วิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าทีมี การจัดเก็บแบบกระจาย

AN ISSUANCE OF CERTIFICATE REVOCATION LIST METHOD USING OVER-ISSUED DELTA-CRLS WITH DISTRIBUTION POINTS

อารดี โรจนภาสกร

ARADEE ROJANAPASAKORN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2547

ISBN 974-9708-86-5

วิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย

AN ISSUANCE OF CERTIFICATE REVOCATION LIST METHOD USING OVER-ISSUED DELTA-CRLS WITH DISTRIBUTION POINTS

อารดี โรจนภาสกร
ARADEE ROJANAPASAKORN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ
บัณฑิตวิทยาลัย
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ.2547

ISBN 974-9708-86-5

AN ISSUANCE OF CERTIFICATE REVOCATION LIST METHOD USING OVER-ISSUED DELTA-CRLS WITH DISTRIBUTION POINTS

ARADEE ROJANAPASAKORN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
MASTER OF SCIENCE IN INFORMATION TECNOLOGY
SCHOOL OF GRADUATE STUDIES
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2004

ISBN 974-9708-86-5

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ วิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย

AN ISSUANCE OF CERTIFICATE REVOCATION LIST METHOD USING OVER-ISSUED DELTA –CRLs WITH DISTRIBUTION POINTS

ชื่อนักศึกษา นางสาวอารดี โรจนาภาสกร

รหัสประจำตัว 44067031

ปริญญา วิทยาศาสตรมหาบัณฑิต

สาขาวิชา เทคโนโลยีสารสนเทศ

อาจารย์ผู้ควบคุมวิทยานิพนธ์ ผศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
ผศ.ดร.จันทร์บูรณ์	สถิตวิริยวงศ์	
รศ.ดร.รัตติกร	วรากูลศิริพันธุ์	
ผศ.ดร.นพพร	โชติกกำธร	
ผศ.ดร.โชติพัชร์	ภรณวลัย	
ผศ.อัครินทร์	คุณกิตติ	

วัน/เดือน/ปี ที่สอบ 18 พฤษภาคม 2547 เวลา 9.30 น. เป็นต้นไป

สถานที่สอบ ณ ห้อง M 23 (ชั้นลอย) อาคารเรียนรวมและปฏิบัติการคณะเทคโนโลยีสารสนเทศ

บัณฑิตวิทยาลัยรับรองแล้ว

(ผศ.ดร.จารุวัตร เจริญสุข)

คณบดีบัณฑิตวิทยาลัย

วันที่ 28 **เดือน** มิถุนายน **พ.ศ.** 2547

หัวข้อวิทยานิพนธ์	วิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย
นักศึกษา	นางสาวอารดี โรจนภาสกร
รหัสประจำตัว	44067031
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
พ.ศ.	2547
อาจารย์ผู้ควบคุมวิทยานิพนธ์	ผศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์

บทคัดย่อ

ในปัจจุบันนี้องค์กรต่างๆ ได้ตระหนักถึงการรักษาความปลอดภัยในการติดต่อสื่อสารผ่านระบบเครือข่ายมากขึ้น โครงสร้างพื้นฐานกุญแจสาธารณะเป็นโครงสร้างพื้นฐานการรักษาความปลอดภัยที่เหมาะกับองค์กรที่มีระบบเครือข่ายขนาดใหญ่หรือพาณิชย์อิเล็กทรอนิกส์ ซึ่งมีใบรับรองที่ใช้ในการกระจายกุญแจสาธารณะและพิสูจน์ตัวบุคคล รายการยกเลิกใบรับรองเป็นกลไกหลักอย่างหนึ่งของโครงสร้างพื้นฐานกุญแจสาธารณะ ซึ่งกลไลการยกเลิกใบรับรองนี้เป็นการประกาศใบรับรองที่ถูกยกเลิกก่อนเวลาหมดอายุจริง วิทยานิพนธ์เล่มนี้ นำเสนอถึงการปรับปรุงวิธีการยกเลิกใบรับรองให้มีรายการยกเลิกใบรับรองนั้นที่มีช่วงอายุการใช้งานเหลื่อมเวลากัน มีการแบ่งส่วนของรายการยกเลิกใบรับรอง และให้แต่ละส่วนนั้นกระจายไปยังเครื่องแม่ข่ายต่างๆ ซึ่งวิธีการนี้ได้ประยุกต์จากวิธีการออกรายการยกเลิกใบรับรองต่อเนื่องแบบแบ่งส่วนและวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้า และวิเคราะห์ผลลัพธ์จากโปรแกรมจำลองวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย ซึ่งวิธีการนี้สามารถกระจายอัตราการร้องขอสูงสุด ลดขนาดของรายการยกเลิกใบรับรอง และลดภาระบนเครือข่าย

Thesis Title	An Issuance of Certificate Revocation List Method using Over-Issued Delta-CRLs with Distribution Points
Student	Miss Aradee Rojanapasakorn
Student ID.	44067031
Degree	Master of Science
Programme	Information Technology
Year	2004
Thesis Advisor	Asst.Prof. Dr.Chanboon Sathitwiriyawong

ABSTRACT

In the present, enterprises are aware of the importance of communication security through network. Public Key Infrastructure (PKI) is the security infrastructure suitable in network enterprise or e-commerce. In particular, certificates are used to distribute public key associated with the identity of its owner. The certificate revocation mechanism is the action of declaring a certificate invalid before its validity period is at an end. This thesis proposes a method that the improvement of certificate revocation method have overlapping validity times, segmented certificate revocation lists and distributed segmented them to locate directories. The method uses the combination of over-issuing segmented CRLs and delta-CRLs. The simulation results show that the proposed certificate revocation system using over-issued delta-CRLs with distribution points can significantly improve the system performance such as spreading out request rate, reducing the size of certification revocation information and reducing the average bandwidth usage.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี ด้วยการให้คำแนะนำและคำปรึกษาเกี่ยวกับวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย จากอาจารย์ผู้ควบคุมวิทยานิพนธ์ ผศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์ ผู้วิจัยรู้สึกซาบซึ้งในความอนุเคราะห์จากท่านและขอกราบขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณคณะกรรมการสอบทุกท่านที่ได้สละเวลาอันมีค่าในการตรวจสอบวิทยานิพนธ์ในครั้งนี้และช่วยแก้ไขวิทยานิพนธ์ฉบับนี้ให้สมบูรณ์ยิ่งขึ้นขอขอบพระคุณบริษัท ไปรษณีย์ไทย จำกัด ที่ให้ทุนการศึกษาปริญญาโทในครั้งนี้

ขอขอบพระคุณบิดา มารดา และครอบครัวผู้วิจัยที่สนับสนุนการศึกษา คำปรึกษาต่างๆ และกำลังใจในการศึกษาให้ผ่านไปได้ด้วยดี

ขอขอบคุณ บุรินทร์ เย็นมั่นคง ที่ช่วยเหลือ คำแนะนำ พร้อมทั้งให้คำปรึกษาที่เกี่ยวกับการศึกษาวิจัยในเรื่องต่างๆ และยังให้กำลังใจต่อผู้วิจัยอย่างใกล้ชิดตลอดมา

ขอขอบพระคุณ ครอบครัวสินเอกเอี่ยม ที่คอยสอบถามและให้กำลังใจในการศึกษาในครั้งนี้

สุดท้ายขอขอบคุณหัวหน้าและเพื่อนๆ ที่บริษัท ไปรษณีย์ไทย จำกัด ที่ให้ความช่วยเหลือในการทำงาน เพื่อให้ผู้วิจัยได้มาศึกษาได้อย่างเต็มที่

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์ฉบับนี้ ผู้วิจัยขอมอบแด่ผู้มีพระคุณทุกท่าน

อารดี โรจนภาสกร

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูป

สารบัญรูป (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันความเจริญก้าวหน้าทางเทคโนโลยีด้านการสื่อสารข้อมูลผ่านเครือข่ายคอมพิวเตอร์ได้ถูกพัฒนาเพื่อให้มีการติดต่อสื่อสารถึงกันไม่ว่าผู้รับและผู้ส่งจะอยู่ห่างกันคนละซีกโลก ก็สามารถรับส่งข้อมูลได้อย่างมีประสิทธิภาพ โดยผ่านเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เรียกว่าเครือข่ายอินเตอร์เน็ต แต่อย่างไรก็ตามการใช้งานผ่านเครือข่ายคอมพิวเตอร์ภายใต้เครือข่ายอินเตอร์เน็ตไม่ค่อยมีความปลอดภัยของข้อมูลมากนัก เนื่องจากมีภัยคุกคามหรือการโจมตีข้อมูลผ่านทางระบบเครือข่ายโดยกลุ่มนักขโมยข้อมูล (Hackers) ดังนั้นองค์กรต่างๆ จึงได้ตระหนักถึงความปลอดภัยของข้อมูลมากขึ้น และได้นำเทคโนโลยีต่างๆ มาใช้ในการลดความเสี่ยงและรักษาความปลอดภัยในระบบเครือข่ายคอมพิวเตอร์และข้อมูลขององค์กร เช่น การใช้วิธีการเข้ารหัสข้อมูล (Encryption) เพื่อปกป้องความลับของข้อมูล โดยการเข้ารหัสข้อมูลก่อนทำการส่งข้อมูลผ่านระบบเครือข่ายอินเตอร์เน็ต หากมีการขโมยข้อมูลไปในระหว่างการส่งก็ไม่สามารถอ่านข้อมูลนั้นได้เนื่องจากนักขโมยข้อมูล ไม่มีกุญแจอิเล็กทรอนิกส์ลับ ซึ่งผู้ส่งและผู้รับเท่านั้นที่มีกุญแจรหัสลับนั้น แต่วิธีการนี้ยังมีปัญหาด้านมาตรฐานและการจัดการที่ดี ประโยชน์ของการใช้วิธีการเข้ารหัสลับข้อมูล นอกจากการปกป้องข้อมูลยังสามารถใช้ในการพิสูจน์ได้ว่าผู้ส่งเป็นตัวจริง โดยใช้วิธีการในการเข้ารหัสซึ่งอาจเป็นทั้งวิธีการเข้ารหัสลับแบบกุญแจลับ (Secret Key Encryption) หรือ วิธีการเข้ารหัสลับแบบกุญแจสาธารณะ (Public Key Encryption) นอกจากวิธีการเข้ารหัสลับยังมีวิธีการที่ช่วยในการป้องกันการปลอมแปลงข้อมูลและพิสูจน์ว่าผู้ส่งเป็นผู้ส่งตัวจริงวิธีการนี้เรียกว่า ลายมือชื่อดิจิทัล (Digital Signature) ในปัจจุบันได้มีระบบที่รวมวิธีการเข้ารหัสลับแบบกุญแจสาธารณะ ลายมือชื่อดิจิทัล การออกใบรับรองทางอิเล็กทรอนิกส์ (Digital Certificate) อยู่ในระบบเดียวระบบนี้เรียกว่า โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI) ซึ่งเป็นระบบที่เหมาะกับองค์กรขนาดใหญ่และเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต หรือการติดต่อแบบตัวต่อตัว เพื่อให้เกิดความน่าเชื่อถือ การยืนยันตัวบุคคล และความปลอดภัยของข้อมูลในระหว่างการรับ-ส่ง โดยวิธีการรักษาความปลอดภัยของโครงสร้างพื้นฐานกุญแจสารธารณะนั้นเป็นวิธีการที่จะต้องทำผ่านผู้ประกอบการรับรอง (Certification Authority) ที่น่าเชื่อถือเป็นผู้ออกใบรับรอง กุญแจสาธารณะ ให้แก่ผู้ใช้ ซึ่งพื้นฐานโครงสร้างกุญแจสาธารณะไม่ได้ให้บริการทางด้านธุรกิจ แต่พื้นฐานโครงสร้างกุญแจสาธารณะให้บริการโดยการรักษาความปลอดภัยในการ

ติดต่อสื่อสารผ่านเครือข่าย หน้าที่หลักของพื้นฐานโครงสร้างกุญแจสาธารณะคือการใช้กุญแจสาธารณะและการรักษาความปลอดภัยและความคงสภาพของข้อมูลด้วยใบรับรอง ซึ่งโครงสร้างพื้นฐานกุญแจสาธารณะนี้จะถูกใช้ร่วมกับโปรแกรมและการรักษาความปลอดภับบนเครือข่าย โดยระบบที่ใช้พื้นฐานโครงสร้างกุญแจสาธารณะนี้ เช่น จดหมายอิเล็กทรอนิกส์ พาณิชย์อิเล็กทรอนิกส์ ธนาคาร และระบบไปรษณีย์อิเล็กทรอนิกส์ เป็นต้น

โครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) เป็นที่นิยมใช้มากขึ้นจึงได้มีการพัฒนาในส่วนของฟังก์ชันต่างๆของ PKI และได้กำหนดมาตรฐานเอ็กซ์ห้าศูนย์เก้าใบรับรองกุญแจสาธารณะ (X.509 Public Key Certificate) เวอร์ชัน 3 ซึ่งได้นำเสนอวิธีการปรับปรุงโดยเพิ่มการกระจายและเพิ่มความยืดหยุ่นของ PKI มากขึ้น ซึ่ง PKI มีการออกใบรับรองทางอิเล็กทรอนิกส์เพื่อใช้ในการรับรองและสามารถใช้ในการตรวจสอบระหว่างผู้ส่งและผู้รับได้ โดยใบรับรองทางอิเล็กทรอนิกส์นี้มีช่วงอายุของใบรับรอง ซึ่งถ้าผู้ใช้ใบรับรองมีการเปลี่ยนแปลงข้อมูลภายในใบรับรอง มีการยกเลิกใบรับรองก่อนที่ใบรับรองหมดอายุตามกำหนดนั้น ผู้ประกอบการรับรอง (Certification Authority: CA) จะทำการประกาศข้อมูลการยกเลิกใบรับรองโดยใช้รายการยกเลิกใบรับรอง (Certificate Revocation List : CRL) ในปัจจุบันรายการยกเลิกใบรับรองที่ใช้อยู่นี้เป็น X.509 เวอร์ชัน 2 ซึ่งเป็นส่วนสำคัญใน PKI ซึ่งในส่วนรายการยกเลิกใบรับรองดังกล่าวมีปัญหา 2 ประการ เมื่อรายการยกเลิกใบรับรองที่เก็บในแต่ละกลุ่มผู้ใช้มีสถานะหมดอายุพร้อมกันทุกกลุ่มจะทำให้เกิดปัญหาแรกคือผู้ใช้ทุกกลุ่มจะต้องทำการร้องขอรายการยกเลิกใบรับรองที่เซิฟร์เวอร์ที่เก็บรายการยกเลิกใบรับรองไว้พร้อมๆ กันทำให้เกิดอัตราการร้องขอสูงสุดที่เครื่องแม่ข่ายที่เก็บรายการยกเลิกใบรับรอง (Repository) และทำให้ปริมาณการใช้เครือข่ายสูงขณะที่มีการร้องขอรายการยกเลิกใบรับรองนี้ ทำให้เกิดปัญหาที่สองคือ ขนาดของรายการยกเลิกใบรับรองที่มีขนาดใหญ่ทำให้การดาวน์โหลดใช้เวลานาน ต่อมาได้มีการพัฒนาวิธีการออกรายการยกเลิกใบรับรองเป็นรายการยกเลิกใบรับรองแบบเดลต้า (Delta-CRLs) เพื่อแก้ปัญหาข้างต้นโดยทำการออกรายการยกเลิกใบรับรองให้มีความถี่มากกว่ารายการยกเลิกใบรับรอง (Certificate revocation List:CRL) แต่วิธีการนี้ก็ยังทำให้ระบบยังคงมีปริมาณการใช้เครือข่ายสูง ซึ่งแต่ละวิธีการของการออกรายการยกเลิกใบรับรองของแต่ละงานวิจัยที่ผ่านมามีผู้วิจัยได้พบทั้งข้อดี ข้อเสียและข้อจำกัดที่แตกต่างกัน ซึ่งผู้วิจัยได้นำวิธีการเหล่านั้นมาใช้เป็นแนวทางในการพัฒนาวิธีการออกรายการยกเลิกใบรับรอง (CRL) ต่อไปในอนาคต

ดังนั้น ในงานวิจัยนี้จึงมุ่งเน้นในการพัฒนาวิธีการออกรายการยกเลิกใบรับรอง (CRL) เพื่อให้เครื่องแม่ข่าย (Repository) ที่ใช้ในการเก็บรายการยกเลิกใบรับรองให้การตอบสนองต่อคำร้องขอของผู้ใช้ได้รวดเร็วยิ่งขึ้น ลดอัตราการร้องขอ ลดปริมาณการใช้เครือข่ายและลดขนาดของรายการยกเลิกใบรับรองได้

1.2 ความมุ่งหมายและวัตถุประสงค์ของงานวิจัย

1.2.1 เพื่อศึกษาวิธีการออกรายการยกเลิกใบรับรอง

1.2.2 เพื่อศึกษาเทคนิควิธีการออกรายการยกเลิกใบรับรองในวิธีการต่างๆ

1.2.3 เพื่อนำความรู้ที่ได้ศึกษามาทั้งหมด พัฒนาวิธีการออกรายการยกเลิกใบรับรองที่ใช้ลักษณะการออกรายการยกเลิกใบรับรองให้มีช่วงเวลาที่ใช้ได้เหลื่อมกันและมีการแบ่งรายการยกเลิกใบรับรองให้กระจายไปยังเครื่องแม่ข่ายต่างๆ

1.3 แผนการดำเนินการวิจัย

1.3.1 ขั้นตอนการดำเนินงานวิจัย

1.3.1.1 ศึกษาบทความและผลงานวิจัยต่างๆ ที่เกี่ยวข้องกับงานวิจัยนี้

1.3.1.2 กำหนดหัวข้อ เป้าหมาย วัตถุประสงค์ และขอบเขตของวิทยานิพนธ์

1.3.1.3 ศึกษาทฤษฎีและหลักการที่เกี่ยวข้อง

1.3.1.4 ทดลองวิธีการออกใบรับรองที่ได้ศึกษาโดยใช้วิธีการทางคณิตศาสตร์

1.3.1.5 วิเคราะห์และออกแบบวิธีการใหม่ โดยใช้หลักการของการออกรายการยกเลิกใบรับรองต่อเนื่องแบบแบ่งส่วน (Over-issuing segmented CRLs) กับวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้า (Delta-CRLs)

1.3.1.6 พัฒนาโปรแกรมสำหรับจำลองวิธีการยกเลิกใบรับรองแบบใหม่

1.3.1.7 ทดลองวิธีการออกใบรับรอง โดยใช้โปรแกรมที่พัฒนา

1.3.1.8 วิเคราะห์ผล เปรียบเทียบ และสรุปผล

1.3.1.9 จัดทำเอกสารประกอบวิทยานิพนธ์

1.3.2 ระยะเวลาที่ใช้ในแต่ละขั้นตอน

ขั้นตอนการทำงาน	ระยะเวลาที่ใช้ (เดือนที่)											
	1	2	3	4	5	6	7	8	9	10	11	12
1. ศึกษาบทความและผลงานวิจัยต่างๆ ที่เกี่ยวข้องกับงานวิจัยนี้												
2. กำหนดหัวข้อ เป้าหมาย วัตถุประสงค์ และขอบเขตการทำวิทยานิพนธ์												

ขั้นตอนการทำงาน	ระยะเวลาที่ใช้ (เดือนที่)											
	1	2	3	4	5	6	7	8	9	10	11	12
3. ศึกษาทฤษฎีและหลักการที่เกี่ยวข้อง												
4. ทดลองวิธีการออกใบรับรองที่ได้ศึกษาโดยใช้วิธีการทางคณิตศาสตร์												
5. วิเคราะห์และออกแบบวิธีการใหม่												
6. พัฒนาโปรแกรมสำหรับจำลองวิธีการยกเลิกใบรับรองแบบใหม่												
7. ทดลองวิธีการออกใบรับรองโดยใช้โปรแกรมที่พัฒนา												
8. วิเคราะห์ผล เปรียบเทียบ และสรุปผล												
9. จัดทำเอกสารประกอบวิทยานิพนธ์												

1.4 ขอบเขตของงานวิจัย

การออกรายการยกเลิกใบรับรอง (CRLs) ประกอบด้วยงานหลักๆ คือ การรวบรวมรายชื่อใบรับรองที่หมดอายุ การกำหนดโครงสร้างของรายการยกเลิกใบรับรอง การกำหนดเวลาในการออกใบรับรอง การกระจายรายการยกเลิกใบรับรองให้แก่ผู้ใช้ แต่สำหรับงานวิจัยนี้จะมุ่งเน้นในส่วนของขั้นตอนการออกรายการยกเลิกใบรับรองให้แก่ผู้ใช้เท่านั้นและเครื่องมือที่จะใช้ในการพัฒนางานวิจัยนี้มีดังนี้

1.4.1 ภาษาที่ใช้เขียนโปรแกรมแบบจำลองนั้นใช้ภาษา JAVA Simulator (JSIM)

1.4.2 เครื่องคอมพิวเตอร์ที่ใช้ในการทดสอบผลการทำงานเป็นเครื่อง Pentium III ความเร็ว 1,000 MHz หน่วยความจำ 256 MB

1.4.3 ข้อมูลที่ใช้ในการทดสอบเป็นข้อมูลที่ได้จากเว็บไซต์ http://www.pvv.ntnu.no

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ได้ศึกษาถึงผลงานวิจัยที่เกี่ยวข้องกับวิธีการยกเลิกใบรับรองและปัญหาที่เกิดขึ้นสำหรับวิธีการยกเลิกใบรับรอง

1.5.2 เพื่อพัฒนาวิธีการยกเลิกใบรับรองในส่วนของวิธีการออกรายการยกเลิกใบรับรองให้มีประสิทธิภาพมากขึ้น

1.5.3 สามารถนำแนวคิดของวิธีการออกรายการการยกเลิกใบรับรองไปประยุกต์ใช้งานได้จริง

1.6 โครงสร้างของวิทยานิพนธ์

โครงสร้างของวิทยานิพนธ์ ประกอบด้วย 5 ส่วนคือ

บทที่ 1 บทนำ ซึ่งกล่าวถึง ความเป็นมาและความสำคัญของปัญหาที่จะต้องทำงานวิจัยนี้ วัตถุประสงค์ของงานวิจัย แผนการดำเนินงานวิจัย และประโยชน์ที่คาดว่าจะได้รับ

บทที่ 2 งานวิจัยที่เกี่ยวข้องและทฤษฎี ซึ่งจะกล่าวถึง พื้นฐานของโครงสร้างกุญแจสาธารณะ โครงสร้างของใบรับรอง วิธีการและโครงสร้างของรายการยกเลิกใบรับรอง วิธีการต่างๆ ของการออกรายการยกเลิกใบรับรอง

บทที่ 3 กล่าวถึงวิธีการออกรายการยกเลิกใบรับรอง โดยใช้วิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย

บทที่ 4 การทดลองและผลการทดลอง

บทที่ 5 สรุปผลการวิจัยและข้อเสนอแนะ

บทที่ 2
งานวิจัยที่เกี่ยวข้องและทฤษฎี

2.1 งานวิจัยที่เกี่ยวข้อง

งานวิจัยที่เกี่ยวข้องกับโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) หรือพีเคไอและวิธีการออกรายการยกเลิกใบรับรองนั้นได้มีการพัฒนาขึ้นในปี พ.ศ. 2537 สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (The National Institute of Standard and Technology: NIST) ร่วมกับบริษัทเอ็มไอทีอาร์อี (MITRE Corporation) [1] ได้ร่วมกันศึกษาแนวทางการจัดการกุญแจสาธารณะร่วมกับใบรับรองกุญแจสาธารณะร่วมกันแบบทำให้เป็นอัตโนมัติสำหรับรัฐบาลกลาง ซึ่งทางสถาบันได้เล็งเห็นว่ากุญแจสาธารณะนั้นสามารถใช้ในการรักษาความปลอดภัยบนระบบพาณิชย์อิเล็กทรอนิกส์ โดยใช้โครงสร้างพื้นฐานกุญแจสาธารณะ ในการศึกษานโยบายและกฎหมายที่ออกมาเกี่ยวข้องกับการปฏิบัติการและการจัดการโครงสร้างพื้นฐานกุญแจสาธารณะในการพิสูจน์เอกลักษณ์ และได้พัฒนาอีกวิธีการหนึ่งของโครงสร้างใบรับรองและการใช้โครงสร้างพื้นฐานกุญแจสาธารณะ โดยเพิ่มวิธีการในการกำหนดการหาค่าประเมินโครงสร้างพื้นฐานกุญแจสาธารณะ ในปีเดียวกันนั้น อิลลิ มูเลอร์ (Ueli Maurer) [2] ได้เสนอการกำหนดและความน่าจะเป็นของรูปแบบโครงสร้างพื้นฐานกุญแจสาธารณะสำหรับผู้ใช้ รวมทั้งเสนอแนะพารามิเตอร์ตัวแปรเสริมที่น่าเชื่อถือ ซึ่งผู้ใช้สามารถใช้ได้ง่าย โดยการประยุกต์ใช้พารามิเตอร์ที่เชื่อถือได้ที่ทำให้ใบรับรองหมดอายุในวันที่ถูกกำหนดโดยเฉพาะ ซึ่งทำให้เกิดพารามิเตอร์ที่น่าเชื่อถือในการลดเวลา

