-1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

An Experimental Mobile IPv6 For Linux Testbed System

Warodom Werapun and Apinetr Unakul
Department of Computer Engineering,
King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand
Email: warodom@graduate.kmitl.ac.th, apinetr@yahoo.com

Abstract

The challenge of mobility in IP layer allows hosts to retain their addresses without requiring routers to propagate specific routes or breaking current connections [1, 2].

Mobile IPv6 makes transparency of IP layer. In particular, as long as they remain idle, all open TCP connections survive a change in network and are ready for further use [1, 2, 8].

This paper proposes an experiment of mobile IPv6 for Linux testbed system, and we have analyzed some testbed results. This testbed uses Mobile IPv6 implementation on Linux.

Key-words: IPv6, Mobile IP, MobileIPv6, MIPL, Linux

1. Introduction

Nowadays, most people use TCP/IP [9, 10] to reach the outside world. All devices that use TCP/IP must have a unique number to specify its location called IP address. Device cannot move its location to another network without changing its IP address.

If a device would like to move to another network, it needs to terminate the old connection and create a new connection with a new IP address. For example, if an organization changes ISP, all clients need to change their IP addresses too.

This is not a problem if the connection is not mission critical and you do not move location to another network frequently. Because after you move to a new network, you can have new connection with new IP address.

On the other hand, this situation can cause problems to some types of applications that need to connect to the Internet permanently. Focus on IP layer, users need to keep the connection alive at the IP layer. How can it be done? Mobile IPv6 [1, 2, 8] is the solution. We tested IP mobility using *Mobile IPv6 for Linux (MIPL)* software [17].

1.1. Why IPv6 is needed

IPv6 and IPv4 are used for transferring packet from a host to another host [9, 10]. Both sender and receiver need to have IP address. Presently, there are not enough IPv4 addresses. The current solution is using *Network Address Translator (NAT)* and private addresses. However, this solution breaks end-to-end connections. Other improvements of Ipv6 over IPv4 include areas such as security, autoconfiguration [6], address grouping, etc.

1.2. What are the issues in IPv6

1.2.1. Growth

IPv6 address space uses 128 bits length to identify each node. There are approximately $2^{128} \approx 3.4 \times 10^{38}$ unique addresses [4].

1.2.2. End-to-end

The basic Internet requires end-to-end connection. With sufficient addresses, each host can have its own IP address, allowing them to communicate with each other directly. NAT will no longer be necessary and users can use true end to end connections [4, 16].

1.2.3. Security

IPv6 is integrated with IPSec as extension header. Both *Authentication (AH)* and *Encryption Security Payload (ESP)* extension [4] headers have been defined and are required for a full implementation of IPv6. The authentication and encryption functions have been separated so that individual implementations can use one or both of the functions as needed by the upper layer applications. Encryption, for example, may be restricted by government regulation; however, only authentication is implemented in some cases.

1.2.4. Stateless and stateful autoconfiguration

The autoconfiguration process [6] includes creating a Link-Local address and verifying its uniqueness on the link, as well as determining what information should be autoconfigured. Stateless autoconfiguration is a new feature of IPv6. It can assign IP address automatically without manual configuration by an

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

administrator or using *Dynamic Host Configuration Protocol (DHCP)*. This method uses network prefix from router advertisement packet and append interface ID with IEEE EUI-64 converting from MAC address. In addition, IPv6 also supports stateful configuration using DHCPv6 [4, 5, 6].

1.2.5. IP aggregation

Many communication networks, such as the global telephone network, are based on a hierarchical addressing scheme. A hierarchy facilitates easier scaling and routing. The hierarchy for the aggregatable addresses is organized into three levels: a public topology, a site topology, and an interface identifier [4, 16].

2. Mobile IPv6

2.1. Overview of mobile IPv6

Roaming with mobile internet devices is still difficult. Because when *Mobile Node (MN)* [1, 2] disconnects itself from the internet to connect else where, it cannot communicate until configuration with new IP address is modified successfully with either net mask or default gateway.

The key success of IP mobility is Home agent. Home agent is a router that take care packet, sent from the home network to foreign network [3].