ในปี พ.ศ. 2539 ซิลวิโอ มิคาลิ (Silvio Micali) [3] ได้กล่าวถึงระบบการยกเลิกใบรับรองใหม่ที่เกี่ยวกับการปฏิบัติ ความปลอดภัย และประสิทธิภาพของระบบ ซึ่งได้อ้างถึงวิธีการเดิมและทำให้เกิดการค้นคว้าวิจัยทางด้านนี้มากขึ้น

ต่อมาในปี พ.ศ. 2540 มาร์ค บรานซ์ซวดค์ [4] ได้กล่าวถึงภาพรวมของโครงสร้างพื้นฐานกุญแจสาธารณะพร้อมทั้งกล่าวถึงโครงสร้างใบรับรองและโครงสร้างรายการยกเลิกใบรับรองบนมาตรฐาน X.509

ในปี พ.ศ. 2541 คารลิสล์ อดัมส์ (Carlisle Adams) และโรเบิร์ต ซูซเซอราโต้ (Robert Zuccherato) ของบริษัทเอ็นทรัส [5] ได้เสนอโครงสร้างรายการยกเลิกใบรับรองขนาดเล็กที่ให้ข้อมูลที่เหมาะสมที่ผู้ใช้ต้องการ ซึ่งสามารถวัดได้และมีความยืดหยุ่น เพื่อเป็นประโยชน์ในการจัดการในระยะเริ่มแรก ซึ่งจะให้บริการในการเว้นระยะการออกรายการยกเลิกใบรับรอง (Certificate Revocation List: CRL) หรือซีอาร์แอลให้เหมาะสมและตามความต้องการ โดยจะทำ

การแก้ไขได้ภายหลังถ้าต้องการ ซึ่งโครงสร้างนี้เป็นพื้นฐานในการกำหนดมาตรฐานและความต้องการ ซึ่งโครงสร้างเป็นส่วนขยายของใบรับรองและส่วนขยายของรายการยกเลิกใบรับรอง ในปีเดียวกันโมนิ นาออ (Moni Naor) และโคบบี นิซซิม (Kobbi Nissim) [6] ได้เสนอวิธีการใหม่ในการแก้ไขปัญหาการยกเลิกใบรับรอง ซึ่งวิธีการแก้ปัญหาคือใช้การค้นหาโครงสร้างข้อมูลที่น่าเชื่อถือโดยกระบวนการตรวจสอบใบรับรองที่อยู่ในรายการซึ่งจะคล้ายกับการปรับปรุงโครงสร้างข้อมูล (Data Structure) ของรายการยกเลิกใบรับรอง ต่อมาในปีเดียวกันโรนัลด์ ไรเวส (Ronald Rivest) [7] ได้กล่าวถึงการโครงสร้างในการปรับปรุงรายการยกเลิกใบรับรองและเสนอแนวคิดในการยกเลิการใช้รายการยกเลิกใบรับรอง ซึ่งเป็นไปได้ในการสร้างโครงสร้างใบรับรอง โดยให้ผู้ประกอบการรับรองแสดงใบรับรองที่เก็บไว้ไปยังผู้รับซึ่งคล้ายกับเป็นหลักฐานในการยืนยันการลงลายมือชื่อดิจิทัลในบนข้อมูล โดนผู้รับและผู้ส่งทำการแลกเปลี่ยนใบรับรองบางใบที่มีการปรับปรุงใหม่ ซึ่งในกรณีนี้ภาระหน้าที่จะเป็นของผู้ส่ง

ในปี พ.ศ. 2542 เดอะอินเทอร์เน็ตโซไซตี ได้ออกมาตรฐานอาร์เอฟซี 2459 (Request for Comments: 2459) อินเทอร์เน็ต เอ็กซ์ 509 โครงสร้างพื้นฐานกุญแจสาธารณะ ใบรับรองและโครงสร้างรายการยกเลิกใบรับรอง (Internet X.509 Public Key Infrastructure Certificate and CRL Profile) [8] ซึ่งได้กล่าวถึงโครงสร้างเอ็กซ์ 509 เวอร์ชั่น 3 ใบรับรอง (X.509 v3 Certificate) และเอ็กซ์ 509 เวอร์ชั่น 2 รายการยกเลิกใบรับรอง (X.509 v2 CRL) สำหรับใช้ในอินเทอร์เน็ต โดยกล่าวถึงภาพรวมของวิธีการและรูปแบบเอ็กซ์ 509 เวอร์ชั่น 3 ใบรับรองรวมทั้งข้อมูลในการพิจารณารูปแบบและความหมายที่กำหนดให้สำหรับคำและสัญลักษณ์ของหมายเลขไอพี (IP address) มาตรฐานส่วนเพิ่มเติมของใบรับรองและการกำหนดความต้องการของส่วนเพิ่มเติมนั้นๆ ในส่วนรูปแบบเอ็กซ์ 509 เวอร์ชั่น 2 รายการยกเลิกใบรับรองได้อธิบายและระบุถึงความต้องการในการกำหนดส่วนเพิ่มเติม รวมทั้งอัลกอริทึมสำหรับเอ็กซ์ 509 เวอร์ชั่น 3 เส้นทางการพิสูจน์ความถูกต้องของใบรับรอง

ต่อมาในปีเดียวกันเดวิด คูเปอร์ (David Cooper) [9] ได้นำเสนอวิธีการออกรายการยกเลิกใบรับรอง ซึ่งเป็นวิธีการพื้นฐานการออกรายการยกเลิกใบรับรอง โดยนำวิธีการทางคณิตศาสตร์มาใช้ในการอธิบายวิธีการนั้น ซึ่งวิธีการออกรายการยกเลิกใบรับรองแบบเดิม (Traditional Certificate Revocation List) เป็นการออกรายการยกเลิกใบรับรองที่มีรายการเดียวในช่วงเวลาที่กำหนดซึ่งเป็นสาเหตุให้อัตราการร้องขอในระบบสูง ต่อมาจึงได้พัฒนาวิธีการออกรายการยกเลิกใบรับรองแบบที่มีการจัดเก็บแบบกระจาย (Segmented CRLs) โดยวิธีการนี้จะทำการแบ่งรายการยกเลิกใบรับรองเป็นส่วนย่อยๆ และกระจายไปยังเครื่องแม่ข่ายที่ใช้ในการจัดเก็บเพื่อทำเกิดการกระจายอัตราการร้องขอของแต่ละเครื่องแม่ข่าย หลังจากนั้นได้นำเสนอสองวิธีการออกรายการยกเลิกใบรับรองแบบเหลื่อมเวลา (Over-issuing CRLs) โดยวิธีการนี้ได้กำหนดเวลาการ

ออกรายการยกเลิกใบรับรองโดยไม่สนใจว่ารายการยกเลิกใบรับรองในระบบนั้นหมดอายุหรือไม่ ทำให้ผู้ใช้ที่มีรายการยกเลิกใบรับรองที่ยังไม่หมดอายุนั้นไม่ต้องทำการร้องขอ ผลก็คืออัตราการร้องของรายการยกเลิกใบรับรองจะลดลง

ในปี พ.ศ. 2542 แพททริค แมคเดเนียล (Patrick Mcdaniel) และเอวิล รูบิน (Aviel Rubin) [11] ได้โต้ตอบแนวคิดของไรเวสเกี่ยวกับแนวคิดในการไม่ใช้รายการยกเลิกใบรับรองนั้นว่าไม่สมควร เนื่องจากรายการยกเลิกใบรับรองนั้นเหมาะสมและมีความจำเป็นอย่างยิ่งกับระบบความปลอดภัยทางอินเทอร์เน็ต เพราะถ้าไม่ใช้จะทำให้การติดต่อสื่อสารนั้นขาดความน่าเชื่อถือ ซึ่งนักวิจัยทั้งสองได้ยืนยันถึงความต้องการขั้นตอนการยกเลิกใบรับรองแบบทันทีซึ่งไม่ได้นำเสนอในการทำทรานแซคชันบนอินเทอร์เน็ต โดยใบรับรองนี้เป็นพื้นฐานในการทำพาณิชย์อิเล็กทรอนิกส์ ที่ใช้กลไกในการยกเลิกใบรับรองอย่างกว้างขวาง โดยขึ้นอยู่กับวิธีการที่นำมาใช้ซึ่งมีหลายวิธีการที่ทำให้รายการยกเลิกใบรับออกมาในเวลาที่เหมาะสมและช่วงเวลาที่เหมาะสมตามความต้องการ ซึ่งรายการยกเลิกใบรับรอง (CRLs) นั้นเหมาะสมที่สุดซึ่งเป็นการติดต่อสื่อสารที่รัดกุมในสภาพแวดล้อมบนอินเทอร์เน็ตหรือองค์กรขนาดใหญ่ที่มีการติดต่อสื่อสารทั้งภายในและภายนอก ซึ่งการติดต่อสื่อสารเหล่านี้จะต้องให้ผู้ประกอบการรับรองนั้นรับรองผู้ใช้เหล่านั้น ซึ่งเป็นไปได้ที่จะประสบผลสำเร็จในการยกเลิกใบรับรองแบบทันทีโดยใช้ CRLs ในกลไกการประกาศหรือลงลายมือชื่อดิจิทัลของรายการยกเลิกใบรับรอง ซึ่ง CRLs นั้นถูกสร้างขึ้นและถูกส่งไปยังผู้ต้องการตรวจสอบความถูกต้อง ดังนั้นนักวิจัยสองคนนี้จึงกล่าวไว้ว่าการใช้โครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) โดยไม่ใช้รายการยกเลิกใบรับรอง (CRLs) นั้นยาก เนื่องจาก CRLs นั้นเป็นเครื่องมือในการจำกัดค่าใช้จ่ายที่ใช้ร่วมกับรายการยกเลิกใบรับรอง และในตอนท้ายได้กล่าวถึงการออกแบบกลไกการยกเลิกซึ่งปัจจุบันยังไม่มีวิธีการออกรายการยกเลิกใบรับรองที่สามารถปรับใช้กับทุกสภาพแวดล้อม

ในปี พ.ศ. 2543 เดวิด คูเปอร์ (David Cooper) [10] ได้เสนอวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้า (Delta-Certificate Revocation Lists: Delta-CRLs) โดยวิธีการนี้จะทำการออกรายการยกเลิกใบรับรองหลายครั้งในช่วงเวลาที่กำหนด ซึ่งวิธีการนี้ไม่ได้ลดอัตราการร้องขอของระบบแต่เป็นการออกรายการให้มีความถี่มากขึ้นทำให้ข้อมูลการยกเลิดใบรับรองน้อยลงทำให้รายการยกเลิกใบรับรองมีขนาดเล็กลง ต่อมาได้เสนอวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้า (Over-issuing delta-CRLs) ซึ่งเป็นวิธีการที่ออกรายการยกเลิกใบรับรองโดยการกำหนดเวลาการออก ซึ่งทำให้ผู้ใช้ไม่ต้องทำการร้องขอถ้ารายการยกเลิกใบรับรองนั้นยังไม่หมดอายุ ซึ่งวิธีการต่างๆ นั้นเดวิด ได้นำคณิตศาสตร์มาใช้ในการอธิบาย

หลังจากปลายปี พ.ศ. 2543 นั้นแอนเดรีย อาร์เนส (Andre Årnes) [12] ได้มีการพิจารณาและวิเคราะห์ประเภทของการยกเลิกใบรับรองที่เหมาะสมในแต่ละองค์กร โดยพิจารณาในแต่ละ

เกณฑ์ (criterion) และได้ทำการเปรียบเทียบแต่ละวิธีการออกใบรับรองว่าวิธีใดเหมาะสมกับสภาพแวดล้อมแบบไหนและในปลายปีเดียวกันได้ออกเอกสาร [13]ในการวิเคราะห์และทำการเปรียบเทียบวิธีการออกรายการยกเลิกใบรับรองพร้อมทั้งแสดงผลการจำลองสภาพแวดล้อมและทำการทดสอบแต่ละวิธีการออกรายการยกเลิกใบรับรอง ในปีเดียวกันริชชาร์ด แอคนี (Richard C. Ankney) แห่งบริษัทเซิร์ทโค (CertCo, Inc.) [14] ได้นำเสนอวิธีการต่างๆของวิธีการออกรายการยกเลิกใบรับรองซึ่งได้กล่าวถึงวิธีการออกรายการยกเลิกใบรับรองหลายวิธีการ แนะนำวิธีการออกรายการยกเลิกใบรับรองแบบกระจายและวิธีการออกรายการยกเลิกใบรับรองแบบออนไลน์

ต่อมาในปี พ.ศ. 2544 อะซา แฮงสตรอม (Åsa Hagström) คริสโตเฟอร์ มิเชลเซน (Christopher Michelsen) และเดวิด โรว (David Rowe) [15]ได้กล่าวถึงภาพรวมของกลไกการยกเลิกใบรับรองหลักที่ใช้อยู่ในปัจจุบันและประเมินแต่ละวิธีการ เพื่อใช้ในการพิจารณาในการเลือกกลไกให้เหมาะสมกับแต่ละองค์กร

ในปี พ.ศ. 2545 ได้ออกมาตรฐานอาร์เอฟซี 3280 (Request for Comments: 3280) อินเทอร์เน็ต เอ็กซ์ 509 [16] ซึ่งได้กล่าวถึงโครงสร้างเอ็กซ์ 509 เวอร์ชั่น 3 ใบรับรอง (X.509 v3 Certificate) และเอ็กซ์ 509 เวอร์ชั่น 2 รายการยกเลิกใบรับรอง (X.509 v2 CRL) สำหรับใช้ในอินเทอร์เน็ต โดยกล่าวถึงภาพรวมของวิธีการและรูปแบบเอ็กซ์ 509 เวอร์ชั่น 3 ใบรับรองรวมทั้งข้อมูลในการพิจารณารูปแบบมาตรฐานส่วนเพิ่มเติมของใบรับรองและการกำหนดความต้องการของส่วนเพิ่มเติมนั้นๆ ในส่วนรูปแบบเอ็กซ์ 509 เวอร์ชั่น 2 รายการยกเลิกใบรับรองได้อธิบายและระบุถึงความต้องการในการกำหนดส่วนเพิ่มเติม รวมทั้งอัลกอริทึมสำหรับเอ็กซ์ 509 เวอร์ชั่น 3 เส้นทางการพิสูจน์ความถูกต้องของใบรับรอง

จากงานวิจัยที่เกี่ยวข้องนั้นได้เสนอว่ารายการยกเลิกใบรับรองนั้นมีความจำเป็นในโครงสร้างพื้นฐานกุญแจสาธารณะ เพื่อเพิ่มความน่าเชื่อถือให้แก่ระบบการรักษาความปลอดภัยที่ใช้ใบรับรอง ซึ่งวิธีการออกรายการยกเลิกใบรับรองนั้นมีหลายวิธีการในการเลือกใช้ให้เหมาะสมกับองค์กร และแต่ละวิธีการมีข้อดีข้อเสียที่แตกต่างกัน จึงได้มีการพัฒนาวิธีการออกรายการยกเลิกใบรับรองเพื่อให้มีประสิทธิภาพเพิ่มขึ้นเพื่อรองรับการทำงานให้เหมาะสมในแต่ละองค์กร

2.2 ทฤษฎี

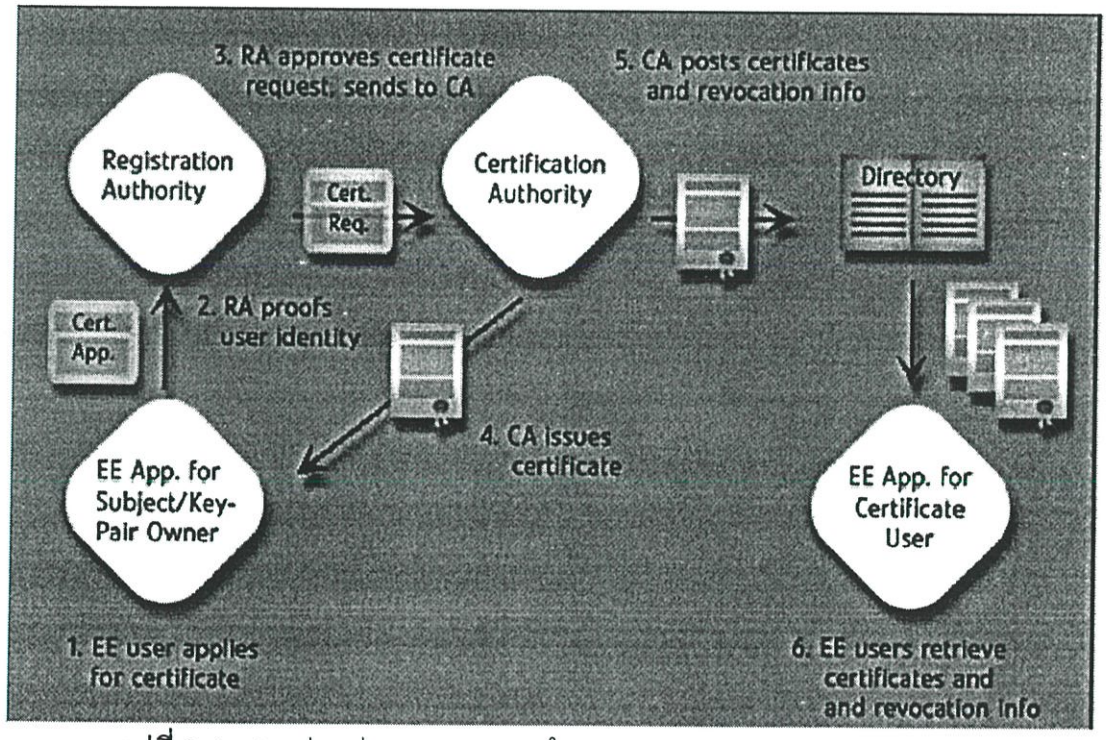
2.2.1 โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI)

สถาบันไออีทีเอฟ (Internet Engineering Task Force: IETF) ได้ออกเอกสาร PKIX [21] โดยให้คำนิยามของ Public Key Infrastructure (PKI) ว่าเป็นกลุ่มของฮาร์ดแวร์ ซอฟท์แวร์ คน

นโยบาย และกระบวนการที่จำเป็นต้องสร้าง จัดการ เก็บ กระจายและยกเลิกใบรับรอง ซึ่งเป็นพื้นฐานของวิทยาการเข้ารหัสลับแบบกุญแจสาธารณะ

PKI เป็นโครงสร้างพื้นฐานของการรักษาความปลอดภัยที่ใช้กันอย่างแพร่หลายใน 2-3 ปีที่ผ่านมา PKI มีบริการหลัก 4 บริการคือ [18][22]

- Authentication รับประกันการตรวจสอบเพื่อยืนยันตัวตนว่าผู้ส่งเป็นใคร
- Confidentiality รับประกันว่าข้อมูลเป็นความลับ ผู้ที่มีสิทธิ์เท่านั้นที่สามารถเข้าถึงข้อมูลได้
- Integrity รับประกันว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงแก้ไขขณะส่ง ซึ่งผู้รับจะแน่ใจได้ว่าข้อมูลที่ได้รับนั้นเหมือนกับข้อมูลที่ถูกส่งจากต้นทาง ไม่ถูกเปลี่ยนแปลงแก้ไขระหว่างการส่ง
- Non-repudiation รับประกันว่าผู้ส่งข้อมูลและผู้รับข้อมูลไม่สามารถปฏิเสธการรับส่งข้อมูลนั้นได้



รูปที่ 2.1 แสดงส่วนประกอบและการทำงานของ Public Key Infrastructure

ใน PKI ประกอบด้วยส่วนต่างๆ ดังรูปที่2.1 ดังต่อไปนี้

1. ผู้ใช้ (User) ผู้ใช้ในระบบแบ่งได้เป็นสองประเภท คือ

    1.1 ผู้ลงลายมือชื่อดิจิทัล (Signer) เป็นผู้ใช้กุญแจส่วนตัวและกุญแจสาธารณะในการลงลายมือชื่อดิจิทัลบนข้อมูลและใช้ใบรับรองในการพิสูจน์ตังผู้ลงลายมือชื่อเอง

1.2 ผู้ตรวจสอบ (Verifiers) เป็นผู้รับข้อมูลที่ลงลายมือชื่อดิจิทัลและต้องการทำการตรวจสอบลายมือชื่อดิจิทัลว่าเป็นของผู้ส่งจริงและใบรับรองนั้นถูกต้อง ซึ่งผู้ตรวจสอบเหล่านี้จะทำการเก็บการพิสูจน์ต่างๆ

2. ผู้ตรวจสอบการลงทะเบียน (Registration Authority) เป็นส่วนการตรวจสอบหลักฐานของผู้ร้องขอใบรับรองว่าผู้ร้องขอนั้นเชื่อถือได้และทำการตรวจสอบเครื่องที่ผู้ร้องขอใช้ เมื่อทำการตรวจสอบหลักฐานต่างๆ แล้วจะทำการส่งหลักฐานนั้นไปยังผู้ประกอบการรับรองต่อไป
3. ผู้ประกอบการรับรอง (Certificate Authority: CA) เป็นบุคคลที่ 3 ที่ผู้ใช้ทุกคนเชื่อถือได้ มีหน้าที่ออกใบรับรองและยกเลิกใบรับรอง โดยจะสร้างความสัมพันธ์ระหว่างข้อมูลผู้ใช้กับกุญแจสาธารณะ ซึ่ง CA จะทำการเชื่อมความสัมพันธ์นี้โดยการลงลายมือชื่อดิจิทัลทั้งข้อมูลและทำการประกาศลายมือชื่อดิจิทัล ซึ่งลายมือชื่อดิจิทัลที่ลงโดย CA นั้นสามารถพิจารณาได้เหมือนกับใบรับรอง ซึ่ง CA จะเก็บรายชื่อของใบรับรองที่ CA ได้ออกไปและใบรับรองที่ถูกยกเลิก โดย CA ทำการสร้าง CRL หรือ โครงสร้างข้อมูลใบรับรอง ซึ่ง CA เป็นตัวแทนที่เชื่อถือได้แต่ CA ไม่ได้จัดการเกี่ยวกับการร้องขอของผู้ใช้
4. เครื่องแม่ข่าย (Repository) ทำการจัดเก็บใบรับรองหรือ CRLs โดยรีพอสซิทีรีได้ทำให้ทุกการสอบถามของผู้ใช้เกี่ยวกับใบรับรองและสถานะของผู้ใช้ ดังนั้นรีพอสซิทีรีจะให้ข้อมูลที่ดีกว่าแก่ผู้ใช้ ซึ่งรีพอสซิทีรีจะได้ข้อมูลต่างๆ ที่ให้แก่ผู้ใช้จาก CA

โดยปกติ PKI มีการทำงานคล้าย X.509 โครงสร้างกุญแจสาธารณะ [22] ก่อนที่ PKI สามารถทำงานได้จะต้องมีบางงานที่จะต้องทำก่อน โดย CA จะทำการประกาศกุญแจสาธารณะให้ทราบโดยทั่วกัน หรือ CA ทำการรับรองกุญแจสาธารณะ ซึ่งทั้งสองกรณีนี้ใบรับรองของ CA จะถูกประกาศ

ก่อนที่ผู้ใช้ใหม่จะเข้าร่วมในระบบและทำรายการเปลี่ยนแปลงต่างๆ (transaction) จะต้องเกี่ยวข้องกับกุญแจสาธารณะ แต่ผู้ใช้ไม่สามารถทำการประกาศกุญแจสาธารณะและคาดหวังว่าผู้อื่นจะเชื่อถือกุญแจที่เป็นของผู้ใช้เอง ดังนั้นความสัมพันธ์ของผู้ใช้กับกุญแจที่ให้เป็นความเชื่อมั่นของกุญแจและข้อมูลบางอย่างที่บอกถึงการแสดงตัวของเจ้าของกุญแจสาธารณะ

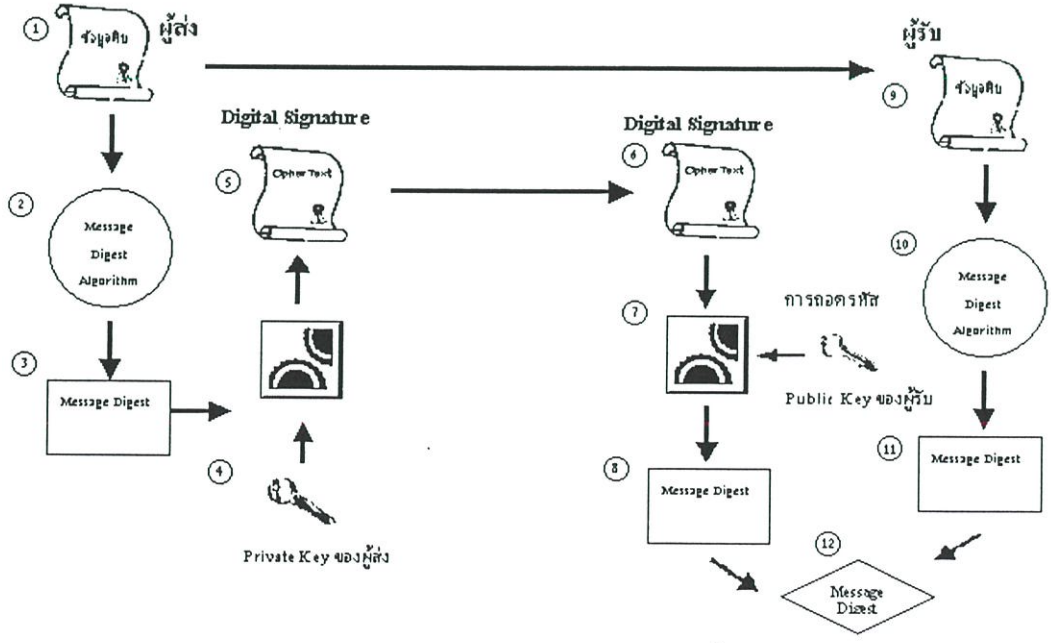
ตามกระบวนการที่ปรากฏ วิธีการแก้ไขปัญหาเกี่ยวกับการพิสูจน์หรือการระบุตัวบุคคล ซึ่งผู้ใช้ได้ติดต่อกับ CA ที่ให้บริการแบบออฟไลน์หรือ CA ที่ให้บริการแบบออนไลน์และทำการพิสูจน์ตัวบุคคล ในขณะที่ CA สร้างใบรับรอง ซึ่งในใบรับรองนี้เก็บสามส่วนคือข้อมูลเกี่ยวกับผู้ใช้ อัลกอริทึมในการพิสูจน์ตัวบุคคลจะใช้ในการลงลายมือชื่อดิจิทัล และข้อมูลผู้ใช้ในการลงลายมือชื่อดิจิทัลโดย CA หลังจากนั้น CA จะทำการสร้างใบรับรองนี้ โดยจะทำการเปิดเผยใบรับรองบนเครื่องแม่ข่ายหรือที่เก็บใบรับรอง (repository) ซึ่งในที่นี้ผู้ใช้จะเริ่มทำรายการเปลี่ยนแปลงต่างๆ ซึ่งมีกุญแจสาธารณะเข้ามาเกี่ยวข้อง ซึ่งจะใช้กุญแจสาธารณะในการรับรองด้วย

ผู้ตรวจสอบจะทำการตรวจสอบว่าลายมือชื่อดิจิทัลนั้นน่าเชื่อถือและใบรับรองนี้ใช้ได้ ซึ่งผู้ตรวจสอบจะยอมรับการทำรายการเปลี่ยนแปลงทุกรายการ โดยผู้ตรวจสอบใช้กุญแจสาธารณะที่ถูกเก็บในใบรับรองที่ถูกตรวจสอบว่าลายมือชื่อดิจิทัลนั้นเป็นของจริง ดังนั้นการตรวจสอบว่าใบรับรองนั้นน่าเชื่อถือทำได้โดยตรวจสอบลายมือชื่อดิจิทัลของ CA ในใบรับรองและทำการตรวจสอบว่าใบรับรองนั้นใช้ได้ การดำเนินงานให้บรรลุผลสำเร็จนั้นผู้ตรวจสอบต้องตรวจสอบช่วงเวลาที่ใบรับรองนั้นใช้ได้ (validity period) และใบรับรองนั้นไม่ถูกยกเลิก ดังนั้นผู้ใช้ควรตรวจสอบ CRLs สุดท้ายที่ออก ซึ่งถ้าทุกๆ การตรวจสอบผ่านแล้ว ผู้ตรวจสอบทราบว่าใบรับรองใบนั้นใช้ได้และใบรับรองใบนั้นลงลายมือชื่อดิจิทัลโดยผู้ลงลายมือที่ถูกต้อง จากนั้นผู้ตรวจสอบเก็บข้อมูลที่บันทึกวันเวลาของรายการเปลี่ยนแปลงเช่นเดียวกับลายมือชื่อดิจิทัลและใบรับรองของผู้ใช้

กลไกที่กล่าวมาข้างต้นนี้จะล้มเหลว ถ้า CA ไม่ทำการประกาศ CRLs ในเวลาที่เหมาะสมซึ่ง CA จะทำการประกาศ CRLs ที่ใหม่ ดังนั้นผู้ใช้สามารถค้นคืนรายการเปลี่ยนแปลงของใบรับรองที่ถูกยกเลิก ข้อเสียของระบบนี้คือการเสียเวลาระหว่างลงวันในใบรับรองที่ถูกยกเลิกและวันเวลาที่ปรากฏใน CRLs ซึ่งอาจเป็นสาเหตุให้บางรายการเปลี่ยนแปลงเกิดขึ้นและใบรับรองถูกใช้ แม้ว่าใบรับรองนั้นใช้ไม่ได้แล้วก็ตาม

2.2.2 **ลายมือชื่อดิจิทัล** (Digital Signature)

การลงลายมือชื่อดิจิทัล [20] มีจุดประสงค์เดียวกับการลงลายมือชื่อบนกระดาษ เพื่อใช้ตรวจสอบว่าใครเป็นผู้เขียนเอกสารและป้องกันการปลอมแปลงเอกสาร ซึ่งเหมาะกับการเข้ารหัสลับแบบกุญแจสาธารณะ โดยการลงลายมือชื่อดิจิทัลมีกระบวนการดังรูปที่ 2.2



รูปที่ 2.2 แสดงการทำงานของลายมือชื่อดิจิทัล

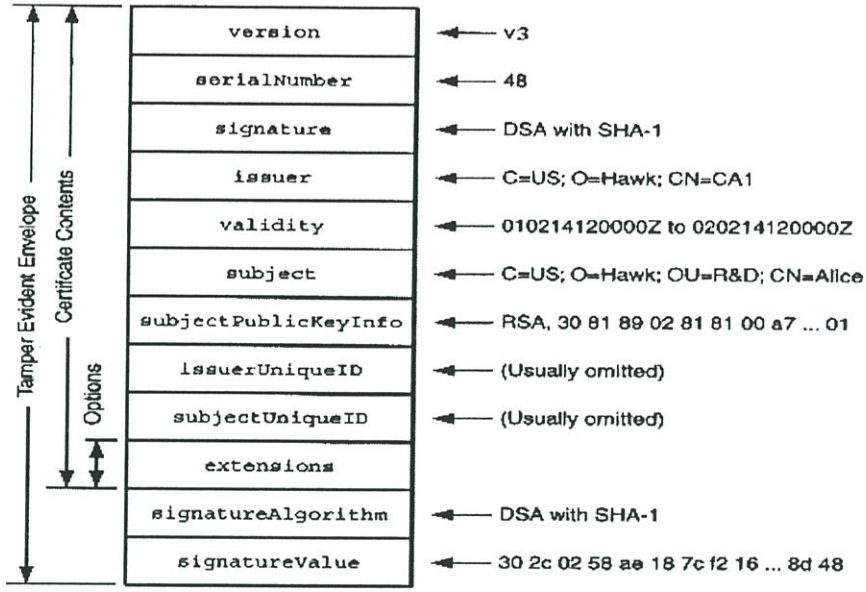
จากรูปที่ 2.2 แสดงการทำงานของลายมือชื่อดิจิทัลนี้จะเห็นได้ว่าผู้ส่งนำข้อความที่ต้องการส่งมาย่อขนาดของข้อความโดยผ่านฟังก์ชันแฮชซึ่งจะได้ข้อความที่ย่อแล้ว (Message Digest) จากนั้นผู้ส่งจะนำข้อความที่ย่อแล้วนั้นมาเข้ารหัสลับข้อความโดยใช้กุญแจส่วนตัวจะได้ลายมือชื่อดิจิทัลบนข้อความนั้น จากนั้นผู้ส่งจะทำการส่งข้อความและลายมือชื่อดิจิทัลให้แก่ผู้รับ เมื่อผู้รับได้รับลายมือชื่อดิจิทัลและข้อความแล้ว ผู้รับจะนำลายมือชื่อดิจิทัลมาถอดรหัสโดยใช้กุญแจสาธารณะของผู้ส่งจะได้ข้อความย่อออกมา จากนั้นผู้รับจะนำข้อความที่ได้มาทำการย่อขนาดข้อความโดยใช้ฟังก์ชันแฮชก็จะได้ข้อความย่อของผู้รับ นำข้อความย่อของผู้รับและผู้ส่งมาเปรียบเทียบกัน ถ้าข้อความย่อของผู้รับและผู้ส่งมาเปรียบเทียบกัน ถ้าข้อความย่อนั้นถูกต้องตรงกันแสดงว่าข้อความนี้ถูกส่งโดยผู้ส่งตัวจริง ซึ่งการทำงานของลายมือชื่อดิจิทัลนี้จะเห็นได้ว่าข้อความที่ไม่ได้ถูกเข้ารหัสลับสามารถอ่านข้อความได้โดยตรง ดังนั้นลายมือชื่อดิจิทัลไม่ได้ใช้เพื่อป้องกันข้อมูลแต่มีไว้เพื่อทำการตรวจสอบว่าข้อมูลนั้นถูกส่งมาจากผู้ส่งตัวจริง

2.2.3 **ใบรับรองดิจิทัล** (Digital Certificates)

ใบรับรองดิจิทัล [23] เป็นเอกสารที่มีความสัมพันธ์ระหว่างกุญแจสาธารณะและชื่อผู้ใช้ที่ใบรับรองอ้างถึงซึ่งผู้ใช้มีความสัมพันธ์กับกุญแจส่วนตัว ถ้า CA ที่ถูกต้องตามกฎหมายเท่านั้นที่ออกใบรับรอง โดยใบรับรองใบนั้นควรใช้ได้อย่างถูกต้องตามกฎหมาย

สถาบัน CCITT/ITU ได้มีการริเริ่มมาตรฐานระบบการรับรองขึ้นในปี ค.ศ. 1997 ได้กำหนดมาตรฐาน X.509 Public key certificate เวอร์ชัน 3 โดยพัฒนามาจากเวอร์ชัน1 โดยใช้โครงสร้างการตรวจสอบที่ปรับให้เข้ากับ X.500 รีพอสซิทีรีและพยายามที่จะทำงานกับลำดับชั้นของระบบโครงสร้างการรับรองทางอิเล็กทรอนิกส์ (Distinguish Name (DN)) ต่อมา X.509 เวอร์ชัน 1 ถูกพัฒนากลายเป็น X.509 เวอร์ชัน 2 และ X.509 เวอร์ชัน 3 ตามลำดับเพื่อลดข้อบกพร่องในเวอร์ชันก่อนหน้า (ปัจจุบันเวอร์ชัน 4 เป็น draft) ซึ่งใน X.509 เวอร์ชัน 3 เป็นพื้นฐานของ IETF PKIX working group ซึ่งการพัฒนาใบรับรองกุญแจสาธารณะ เพื่อการสื่อสารทางอินเทอร์เน็ตสามารถเพิ่มจำนวนในการใช้ใบรับรองที่สามารถปรับใช้ในองค์กร

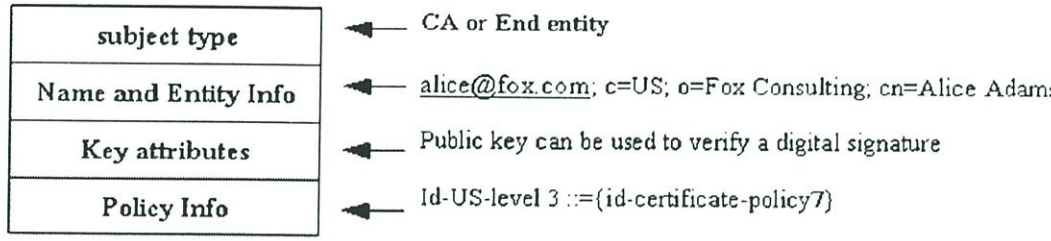
โครงสร้างของใบรับรองเก็บข้อมูลดังรูปที่ 2.3



รูปที่ 2.3 โครงสร้าง X.509 Certificate Version 3

ในโครงสร้างของใบรับรอง X.509 เวอร์ชัน 3 มีรายละเอียดดังนี้

- Version แสดงเวอร์ชันของใบรับรอง
- Serial Number เป็นตัวเลขที่ใช้ในการพิสูจน์ตัวบุคคลของใบรับรองซึ่งสัมพันธ์กับผู้ออกใบรับรอง
- Signature algorithm ID แสดงอัลกอริทึมที่ใช้ในการคำนวณลายมือชื่อดิจิทัลบนใบรับรอง
- Issuer name ชื่อพิเศษของผู้ออกใบรับรอง ซึ่งใช้ในการพิสูจน์ตัวจริง
- Validity period เป็นฟิลด์ที่ระบุวันเวลาของใบรับรองโดยพิจารณาจากเวลาเริ่มใช้และเวลาหมดอายุของใบรับรอง
- Subject name ชื่อผู้ส่งที่ใช้เปิดเผย
- Subject public key info เก็บรายละเอียดของกุญแจสาธารณะ เช่น อัลกอริทึม ค่าต่างๆ ของกุญแจสาธารณะ
- Issuer unique ID เป็นหมายเลขของผู้ออกใบรับรองที่ใช้แสดงตน อยู่ในเวอร์ชัน 2 และ 3
- Subject unique ID เป็นหมายเลขของเจ้าของใบรับรองที่ใช้แสดงตนอยู่ในเวอร์ชัน 2 และ 3
- Extensions เป็นส่วนเพิ่มเติมในเวอร์ชัน 3 ซึ่งมีการตรวจสอบกุญแจที่ใช้ในการลงลายมือชื่อดิจิทัล หมายเลขที่สัมพันธ์กับกุญแจสาธารณะ กุญแจสาธารณะที่ใช้ ระยะเวลาในการใช้กุญแจส่วนตัว นโยบายของใบรับรอง นโยบายที่ตรงกันระหว่าง CA ทั้งสองและรายละเอียดต่างของใบรับรอง ดังในรูปที่ 2.4



รูปที่ 2.4 โครงสร้างของข้อมูลในส่วนขยายของ X.509 Certificate เวอร์ชัน 3

ในโครงสร้างของใบรับรองกุญแจสาธารณะ X.509 นั้น ผู้ใช้แต่ละคนมีใช้ที่ใช้ในการจำแนกความแตกต่าง (Distinguished Name: DN) ที่ถูกกำหนดโดย CA โดย CA ทำการออกใบรับรองที่ลงลายมือชื่อภายใต้กุญแจสาธารณะของ CA เอง ซึ่งในโครงสร้างของ X.509 ทำการเก็บข้อมูลดังในรูปที่ 2.3 ซึ่งเมื่อผู้ใช้ A ทำการติดต่อสื่อสารกับผู้ใช้ B โดยผู้ใช้ A ได้ใบรับรองของ B จากเครื่องแม่ข่ายและทำการตรวจสอบความถูกต้องกุญแจสาธารณะของ CA โดยผู้ใช้จะรู้กุญแจสาธารณะของ CA ล่วงหน้า

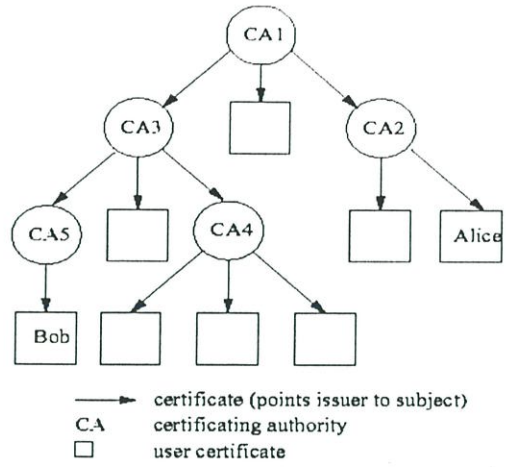
2.2.4 **เส้นทางใบรับรอง** (Certificate Paths)

ถ้าในระบบมี CA มากกว่าหนึ่ง CA มาเกี่ยวข้อง ผู้ใช้สองคนที่ทำการติดต่อสื่อสารกันอาจถูกรับรองจาก CA ที่ต่างกัน โดย CA ไม่สามารถสันนิษฐานไว้ก่อนว่าผู้ใช้มีกุญแจสาธารณะของ CA ที่ได้รับรองผู้ใช้คนอื่น เพื่อที่จะได้รับกุญแจสาธารณะ ซึ่งผู้ใช้จะได้รับใบรับรองของผู้ใช้คนอื่นจาก CA อื่น โดยกุญแจสาธารณะของ CA นั้นผู้ใช้จะได้รับอย่างปลอดภัยไม่ถูกโจมตีจากผู้ประสงค์ร้ายระหว่างการส่ง การรับรองของ CA เป็นการรับรอง CA ที่ถูกออกโดย CA อื่น ซึ่งหมายความว่ามีความสัมพันธ์ที่เชื่อถือได้ระหว่างสอง CAs [19]

โดยวิธีการเหล่านี้สามารถนำมาใช้ให้เป็นประโยชน์ในการเพิ่มจำนวนการออกใบรับรองของ CA จนกระทั่งกุญแจสาธารณะของ CA รับได้ ในวิธีการนี้มีเส้นทางของใบรับรอง (Certificate Paths) ไปยังผู้ใช้อื่นที่เกี่ยวข้องใน CA ส่วนกลางที่ได้รับกุญแจสาธารณะ

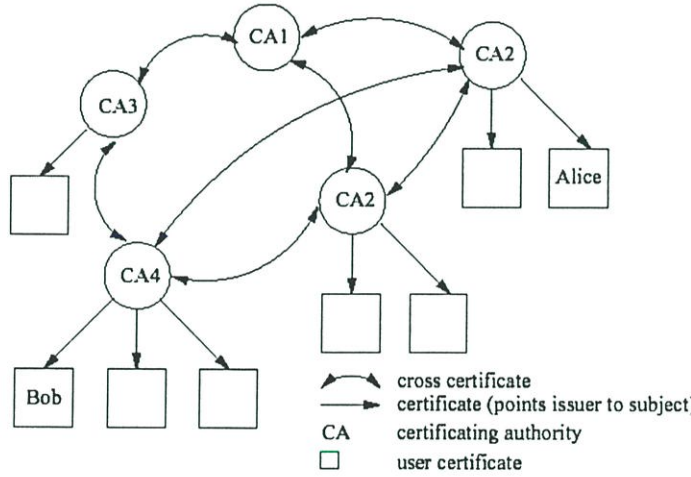
รูปแบบในการสร้างระบบกับความสัมพันธ์ระหว่าง CA มี 3 รูปแบบ ดังนี้คือ

1. รูปแบบลำดับชั้น (Hierarchical Model) เป็นโครงสร้างของ CA ที่มีรูปแบบคล้ายต้นไม้ โดยมีCA ที่เป็นรูท (root) โหนด 1 รูทโหนด [24]



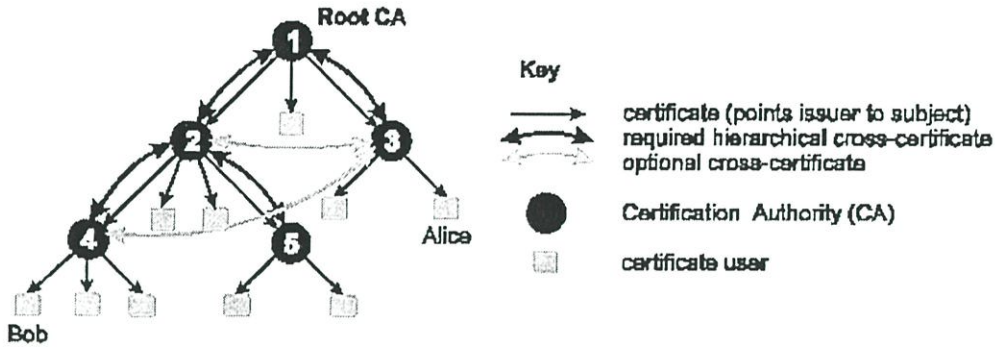
รูปที่ 2.5 ความสัมพันธ์ระหว่าง CA แบบลำดับชั้น

2. รูปแบบการรับรองไขว้กัน (Cross Certificates Model) เป็นโครงสร้างของ CA ที่ทุกๆ CA ทำการรับรองซึ่งกันและกัน [24]



รูปที่ 2.6 ความสัมพันธ์ระหว่าง CA แบบการรับรองข้ามกัน

3. รูปแบบผสม (Hybrid Model) เป็นโครงสร้างที่นำแบบลำดับชั้นและแบบการรับรองข้ามกันมารวมกัน โดยแบบผสมนี้เหมาะสำหรับการสร้างความสัมพันธ์ที่เชื่อถือได้ระหว่างองค์กรที่แตกต่างกันสององค์กร โดยที่ไม่เป็นโครงสร้างแบบลำดับชั้น [25]



รูปที่ 2.7 ความสัมพันธ์ระหว่าง CA แบบผสม

2.2.5 **การพิสูจน์ความถูกต้องของใบรับรอง** (Certificate Validation)

การพิสูจน์ความถูกต้องของใบรับรองเป็นกระบวนการพิสูจน์ว่าใบรับรองนั้นยังใช้ได้ ซึ่งจะทำการพิสูจน์ความถูกต้องว่าใบรับรองนั้นอยู่ในช่วงเวลาที่ใช้ได้และใช้การตรวจสอบการปลอมแปลงข้อมูล (Integrity check) ซึ่งจะขึ้นอยู่กับลายมือชื่อดิจิทัลของ CA ถ้าลายมือชื่อดิจิทัลใช้ได้ โดยการพิสูจน์ความถูกต้องของเส้นทางใบรับรอง (certificate path validation) ถูกแสดงขึ้นมา และ CA ที่เป็นรูท (anchors root node) จะถูกยอมรับและเชื่อถือ โดยกระบวนการพิสูจน์ความถูกต้องทำการตรวจสอบความสอดคล้องตรงกันในการใช้กุญแจสาธารณะและข้อจำกัดของนโยบายใบรับรอง สุดท้ายคือกระบวนการตรวจสอบสถานะการยกเลิกใบรับรองเพื่อให้แน่ใจได้ว่าใบรับรองใบนั้นยังใช้ได้ไม่ถูกยกเลิก [18]

2.2.6 **โครงสร้างการยกเลิกใบรับรอง** (Certificate Revocation Scheme)

การยกเลิกใบรับรอง (Certificate Revocation) [26,27,28] เป็นการประกาศว่าใบรับรองใบนี้ใช้ไม่ได้ก่อนที่ใบรับรองนั้นจะหมดอายุของใบรับรองเอง ซึ่งสามารถดูได้จากรายชื่อใบรับรองที่ถูกยกเลิก ซึ่งคล้ายกับ "Blacklist" บัญชีดำของบัตรเครดิตทั่วไป วิธีการยกเลิกใบรับรองและการกระจายข้อมูลการยกเลิกไปยังกลุ่มที่เกี่ยวข้องซึ่งเป็นสิ่งจำเป็นอย่างยิ่งใน PKI โดยมีหลายเหตุผลที่เป็นไปได้ที่ไม่ต้องการใช้ใบรับรองก่อนหน้าที่ใบรับรองใบนั้นหมดอายุ