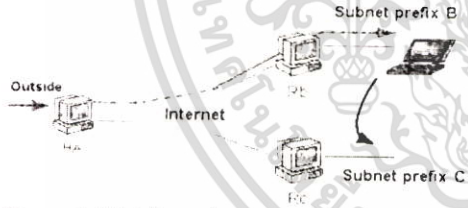


Figure 1. Mobile node move without changing IP address

In figure 1, packets from outside network are still sent through Rb to mobile node, if mobile node move from subnet prefix B to subnet prefix C. Although mobile node moved to a new location, packets from outside still go through *Home Agent (HA)* [1, 2] first. HA knows mobile node has moved from network B to network C by binding update message, so HA just has forwards packets to the mobile node's new location.

After mobile node is relocated on subnet C, and mobile node moves back to subnet B, mobile node needs to inform the position to HA. Now HA knows that the mobile node stays at home and will not forward packet to foreign network.

2.2. Movement detection

There are 2 mechanisms to check new location of mobile node

2.2.1. Detect from lifetime of ICMP packet.

Normally, Agent will broadcast ICMP [7] *router advertisement (RA)* message [5]. RA has maximum registration lifetime field. Mobile node will record lifetime value for each message. The Agent sends this message to update lifetime. So, if lifetime were to run out, it means mobile node had moved to new location.

2.2.2. Detect by compare network prefix from routing advertisement

Mobile node can compare old prefix with current prefix that is sent by agent. If prefix differs from the old one, then it means the mobile node had moved to new location.

2.3. Home agent registration

After mobile node moves to foreign network and configure network configuration successfully, it needs to communicate with HA to tell its new location. This method is done by sending binding update packet. When HA receives binding update packet, HA registers binding update to know new location of mobile node. HA replies to mobile node with binding acknowledgement. After this process completes successfully, HA can route packets to new location.

2.4. Triangle Routing

When mobile node is away from home to the foreign network, *Correspondent Node (CN)* [1, 2] sends packet to home address. HA must intercept packet and forward to mobile node by tunneling using IP encapsulation. Packets that arrive to the destination will be decapsulated [12] for mobile node. Next, mobile node can send packet to CN directly. This type of transfer is called triangle routing.

To decrease overhead at border router, we should to avoid triangle routing by using routing optimization. Routing optimization presents the method for MN and CN to send packets to each other directly without forwarding from home agent.

CN sends packet to check binding cache on HA for destination IP address. If there is information in cache, then mobile node is moved to new location. CN can send packet to

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

MN directly. Otherwise, if no information in cache on HA, mobile node is back to home address. CN can send packet to its home address