โดยปกติใบรับรองทุกใบจะใช้ได้จนกระทั่งถึงวันหมดอายุของใบรับรองนั้น แต่สถานการณ์อยู่เหนือความคาดหมายที่บีบบังคับให้ผู้ใช้ยกเลิกการรับรองกุญแจสาธารณะ ซึ่งมีเหตุผลที่ทำให้ใบรับรองใช้ไม่ได้ก่อนหมดอายุดังต่อไปนี้

1. มีการเปลี่ยนแปลงในสถานะของผู้ใช้ ซึ่งผู้ใช้อาจมีการเปลี่ยนชื่อ ชื่อที่ทำงาน หรือข้อมูลอื่นๆ ในใบรับรอง ดังนั้นข้อมูลที่ถูกเก็บในใบรับรองจึงใช้ไม่ได้
2. กุญแจส่วนตัวของผู้ใช้อยู่ในอันตรายอาจถูกโจมตีจากผู้ประสงค์ร้าย ซึ่งผู้ใช้ต้องการยกเลิกกุญแจสาธารณะและกุญแจส่วนตัว เพื่อหลีกเลี่ยงการปลอมแปลงลายมือชื่อดิจิทัล

3. CA อยู่ในอันตราย กุญแจส่วนตัวของ CA อยู่ในอันตราย ดังนั้นเฉพาะ CA ที่อยู่ในอันตราย จึงต้องทำการยกเลิกใบรับรองทุกใบที่ทำการออกไป โดย CA จะหยุดทำงาน ดังนั้นทุกใบรับรองจึงถูกยกเลิกเหมือนกัน
4. ใบรับรองถูกใบรับรองอื่นแทนที่
5. ใบรับรองไม่ถูกใช้นานเพราะเป็นนโยบายเดิม
6. อัลกอริทึมที่ใช้ในการลงลายมือชื่อดิจิทัลในเอกสารอยู่ในอันตราย หรือไม่ให้การป้องกันเท่าที่จำเป็น

ระบบการยกเลิกใบรับรอง (Certificate Revocation Systems) สามารถแบ่งระดับได้ตามตัวแปรต่างๆ ดังต่อไปนี้

1. โดยการยกเลิกหรือข้อมูลที่ใช้ได้ถูกเก็บ ซึ่งในบางกรณีระบบได้เก็บบัญชีรายชื่อใบรับรองที่ใช้ไม่ได้ หรือเก็บบัญชีรายชื่อของใบรับรองที่ใช้ได้ หรือทั้งสองอย่าง
2. โดยกลไกที่ผู้ใช้ใช้ทำการตรวจสอบใบรับรองว่าใบรับรองนั้นใช้ได้ โดยเครื่องแม่ข่ายที่เชื่อถือได้ และให้ข้อมูลที่คำนวณได้นั้นแก่ผู้ใช้ ซึ่งเหมือนกับข้อมูลที่ถูกกระจายไปโดยใช้เครื่องแม่ข่ายไม่ได้ ในขณะที่ระบบอื่นใช้เครื่องแม่ข่ายได้
3. โดยกลไกที่ใช้การกระจายข้อมูลจาก CA ไปยังผู้ใช้ ในบางระบบผู้ใช้ได้รับข้อมูลที่ใหม่จาก CA ในขณะที่ระบบอื่นผู้ใช้ต้อการได้รับข้อมูลใหม่จาก CA (กลไกในการ Push และ Pull)

การยกเลิกใบรับรองมีหลายวิธีการ ซึ่งวิธีการเดิมเป็นแบบการตีพิมพ์รายชื่อใบรับรองที่ถูกยกเลิกตามช่วงเวลา เรียกว่า Certificate Revocation List (CRLs) ซึ่งเป็นรายชื่อใบรับรองที่ถูกยกเลิกภายในโดเมนเดียว ปัญหาของวิธีการนี้คือข้อมูลรายชื่อใบรับรองที่ถูกยกเลิกที่มีขนาดใหญ่ขึ้นสำหรับโดเมนขนาดใหญ่และความหนาแน่นของเครือข่ายที่เกี่ยวข้องในทุกๆ การดาวน์โหลดข้อมูลรายชื่อต่างๆ ของแต่ละเครื่องลูกข่ายทุกๆ เครื่อง (client) พร้อมกันจนเครื่องแม่ข่ายไม่สามารถให้บริการได้จึงทำให้มีการรอคิวของการร้องขอเป็นจำนวนมาก ซึ่งเป็นไปได้ที่ยากที่จะทำการเก็บบัญชีรายชื่อไว้ที่เครื่องลูกข่าย แต่บ่อยครั้งรายการยกเลิกใบรับรองนั้นมีการปรับปรุงอาจจำกัดในบางกรณี เช่น ข้อมูลในรายการยกเลิกใบรับรองที่ได้รับอาจไม่ใหม่เสมอไป โดยความแตกต่างของวิธีการมาตรฐานที่ให้เครื่องแม่ข่ายให้บริการ ซึ่งในกรณีนี้เครื่องลูกข่ายได้ออกคำร้องขอรายการยกเลิกใบรับรอง ซึ่งปัญหาของวิธีการนั้นแต่ละการตอบสนองได้มีการลงลายมือชื่อดิจิทัล ดังนั้นมีกระบวนการสำคัญและเกิดความหนาแน่นของเครือข่ายในแต่ละการตอบสนอง

วิธีการออกรายการยกเลิกใบรับรองนั้นสามารถอธิบายได้ว่า CA ได้ทำการประกาศข้อมูลใบรับรองที่ถูกยกเลิกทั้งหมดที่เครื่องแม่ข่ายหรือที่เก็บรายการยกเลิกใบรับรอง [12] ได้แนะนำประการแรกคือระบบที่มีข้อมูลเพียงพอในการพิสูจน์สถานะยกเลิกของใบรับรองบางส่วน โดย

ไม่ได้ทำการประกาศข้อมูลการยกเลิกทั้งหมดในแต่ละใบรับรอง โดยบอกเป็นนัยว่า เครื่องลูกข่ายได้ทำการร้องขอข้อมูลการยกเลิกจากเครื่องแม่ข่ายสำหรับแต่ละใบรับรองซึ่งจะดีกว่าช่วงเวลาละครั้ง ซึ่งหลายระบบมีวิธีการที่คล้ายคลึงกัน เพื่อที่จะได้เงื่อนไขที่เหมาะสมที่สุดของขนาดข้อมูลในการยกเลิกใบรับรองและลดงานในเครือข่าย ซึ่งบางปัญหาส่วนใหญ่เกิดกับระบบที่มีรูปแบบทางทฤษฎีที่ไม่เหมือนกันและบางระบบให้การตอบสนองได้น้อย ตั้งแต่นั้นระบบจึงไม่ให้ข้อมูลการยกเลิกผ่านใบรับรอง ซึ่งใช้ในระบบอื่น

ในบางปัญหาที่เกี่ยวกับ PKI ที่ได้กล่าวถึงใน [5][18] โดยได้ทำการจัดปัญหาที่พบใน PKI ได้ดังนี้

1. ความน่าเชื่อถือของผู้ใช้เป็นปัญหาสำหรับ CA ความน่าเชื่อถือของผู้ใช้จะเป็นไปได้ถ้าผู้ใช้และ CA อยู่ในโดเมนเดียวกัน เช่นผู้ใช้ติดต่อไปยัง CA และ CA ทำการตรวจสอบตัวบุคคลของผู้ใช้ได้ แต่ถ้าผู้ใช้และ CA อยู่ต่างโดเมนกันจะทำให้เกิดปัญหาจาก CA ได้
2. ความน่าเชื่อถือของ CA ทำให้เกิดปัญหา ซึ่งปัญหานี้เกี่ยวข้องกับการกระจายและการประกาศกุญแจสาธารณะของ CA
3. การสร้างโครงสร้างพื้นฐานการยกเลิกกุญแจสาธารณะ (Public Key Revocation Infrastructure) ซึ่งเป็นปัญหาร้ายแรงกับ PKI ปัจจุบัน ซึ่งเป็นการยากในการยกเลิกกุญแจสาธารณะและมีข้อมูลที่จะต้องรู้โดยตรงไปยังทุกฝ่ายที่เกี่ยวข้อง
4. การจัดการกุญแจส่วนตัว ซึ่งปัญหานี้จะครอบคลุมการเก็บ การใช้กุญแจส่วนตัว ซึ่งรวมถึงปัญหาการป้องกันกุญแจส่วนตัว
5. การกระจายกุญแจสาธารณะ ซึ่งในบางระบบ CA ใช้เครื่องแม่ข่ายในการประกาศกุญแจสาธารณะของผู้ใช้ ขณะที่ระบบอื่นผู้ใช้มีหน้าที่ในการให้และได้รับกุญแจสาธารณะของกลุ่มที่ผู้ใช้เหล่านั้นทำการติดต่อสื่อสารด้วย

ในโครงสร้างกุญแจลับ ถ้ากุญแจอยู่ในอันตราย กลุ่มของกุญแจที่อยู่ในอันตรายนั้นจะต้องแจ้งให้ทำสำเนา ซึ่งกุญแจที่อยู่ในอันตรายจะถูกยกเลิกและละทิ้ง และต้องทำการสร้างกุญแจคู่ขึ้นมาใหม่ โดยผู้ใช้จะต้องเริ่มทำการติดต่อสื่อสารใหม่ แต่ใน PKI นั้นเป็นเรื่องยากที่จะทำเช่นนั้น ถ้ากุญแจลับของผู้ใช้อยู่ในอันตราย ผู้ใช้จะต้องทำการแจ้งแก่ผู้ใช้คนอื่นในระบบ ซึ่งจะเป็นปัญหาภายหลัง เพราะมันไม่ได้ทำการแจ้งแก่ผู้ใช้เท่านั้นยังจะให้กุญแจที่มีอยู่อันตรายแก่ผู้ใช้ด้วย แต่ปัจจุบันผู้ใช้แต่ละคนได้ทำการตรวจสอบสถานะของทุกๆ กุญแจเพื่อให้แน่ใจได้ว่ากุญแจนั้นใช้ได้

2.2.6.1 **รายการยกเลิกใบรับรอง** (Certificate Revocation List: CRL)

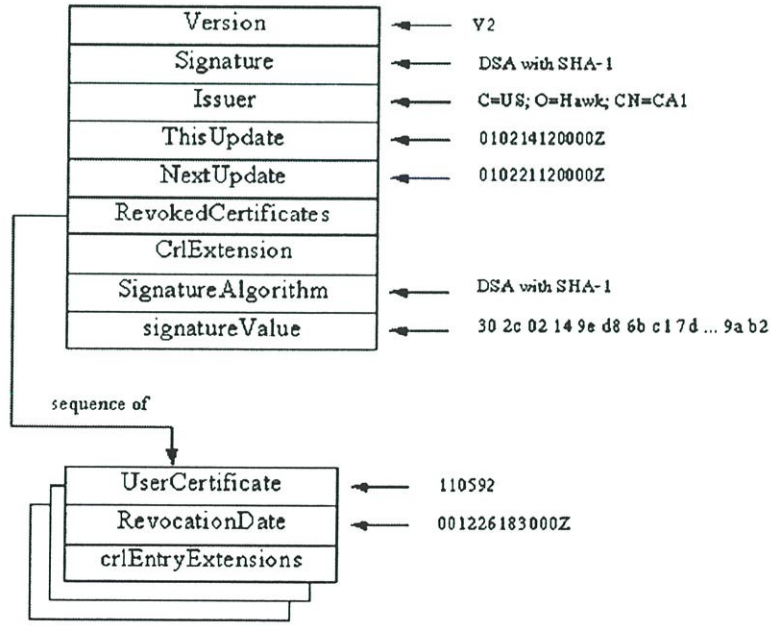
รายการยกเลิกใบรับรองเป็นรูปแบบโดยทั่วไปของการยกเลิกใบรับรองของ PKI โดย CA เป็นผู้ออกใบรับรองให้ผู้ใช้ เมื่อกุญแจส่วนตัวของผู้ใช้อยู่ในอันตรายอาจถูกโจมตีจากผู้ไม่ประสงค์ดีหรือกุญแจสาธารณะถูกยกเลิก ผู้ใช้จะต้องทำการติดต่อไปยัง CA โดย CA จะทำการประกาศ

ตามหมายเลขที่เรียงตามลำดับ (Serial number) ของใบรับรองที่ถูกยกเลิกในบัญชีรายชื่อยกเลิกใบรับรอง ซึ่งข้อมูลรายชื่อใบรับรองที่ถูกยกเลิกนี้จะถูกส่งไปให้ผู้ใช้ต่อไป โดยรายชื่อใบรับรองที่ถูกยกเลิก (Certificate Revocation List: CRL) มีโครงสร้างข้อมูลคล้ายกับโครงสร้างของใบรับรอง แต่แทนที่จะมีความสัมพันธ์ระหว่างกุญแจสาธารณะกับผู้ใช้ จะเป็นความสัมพันธ์ระหว่างข้อมูลรายชื่อใบรับรองที่ถูกยกเลิกกับ CA

ในปัจจุบันรายชื่อใบรับรองที่ถูกยกเลิก(CRL) ที่ใช้อยู่นี้เป็น X.509 เวอร์ชัน 2 ซึ่งถูกพัฒนาจาก X.509 เวอร์ชัน 1 (ปี ค.ศ. 1988) ซึ่งเวอร์ชัน 1 มีเนื้อหาดังต่อไปนี้

- การขยายขนาด ซึ่งขนาดของ CRLs ในเวอร์ชัน 1 มีการเติบโตขึ้นง่ายเกินขนาดที่จำกัด
- จำกัดหน้าที่ที่เกี่ยวข้องกับ ทำให้ไม่สามารถขยาย CRLs กับเพิ่ม ลักษณะสำคัญที่ต้องการ
- CRLs เวอร์ชัน 1 เป็นเรื่องของ การโจมตีโดยนำ CRL มาแทนโดยปราศจากการตรวจสอบ

CRLs เวอร์ชัน 2 ได้แก้ไขปัญหาโดยเสนอแนวคิดของการขยาย ซึ่งส่วนใหญ่จะเหมือนกับการเสนอส่วนขยายใน X.509 Public key certificate เวอร์ชัน3 โดยมีโครงสร้างข้อมูลของรายชื่อใบรับรองที่ถูกยกเลิก (CRL) ดังต่อไปนี้ [26]



รูปที่ 2.8 โครงสร้างข้อมูลของ Certificate Revocation List เวอร์ชัน 2

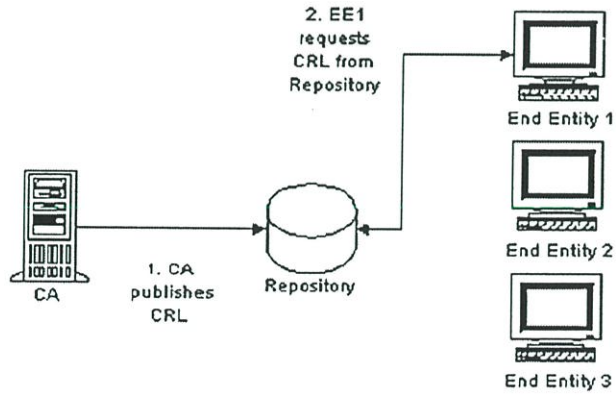
จากรูปที่ 2.8 โครงสร้างข้อมูลของ CRL เวอร์ชัน 2 มีรายละเอียดดังต่อไปนี้

- Version แสดงเวอร์ชันของ CRL ถ้ามีค่าเป็น 0 แสดงว่าเป็น CRL เวอร์ชัน1 และถ้ามีค่าเป็น 1 แสดงว่าเป็น CRL เวอร์ชัน 2
- Signature algorithm ID แสดงถึงหมายเลขที่ระบุอัลกอริทึมที่ถูกใช้ในการคำนวณลายมือ

ชื่อดิจิทัลบน CRL ตัวอย่างเช่น หมายเลขที่ระบุอัลกอริทึม Message Digest 5 (MD5)

- Issuer name ชื่อพิเศษของผู้ออก CRL ซึ่งจะต้องแสดงและมีชื่อเดียวเสมอ
- This update date/time แสดงวัน - เวลา ที่ CRL ออก ซึ่งแสดงเวลาปกติ
- Next update date/time แสดงวัน - เวลา ที่ CRL ต่อไปจะออก
- Revoked Certificate เป็นรายการใบรับรองที่ถูกเรียกคืน ซึ่งแต่ละ CRL จะถูกอ้างโดยหมายเลขที่เป็นตัวบอกภายใน Revoked Certificate จะเก็บหมายเลข serial number ซึ่งแต่ละรายการจะรวมเวลาที่ใบรับรองถูกเรียกคืน
- CrlExtension เป็นส่วนข้อมูลเพิ่มเติมที่ได้อธิบายถึงใบรับรองที่ถูกยกเลิก หรือพื้นฐานของ CRL โดยในส่วนขยายนี้จะมีค่า flag ต่างๆ คล้ายโครงสร้างของ X.509

เนื่องจาก CRL ถูกประกาศตามช่วงเวลาที่กำหนดอย่างสม่ำเสมอ โดยอนุญาตให้ผู้ใช้ทำการตรวจสอบว่ากุญแจสาธารณะของผู้ใช้คนใดใช้ได้ เมื่อผู้ใช้ทำรายการเปลี่ยนแปลงที่เกี่ยวข้องกับกุญแจสาธารณะ โดย CRL ทำการส่งข้อความที่มีลายมือชื่อดิจิทัลและสำเนาของใบรับรองที่ถูกยกเลิก หรือผู้ใช้อาจได้รับสำเนาจากเครื่องแม่ข่าย เมื่อกลุ่มที่ทำการติดต่อสื่อสารได้รับ CRL มาเพื่อทำการตรวจสอบกุญแจสาธารณะที่ใช้ได้ ซึ่งการตรวจสอบใบรับรองนั้นใช้ลายมือชื่อดิจิทัลของ CA บนใบรับรองนั้น โดยลายมือชื่อดิจิทัลบนข้อความประกอบด้วยกุญแจสาธารณะ ช่วงเวลาที่ใช้ใบรับรองนั้นได้ เป็นต้น



รูปที่ 2.9 ตัวอย่างระบบ CRL

จากรูปที่ 2.9 ที่แสดงระบบ CRL อย่างง่ายกับ CA โดยมีเครื่องแม่ข่ายเป็นฐานข้อมูลที่เก็บ CRL และมี 3 เอนทิที (End-Entities: EEs) ซึ่งกระบวนการทำงานจะเริ่มจาก CA ทำการประกาศ CRL ไปยังฐานข้อมูลที่เก็บ CRL แล้ว เอนทิทีปลายทางได้ทำการร้องขอหนึ่งคำร้องขอไปยังฐานข้อมูลที่เก็บ CRL จากนั้น เอนทิทีปลายทางจะได้รับ CRL จากฐานข้อมูลบนเครื่องแม่ข่ายและ

ทำการเก็บ CRL ไว้ที่เอนทิทีปลายทาง ต่อมาเอนทิทีปลายทางที่ 2 และ 3 ได้ทำการร้องขอ CRL ปัจจุบันและ CRL ถัดไปซึ่งโดยปกติ CRL ถัดไปจะประกาศหลังจากช่วงเวลาที่ใช้ CRL ก่อนหน้าหมดอายุ

เนื่องจากกุญแจสาธารณะสามารถยกเลิกได้ก่อนถึงวันหมดอายุบนใบรับรอง กลุ่มที่ได้รับใบรับรองจะทำการตรวจสอบว่าใบรับรองใบนั้นยังไม่ถูกยกเลิก ดังนั้นผู้รับจะได้รับ CRL ที่ใหม่ที่สุดจากเครื่องแม่ข่ายเพื่อทำการตรวจสอบ CRL ซึ่งถ้าเลขหมายประจำ (serial number) ของใบรับรองนั้นปรากฏบน CRL แสดงว่าใบรับรองใบนั้นถูกยกเลิก แต่ถ้าไม่มีข้อมูลที่กล่าวมาแล้วปรากฏบน CRL แสดงว่าใบรับรองใบนั้นใช้ได้

ยังมีบางปัญหาที่น่าสนใจเกี่ยวกับ CRLs ที่ถูกกล่าวถึงใน [20, 14] มีดังนี้

- ความยาวของบัญชีรายชื่อใบรับรองที่ถูกยกเลิก เนื่องมาจากใบรับรองถูกยกเลิกก่อนวันหมดอายุ ดังนั้นบัญชีรายชื่อใบรับรองที่ถูกยกเลิกจึงมีระดับความยาวเพิ่มขึ้น

- ข้อมูลรายชื่อของ CRL เป็นข้อมูลที่ถูกต้องเกี่ยวกับสถานะของใบรับรอง ซึ่งถ้าใบรับรองถูกยกเลิก CA จะต้องคอยจนกระทั่ง CRL ต่อไปออกมา ดังนั้นจึงมีการเสียเวลาในการรอระหว่างที่ใบรับรองถูกยกเลิกกับเวลาที่ CRL ต่อไปถูกประกาศออกมา ซึ่งการเสียเวลานั้นเองที่เป็นโอกาสให้ผู้ไม่ประสงค์ดีใช้กุญแจส่วนตัวหรือกุญแจสาธารณะที่ถูกยกเลิก

- เฉพาะ CRL เท่านั้นที่ให้ข้อมูลเกี่ยวกับใบรับรองที่ถูกยกเลิก แต่ไม่สามารถบอกรายละเอียดต่างๆ ของใบรับรองนั้นได้ ดังนั้นจึงเป็นการยากในการพิสูจน์ใบรับรองว่าใบรับรองใบนั้นมีอยู่หรือไม่มีอยู่จริง ซึ่งถ้าผู้ไม่ประสงค์ดีทำการปลอมแปลงใบรับรองแล้วนั้น CRL ไม่สามารถช่วยผู้ใช้ในการตรวจจับหรือยกเลิกใบรับรองปลอมเหล่านั้น

- CA ทำการกระจาย CRL ไปยังผู้ใช้ ซึ่งอาจเป็นสาเหตุของปัญหาเกี่ยวกับการคำนวณ โดยประการแรกคือ CA ทำการประกาศ CRL อย่างไร และ CA ทำการส่ง CRL ไปยังผู้ใช้หรือผู้ใช้มีส่วนร่วมในการได้รับ CRL ใหม่ที่สุดเมื่อผู้ใช้ต้องการ

การกำหนดปัญหาของ CRL [20][14] ได้นำเสนอการตัด CRL ออกและแนะนำให้ CA ทำการพิสูจน์ความเชื่อถือให้เร็วขึ้น เช่นการลงลายมือชื่อดิจิทัลบนใบรับรองให้เร็วขึ้น ตัวอย่างเช่นผู้รับใบรับรองต้องการสำเนาของ CRL ใหม่ของใบรับรอง แม้ว่าอาจจะแก้ไขปัญหาได้บางปัญหาที่เกี่ยวกับการยกเลิกกุญแจ เช่น ต้องการประกาศ CRL และการตัดเวลาที่เสียไประหว่างการยกเลิกกุญแจกับเวลาในการแจ้งให้ผู้ใช้ทราบว่ากุญแจนั้นถูกยกเลิกออกหรือสาเหตุของการใช้ปัญหาอื่น เช่นการเพิ่มขึ้นของจำนวนคำร้องขอไปยัง CA ดังนั้นการเพิ่มขึ้นของการใช้เครื่องแม่ข่ายที่เก็บใบรับรองและการตอบกลับไปยังผู้ใช้ที่ทำการร้องขออาจไม่ใช่ในกรณีนี้ เนื่องจาก CA ต้องการออกใบรับรองใหม่เป็นรายวันหรือรายชั่วโมงเป็นหลัก

สังเกตได้ว่า CRL ทำงานได้ดีในสภาพแวดล้อมที่มีจำนวนผู้ใช้ไม่มากและจำนวนการยกเลิกใบรับรองไม่มากและไม่บ่อย โดย CRL ยังเป็นการยกเลิกใบรับรองที่เหมาะสมและง่าย ซึ่งในแต่ละใบรับรองมีฟิลด์ CRL Distribution Point ซึ่งอยู่ในส่วนขยาย โดยฟิลด์ที่ได้ระบุให้ CRL Distribution Point สัมพันธ์กับใบรับรอง ซึ่งจะอธิบายในหัวข้อถัดไป โดยทั่วไปมีส่วนขยาย 3 ส่วนที่ใช้ใน CRL เพื่อความเหมาะสมกับโครงสร้างของ CRL โดยส่วนขยายที่ใช้ใน CRL มี 3 ส่วนดังนี้