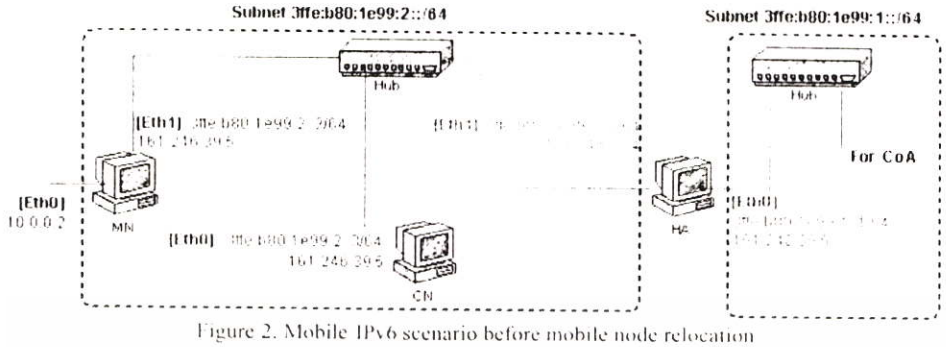


Figure 2. Mobile IPv6 scenario before mobile node relocation

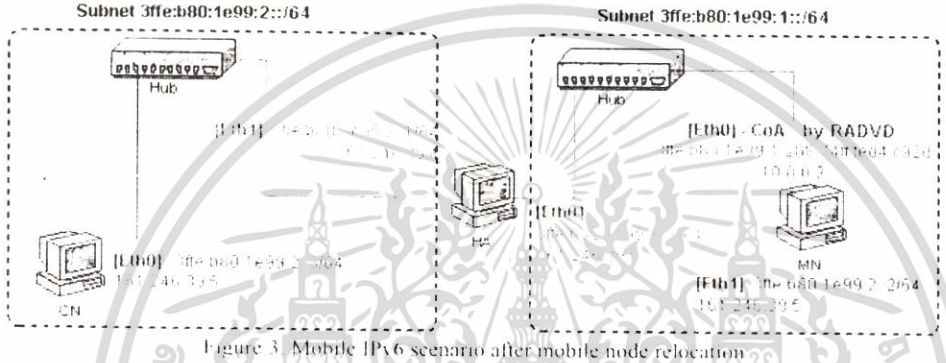


Figure 3. Mobile IPv6 scenario after mobile node relocation

3. Testbed experimental and results

3.1 Testbed specification

Our testbed environment consists of 3 computers with kernel patch from MIPL [17]. All of these computers run Linux Red Hat 8.0 with kernel 2.4.20 as operating system.

We set up Mobile IPv6 configuration as illustrated in Figures 4, 5, and 6.

```
interface eth0
{
AdvSendAdvert on;
MinRtrAdvInterval 3;
MaxRtrAdvInterval 10;
AdvHomeAgentFlag on;

    prefix 3ffe:b80:1e99:1::/64
    {
    AdvOnLink on;
    AdvAutonomous on;
    AdvRouterAddr on;
    };
};
```

Figure 4. RADVD configuration

```
FUNCTIONAL
HOME
MIN_TUNNEL
MAX_TUNNEL
HOMEDEV=eth1
HOMEADDRESS=3ffe:b80:1e99:2::2/64
HOMEAGENT=3ffe:b80:1e99:2::1/64
```

Figure 5. Mobile IPv6 configuration

```
DEVICE=eth0
BOOTPROTO=static
BROADCAST=10.0.0.255
IPADDR=10.0.0.2
NETMASK=255.255.255.0
NETWORK=10.0.0.0
ONBOOT=yes
IPV6INIT=yes
IPV6_AUTOCONF=yes
```

Figure 6. Ethernet interface configuration

3.2 Methodology

After computer started, network services will start automatically. We can check IPv6 address by using ifconfig command. At this time, MN will get IPv6 link local address (fe80::/10) only, because we have not yet defined IPv6 address to interface card. Next, we start mobile-ip6 service and we get IPv6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

address following specific in network-mip6.conf file due to config device.

On HA router, we cannot use AUTOCONF because mobile IPv6 kernel does not support autoconfiguration for router. In addition, we start RADVD service to make ability of HA to advertise network prefix into network.

In our test, we use ping6 command to ping6 from CN as the source (eth0 3ffe:b80:1:2::3/64) to MN as the destination (eth1 3ffe:b80:1:2::2/64). After that, we disconnected LAN cable which is connected to eth1 of MN. Move MN from subnet 3ffe:b80:1:2::/64 through 3ffe:b80:1:1::/64 by connect LAN cable into eth0 following Fig3.

We try to ifconfig again to see MN IPv6 address. We can see new IPv6 address that was created by RADVD service. New MN IPv6 address gets network prefix from RADVD service. The Interface Identifier for an Ethernet interface is based on the EUI-64 identifier [EUI64] derived from the interface's built in 48-bit IEEE 802 address. Notice, packets from CN still can be sent to MN without breaking current connection.

4. Analyze test result

There is delay time while handoff occurred. This delay is the time of MN registration to HA.

4.1. Increased router advertisement rate

MinRtrAdvInterval is the minimum time allowed is sending unsolicited multicast router advertisements from the interface. In this test we use 3 seconds as default value, we ignore *Router Solicitation (RS)* messages sent by mobile node. Because we want the performance effected by MinRtrAdvInterval only, we set RTR_SOLICITATION_INTERVAL = 10. After we try to increase/decrease router advertisement rate, the response time is increased/decreased respectively. However, we achieved the least MinRtrAdvInterval time of 0.05 seconds following by RADVD implementation [19].

In contrast, if we set minRtrAdvInterval to the minimum value, it consumes more bandwidth. That mean, performance in figure 7 is better in small network but it might worse in large network because HA needs to send a lot of RA messages.

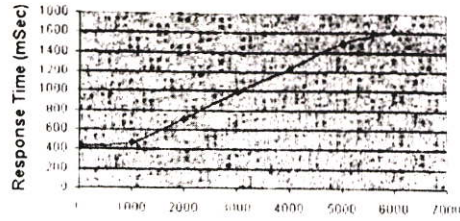


Figure 7. MinRtrAdvInterval vs. Response Time comparison (RTR_SOLICITATION_INTERVAL = 10)

4.2. Triggered router advertisement

As we mention in 4.1, mobile node needs to wait for RA from router. Instead of waiting, mobile node may send RS message to ask router for RA directly. Following IPv6 specification, mobile nodes are allowed to send RS messages at a shorter minimum interval than normal IPv6 nodes (default: 4 seconds). This value controls the mobile nodes with minimum RS interval in seconds (default: 1 second). We set RTR_SOLICITATION_INTERVAL=1. This can reduce delay time for handoff operation.

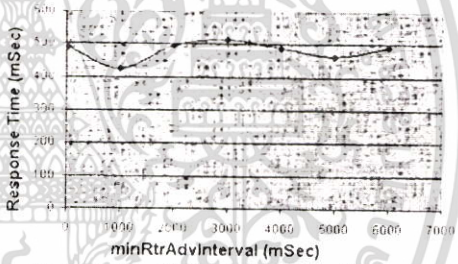


Figure 8. MinRtrAdvInterval vs. Response Time comparison (RTR_SOLICITATION_INTERVAL = 1)

Using RS message, sent by mobile node, will reduce bandwidth consummation. This method is more suitable than sending a lot of RA messages by HA.

5. Conclusion

After we tried the MIPL software, we perceive the benefit of mobile IPv6. Mobile node can move to other networks without breaking current connection and no IP changing is needed. In addition, we tried to reduce handoff time by reducing router advertisement rate or sending RS by mobile node for the better performance.

6. Future work

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.1 Mobile IPv6 with IP Security Implementation

Current MIPL version is based on kernel 2.4, which does not support IPSec. Although, we can patch kernel 2.4 to support IPSec by USAGI IPv6 [20] with integrated IPSec, but IPSec and MIPv6 code was implemented quite differently. In the future, MIPL will support the draft-15 authentication style. Anyway, using of IPSec between MN and HA will be available on the Linux 2.5 kernels, when they have IPv6 IPSec built-in [17, 18].

6.2 Multiple HA router advertisements

Some mobile nodes use network prefix from RA messages to detect movement. If there are multiple HA router advertisements in the network, then mobile node may always realize to move new network all times that it gets in RA from HA. IPv6 multiple routers are allowed on a link, and these routers do not have to advertise overlapping prefixes [5]. Therefore, mobile nodes can check the reachability of the current router. Mobile nodes slowly determine reachability of current router. To reduced determine reachability of current router time, we may add link-ID in RA message [14].

7. References

[1] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6", IETF draft, work in progress.

[2] W. Simpson, "IPng Mobility Considerations, RFC 1688", August 1994.

[3] F. Teraoka, "Options for Mobility Support in IPv6", January 1996.

[4] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[5] T. Narten, E. Nordmark and W. Simpson, "IPv6 Neighbor Discovery", RFC 2461, December 1998.

[6] S. Thompson and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, November 1998.

[7] A. Conta, S. Deering, "Internet Control Message Protocol for the Internet Protocol Version 6", RFC 2463, December 1998.

[8] D. Solomon, Mobile IP The Internet Unplugged, Prentice Hall, New Jersey, 1998.

[9] J. Postel, "Internet Protocol", RFC 791, September 1981.

[10] J. Postel, "Transmission Control Protocol", RFC 792, September 1981.

[11] S. Hanks, T. Li, D. Farinacci and P. Traine, "Generic Routing Encapsulation (GRE)", RFC 1701, October 1994.

[12] C. Perkins, "IP Encapsulation within IP", RFC 2003, October 1996.

[13] D. Johnson, "Scalable and Robust Internetwork Routing for Mobile Hosts, in Proceedings of IEEE 14th International Conference on Distributed Computing Systems", June 1994.