- Issuing Distribution Point เป็นฟิลด์ที่ระบุถึง CRL Distribution Point ของใบรับรองโดยเฉพาะและระบุถึง CRL ข้อจำกัดในการยกเลิกของใบรับรองสำหรับแต่ละผู้ใช้โดยเฉพาะ หรือสำหรับ CA โดยเฉพาะ หรือข้อจำกัดเฉพาะกลุ่ม
- Certificate Issuer เป็นฟิลด์ที่ระบุถึงผู้ออกใบรับรอง ซึ่งสัมพันธ์กับ indirect CRL
- Delta CRL Indicator เป็นฟิลด์ที่ระบุถึง CRL ซึ่งคล้ายกับ Delta CRL

2.2.6.2 วิธีการออกรายการยกเลิกใบรับรอง

ในการวัดประสิทธิภาพวิธีการออกรายการยกเลิกใบรับรองนั้น คูเปอร์ [9][10] ได้สังเกตว่าอัตราการร้องขอสูงสุดของรายการยกเลิกใบรับรองมีความสำคัญมากกว่าอัตราการร้องขอเฉลี่ย เนื่องจากระบบควรใช้เวลาตอบสนอง (response time) ให้น้อยที่สุดได้ตลอดเวลา ซึ่งในกรณีนี้อัตราการร้องขอเฉลี่ยนั้นน่าสนใจน้อยที่สุด จึงได้ให้สมมติฐานว่าจำนวนเอนทิทีปลายทางนั้นมีขนาดใหญ่ คูเปอร์ได้สันนิษฐานว่าอัตราการร้องขอในการพิสูจน์ความถูกต้องของใบรับรองนั้นไม่ขึ้นกับใคร แต่ขึ้นอยู่กับรูปแบบวิธีการออกรายการยกเลิกใบรับรอง จึงได้คิดวิธีการออกรายการยกเลิกใบรับรองแบบต่างๆ เพื่อลดอัตราการร้องขอและให้เครื่องแม่ข่ายให้บริการได้เร็วมากยิ่งขึ้น โดยแต่ละวิธีการนั้นคูเปอร์ได้นำคณิตศาสตร์มาใช้อธิบายการหาอัตราการร้องขอ ซึ่งจะกล่าวต่อไป

2.2.6.2.1 วิธีการออกรายการยกเลิกใบรับรองแบบเดิม (Traditional CRL)

วิธีการในการกระจายข้อมูลสถานะใบรับรองที่เกี่ยวข้องกับผู้ประกอบการรับรอง (CA) ที่เป็นผู้ทำการออกรายการยกเลิกใบรับรอง (CRL) ตามเวลาที่กำหนดอย่างต่อเนื่อง โดยส่งไปเก็บยังเครื่องแม่ข่ายโดยข้อมูลในรายการยกเลิกใบรับรอง ที่กล่าวถึงนี้ได้รวมถึงใบรับรองที่ยังไม่หมดอายุที่ถูกออกโดย CA ซึ่งเป็นผู้ออกและยกเลิก CRL โดยแต่ละรายการยกเลิกใบรับรองนี้จะมีรายละเอียดสถานะใบรับรองที่หมดอายุ ที่ถูกออกโดย CA และในแต่ละฟิลด์ในรายการยกเลิกใบรับรองเป็นการกำหนดข้อมูลของผู้ประกอยการรับรองและรายละเอียดเจ้าของใบรับรอง ซึ่งรวมทั้งฟิลด์วันเวลาที่รายการยกเลิกใบรับรองต่อไปออกมา (nextUpdate) กลุ่มผู้ใช้ใดๆ ที่ต้องการข้อมูลสถานะใบรับรองโดยกลุ่มผู้ใช้นั้นไม่มีรายการยกเลิกใบรับรองที่เป็นปัจจุบัน กลุ่มผู้ใช้จะทำการดาวน์โหลดรายการยกเลิกใบรับรองมาจากเครื่องแม่ข่าย แต่เพื่อให้ประสิทธิภาพในการดาวน์โหลดดีขึ้น ผู้ประกอบการรับรองสามารถกระจายรายการยกเลิกใบรับรองไปยังเครื่องแม่ข่ายหลาย

เครื่องได้ เพื่อให้ทุกกลุ่มผู้ใช้สามารถดาวน์โหลดรายการที่เป็นปัจจุบันมากที่สุด ดังนั้นช่วงเวลาที่รายการยกเลิกใบรับรองใช้ได้ทุกๆ กลุ่มผู้ใช้จะทำการร้องขอจากเครื่องแม่ข่ายซึ่งการร้องขอนี้จะทำครั้งแรกเมื่อรายการยกเลิกใบรับรองปัจจุบันถูกออกมาโดยกลุ่มผู้ใช้ที่ต้องการทำการพิสูจน์ความถูกต้องของรายการยกเลิกใบรับรอง

ในการวัดประสิทธิภาพวิธีการออกรายการยกเลิกใบรับรองนั้น คูเปอร์ [9][10] ได้สังเกตว่าอัตราการร้องขอสูงสุดของรายการยกเลิกใบรับรองมีความสำคัญมากกว่าอัตราการร้องขอเฉลี่ย เนื่องจากระบบควรใช้เวลาตอบสนอง (response time) ให้น้อยที่สุดได้ตลอดเวลา ซึ่งในกรณีนี้อัตราการร้องขอเฉลี่ยนั้นน่าสนใจน้อยที่สุด จึงได้ให้สมมติฐานว่าจำนวนเอนทิทีปลายทางนั้นมีขนาดใหญ่ คูเปอร์จึงสันนิษฐานว่าความพยายามในการพิสูจน์ความถูกต้องของใบรับรองนั้นไม่ขึ้นอยู่กับใคร

การคำนวณอัตราการร้องขอรายการยกเลิกใบรับรองนั้นจะใช้ probability density function ในการพิสูจน์ความถูกต้อง เมื่อช่วงห่างของการพิสูจน์ความถูกต้องและเวลาการให้บริการเป็นโมเดลที่ไม่ขึ้นกับค่าตัวแปรสุ่มจากการกระจายแบบเอ็กซโปเนนเชียล (exponential distribution) กับค่าเฉลี่ย 1 นาทีสำหรับช่วงเวลาการออกรายการยกเลิกใบรับรองและค่าเฉลี่ย 0.5 นาทีสำหรับเวลาที่ให้บริการ การกระจายแบบเอ็กซโปเนนเชียลกับค่าเฉลี่ย β (β เป็นจำนวนจริงบวก) อย่างต่อเนื่องจะได้สมการดังนี้

$$f(x)=\frac{1}{\beta}e^{-x/\beta} \qquad for\ x \geq 0$$

ทางเลือกการกระจายแบบเอ็กซโปเนนเชียลกับค่าของ β ที่มีความสำคัญเนื่องจากเป็นสมการสำคัญในการสร้างความผันแปรของการสุ่มแบบเอ็กซโปเนนเชียล โดยการกระจายแบบเอ็กซโปเนนเชียลเป็นการกระจายอย่างต่อเนื่อง ถ้าผู้ใช้ทำการพิสูจน์ความถูกต้องไปยังเครื่องแม่ข่ายเป็นการกระจายแบบเอ็กซโปเนนเชียล โดยแทนด้วย ค่าเฉลี่ย $1/\lambda$ ซึ่งจะได้ฟังก์ชั่นความน่าจะเป็นของการกระจายคือ

$$F(\tau)=P(\tau<t)=1-e^{-\lambda t} \quad , \qquad t \geq 0$$

ซึ่งจะเห็นว่าการพิสูจน์ความถูกต้องและเวลาเริ่มที่ t = 0 โดยเวลาเฉลี่ยที่จะทำการพิสูจน์ครั้งต่อไปจะเป็น $1/\lambda$ ซึ่งจะสมมติให้เวลาที่จะไม่ทำการพิสูจน์ความถูกต้องจนกระทั่งเวลา t = x การกระจายของเวลาจนกระทั่งทำการพิสูจน์ครั้งต่อไปคือ

$$P(\tau - x < t \mid \tau > x) = \frac{P(x < \tau < x + t)}{P(\tau > x)}$$
$$= \frac{P(\tau < x + t) - P(\tau < x)}{P(\tau > x)}$$
$$= \frac{(1 - e^{-\lambda(x+t)}) - (1 - e^{-\lambda x})}{e^{-\lambda t}}$$
$$= 1 - e^{-\lambda x}$$

ซึ่งเหมือนกับว่าเหตุการณ์ได้เกิดขึ้น ณ เวลา t = 0 โดยเฉพาะเวลาเฉลี่ยที่จะทำการพิสูจน์ความถูกต้องครั้งต่อไปคือ $1/\lambda$ ดังนั้นเวลาที่คาดว่าจะทำการพิสูจน์ครั้งต่อไปจะเป็น $1/\lambda$ เสมอ โดยไม่สนใจเวลาตั้งแต่การพิสูจน์ครั้งสุดท้าย การกระจายแบบเอ็กซโปเนนเชียลจะใช้โมเดลเวลาระหว่างเหตุการณ์ที่ต่อเนื่อง โดยเฉพาะถ้าเหตุการณ์นั้นเกิดจากปัจจัย (factor) จำนวนมาก ตัวอย่างเช่น

1. เวลาระหว่างการมาของอัตราการร้องขออย่างต่อเนื่องไปยังเครื่องแม่ข่าย
2. เวลาระหว่างการล่ม (failure) ของเครื่องแม่ข่าย

เวลาการให้บริการของเครื่องแม่ข่ายเป็นรูปแบบการกระจายแบบเอ็กซโปเนนเชียล

โดยจากทฤษฎีของ exponential interarrival probability density ที่กล่าวข้างต้นได้นำมาประยุกต์ใช้ในการหาอัตราการร้องขอการออกรายการยกเลิกใบรับรอง ซึ่งเริ่มจากกลุ่มผู้ใช้ต้องการรายการยกเลิกใบรับรองโดยเฉพาะถ้าผู้ประกอบการรับรองทำการออกรายการยกเลิกใบรับรองใหม่ ณ เวลา $t = 0$ ความน่าจะเป็นที่กลุ่มผู้ใช้จะทำการพิสูจน์ความถูกต้องครั้งแรกหลังจากเวลา $t = 0$ เป็นเวลา $t = t$ exponential interarrival probability density สามารถนำมาใช้ในโครงสร้างเวลาในการพิสูจน์ความถูกต้อง ซึ่งโครงสร้างนี้เป็นความน่าจะเป็นที่กลุ่มผู้ใช้ทำการพิสูจน์ความถูกต้องครั้งแรก ซึ่งจะทำในช่วงระยะห่างเวลาระหว่างรายการยกเลิกใบรับรองสองรายการ (interval) เป็น $[t...t + dt]$ เมื่อ *limit* $dt \rightarrow 0$ จะได้

$$ve^{-vt}dt \qquad (2.1)$$

เมื่อ v เป็นอัตราการพิสูจน์ความถูกต้อง เนื่องจากแต่ละกลุ่มผู้ใช้ทำการดาวน์โหลดรายการยกเลิกใบรับรอง ณ เวลาที่ทำการพิสูจน์ความถูกต้องครั้งแรกหลังจากเวลา $t = 0$ โดยสมการนี้ได้แสดงถึงความน่าจะเป็นที่กลุ่มผู้ใช้จะส่งการร้องขอไปยังเครื่องแม่ข่ายในช่วงเวลา $[t...t + dt]$ ถ้า

สมการนี้คูณด้วยจำนวนกลุ่มผู้ใช้ N และหารด้วย dt ผลที่ได้จะเป็นอัตราการร้องขอรายการยกเลิกใบรับรองจากเครื่องแม่ข่าย ณ เวลา $t = t$

$$R(t) = Nve^{-vt} \tag{2.2}$$

2.2.6.2.2 **วิธีการออกรายการยกเลิกใบรับรองที่มีการจัดเก็บแบบกระจาย** (CRL with Distribution Points)

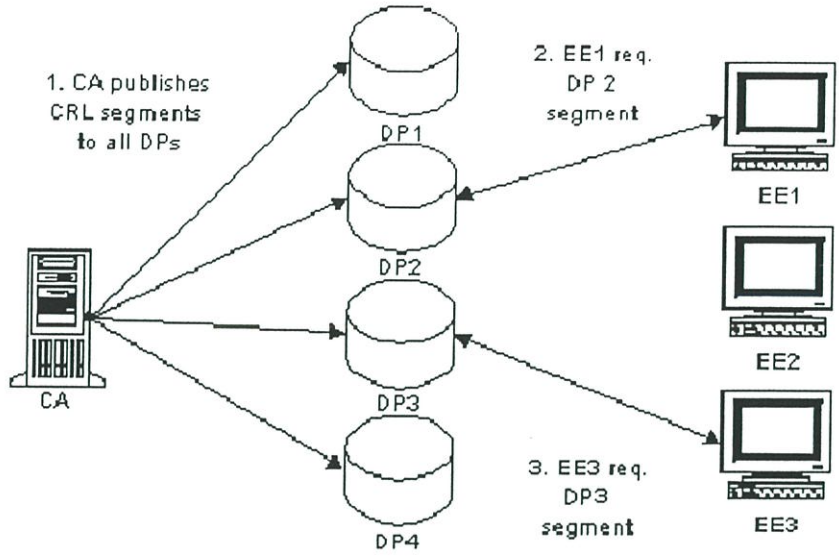
รายการยกเลิกใบรับรองแบบการจัดเก็บกระจาย (บางครั้งเรียกว่า รายการยกเลิกใบรับรองแบบแบ่งส่วน: Segmented CRLs) [16][29] ซึ่งจะให้ข้อมูลการยกเลิกภายใต้โดเมน CA ที่ทำการส่ง CRLs เดียวกัน โดยรายการยกเลิกใบรับรองแบบการจัดเก็บกระจาย มีสองลักษณะสำคัญคือ

- ข้อมูลการยกเลิกสามารถแบ่งออกเป็นส่วนย่อยๆ หรือแบ่งเป็นส่วนๆ ที่สามารถจัดการกับส่วนนั้นๆ ได้ เพื่อหลีกเลี่ยงการเพิ่มขึ้นอย่างรวดเร็วของ CRL ขนาดใหญ่ได้
- ใบรับรองสามารถบอกถึงที่ตั้งของ CRL Distribution Point ดังนั้นจึงไม่ต้องการที่จะรู้ที่เก็บข้อมูลการยกเลิกล่วงหน้า

ดังนั้นรูปแบบโครงสร้างส่วนเพิ่มเติมของรายการยกเลิกใบรับรองแบบการจัดเก็บกระจาย (CRL Distribution Point extension) สามารถระบุที่ตั้งเฉพาะส่วนของ CRL ที่ตอบสนอง ดังตัวอย่างเช่น รายการยกเลิกใบรับรองแบบกระจายสามารถระบุที่ตั้งเครื่องแม่ข่ายที่สามารถพบส่วนของ CRL ที่ถูกแบ่ง

โครงสร้างของรายการยกเลิกใบรับรองแบบการจัดเก็บกระจายได้ขยายโครงสร้าง โดยการเตรียม CRL ที่มีขนาดใหญ่ที่สุด ซึ่งขนาดที่ใหญ่ของ CRL ที่ถูกจำกัดโดยการแบ่ง CRL ของ CA เดียวออกเป็นส่วนย่อยๆ เมื่อ CRL ถูกแบ่งออกเป็นส่วนๆ และแต่ละส่วนถูกรวมกับ CRL Distribution Point ซึ่งเป็นที่ตั้งบนเครื่องที่ต่างกันหรือเครื่องแม่ข่ายบนเครื่อง (host) เดียวกันซึ่งแต่ละใบรับรองมีตัวชี้ไปยังที่ตั้ง (Location) ของรายการยกเลิกใบรับรองแบบกระจาย ดังนั้นจึงไม่ต้องการทั้งการค้นหาผ่านฟิลด์ crl distribution points ซึ่งระบุถึงวิธีการเข้าถึงรายการยกเลิกใบรับรอง (CRL) หรือรู้ที่ตั้งข้อมูลการยกเลิกก่อนหน้า

โครงสร้างของรายการยกเลิกใบรับรองแบบการจัดเก็บกระจายนี้ได้รวมเข้าใน X.509 ใบรับรองเวอร์ชัน 3 และ X.509 รายการยกเลิกใบรับรองเวอร์ชัน 2 [7] โดยใบรับรองใช้ส่วนขยายของรายการยกเลิกใบรับรองแบบการจัดเก็บกระจายชี้ไปยังเครื่องแม่ข่ายต่างๆ ที่เหมาะสม โดยแต่ละส่วนของ CRL ใช้ การออกแบบการจัดเก็บกระจาย (Distribution Points) ที่เหมาะสมในการขยายให้กว้างออกไป ซึ่งรวมถึงคุณสมบัติที่ต้องการประกอบกับค่าในส่วนขยายของใบรับรอง



รูปที่ 2.10 ตัวอย่างระบบการออกรายการยกเลิกใบรับรองแบบการจัดเก็บกระจาย (CRL Distribution Points)

จากรูปที่ 2.10 แสดงตัวอย่างระบบการออกรายการยกเลิกใบรับรองแบบการจัดเก็บกระจาย (CRL Distribution Points) อย่างง่ายกับ CA โดยมีสี่จุดในการจัดเก็บกระจาย (Distribution Points: DPs) และสามเอนทิทีปลายทาง (End-Entity: EEs) ซึ่งระบบมีการทำงานตามลำดับคือ เริ่มแรก CA ทำการประกาศส่วนของ CRL ที่ถูกแบ่ง (CRL segments) ไปยังเครื่องแม่ข่ายที่กระจายแล้วจากนั้น EE1 ทำการร้องขอ CRL ส่วนที่ 2 จาก DP2 และ EE3 ทำการร้องขอ CRL ส่วนที่ 3 จาก DP3 โดยจะเห็นว่าเอนทิทีปลายทางใดๆ สามารถทำการร้องขอ CRL ส่วนต่างๆจากเครื่องแม่ข่ายใดๆ ก็ได้ ยกเว้นถ้าหากว่า ส่วนแบ่งต่างๆ ของ CRL ถูกเก็บบนเอนทิทีปลายทางเรียบร้อยแล้ว เมื่อ CRL ปัจจุบันที่เก็บในแต่ละ EE หมดอายุ CA ก็จะทำการประกาศส่วนแบ่งใหม่ของ CRL

สรุปก็คือการออกรายการยกเลิกใบรับรองแบบการจัดเก็บกระจาย (CRL Distribution Points) ได้เสนอทางเลือกต่างๆ ในการเปรียบเทียบกับการประกาศ CRL ซึ่งสามารถใช้การออกรายการยกเลิกใบรับรองแบบการจัดเก็บกระจายนี้ ในการลดการใช้เครือข่าย (network usage) ซึ่งในการออก CRL เมื่อใช้ร่วมกับส่วนแบ่งของ CRL ที่มีอยู่เดิมและที่เก็บใหม่ อย่างไรก็ตามยังมีข้อบกพร่องที่ไม่เห็นด้วยในการใช้การออกรายการยกเลิกใบรับรองแบบการจัดเก็บกระจายคือส่วนแบ่งของ CRL (CRL Partitions) ที่ถูกกำหนดให้ไม่สามารถเปลี่ยนแปลงได้หรือขยายไม่ได้ ซึ่งการคิดที่จะนำโครงสร้าง dynamic partitioning scheme ที่สามารถพัฒนาผ่านการออกรายการยกเลิกใบรับรองแบบการจัดเก็บกระจายได้

ในการวัดประสิทธิภาพวิธีการออกใบรับรองแบบกระจายนั้นจะนำจำนวนอัตราการร้องขอและจำนวนการสื่อสารของแต่ละส่วนของรายการยกเลิกใบรับรองซึ่งลดลงเมื่อเปรียบเทียบกับวิธีการประกาศรายการยกเลิกใบรับรองแบบเต็ม โดยปกติถ้าเอนทิทีปลายทางต้องการบางส่วนของรายการยกเลิกใบรับรองเท่านั้น อัตราการใช้เครือข่ายโดยเฉลี่ยจะใช้น้อยกว่าเมื่อเปรียบเทียบกับอัตราการใช้เครือข่ายของรายการยกเลิกใบรับรองแบบเต็ม แต่ถ้าเอนทิทีปลายทางนั้นใช้ใบรับรองที่แตกต่างจากทุกส่วนของรายการยกเลิกใบรับรองที่เป็นไปได้บ่อยขึ้น แล้วนั้นวิธีการนี้จะไม่ลดอัตราการใช้เครือข่ายเฉลี่ย เนื่องจากทุกๆ ส่วนของรายการยกเลิกใบรับรองจะถูกดาวน์โหลด ซึ่งในกรณีนี้อัตราการใช้เครือข่ายสูงสุดจะลดลง แต่อัตราการใช้เครือข่ายเฉลี่ยจะยังคงเดิม เนื่องจากการดาวน์โหลดข้อมูลหลายๆ ส่วนก็จะคล้ายกับการดาวน์โหลดรายการยกเลิกใบรับรองแบบเต็ม

พื้นฐานการวิเคราะห์ของคูเปอร์นั้นคำนวณจากอัตราการร้องของทั้งหมด R_s สำหรับทุกๆ ส่วนของรายการยกเลิกใบรับรอง โดยคำนวณตามสมมติฐานต่อไปนี้

1. ข้อมูลการยกเลิกใบรับรองนั้นถูกออกแบบสุ่ม ดังนั้นทุกๆ อัตราการร้องขอข้อมูลการยกเลิกใดๆ จะเท่ากับการกระจายไปยังเครื่องแม่ข่ายต่างๆ
2. ทุกส่วนของรายการยกเลิกใบรับรองถูกออก ณ เวลาเดียวกัน

วิธีการออกรายการยกเลิกใบรับรองแบบแบ่งส่วนนี้ได้ถูกเสนอให้ใช้ในการกำหนดผลกระทบของการแบ่งอัตราการร้องขอ (request rate) ซึ่งในบางกรณีใบรับรองอาจถูกแบ่งเป็นส่วนๆ (CRL segments) โดยวิธีการแบบสุ่มเพื่อให้รายการยกเลิกใบรับรองมีขนาดเล็กลง ซึ่งกลุ่มผู้ใช้จะทำการดาวน์โหลดใบรับรองที่ถูกแบ่ง โดยแต่ละการพิสูจน์ความถูกต้องจะเท่ากับความต้องที่ถูกเข้าถึงในทุกๆ ส่วนของรายการยกเลิกใบรับรอง

Probability density function ของกลุ่มผู้ใช้คนหนึ่งกับส่วนหนึ่งส่วนใดของรายการยกเลิกใบรับรอง ซึ่งถ้ารายการยกเลิกใบรับรองไม่ได้ออกแบบเหลื่อมเวลาและแบ่งส่วนแล้วรายการยกเลิกใบรับรองใหม่จะถูกออกมา ณ. เวลา $t = 0$ แล้วกลุ่มผู้ใช้จะทำการร้องขอแต่ละส่วนจากเครื่องแม่ข่ายในช่วงระหว่างเวลา t ถึง $t+ dt$ ก็ต่อเมื่อการพิสูจน์ความถูกต้องของใบรับรองในช่วงระหว่างเวลา t ถึง $t + dt$ ต้องการใช้รายการยกเลิกใบรับรองหนึ่งส่วนนั้นและไม่มีการใช้ใบรับรองใดๆ ในช่วงเวลา $[0...t]$ ที่ต้องการใช้ส่วนแบ่งของรายการยกเลิกใบรับรองนั้น โดยในการทำการแบ่งส่วนของรายการยกเลิกใบรับรองมีการทำสองขั้นตอนดังนี้