[14] P. Brett, D. Greg, "Router Advertisement Link Identification for Mobile IPv6 movement Detection draft-pentland-mobileip-linkid-00", May 2003.

[15] T. Comall, B. Pentland and P. Khee "Communication Systems, 2002. ICCS 2002. The 8th International Conference" , Volume: 2 , 2002 Page(s): 857 -861.

[16] E. Robert, The future with IPv6, "Information and Computer Engineering Postgraduate Workshop 2002 (ICEP 2002)", January 2002.

[17] Linux Mobile IPv6, http://www.mipl.mediapoli.com/

[18] Linux IPv6 Tutorial, http://www.bieringer.de/linux/IPv6/

[19] Linux IPv6 Router Advertisement Daemon, http://v6web.litech.org/radvd/

[20] USAGI Project - Linux IPv6 Development Project, http://www.linux-ipv6.org

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

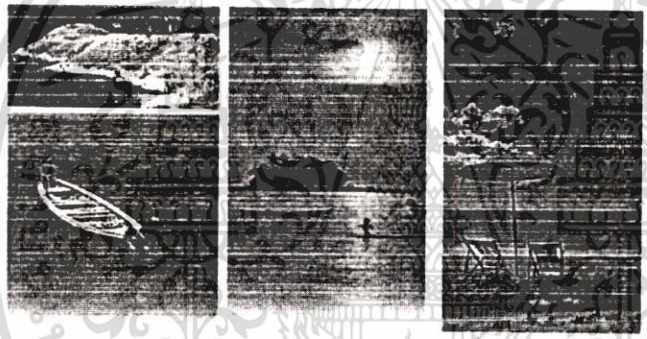
PROCEEDINGS

The 4th Information and Computer Engineering Postgraduate Workshop 2004

ICEP 2004

22nd - 23rd January 2004

Phuket, Thailand



Prof Jun Marai, KEIO University, Japan

Organised and Sponsored by
Department of Computer Engineering,
Faculty of Engineering,
Prince of Songkla University, Thailand
and Prof Jun Marai, KEIO University, Japan

In cooperation with
IEEE ComSoc, Thailand Chapter,
ECTI (Electrical Engineering/Electronics,
Computer, Telecommunications and Information
Technology Association of Thailand)

ISBN 974-644-518-9

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Secure Mobile IPv6 Binding Updates with Identity-based Signature

Warodom Werapun and Apinetr Unakul***
Department of Computer Engineering, Faculty of Engineering
King Mongkut's Institute of Technology Ladkrabang.
Bangkok 10520, Thailand
Email: warodom@graduate.kmitl.ac.th, apinetr@yahoo.com***

Abstract

Updates are used to tell current location of the node for routing optimization purpose. However, Updates for mobile IPv6 system requires research to improve on the security protocols. paper is proposed to apply Identity-based signature work to secure Binding Updates.

Introduction

IPv6 makes transparency of IP layer. In particular, as they remain idle, all open TCP connections a change in network and are ready for further use When the *Mobile Node (MN)* is away from home to foreign network, the *Correspondent Node (CN)* [1, 2] packets to home address. *Home Agent (HA)* must packets and forward them to the mobile node by using IP encapsulation. Packets that arrive to the will be decapsulated for the mobile node. the mobile node can send packet to the CN directly pe of transfers is called triangle routing. crease overhead at the border router, we should avoid routing by using routing optimization. Routing mization presents the method for the mobile node and CN to send packets to each other directly without ting from the HA.

optimization was done by sending *Binding (BU)* to the CN. Without the security mechanism, does not know which node send the BU. So an ary makes bogus the BU to the CN that tell, the node was moved to the other location again, to the So, the connection is lost.

BU is not so secret but it needs to be sent from the mobile node. To get bandwidth efficiency with , the mobile node signs the BU and sends it to the de to inform the real location of the mobile node.