ขั้นตอนแรก ความน่าจะเป็นที่กลุ่มผู้ใช้ไม่มีการร้องขอแต่ละส่วนของรายการยกเลิกใบรับรองในช่วงเวลา $[0...t]$ ซึ่งถูกกำหนด เนื่องจาก exponential interarrival probability ของการพิสูจน์ความถูกต้องถูกตั้งสมมติฐาน ซึ่งจากความรู้ที่ได้จาก Poisson Law ว่าความน่าจะเป็นที่ n พิสูจน์ความถูกต้อง (validation attempt) จะทำ ณ เวลา t จะได้สมการ

$$\left[\frac{(vt)^n}{n!}\right]e^{-vt} \tag{2.3}$$

ถ้าผู้ประกอบการรับรองได้ทำการแบ่งรายการยกเลิกใบรับรองออกเป็น s ส่วนแล้วจะได้ความน่าจะเป็นของส่วนแบ่งแต่ละส่วนเป็น $1/s$ โดยแต่ละส่วนของรายการยกเลิกใบรับรองจะถูกต้องการในการทำการพิสูจน์ความถูกต้อง ดังนั้นความน่าจะเป็นที่ส่วนแบ่งจะไม่ถูกต้องการสำหรับทุกๆ n การพิสูจน์ความถูกต้องจะได้

$$\left(1-1/s\right)^n \tag{2.4}$$

จากสมการ (2.3) และ (2.4) สามารถรวมกันได้โดยการกำหนดความน่าจะเป็นที่กลุ่มผู้ใช้ใดๆ ที่ไม่ทำการร้องขอส่วนแบ่งของรายการยกเลิกใบรับรองระหว่างช่วงเวลา $[0...t]$ จะได้

$$\sum_{n=0}^{\infty}\left(1-1/s\right)^n\left[\frac{(vt)^n}{n!}\right]e^{-vt}=e^{-vt/s} \tag{2.5}$$

ขั้นตอนที่สอง ความน่าจะเป็นที่กลุ่มผู้ใช้จะต้องการส่วนแบ่งของรายการยกเลิกใบรับรองระหว่างช่วงเวลา $[t...t + dt]$ โดย *limit* $dt \rightarrow 0$ ถูกกำหนด ซึ่งความน่าจะเป็นที่ทำการพิสูจน์ความถูกต้องครั้งแรกจะทำในช่วงเวลา $[t...t + dt]$ เป็น $ve^{-vdt}dt = vdt$ เนื่องจากความน่าจะเป็นที่พิสูจน์ความถูกต้องใดๆ ต้องการใช้ส่วนแบ่งของรายการยกเลิกใบรับรองเป็น $1/s$ ดังนั้นความน่าจะเป็นที่แต่ละส่วนถูกต้องการในช่วงเวลา $[t...t + dt]$ เป็น

$$\frac{v\,dt}{s} \tag{2.6}$$

จากสมการ (2.5) และ(2.6) นำมารวมกันและคูณด้วยจำนวนกลุ่มผู้ใช้ จำนวนการร้องขอแต่ละส่วนของรายการยกเลิกใบรับรองในช่วงเวลา $[t...t + dt]$ จะได้สมการดังนี้

$$N_s'(t)=\frac{Nve^{-vt/s}dt}{s} \tag{2.7}$$

นำสมการ (2.7) มาหารด้วย dt และคูณด้วยจำนวนส่วนของรายการยกเลิกใบรับรองจะได้ผลลัพธ์ของอัตราการร้องขอส่วนแบ่งของรายการยกเลิกใบรับรองรวม ดังสมการนี้

$$R_s(t) = \frac{sN'_s(t)}{dt} = Nve^{-vt/s} \tag{2.8}$$

เมื่อ s เป็นจำนวนการแบ่งของรายการยกเลิกใบรับรอง ซึ่งสมการ (2.8) นั้นแสดงอัตราการร้องขอสูงสุดในระบบ ส่วนอัตราการร้องขอเฉลี่ยจะสูงกว่าอัตราการร้องขอรายการยกเลิกใบรับรองแบบเดิม เนื่องจากแต่ละเอนทิทีปลายทางจะร้องขอมากกว่าหนึ่งส่วนในช่วงเวลาระหว่างที่ใช้ได้ (validity period) อย่างไรก็ตามโดยปกติทุกส่วนของรายการยกเลิกใบรับรองไม่ถูกร้องขอ ซึ่งทั้งอัตราการใช้เครือข่ายสูงสุดและอัตราการใช้เครือข่ายเฉลี่ยจะลดลงเมื่อเปรียบเทียบกับการออกรายการยกเลิกใบรับรองแบบเดิม

2.2.6.2.3 **วิธีการออกรายการยกเลิกใบรับรองแบบเหลื่อมเวลา** (Over-Issued CRLs)

การออกรายการยกเลิกใบรับรองแบบเหลื่อมเวลา [9] มีความเป็นไปได้ในการลดอัตราการร้องขอสูงสุด (peak request rate) โดยให้ CRLs หลาย CRLs มีช่วงเวลาในการใช้ส่วนหนึ่งที่ซ้อนทับกัน ซึ่งวิธีการนี้มีหลาย CRLs ใช้งานได้ โดยแต่ละ CRL จะมีเวลาการหมดอายุที่แตกต่างกัน แบบแผนนี้สามารถใช้ CRL ได้โดยไม่ต้องรอคอยจนกระทั่งถึงเวลา "NextUpdate" ของ CRL แต่จะต้องทำการออก CRL ใหม่ก่อน [18] ซึ่งการการะทำนี้ทำให้มี CRL ที่ยังไม่หมดอายุจำนวนมากกับการซ้อนทับของช่วงเวลาที่ CRL ใช้ได้ ซึ่งเอนทิทีปลายทางจะทำการร้องของ CRL ใหม่ที่สุดอย่างสม่ำเสมอ แต่ช่วงเวลาของ CRL นั้นยาวนานกว่าช่วงระยะเวลาของ CRL ต่อไปออก

ในการวัดประสิทธิภาพของวิธีการนี้จะพิจารณาจากวิธีการออกรายการยกเลิกใบรับรองพื้นฐาน ซึ่งได้ทดลองโดยการให้ทุก CRLs หมดอายุพร้อมกัน ดังนั้นเวลาที่เกิดอัตราการร้องขอสูงสุดจะปรากฏ ณ ช่วงเวลาที่เริ่มใช้ CRL ได้ ซึ่งวิธีการออกรายการใบรับรองแบบเหลื่อมเวลาเป็นวิธีการกระจายการร้องขอ ทำให้อัตราการร้องขอสูงสุดนั้นลดน้อยลงแต่มีการเกิดอัตราการร้องขอสูงสุดบ่อยขึ้น

ดังที่ได้อธิบายก่อนหน้านี้ว่ากลุ่มผู้ใช้จะทำการร้องขอรายการยกเลิกใบรับรองจากเครื่องแม่ข่ายในช่วงเวลาที่ให้เท่านั้น ถ้ากลุ่มผู้ใช้ทำการพิสูจน์ความถูกต้องในช่วงเวลาที่กำหนดและไม่มีรายการยกเลิกใบรับรองที่หมดอายุในที่เก็บของกลุ่มผู้ใช้ ถ้า O แสดงถึงจำนวนรายการยกเลิกใบรับรองที่ใช้ได้ ณ. เวลาใดๆ เมื่อสถานะระบบเป็น steady state และ P_{val} เป็นความน่าจะเป็นที่กลุ่มผู้ใช้จะทำการพิสูจน์ในช่วงเวลาใดๆ แล้วความน่าจะเป็นที่กลุ่มผู้ใช้จะทำการร้องขอรายการ

ยกเลิกใบรับรองในช่วงระยะเวลา n เป็น P_{val} ครั้ง ดังนั้นความน่าจะเป็นที่กลุ่มผู้ใช้ไม่ทำการร้องขอรายการยกเลิกใบรับรองในช่วงระยะเวลา O - 1 ก่อนหน้านี้เป็น

$$P_{I,n} = P_{val}\left[1 - \sum_{j=n-O+1}^{n-1} P_{I,j}\right] \tag{2.9}$$

เมื่อระบบได้มาถึงสถานะคงที่ (Steady state) ความน่าจะเป็นที่กลุ่มผู้ใช้จะร้องขอ CRL ในช่วงระยะเวลาเดียวกันในแต่ละช่วงที่ต่อเนื่องกัน (เช่น $P_I = P_{I,n} = P_{I,n-1} = P_{I,n-2} = \ldots$) ดังนั้นในสถานะคงที่ของระบบจะได้

$$P_I = P_{val}\left[1-(O-1)P_I\right] \tag{2.10}$$

สมการที่ (9) สามารถแก้ P_I จากสมการ (10) ได้ดังนี้

$$\begin{aligned} P_I &= P_{val} - P_{val}P_I(O-1) \\ P_I + P_{val}P_I(O-1) &= P_{val} \\ P_I\left(1+P_{val}(O-1)\right) &= P_{val} \\ P_I &= \frac{P_{val}}{(O-1)P_{val}+1} \end{aligned} \tag{2.11}$$

ถ้าช่วงระยะห่างเริ่มจากเวลา t = 0 แล้วความน่าจะเป็นที่กลุ่มผู้ใช้จะทำการร้องขอรายการยกเลิกใบรับรองจากเครื่องแม่ข่ายระหว่างเวลา t ถึง dt โดย *limit* $dt \longrightarrow 0$ นั้นเป็นความน่าจะเป็นที่กลุ่มผู้ใช้ทำการพิสูจน์ความถูกต้องครั้งแรกของช่วงเวลา t ถึง dt ซึ่งถูกคูณด้วยความน่าจะเป็นที่กลุ่มผู้ใช้ไม่มีรายการยกเลิกใบรับรองที่ใช้ได้ในที่เก็บของกลุ่มผู้ใช้ ซึ่งกลุ่มผู้ใช้ได้ทำการพิสูจน์ความถูกต้องครั้งแรกของช่วงเวลา t ถึง $t + dt$ ซึ่งจะนำมาคูณด้วยความน่าจะเป็นที่กลุ่มผู้ใช้ไม่มี รายการยกเลิกใบรับรองที่ใช้ได้ในที่เก็บของกลุ่มผู้ใช้ โดยที่กลุ่มผู้ใช้ได้นำรายการยกเลิกใบรับรองมาในช่วงเวลาก่อนหน้านี้แล้ว ซึ่งความน่าจะเป็นที่กลุ่มผู้ใช้ทำการพิสูจน์ความถูกต้องครั้งแรกในช่วงห่างระหว่างเวลา t ถึง $t + dt$ เป็น $ve^{-vt}dt$ ซึ่งความน่าจะเป็นที่กลุ่มผู้ใช้ไม่มีรายการยกเลิกใบรับรองที่ใช้ได้นั้นสามารถคำนวณคล้ายกับความน่าจะเป็นที่กลุ่มผู้ใช้จะทำการร้องขอรายการยกเลิกใบรับรองระหว่างช่วงเวลาที่ถูกแบ่งโดยความน่าจะเป็นที่กลุ่มผู้ใช้จะทำการพิสูจน์ความถูกต้องในช่วงเวลาระหว่างสองรายการยกเลิกใบรับรอง ดังนั้นความน่าจะเป็นที่กลุ่มผู้ใช้จะร้องขอในช่วง เวลา t ถึง $t + dt$ เป็น

$$\frac{ve^{-vt}dt}{(O-1)P_{val}+1} \tag{2.12}$$

นำสมการ (2.12) คูณด้วยจำนวนกลุ่มผู้ใช้ (*N*) และหารด้วย *dt* จะได้ผลลัพธ์เป็นอัตราการร้องขอรายการยกเลิกใบรับรองจากเครื่องแม่ข่าย ณ. เวลา $t = t$ จะได้

$$R_I(t) = \frac{Nve^{-vt}}{(O-1)P_{val}+1} \tag{2.13}$$

เนื่องจากการพิสูจน์ความถูกต้องตาม Exponential interarrival probability distribution นั้น ความน่าจะเป็นที่กลุ่มผู้ใช้จะไม่ทำการพิสูจน์ความถูกต้องระหว่างช่วงระยะห่างเป็น $e^{-vl/O}$ เมื่อ *l* เป็นระยะเวลาที่รายการยกเลิกใบรับรองใช้ได้ (เช่น ช่วงระยะห่างเป็นเวลา l/O) จะได้ $P_{val} = 1 - e^{-vl/O}$ ดังนั้นอัตราการร้องขอรายการยกเลิกใบรับรองที่ครอบคลุมช่วงห่างระหว่างสองรายการยกเลิกใบรับรองเป็น

$$R_I(t) = \frac{Nve^{-vt}}{(O-1)(1-e^{-vl/O})+1} \tag{2.14}$$

เมื่อ *N* เป็นจำนวนเอนทิทีปลายทาง *v* เป็นอัตราการพิสูจน์ความถูกต้องใบรับรอง *O* เป็นจำนวน CRLs ในช่วงเวลาที่ใช้ได้ และ *l* เป็นเวลาที่ใช้ CRL หนึ่ง CRL ได้

2.2.6.2.4 การออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบแบ่งส่วน (Over-Issuing Segmented CRLs)

จากที่กล่าวไปข้างต้นว่าโครงสร้างการออกรายการยกเลิกใบรับรองแบบการจัดเก็บกระจาย (CRL Distribution Points) [9] ซึ่งไม่ได้ลดอัตราการร้องของสูงสุด เมื่อเปรียบเทียบกับการประกาศรายการยกเลิกใบรับรองแบบเต็ม (full CRL) โดยประโยชน์ของวิธีการออกรายการยกเลิกใบรับรองแบบเหลื่อมเวลา (over-issued CRLs) และการประยุกต์วิธีการออกรายการยกเลิกใบรับรองแบบเหลื่อมเวลากับโครงสร้าง การออกรายการยกเลิกใบรับรองแบบการจัดเก็บกระจายเพื่อลดอัตราการร้องขอสูงสุดเป็นสำคัญ

ในการวัดประสิทธิภาพของวิธีการออกใบรับรองต่อเนื่องแบบแบ่งส่วนนั้นได้นำข้อดีของสองวิธีการคือการกระจาย การลดอัตราการร้องขอ และการลดอัตราการใช้เครือข่าย ซึ่งจะคล้ายกับ

วิธีการออกใบรับรองแบบเหลื่อมเวลา โดยคูเปอร์ [18] ได้นำเสนอวิธีการพื้นฐานสองวิธีสามารถใช้ร่วมกันได้ คือ

วิธีการแรก คือ ให้ทุกๆ ส่วนของรายการยกเลิกใบรับรองออกในเวลาเดียวกัน แต่ให้ออกส่วนของรายการยกเลิกใบรับรองบ่อยกว่าความต้องการของช่วงเวลาที่ใช้รายการยกเลิกใบรับรอง (validity period CRLs)

วิธีที่สอง คือ ให้แต่ละส่วนออกได้บ่อยเท่าที่จำเป็น แต่ให้แต่ละส่วนออกในเวลาที่เหลื่อมกัน ดังนั้น อัตราการร้องขอสูงสุดของแต่ละส่วน ที่ต่างกันจะปรากฏในเวลาที่ต่างกัน

เนื่องจากมีจำนวนส่วนแบ่งของรายการยกเลิกใบรับรองมากทำให้อัตราการร้องขอสูงสุดมีมากจนใกล้เคียงกับอัตราการร้องขอของรรายการยกเลิกใบรับรองแบบไม่แบ่งส่วน (unsegmented CRL) โดยปกติแล้วอัตราการร้องขอส่วนแบ่งของรายการยกเลิกใบรับรองถูกออกให้กระจายในช่วงห่างระหว่าง CRLs ซึ่งจะได้สมการดังนี้

$$\frac{Nve^{-vt'/s}}{s}\sum_{i=0}^{s-1}e^{-ivl/s^2}=\frac{Nve^{-vt'/s}}{s}\left(\frac{1-e^{-(s-1+1)^{-vl/s}}}{1-e^{-vl/s}}\right)=\frac{Nve^{-vt'/s^2}}{s}\left(\frac{1-e^{-svl/s^2}}{1-e^{-vl/s^2}}\right) \quad (2.15)$$

เมื่อ $t'=t \bmod (1/s)$ ถ้าผู้ประกอบการรับรอง (CA) ทำการออกรายการยกเลิกใบรับรองแบบเหลื่อมเวลาในแต่ละส่วนของรายการยกเลิกใบรับรองแล้วอัตราการร้องขอสูงสุดจะลดลงอย่างสม่ำเสมอ โดยเฉพาะอย่างยิ่งแต่ละส่วนที่ออกมาถี่มากขึ้นจะทำให้อัตราการร้องขอสูงสุดลดลงได้มากขึ้น เนื่องจากจำนวนส่วนแบ่งของรายการยกเลิกใบรับรองเพิ่มขึ้นระดับอัตราการร้องขอสูงสุดลดลง ดังนั้นถ้าข้อมูลรายการยกเลิกใบรับรองถูกแบ่งเป็นส่วนๆ จำนวนมากเพื่อลดขนาดของแต่ละส่วนของรายการยกเลิกใบรับรองแล้วอาจไม่มีประโยชน์ในรูปของอัตราการร้องขอสูงสุด โดยใช้วิธีการออกรายการยกเลิกใบรับรองแบบเหลื่อมเวลาและแบ่งส่วน (over-issuing segmented CRLs) หรือการวิธีการออกรายการยกเลิกใบรับรองแต่ละส่วนให้มีช่วงระยะเวลาการใช้งานเหลื่อมกัน

โดยปกติ อัตราการร้องขอรายการยกเลิกใบรับรองแบบเหลื่อมเวลาและแบ่งส่วนจะเป็น

$$R_I(t)=\frac{Nve^{-vt/s}}{(O-1)\left(1-e^{-vl/sO}\right)+1} \quad (2.16)$$

เมื่อ t เป็นเวลารวมทั้งหมดตั้งแต่ แต่ละส่วนแบ่งของรายการยกเลิกใบรับรองออกมา และ O เป็นระดับการซ้อนทับของแต่ละส่วนของ CRL

2.2.6.2.5 **วิธีการออกรายยกเลิกใบรับรองแบบเดลต้า** (Delta-CRLs)

การออกรายการยกเลิกใบรับรองแบบเดลต้า [10] เป็นรายการที่มีการเปลี่ยนแปลงเพิ่มขึ้น ซึ่งปรากฏตั้งแต่การประกาศ CRL ที่สมบูรณ์ครั้งสุดท้าย [8] ซึ่ง Delta-CRLs เป็นการประกาศตามกำหนดเวลาและดำเนินการคล้ายกับการปรับ CRL แบบเต็ม (full CRL) ที่ปิดประกาศครั้งสุดท้ายให้ข้อมูลใน CRL นั้นใหม่ Delta-CRLs มีขนาดเล็กกว่า CRL แบบเต็ม แต่ Delta-CRLs สามารถประกาศได้บ่อยกว่า CRL ซึ่งการประกาศ CRL แบบเต็มที่ถูกเก็บบนเอนทิทีปลายทางและอ้างถึงการประกาศ CRL พื้นฐาน ในขณะที่ Delta-CRLs ถูกพิจารณาในการประกาศข้อมูลเพิ่ม น่าสังเกตว่าความเป็นไปได้ของการประกาศ Delta-CRLs หลาย Delta-CRLs นั้นเหมือนกับ CRL พื้นฐาน โดย Delta-CRLs เป็นการเพิ่มขึ้นของ CRL พื้นฐาน CRL เดียวเท่านั้น (และไม่มี Delta-CRLs อื่น) ข้อมูลการยกเลิกที่ใหม่ที่สุดได้รับมาจากการประกาศ CRL พื้นฐานที่ใหม่ที่สุดและ Delta-CRLs ที่ใหม่ที่สุด

Delta-CRLs ถูกนำมาใช้เพื่อเพิ่มข้อมูลรายการยกเลิกใบรับรองตามเวลาที่เหมาะสม โดยไม่มีผลกระทบที่สำคัญต่อประสิทธิภาพของ CRL ซึ่งสอดคล้องกับ X.509 Delta-CRLs (ปี ค.ศ. 1997) ซึ่ง Delta-CRLs สามารถใช้ในการเชื่อมโยงกับการประกาศ CRL แบบเต็ม หรือ CRL Distribution Points

แนวความคิดเบื้องหลัง Delta-CRLs ในการเพิ่มการประกาศข้อมูลการยกเลิกใบรับรอง ซึ่งไม่ต้องการให้เกิด CRL แบบสมบูรณ์ (complete CRL) ที่มีขนาดใหญ่มากในแต่ละครั้งที่ออก CRL อย่างไรก็ตาม Delta-CRLs ไม่สามารถทำการลดความต้องการทั้งของการประกาศ CRL แบบเต็มหรือแบบ Distribution Point ซึ่ง Delta-CRLs เป็นพื้นฐานของข้อมูลการยกเลิกที่ปิดประกาศ (posting) ก่อนหน้านี้ โดยข้อมูลที่ปิดประกาศได้อ้างไปยัง CRL พื้นฐาน (based CRL) และ Delta-CRLs ที่เก็บข้อมูลการยกเลิกซึ่งไม่เพียงพอ เมื่อ CRL พื้นฐานถูกสร้างขึ้น ซึ่งจะยอมให้ประกาศ Delta-CRLs ขนาดเล็กที่สามารถออกได้บ่อยกว่า CRL พื้นฐาน

ในการวัดประสิทธิภาพนั้นดูจากช่วงเวลาที่ใช้รายการยกเลิกใบรับรองพื้นฐานได้นานขึ้น เนื่องจาก delta-CRLs เป็นการประกาศรายการยกเลิกใบรับรองที่มีขนาดเล็กกว่าและในเวลาที่เหมาะสม ดังนั้นอัตราการใช้เครือข่ายเฉลี่ยจะลดลง โดยอัตราการร้องขอของทั้งรายการยกเลิกใบรับรองพื้นฐาน (base CRL) และรายการยกเลิกใบรับรองแบบเดลต้า (delta-CRL) คล้ายกับวิธีการออกรายการยกเลิกใบรับรองพื้นฐานในแต่ละช่วงเวลาที่ใช้ได้ โดยวิธีการนี้จะมีอัตราการร้องขอ base CRL สูงสุด ณ เวลาที่เริ่มใช้ CRL ได้ และ อัตราการร้องของ delta-CRL สูงสุด ณ เวลาที่เริ่มใช้ delta-CRL ได้ ช่วงเวลาที่ใช้ delta-CRL มีช่วงเวลาน้อยกว่าจะทำให้เกิดอัตราการใช้

เครือข่ายสูงได้ แต่สามารถปรับเวลาในการออกรายการยกเลิกใบรับรองให้เหมาะสมได้เมื่อเปรียบเทียบกับวิธีการออกรายการยกเลิกใบรับรองแบบเดิม เนื่องจากอัตราการร้องขอเบสซีอาร์แอลถูกกำหนดให้กระจายเป็นช่วงเวลาสองช่วง คือ ช่วงที่รายการยกเลิกใบรับรองใหม่ออกมาในเวลาเดียวกับเดลต้าซีอาร์แอลออกมา (a "synch" interval) และ ช่วงที่รายการยกเลิกใบรับรองใหม่ออกมไม่พร้อมกับเดลต้าซีอาร์แอลออกมา (a "non-synch" interval)

ถ้าเวลา t เป็นช่วงเวลา "synch" แล้วกลุ่มผู้ใช้จะทำการร้องขอเบสซีอาร์แอลจากเครื่องแม่ข่ายที่เวลา $t = t$ ก็ต่อเมื่อไม่ทำการพิสูจน์ความถูกต้องระหว่างช่วงเวลาที่เบสซีอาร์แอลใหม่ล่าสุดก่อนหน้าและทำการพิสูจน์ความถูกต้องครั้งแรกของช่วงเวลาปัจจุบันที่ $t = t$ ถ้าเบสซีอาร์แอลออกจำนวน L ครั้งต่อหน่วยเวลา (L time unitapart) แล้วความน่าจะเป็นที่กลุ่มผู้ใช้จะไม่ทำการพิสูจน์ความถูกต้อง ระหว่างช่วงเวลาที่เบสซีอาร์แอลใหม่เป็น e^{-vL} ซึ่งคล้ายกับว่าถ้าช่วงห่างระหว่างสองเบสซีอาร์แอล ปัจจุบันเริ่มต้นที่เวลา $t = 0$ ความน่าจะเป็นที่กลุ่มผู้ใช้ไม่ทำการพิสูจน์ความถูกต้องจากเวลา $t = 0$ ถึง $t = t$ เป็น e^{-vt} และความน่าจะเป็นที่กลุ่มผู้ใช้ทำการพิสูจน์ความถูกต้องระหว่างเวลา $t = t$ ถึง $t + dt$ โดย *limit* $dt \rightarrow 0$ เป็น $ve^{-vdt}dt = vdt$ ดังนั้นความน่าจะเป็นที่กลุ่มผู้ใช้จะร้องขอเบสซีอาร์แอลระหว่างเวลา $t = t$ ถึง $t + dt$ เป็น $ve^{-v(t+L)}dt$ ถ้าสมการนี้คูณจำนวนกลุ่มผู้ใช้และหารด้วย dt ผลลัพธ์ที่ได้คือ อัตราการร้องขอเบสซีอาร์แอลระหว่างเวลา "synch" ดังนี้

$$R_s(t) = Nve^{-v(t+L)} \tag{2.17}$$

ถ้าเวลา t เป็นช่วงเวลา "non-synch" แล้วกลุ่มผู้ใช้จะร้องขอเบสซีอาร์แอลจากเครื่องแม่ข่ายที่เวลา $t = t$ ก็ต่อเมื่อเวลา $t = t$ นั้นทำการ พิสูจน์ความถูกต้อง ครั้งแรกตั้งแต่เบสซีอาร์แอลใหม่ออกมา ดังนั้นอัตราการร้องขอเบสซีอาร์แอลระหว่างช่วงเวลา "non-synch" จะเหมือนกับ อัตราการร้องขอรายการยกเลิกใบรับรองที่ถูกออกด้วยวิธีการเดิม

$$R_{ns}(t) = Nve^{-vt} \tag{2.18}$$

เมื่อ t เป็นจำนวนเวลาทั้งหมดตั้งแต่เบสซีอาร์แอลใหม่ออกมา

ปัญหาเกี่ยวกับวิธีการออกเดลต้าซีอาร์แอลจะเห็นได้จากสมการ (2.18) โดยอัตราการร้องขอยกเว้นระหว่างช่วงเวลาแรกหลังจากเบสซีอาร์แอลออก คล้ายกับว่าเดลต้าซีอาร์แอลไม่ถูกใช้ทั้งหมด ในขณะที่อัตราการร้องขอสูงสุดลดลงด้วยปัจจัยของ e^{-vl} (เมื่อ l เป็นระยะเวลาที่

เดลต้าซีอาร์แอลใช้ได้) ซึ่งผลลัพธ์ที่ได้จากการลดอัตราการร้องขอระหว่างช่วงเวลา "synch" อาจไม่มีความสำคัญในการลดนั้น ถ้าช่วงเวลามีระยะเวลาสั้นเพื่อให้กลุ่มผู้ใช้ได้ข้อมูลการยกเลิกใบรับรองใหม่ที่สุดได้

วิธีการเปรียบเทียบประสิทธิภาพของกลไกการกระจายสถานะใบรับรองที่แตกต่างกันสองวิธี ซึ่งเป็นการเปรียบเทียบภาระการใช้เครือข่ายสูงสุด (peak bandwidth usage) จากแต่ละกลไก โดยได้จากการประมาณขนาดของรายการยกเลิกใบรับรอง ถ้าในแต่ละวันมีใบรับรองที่ถูกยกเลิกโดยเฉลี่ยประมาณ r ใบ มีจำนวนใบรับรองที่ใช้ได้ L_c วันและใบรับรองหนึ่งใบ ณ.ช่วงเวลาที่ทำการยกเลิกจะมีอายุเฉลี่ย $L_c/2$ วัน จนกระทั่งใบรับรองนั้นหมดอายุ ดังนั้นขนาดของ CRL โดยเฉลี่ยจะเป็น

$$S_f = S_H + S_E r L_c \tag{2.19}$$

ถ้าเดลต้าซีอาร์แอลที่ออกมานั้นให้ข้อมูลเกี่ยวกับสถานะที่เปลี่ยนไปที่ครอบคลุมช่วงเวลา w วัน แล้วขนาดของเดลต้าซีอาร์แอลโดยเฉลี่ยจะเป็น

$$S_\Delta = S_H + S_E r w \tag{2.20}$$

จากวิธีการออกรายการยกเลิกใบรับรองที่ได้กล่าวมาข้างต้น จะเห็นว่ามีการพัฒนาวิธีการออกเพื่อลดอัตราการร้องขอในระบบ ลดขนาดของรายการยกเลิกใบรับรอง แต่ไม่มีวิธีการใดที่สามารถลดอัตราการร้องขอของระบบและลดขนาดของรายการยกเลิกใบรับรองได้พร้อมกัน วิทยานิพนธ์ฉบับนี้ได้นำเสนอวิธีการออกรายการยกเลิกใบรับรองแบบใหม่ ที่มีประสิทธิภาพดีกว่าวิธีการที่กล่าวข้างต้น ซึ่งจะนำเสนอในบทต่อไป

2.2.6.2.6 **วิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้า** (Over-issuing Delta-CRLs)

วิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้า เป็นวิธีการที่เดวิดคูเปอร์ [10] นำเสนอแนวคิดในการนำข้อดีของวิธีการออกรายการยกเลิกใบรับรองแบบเหลื่อมเวลามาประยุกต์กับวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้า โดยแต่ละใบรับรองจะทำการออกตามเวลาที่กำหนดทั้งแบบ CRL และ Delta-CRL โดยไม่คำนึงถึงเวลาหมดอายุของใบรับรองที่ออกมาก่อนหน้านี้ ดังนั้นถ้าผู้ใช้มีใบรับรองที่ยังไม่หมดอายุอยู่แล้วก็ไม่จำเป็นต้องทำการร้องขอใบรับรองใหม่ ทำให้อัตราการร้องขอของระบบลดลง ปริมาณการใช้เครือข่ายลดลงด้วย

จากแนวคิดการนำข้อดีของสองวิธีการมาใช้ร่วมกันนี้ ทำให้ผู้วิจัยเกิดแนวความคิดที่จะนำข้อดีของวิธีการอื่นมาประยุกต์ใช้ร่วมกัน ซึ่งจะนำเสนอในบทต่อไป

บทที่ 3
วิธีการออกรายการยกเลิกใบรับรองแบบใหม่

3.1 บทนำ

จากบทที่ 2 ได้กล่าวถึงวิธีการออกรายการยกเลิกใบรับรองที่มีการพัฒนาวิธีการออกให้มีประสิทธิภาพดียิ่งขึ้นได้แก่ การลดอัตราการร้องขอ การลดขนาดของรายการยกเลิกใบรับรอง การลดปริมาณการใช้เครือข่าย เป็นต้น แต่ไม่มีวิธีการใดที่สามารถนำข้อดีของแต่ละวิธีการมาใช้ร่วมกันให้เกิดประสิทธิภาพสูงสุด วิทยานิพนธ์ฉบับนี้ได้นำเสนอแนวคิดในการออกรายการยกเลิกใบรับรองแบบใหม่ที่มีประสิทธิภาพสูงกว่าที่มีอยู่ โดยได้นำข้อดีของวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้าและวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบกระจายมาใช้ร่วมกัน ซึ่งจะกล่าวในหัวข้อต่อไป

3.2 วิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย (Over-issued Delta-CRLs with Distribution Points)

ในอดีตถึงปัจจุบันได้มีการนำเสนอวิธีการออกรายการยกเลิกใบรับรองมาหลายวิธีซึ่งแต่ละวิธีที่ได้นำเสนอมานั้นได้มีการปรับปรุงวิธีการต่างๆเรื่อยมาและในปัจจุบันนี้วิธีการออกรายการยกเลิกใบรับรองแบบเดลต้าที่เป็นที่นิยมใช้แต่วิธีการออกรายการยกเลิกใบรับรองแบบเดลต้าก็มีข้อเสีย เช่นแต่ละ Delta-CRL ที่แต่ละกลุ่มผู้ใช้ทำการเก็บไว้จะหมดอายุพร้อมกัน เมื่อมี Delta-CRL ใหม่ออกมา ซึ่งทำให้ทุกๆ กลุ่มผู้ใช้ที่ Delta-CRL ที่เก็บไว้หมดอายุพร้อมกันก็จะทำการร้องขอไปยังเครื่องแม่ข่ายเพื่อทำการร้องขอ Delta-CRL ใหม่ที่ออกมา ทำให้เกิดอัตราการร้องขอที่เครื่องแม่ข่ายสูง และหลักจากที่ทุกกลุ่มผู้ใช้ทำการดาวน์โหลด Delta-CRL แล้ว ทุกกลุ่มจะไม่มีการร้องขอใดๆ ไปยังเครื่องแม่ข่ายเลย ทำให้เครื่องแม่ข่ายว่างจนกระทั้งมี Delta-CRL หรือ CRL ใหม่ออกมา

วิทยานิพนธ์ฉบับนี้ได้นำเสนอวิธีการออกรายการยกเลิกใบรับรองเหลื่อมแบบเดลต้าที่มีการจัดเก็บแบบกระจาย (Over-issued Delta-CRL with Distribution Points) ซึ่งเป็นวิธีการที่ใช้ในการออกรายการยกเลิกใบรับรอง ซึ่งอธิบายโดยใช้คณิตศาสตร์ในการมาประยุกต์วิธีการออกรายการยกเลิกใบรับรองสองวิธีการคือวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาที่มีการจัดเก็บแบบกระจาย (Over-Issuing Segmented CRLs) และวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้า (Delta-CRLs) ซึ่งทั้งสองวิธีสามารถกระจายและลดอัตราการร้องขอ โดยการวิเคราะห์อย่างง่ายคือ ถ้ากลุ่มผู้ใช้ต้องการรับข้อมูลสถานะใบรับรองที่ใหม่และบ่อย แล้วจะเป็นไปไม่ได้เลย

ที่จะลดอัตราการร้องขอสูงสุดสำหรับวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้าและสามารถปรับปรุงประสิทธิภาพโดยใช้การแบ่งรายการยกเลิกใบรับรองออกเป็นส่วนๆ อีกทั้งเป็นการลดขนาดของรายการยกเลิกใบรับรองอีกด้วย

จากบทที่ 2 ได้กล่าวถึงอัตราการร้องขอของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาที่มีการจัดเก็บแบบกระจาย ซึ่งจะคล้ายกับอัตราการร้องขอ CRL ของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย โดยสามารถใช้สมการ (2.16) ได้ดังนี้

$$R_I(t) = \frac{Nve^{-vt/s}}{(O-1)(1-e^{-vt/sO})+1}$$

โดยกำหนดให้ I เป็นความช่วงเวลาที่ delta-CRLs ใช้ได้ ให้ O เป็นจำนวน delta-CRLs ที่ใช้ได้ ณ เวลาใดๆ t เป็นช่วงเวลาตั้งแต่ delta-CRLs ปัจจุบันทั้งหมดออก โดยระบบจะต้องอยู่ในสถานะ Steady State ซึ่ง O จะอยู่ในช่วง ($1 < O \leq s$)และ s เป็นจำนวนส่วนแบ่งของรายการยกเลิกใบรับรอง โดย s จะเป็นจำนวนเต็ม $s > 0$

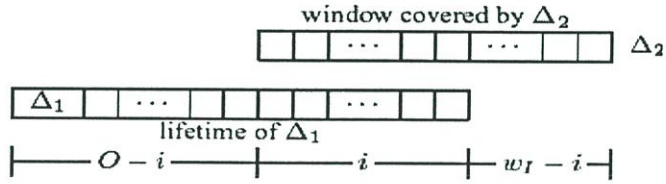
วิธีการกำหนดอัตราการร้องขอของรายการยกเลิกใบรับรอง โดยการกำหนดความน่าจะเป็นอย่างแรกว่ากลุ่มผู้ใช้ที่อยู่ในระบบจะทำการร้องขอส่วนแบ่งรายการยกเลิกใบรับรองส่วนใดส่วนหนึ่งในช่วงห่างระหว่าง delta-CRLs สอง delta-CRLs ซึ่งกลุ่มผู้ใช้จะทำการพิสูจน์ความถูกต้องในช่วงห่างระหว่างการออกรายการยกเลิกใบรับรองสองรายการนี้ โดยการร้องขอ CRL พื้นฐาน (base CRL) หนึ่งส่วน ก็ต่อเมื่อระยะเวลาทั้งหมดตั้งแต่กลุ่มผู้ใช้ได้รับข้อมูลสถานะยกเลิกใบรับรองที่มากกว่าระยะเวลาของขนาดหน้าต่างเวลาของ delta-CRLs (window size of delta-CRLs) โดยข้อดีของการกำหนดขนาดของหน้าต่างของเวลานั้นเพื่อให้การออกรายการยกเลิกใบรับรองตามเวลาที่คงที่ ทำให้อัตราการร้องขอของระบบคงที่ด้วย ซึ่งจะเกิดขึ้นได้หนึ่งในสองวิธีนี้ คือ

วิธีที่หนึ่ง มีความน่าจะเป็นที่กลุ่มไม่ทำการพิสูจน์ความถูกต้องระหว่างขนาดหน้าต่างของเวลา (window) ที่อยู่ในช่วงห่างระหว่าง delta-CRLs

วิธีที่สองมีความน่าจะเป็นที่กลุ่มจะทำการพิสูจน์ความถูกต้องหนึ่งครั้งหรือมากกว่าหนึ่งครั้งแต่ทุกๆ ครั้งที่ทำการพิสูจน์ความถูกต้องจะใช้วิธีการออกรายการยกเลิกใบรับรองแบบเดลต้า ซึ่งจะได้รับก่อนการเริ่มต้นระยะเวลาที่ครอบคลุมช่วง delta-CRLs ซึ่งจะใช้ delta-CRLs ที่ทำการดาวน์โหลดมาก่อนหน้า

ในการกำหนดนั้นได้กำหนดให้ P_{val} เป็นความน่าจะเป็นที่กลุ่มผู้ใช้ทำการพิสูจน์ความถูกต้องในช่วงเวลาระหว่างสอง delta-CRLs ดังนั้นความน่าจะเป็นที่กลุ่มจะไม่ทำการพิสูจน์ความถูกต้องในช่วงเวลาระหว่างสอง delta-CRLs เป็น $1-P_{val}$ เนื่องจากมี wO/l ช่วงเวลาที่ครอบคลุมช่วงเวลาระหว่าง delta-CRLs ซึ่งความน่าจะเป็นที่กลุ่มจะไม่ทำการพิสูจน์ความถูกต้องระหว่างระยะเวลาที่ครอบคลุมช่วงเวลาระหว่าง delta-CRLs เป็น $(1-P_{val})^{wO/l}$

เพื่อให้สอดคล้องกับข้อกำหนดที่กลุ่มทำการพิสูจน์ความถูกต้องระหว่างช่วงเวลาที่ครอบคลุมช่วงห่างระหว่าง delta-CRLs ช่วงอายุของ delta-CRLs ก่อนหน้าต้องเหลื่อมกับขนาดหน้าต่างเวลาของ delta-CRL ดังรูปที่ 3.1



รูปที่ 3.1 ช่วงอายุของ delta-CRLs แรกเหลื่อมกับหน้าต่างของ delta-CRLs ต่อมา

จากรูปที่ 3.1 จะเห็นว่า delta-CRLs ปัจจุบัน (Δ_2) ถูกออกมา ณ เวลาเริ่มต้นของช่วงห่างระหว่างสอง delta-CRLs (p) และมีขนาดหน้าต่างเวลา w_I ดังนั้น Δ_2 ครอบคลุมช่วงห่างระหว่าง $[p-w_I, p-1]$ ซึ่งกลุ่มจะทำการดาวน์โหลด delta-CRLs สุดท้าย (Δ_1) ที่ออกมา ณ ช่วงเริ่มต้นเวลา $p-w_I-O+i$ และใช้ได้ในช่วงระยะห่าง O ดังนั้นช่วงอายุของ Δ_1 และหน้าต่างที่เหลื่อมทับช่วงระยะห่าง i

ความเหมาะสมของรูปที่ 3.1 คือกลุ่มผู้ใช้จะต้องดาวน์โหลดส่วนหนึ่งของ delta-CRLs ที่ถูกแบ่งในช่วงเวลา $p-w_I-O+i$ ซึ่งกลุ่มผู้ใช้จะทำการพิสูจน์ความถูกต้องหนึ่งหรือมากกว่าหนึ่งครั้งในช่วงเวลา $[p-w_I, p-w_I+i-1]$ หลังจากนั้นกลุ่มผู้ใช้จะไม่ทำการพิสูจน์ความถูกต้องอีกในช่วงเวลา $[p-w_I+i, p-1]$ ซึ่งความน่าจะเป็นที่กลุ่มผู้ใช้ทำการพิสูจน์ความถูกต้องหนึ่งหรือมากกว่าหนึ่งครั้งในช่วงห่างระหว่าง $p-w_I-O+i$ เป็น P_Δ ดังนั้นความน่าจะเป็นที่กลุ่มผู้ใช้จะทำการพิสูจน์ความถูกต้องหนึ่งหรือมากกว่าหนึ่งครั้งในช่วงเวลา $[p-w_I, p-w_I+i-1]$ เป็น $1-(1-P_{val})^i$ สุดท้ายจะได้ความน่าจะเป็นที่กลุ่มทำการพิสูจน์ความถูกต้องในช่วงเวลา $[p-w_I+i, p-1]$ เป็น $(1-P_{val})^{w_I-i}=(1-P_{val})^{wO/l-i}$ ดังนั้น

ความน่าจะเป็นที่กลุ่มทำการพิสูจน์ความถูกต้องในช่วงระยะ p จะทำการร้องขอ delta-CRLs ซึ่งจะได้

$$P_{\Delta}\left[1-(1-P_{val})^{i}\right](1-P_{val})^{wO/l-i} \tag{3.1}$$

ซึ่งค่าของ i ในรูปที่ 3.1 เป็นช่วงระหว่าง [1, O-1] จากสมการ (3.1) ต้องทำการรวมทุกค่าระหว่างช่วง [1, O -1] ดังนั้นสมการ (3.1) ต้องรวมทุกค่าของ i ที่มีค่าระหว่าง [1, O -1] ซึ่งสามารถนำมารวมกับ $(1-P_{val})^{wO/l}$ ซึ่งจะได้ความน่าจะเป็นที่กลุ่มผู้ใช้นั้นทำการพิสูจน์ความถูกต้องในช่วงเวลา โดยจะร้องขอบางส่วนของ CRL ในช่วงเวลานั้น

$$(1-P_{val})^{wO/l} + P_{\Delta}\sum_{i=1}^{O-1}\left[1-(1-P_{val})^{i}\right](1-P_{val})^{wO/l-i} \tag{3.2}$$

เพื่อให้ได้ความน่าจะเป็นที่กลุ่มผู้ใช้ทำการร้องขอบางส่วนของ base CRL ในช่วงเวลา ซึ่งสมการ (3.2) ต้องนำมาคูณด้วยความน่าจะเป็นที่กลุ่มจะทำการพิสูจน์ความถูกต้องระหว่างช่วงเวลา ซึ่งจะได้สมการ P_b ดังต่อไปนี้

$$P_b = P_{val}\left\{(1-P_{val})^{wO/l} + P_{\Delta}\sum_{i=1}^{O-1}[1-(1-P_{val})^{i}] \quad (1-P_{val})^{wO/l-i}\right\} \tag{3.3}$$

ความน่าจะเป็นที่กลุ่มผู้ใช้จะไม่ทำการพิสูจน์ความถูกต้องใดๆ ระหว่างช่วงเวลาเป็น $e^{-vl/sO}$ ดังนั้นจะได้ $P_{val}=1-e^{-vl/sO}$ ซึ่งความน่าจะเป็นที่กลุ่มผู้ใช้จะทำการร้องขอแต่ละส่วนของ delta-CRLs ในช่วงเวลาสามารถคำนวณได้โดยใช้สมการ (2.16) โดยให้จำนวนกลุ่มผู้ใช้ (N) เท่ากับ 1 จะได้สมการความน่าจะเป็นที่ผู้ใช้หนึ่งกลุ่มจะทำการร้องขอแต่ละส่วนของ delta-CRLs ในช่วงเวลา ดังนี้

$$P_{\Delta} = \int_{0}^{l/O}\frac{ve^{-vt/s}dt}{(O-1)(1-e^{-vl/sO})+1} \tag{3.4}$$

นำสมการ (3.4) และ P_{val} ที่ได้มาแทนในสมการ (3.3) จะทำการพิสูจน์ได้ดังนี้

$$P_b = P_{val}\left\{(1-P_{val})^{wO/l} + P_{\Delta}\sum_{i=1}^{O-1}[1-(1-P_{val})^{i}] \quad (1-P_{val})^{wO/l-i}\right\}$$

<u>พิสูจน์</u> เนื่องจาก $P_{val} = 1 - e^{-vl/sO}$

เพราะฉะนั้น $(1-P_{val})^{wO/l}$ จะเป็น $(1-(1-e^{-vl/sO}))^{wO/l} = (e^{-vl/sO})^{wO/l} = e^{-vw/s}$

และ $[1-(1-P_{val})^{i}](1-P_{val})^{wO/l-i} = [1-(1-(1-e^{-vl/sO}))^{i}](1-(1-e^{-vl/sO}))^{wO/l-i}$

$$= [1-e^{-ivl/sO}][e^{-(w-il/O)v/s}]$$

นำค่าที่ได้มาแทนในสมการ P_b จะได้

$$P_b = P_{val}\left\{e^{-vw/s} + P_\Delta \sum_{i=1}^{O-1}\left\{[1-e^{-ivl/sO}][e^{-(w-il/O)v/s}]\right\}\right\}$$

$$= P_{val}\left\{e^{-vw/s} + P_\Delta \sum_{i=1}^{O-1}\left\{e^{-vw/s}\,e^{-ivl/sO} - e^{-ivl/sO}\,e^{-vw/s}\,e^{-ivl/sO}\right\}\right\}$$

$$= P_{val}\left\{e^{-vw/s} + P_\Delta \sum_{i=1}^{O-1}(e^{-vw/s}\,e^{-ivl/sO} - e^{-vw/s})\right\}$$

$$= P_{val}\,e^{-vw/s}\left\{1 + P_\Delta \sum_{i=1}^{O-1}(e^{-ivl/sO} - 1)\right\}$$

$$= P_{val}\,e^{-vw/s}\left\{1 + P_\Delta (\sum_{i=1}^{O-1} e^{-ivl/sO} - \sum_{i=1}^{O-1} 1)\right\}$$

$$= P_{val}\,e^{-vw/s}\left\{1 + P_\Delta (\sum_{i=0}^{O-1} e^{-ivl/sO} - \sum_{i=0}^{1} e^{-ivl/sO} - \sum_{i=1}^{O-1} 1)\right\}$$

$$= P_{val}\,e^{-vw/s}\left\{1 + P_\Delta ((\frac{1-e^{vl/s}}{1-e^{vl/sO}}) - O)\right\}$$

จากสมการ $P_{\Delta} = \frac{P_{val}}{(O-1)P_{val}+1}$ นำไปแทนในสมการจะได้

$$= P_{val}\, e^{-vw/s}\left\{1+\left(\frac{P_{val}}{(O-1)P_{val}+1}\right)\left(\left(\frac{1-e^{vl/s}}{1-e^{vl/sO}}\right)-O\right)\right\}$$

$$= P_{val}\, e^{-vw/s}\left\{\frac{e^{-vl/sO}-e^{-vl/sO}(1-e^{vl/s})}{(O-1)P_{val}+1}\right\}$$

$$= \frac{P_{val}\, e^{-wv/s}\, e^{-vl/sO}}{(O-1)P_{val}+1}(1-(1-e^{vl/s}))$$

$$= \frac{P_{val}\, e^{-wv/s}\, e^{-vl/s}\, e^{vl/s}}{(O-1)P_{val}+1}$$

$$= \frac{P_{val}\, e^{-(w+l/O-l)v/s}}{(O-1)P_{val}+1}$$

$$= \frac{(1-e^{-vl/sO})e^{-(w+l/O-l)v/s}}{(O-1)(1-e^{-vl/sO})+1}$$

$$= P_{\Delta}\, e^{-(w+l/O-l)v/s} \qquad (3.5)$$

จากสมการ (3.5) สามารถนำมาใช้ในการคำนวณอัตราการร้องขอบางส่วนของ base CRL ถ้ากลุ่มผู้ใช้ทำการร้องขอบางส่วนของ base CRL ในช่วงเวลาระหว่าง CRL แล้วการร้องขอบางส่วนของ base CRL นี้จะทำ ณ เวลาที่กลุ่มผู้ใช้ทำการพิสูจน์ความถูกต้องครั้งแรกในช่วงเวลานั้น ซึ่งถ้าช่วงเวลาระหว่าง CRL เริ่มที่เวลา = 0 แล้ว ความน่าจะเป็นที่กลุ่มผู้ใช้นั้นจะทำการพิสูจน์ความถูกต้องครั้งแรกของช่วงระยะห่างระว่างเวลา [*t...t+dt*] โดยที่ *limitdt* $\longrightarrow$ 0 จะได้ $ve^{-vt/s}dt$