Motivation

ently, the implementation version of mobile IPv6 [13] Updates are still unfinished and required to improve on the security protocols. Most proposed mobile IPv6 security solutions use cryptography such as Diffie-Hellman and traditional RSA public key [12] to secure the BU. Diffie-Hellman is an algorithm that create a key without pre-requisition, and uses that key to communicate. On the other hand, the key generated by Diffie-Hellman, is not able to verify genuine sender or receiver. To verify sender or receiver, asymmetric cryptography is chosen. RSA is the method of traditional public key cryptography that is widely used in network security included mobile IPv6 but it consumed immense bandwidth because recommendation of RSA key length for good security is 1024 bits. ID-based signature based on an elliptic curve with order of 160-bit prime offers approximately the same level of security as DSA with 1024-bit modulus p and RSA with 1024-bit modulus n. [5, 6]. We applied ID-based signature to protect malicious nodes from forging BU for other nodes and denial of service attacks.

1.2 Assumption

Our framework is suitable for mobile conferencing application within a secure organization boundary. They require a pre-existing security association between MN and its HA. This assumption is necessary because MN must receive cryptographic parameter information and a private key from HA. The MN, HA and CN must implement an identity based cryptosystem and all nodes have been system parameters for signing and verifying. The HA acts as an Identity-based Private Key Generator.

1.3. Mobile IPv6

Roaming with mobile internet devices is still difficult. Because when the mobile node [1, 2] disconnects itself from the internet to connect else where, it is unable to communicate until the configuration with new an IP address is modified successfully with either net mask or default gateway.

The key success of IP mobility is HA. HA is a router that takes care of packets sent from the home network to a foreign network [3].

In figure 1, packets from outside network are still sent

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

through Rb to the mobile node, if the mobile node is moved from subnet prefix B to subnet prefix C. Although the mobile node moves to a new location, packets from outside still go through HA [1, 2] first. HA realizes the mobile node has moved from network B to network C by the BU, so HA forwards packets to the mobile node's new location.

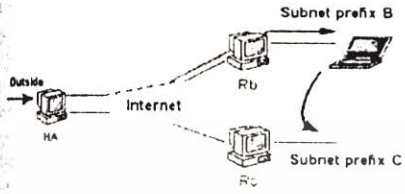


Figure 1. Mobile node move without changing IP address

After the mobile node is relocated on subnet C, and the mobile node moves back to subnet B, the mobile node needs to inform the position to HA. Now HA knows that the mobile node stays at home and will not forward packets to foreign network.

Not only using BU with HA, but also the mobile node has the ability to optimize routes using BU, which specifies an association between the home address of the mobile node and its care of address. When a CN receives a BU from a mobile node, it creates a BU entry and stores the entry into a binding cache. Thereafter, the CN will send packets destined for the mobile node to the mobile node's care of address.

2. Security review

2.1 Previous work in security

Symmetric cryptography uses the same key for encryption and decryption. It is easy to use and implement but there are problems, first how we can exchange secret securely. Second, If we communicate to n users, we need to keep n*(n-1)/2 - n keys.

These problems are able to be eliminated by using asymmetric cryptography. Asymmetric cryptography uses two keys: a private key known only to the owner and public key that can be given to anyone. The system is based on a complicated mathematical formula involving large prime numbers and exponentiation [9]. When someone wishes to send a message to a person, he must find that person's public key and encrypt the message. The recipient then decrypts the message with his or her private key and receives the plaintext.

However, there is still a problem of how we can make sure that public key is given to anyone correctly. The solution proposed for this case is to use certificated issued by certificated authority that derived in hierarchy. Anyone can check public key by examine with the certificate.

Current PKI still works well but disadvantages of traditional PKI still exist, for example, cannot communicate securely without knowing other party's public key, where does one get and store certificates, hard to impose in organizations etc.

In 1984, Shamir asked for a public key encryption schemes in which the public key can be an arbitrary string such as email address, IP address, MAC address etc. however, none of these is fully satisfactory. Some solutions require tamper resistant hardware. Other solutions require the *Private Key Generator (PKG)* to spend a long time for each private key generation request. [5]

Until 2001, D. Boneh and M. Franklin implement An Identity-based cryptosystem which enables any pair of users to communicate securely, to verify each other's signatures without exchanging public or private keys, without keeping any key directories and without using the services of any third party. Problems with the traditional *Public Key Cryptosystems (PKCs)* are the high cost of the infrastructure needed to manage and authenticate public keys, and the difficulty in managing multiple communities. Whilst ID-based PKCs will not replace the conventional Public Key infrastructures, it might prove to be a complementary technology [8].

With mobile environment, there are bandwidth constraints and power saving needed. So, ID-based cryptography is suitable for use with mobile IPv6 the BU because it is optimized and secure.

2.2 Identity-based signature

Also from [4] in 1984 and [5], an Identity-based signature was proposed. An Identity-based signature scheme is a digital signature scheme specified by the following four algorithms:

- **ID_SETUP:** An algorithm, executed by PKG, that takes a (random) parameter k as input and generates from it params (system parameters) and master-key. Params is publicly known while master-key is only known to the PKG.
- **ID_EXTRACT:** An algorithm, executed by the PKG, that takes as input params, master-key and an arbitrary IDi Î {0,1}*, provided by a user, User i, and returns a private key di. IDi is an arbitrary string that is used as a public key and di is the corresponding private key.
- **ID_SIGN:** An algorithm that takes as input params, di and message m and returns a signature Sig defined as follows: Sig = ID_SIGN(params, di, m).
- **ID_VERIFY:** An algorithm that takes as input a message m and its signature Sig, the system params params and a public key IDi and performs as follows: valid = ID_VERIFY(Sig, IDi, params, m). Valid is a

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

binary value that is set to 0 if the signature is invalid and to 1 if the signature is valid.

A secure Identity-based signature scheme must at least satisfy the following properties:

Correctness: Signatures produced by a user using ID_SIGN must be accepted by ID_VERIFY (provided that the correct parameters are used)

Unforgrability: It is computationally hard for everyone that does not know the secret key di of User i to forge his signatures. As a consequence, it must be computationally hard for everyone to retrieve from params the corresponding master-key.

Collition-resistance: A colluding subset of user, that has received their private key from the same PKG and params, cannot generate a valid signature that the PKG cannot link to one of the colluding user.

3. Secure Binding Updates message

Security has been identified as a critical issue in Mobile IPv6. The Mobile IPv6 specification is still unfinished and requires additional research to improve the security protocols. The IETF Mobile IP Workgroup is focusing on Mobile IPv6 security solutions to facilitate approval of the Mobile IPv6 RFC.

We define the mobile node's home address as ID using like public key. Any other nodes can decrypt or verify message by using home address, consisted in BU message

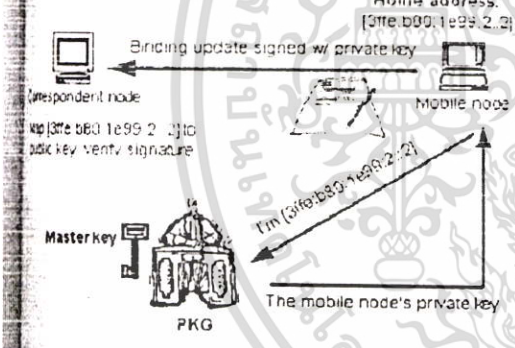


Figure 2. Identity-based signature schema

In figure 2, for first time, the mobile node needs to setup master key and private key that is generated from PKG. PKG generates the mobile node's private key and send to the mobile node which we assumed this communication must be secured. This assumption was reasonable because PKG can stay in the same domain with the mobile node's home network. So, the setup method must be completed before the mobile node was moved.

Next, the mobile node can sign the BU without communication to PKG. The BU schema was shown in figure 3.

Binding Updates	signature

Figure 3. The field of a verifiable message

Binding Updates: contain home address, care of address etc. following IPv6 header extension [1, 2].

Signature: Hash the BU and sign with private key and params.

Notation:

G_1 is an additive group of prime order q.

G_2 is a multiplicative group of the same order q.

$\hat{e} : G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing.

$P \in G_1$ is a known element

$s \in Z_q$ is master secret that know only PKG

System parameters are (G_1, G_2, P, $P_{pub} = sP$, $\hat{e}$, cryptographic hash functions)

$$H_1 : \{0,1\}^* \rightarrow G_1$$
$$H_2 : \{0,1\}^* \rightarrow Z_q$$

The mobile node sent the BU to the CN by using ID_SIGN function.

$$Sig = ID_SIGN(params, PrivKey, BU):$$

$$R = kP, S = k^{-1}(H_2(M)P + D_{id}) \quad (1)$$
$$Where: D_{id} = sH_1(IPv6\text{-}Address) \quad (2)$$
$$Q_{id} = H_1(IPv6\text{-}Address) \quad (3)$$

The mobile node sent the R, S as signature to the CN. The CN verify the BU from the mobile node by using ID_VERIFY function

$$Valid = ID_VERIFY(Sig, ID, params, BU):$$

$$\hat{e}(R, S) = \hat{e}(kP, k^{-1}(H_2(M)P + D_{id})) \quad (4)$$
$$= \hat{e}(P, H_2(M)P + sQ_{id})$$
$$= \hat{e}(P,P)^{H_2(M)} \cdot \hat{e}(P, sQ_{id})$$
$$= \hat{e}(P,P)^{H_2(M)} \cdot \hat{e}(P_{pub}, Q_{id}) \quad (5)$$

Verify signature by compare result from (4) and (5). A valid signature will always satisfy the check.

4. Expected result

When secure BU is used, all mobile nodes must support and should use the following our verifiable message to provide data origin authentication and connectionless integrity.

Compare with traditional PKI, if we used it to secure the BU, the field of verifiable message should included public

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

key certificated and signature of BU's hashed. On the other hand if we applied Identity-based signature, we can get rid of certificates because any nodes do not need to verify public key. However, we still need PKG to authorize cryptographic setting.

Although mobile nodes in the system are needed to be registered with PKG in order to issue their own private key and system parameters, it is expected that the system will increase overhead of traffic in the network as well as maintain security and robustness by effective inspection mechanism.

5. Conclusion

We proposed Identity-based signature framework to secure the BU. A verification system is introduced in this framework. The signature binds a key to the BU. A key challenge is CN does not need to verify the mobile node public key. If verification of the mobile node BU is false, then the CN can detect that a BU was forged.

6. Future work

Based on Identity-based signature algorithm, we will build the code in C programming style with GNU MP's library for arbitrary precision arithmetic and also IBE library for secure the BU. We will mathematically compute the possible key lengths to secure the BU and stay with the best performance. We aim to use network simulator tools to simulate network performance with strong security.

7. References

[1] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6", IETF draft, work in progress

[2] W. Simpson, "IPng Mobility Considerations, RFC 1688", August 1994

[3] F. Teraoka, "Options for Mobility Support in IPv6", January 1996.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes", Advances in Cryptology (Proceedings of Crypto '84), Lecture Notes in Computer Science, vol 196, Springer-Verllag, 1985

[5] D. Boneh, M. Franklin, "Identity-Based Encryption from the Weil Pairing", extend abstract in Advances in Cryptology – Crypto 2001, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, pp. 231-229, Aug. 2001.

[6] A. J. Menezes "Elliptic Curve Public Key Crytosystems", Kluwer International series in Engineering and Computer Science, 1993

[7] Don Johnson, Alfred Menezes and Scott Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", Certicom Research, Canada, 2001

[8] Divya Nalla, K. C. Reddy, "Signcryption scheme for Identity-based Cryptosystems", 2003

[9] Rivest, R, Shamir, A, and Adleman, L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", 1978

[10] Scott Bradner, et al, A Framework for purpose Built Keys (PBK), Jan 2003

[11] Greg O'Shea and Michael Roe, Child-proof Authentication for MIPv6 (CAM), Feb 2002

[12] H. Xiao, "Trust Management for Mobile IPv6 Binding Update", 2003

[13] Linux Mobile IPv6, http://www.mipl.mediapoli.com/

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายวโรดม วีระพันธ์
วันเดือนปีเกิด	วันอาทิตย์ ที่ 5 เดือน พฤศจิกายน พ.ศ. 2521
ที่อยู่	133/67 ถ. เทศบาล 3 ต. สะเตง อ.เมือง จ.ยะลา 95000
	โทร. 0-9733-4480
ประวัติการศึกษา	สำเร็จการศึกษาระดับปริญญาตรี หลักสูตรวิศวกรรมศาสตร์บัณฑิต
	สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
	มหาวิทยาลัยสงขลานครินทร์ ปีการศึกษา 2543

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้