ซึ่งความน่าจะเป็นที่กลุ่มทำการพิสูจน์ความถูกต้องระหว่างระยะห่างจะต้องทำการร้องขอบางส่วนของ base CRL ระหว่างช่วงระยะห่างสามารถทำการคำนวณโดยนำสมการ (3.4) หารด้วย P_{val} จะได้สมการ

$$\frac{e^{-(w+l/O-l)v/s}}{(O-1)(1-e^{-vl/sO})+1} \qquad (3.6)$$

จากนั้นนำสมการ (3.5) มาคูณด้วยจำนวนกลุ่มผู้ใช้ (*N*) โดยคูณทั้งสองสมการและหารด้วย *dt* ดังนั้นผลลัพธ์ในการร้องขอ base CRL ในช่วงเวลา [*t*...*t*+*dt*] จะได้

$$R_b(t) = \frac{Nve^{-(t+w+l/O-l)v/s}}{(O-1)(1-e^{-vl/sO})+1} = R_l(t)\, e^{-(w+l/O-l)v/s} \qquad (3.7)$$

โดยกำหนดให้ *l* เป็นความช่วงเวลาที่ delta-CRLs ใช้ได้ ให้ *O* เป็นจำนวน delta-CRLs ที่ใช้ได้ ณ เวลาใดๆ *t* เป็นช่วงเวลาตั้งแต่ delta-CRLs ปัจจุบันทั้งหมดออก โดยระบบจะต้องอยู่ในสถานะ Steady State ซึ่ง *O* จะอยู่ในช่วง ($1 < O \leq s$)และ *s* เป็นจำนวนส่วนแบ่งของรายการยกเลิกใบรับรอง โดย s จะเป็นจำนวนเต็ม $s > 0$

จากสมการอัตราการร้องขอ delta-CRL ของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย (3.7) นั้น ได้นำไปทดลองว่าได้ผลลัพธ์เป็นไปตามแนวคิดข้างต้นหรือไม่ ซึ่งจะกล่าวในบทต่อไป

บทที่ 4
การทดลองและผลการทดลอง

หลักการและวิธีการที่ได้กล่าวไว้ในบทที่ผ่านมา ในบทนี้จะกล่าวถึงการทดลองโดยใช้วิธีการทางคณิตศาสตร์และการจำลองวิธีการออกรายการยกเลิกใบรับรอง เพื่อนำผลลัพธ์ที่ได้จากการทดลองรูปแบบการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าและการจัดเก็บแบบกระจายมาทำการเปรียบเทียบกับรูปแบบการออกรายการยกเลิกใบรับรองแบบต่างๆ

4.1 การแทนค่าทางคณิตศาสตร์

การทดลองโดยใช้วิธีการทางคณิตศาสตร์นั้นได้นำผลลัพธ์ของสมการอัตราการร้องขอของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย (สมการ 3.7) มาทำการเปรียบเทียบกับอัตราการร้องของของวิธีการออกรายการยกเลิกใบรับรองแบบอื่นที่อธิบายโดยใช้คณิตศาสตร์ในการอธิบายโมเดลของเดวิท คูเปอร์ [9][10] เช่น Traditional CRL, Over-issuing CRL, Segmented CRL, Delta-CRL เป็นต้น โดยสมมติฐานให้งานวิจัยของเดวิท คูเปอร์ [9][10] นั้นถูกต้อง

4.1.1 วิธีการแทนค่าทางคณิตศาสตร์

ในหัวข้อนี้จะนำเสนอวิธีการทดลองเบื้องต้นโดยใช้คณิตศาสตร์และการกำหนดสภาพแวดล้อมให้เหมือนกัน ซึ่งสภาพแวดล้อมที่ใช้ในการกำหนดนั้นจะเหมือนกับสภาพแวดล้อมที่ใช้ในการทดลองของเดวิด คูเปอร์ เพื่อนำไปคำนวณในวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจายและวิธีการออกรายการยกเลิกใบรับรองแบบต่างๆ โดยนำผลลัพธ์ที่ได้มาทำการเปรียบเทียบอัตราการร้องขอ ภาระการใช้เครือข่าย ขนาดของรายการยกเลิกใบรับรอง

การกำหนดสภาพแวดล้อมดังนี้

- จำนวนกลุ่มผู้ใช้ (N) = 300,000 คน
- อัตราการพิสูจน์ความถูกต้อง (v) = 10 ใบรับรองต่อวัน
- จำนวนรายการยกเลิกใบรับรองที่ใช้ได้ ณ เวลาใดๆ (O) = 4 รายการ
- ขนาดหน้าต่างเวลาของ delta-CRL ปัจจุบัน (w) = 9 ชั่วโมง
- ช่วงเวลาที่ใช้ delta-CRL ได้ (l) = 4 ชั่วโมง
- เวลารวมทั้งหมดตั้งแต่ delta-CRL ปัจจุบันออกมา

- จำนวนใบรับรองที่ถูกยกเลิกเฉลี่ย (r) = 1,000 ใบรับรองต่อวัน
- ขนาดของหัวข้อมูล (S_H) และข้อมูล (S_E) = 51 และ 9 ไบต์ในแต่ละใบรับรอง

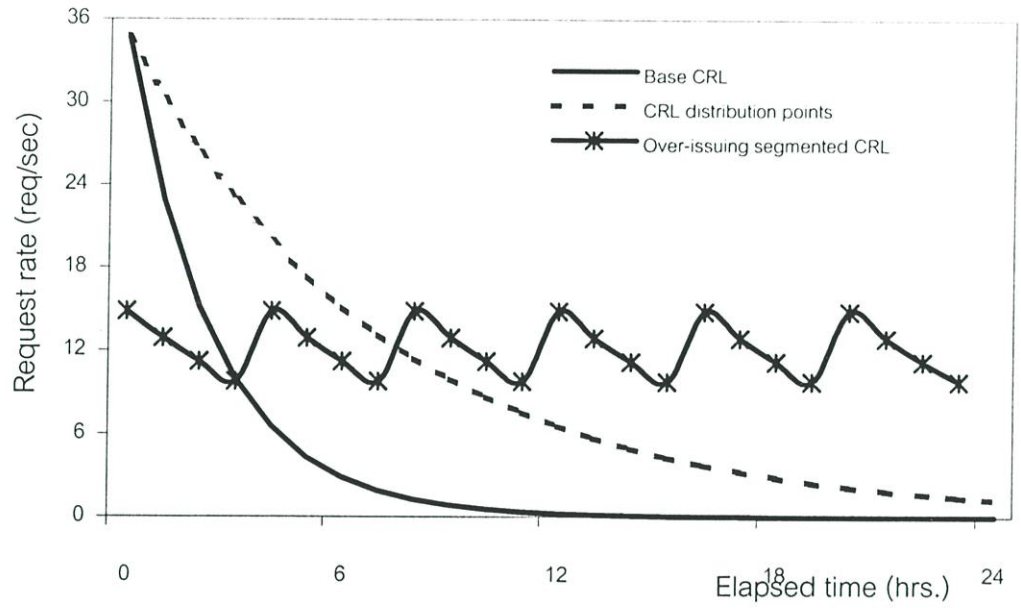
4.1.2 ผลลัพธ์ทางคณิตศาสตร์

จากสภาพแวดล้อมที่กำหนดข้างต้นได้นำไปใช้ในสมการที่กล่าวมาแล้วในบทที่ 3 นั้นจะได้ผลลัพธ์ สรุปได้ดังนี้

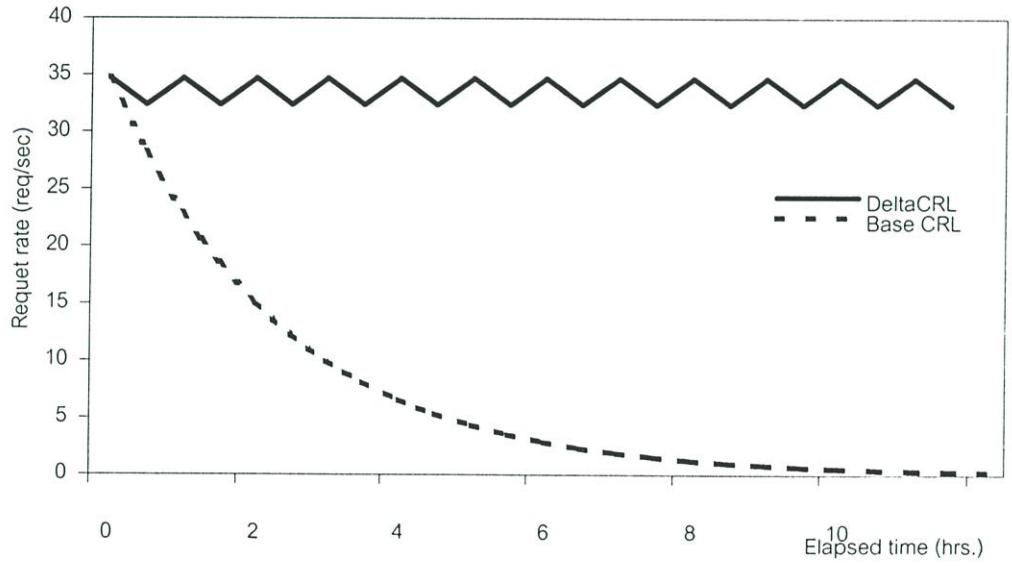
ตารางที่ 4.1 แสดงผลลัพธ์จากการคำนวณอัตราการร้องขอ ปริมาณการใช้เครือข่าย ขนาดของรายการยกเลิกใบรับรองแบบเดิมและแบบเดลต้าทางคณิตศาสตร์

Method	Reqest rate for base CRL (req/sec)	Reqest rate for delta-CRL (req/sec)	Bandwidth usage (Mbytes/sec)	Size of base CRL (Kbytes)	Size of delta-CRL (Kbytes)
CRL	34.72	-	57.03	1,642.55	-
CRL with distribution points	34.72	-	19.01	547.55	-
Over-issuing segmented CRL	25.95	-	14.21	547.55	-
Delta-CRL	34.72	34.70	57.15	1,642.55	3.43
Over-issued delta-CRL with distribution points	2.05	25.00	1.15	547.55	1.18

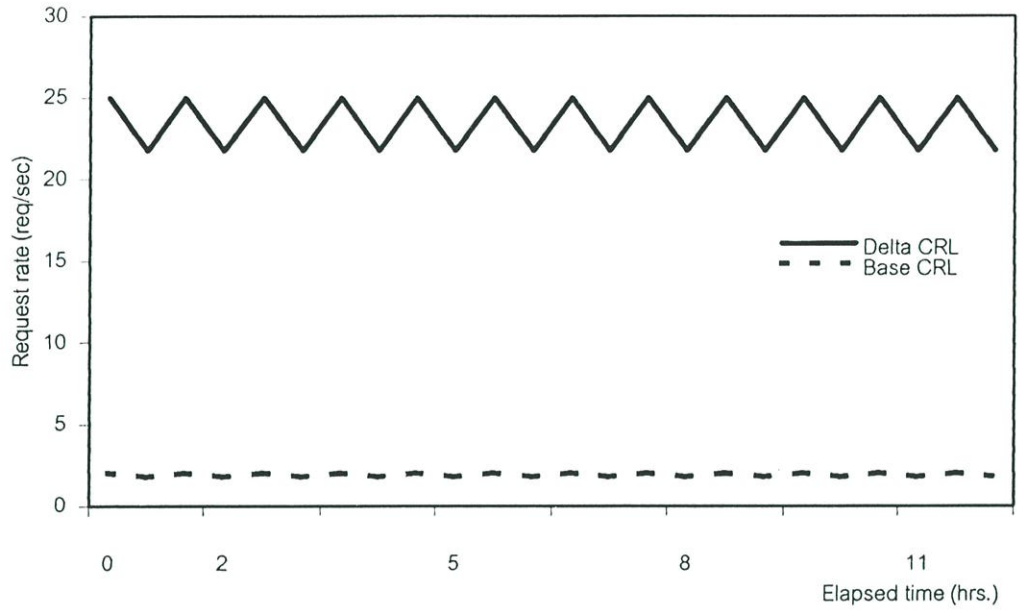
จากตารางที่ 4.1 เป็นการแสดงผลลัพธ์จากการคำนวณอัตราการร้องขอ ปริมาณการใช้เครือข่าย ขนาดของรายการยกเลิกใบรับรองทางคณิตศาสตร์ เพื่อใช้เปรียบเทียบประสิทธิภาพวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจายกับวิธีการออกรายการยกเลิกใบรับรองแบบต่างๆ ที่ใช้สมการทางคณิตศาสตร์ของเดวิด คูเปอร์ โดยนำผลลัพธ์ที่ได้มาทำกราฟจะได้กราฟดังรูปที่ 4.1-4.6



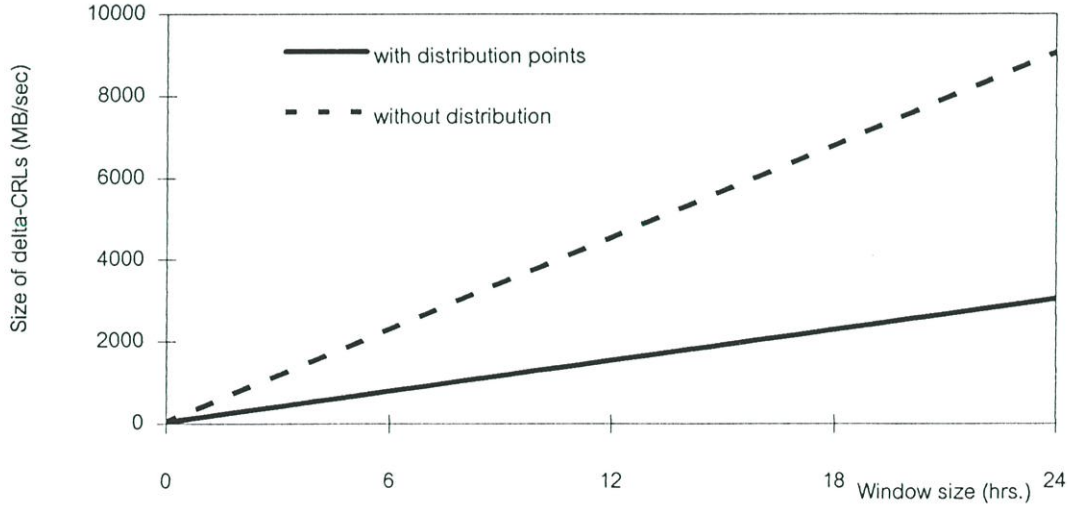
รูปที่ 4.1 กราฟแสดงการเปรียบเทียบอัตราการร้องขอรายการยกเลิกใบรับรองของสามวิธีการ



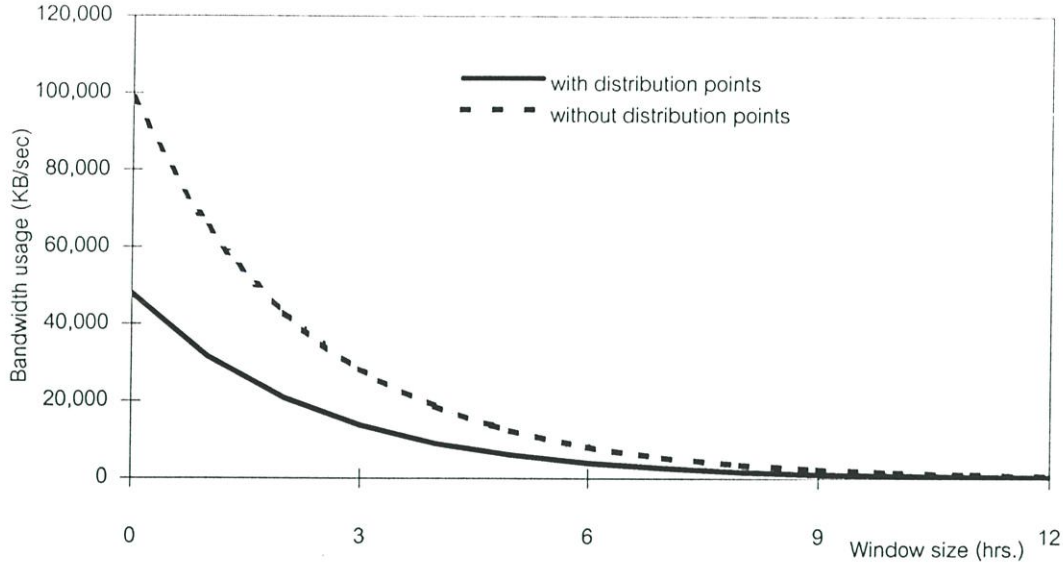
รูปที่ 4.2 กราฟแสดงอัตราการร้องขอรายการยกเลิกใบรับรองของวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้า



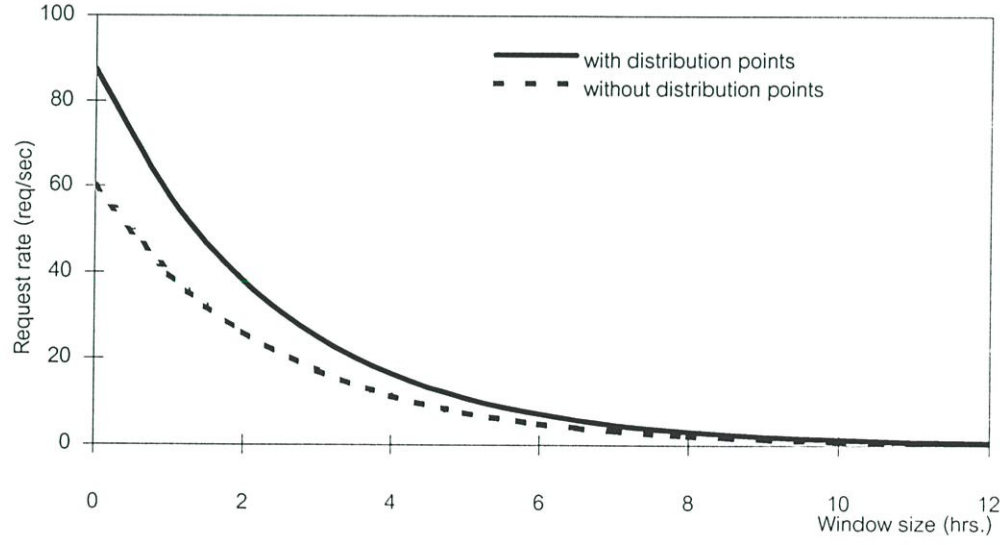
รูปที่ 4.3 กราฟแสดงอัตราการร้องของรายการยกเลิกใบรับรองของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการการจัดเก็บแบบกระจายสามไดเร็กทอรีหรือเครื่องแม่ข่าย



รูปที่ 4.4 กราฟแสดงการเปรียบเทียบขนาดของ delta-CRL ระหว่างวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย กับวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่ไม่มีการจัดเก็บแบบกระจาย



รูปที่ 4.5 กราฟแสดงการเปรียบเทียบปริมาณการใช้เครือข่ายระหว่างวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย กับวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่ไม่มีการจัดเก็บแบบกระจาย



รูปที่ 4.6 กราฟแสดงการเปรียบเทียบอัตราการร้องขอระหว่างวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย กับวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่ไม่มีการจัดเก็บแบบกระจาย

4.1.3 วิเคราะห์ผลลัพธ์ทางคณิตศาสตร์

จากตารางที่ 4.1 เป็นตารางที่ใช้ในการเปรียบเทียบประสิทธิภาพระหว่างวิธีการออกรายการยกเลิกใบรับรองแบบต่างๆ ซึ่งสามารถสรุปผลต่างของการเปรียบเทียบประสิทธิภาพวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจายเป็นเปอร์เซ็นต์ได้ดังตารางที่ 4.2

ตารางที่ 4.2 แสดงผลต่างของการเปรียบเทียบประสิทธภาพภาพวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจายกับวิธีการอื่นโดยแสดงเป็นเปอร์เซ็นต์

Method	Reqest rate for base CRL (req/sec)	Reqest rate for delta-CRL (req/sec)	Peak bandwidth usage (Kbytes/sec)	size CRLs (Kbytes)	size delta-CRL (Kbytes)
CRL	95.33	-	97.98	66.66	-
CRL distribution points	94.10	-	93.94	0.00	-
Over-issuing segmented CRL	92.10	-	91.95	0.00	-
Delta-CRL	94.10	27.95	97.99	66.66	65.67

จากตารางที่ 4.2 สามารถวิเคราะห์ได้ดังนี้

- สำหรับอัตราการร้องขอสูงสุดของ CRL จะเห็นได้ว่าวิธีการออกรายการยกเลิกใบรับรองแบบแบ่งส่วนนั้นไม่ลดอัตราการร้องขอรายการยกเลิกใบรับรองเมื่อเปรียบเทียบกับวิธีการออกรายการยกเลิกใบรับรองแบบเดิม แต่ในส่วน วิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบแบ่งส่วนนั้นสามารถลดอัตราการร้องขอได้อย่างชัดเจนเมื่อเปรียบเทียบกับวิธีการออกรายการยกเลิกใบรับรองแบบเดิมและแบบที่มีการจัดเก็บแบบกระจาย ส่วนอัตราการร้องขอของวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้านั้นจะเหมือนกับวิธีการออกรายการยกเลิกใบรับรองแบบเดิม แต่ในช่วงเวลาระหว่าง base CRL นั้นจะมี delta-CRL ออกมาเพื่อให้ผู้ใช้สามารถดาวน์โหลดรายการยกเลิกใบรับรองเพื่อใช้ในการปรับปรุงข้อมูลของ base CRL เดิมได้ ซึ่ง delta-CRL นี้จะออกมาตามช่วงเวลาที่กำหนด แต่ในส่วนของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจายนั้นจะมีอัตราการร้องขอต่ำกว่าทุกวิธีการออกเนื่องจากจะมี

การกระจายการจัดเก็บรายการยกเลิกใบรับรอง ดังนั้นวิธีการนี้จึงเป็นวิธีการที่กระจายอัตราการร้องของผู้ใช้ให้ทำการดาวน์โหลดรายการยกเลิกใบรับรองในเครื่องแม่ข่ายต่างๆ โดยไม่ทำให้การร้องของผู้ใช้ทั้งหมดมารวมอยู่ที่เครื่องแม่ข่ายเดียว และวิธีการนี้ได้มีการออก delta-CRL เพื่อให้ผู้ใช้ไม่จำเป็นต้องทำการดาวน์โหลด base CRL ทุกๆ ครั้ง ผู้ใช้สามารถดาวน์โหลด delta-CRLs เพื่อนำมาปรับปรุงข้อมูลของ base CRL เดิมได้โดยไม่ต้องทำการดาวน์โหลด base CRL บ่อยๆ

- สำหรับอัตราการร้องขอสูงสุดของ delta-CRL วิธีการออกรายการยกเลิกใบรับรองแบบเดิม แบบที่มีการจัดเก็บแบบกระจาย และ แบบเหลื่อมเวลาที่มีการจัดเก็บแบบกระจายนั้นไม่มีการออก delta-CRL แต่วิธีการออกรายการยกเลิกใบรับรองแบบเดลต้า และวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีจัดเก็บแบบกระจายมีการออก delta-CRL โดยวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีจัดเก็บแบบกระจายมีการกำหนดช่วงเวลาในการใช้ delta-CRL แบบเหลื่อมเวลาทำให้แต่ละ delta-CRL นั้นหมดอายุไม่พร้อมกันทำให้ผู้ใช้ที่ delta-CRL ยังไม่หมดอายุ ไม่ทำการร้องขอ delta-CRL ซึ่งเป็นการลดอัตราการร้องขอ delta-CRL

- ปริมาณการใช้เครือข่าย จากผลลัพธ์ที่ได้จะเห็นว่าวิธีการ base CRL และ delta-CRL นั้นมีอัตราการปริมาณการใช้เครือข่ายสูงเนื่องจากสองวิธีการนี้มีเครื่องแม่ข่ายเดียวและรายการยกเลิกใบรับรองหมดอายุในเวลาเดียวกันจึงทำให้ผู้ใช้ทุกคนส่งคำร้องขอรายการยกเลิกใบรับรองมาที่เครื่องแม่ข่ายเดียวพร้อมๆ กัน ส่วนวิธีการออกใบรับรองแบบแบ่งส่วนเป็นการกระจายใบรับรองไปยังหลายเครื่องแม่ข่ายซึ่งทำให้ผู้ใช้ส่งคำร้องของไปยังเครื่องแม่ข่ายต่างๆ จึงเป็นการกระจายคำร้องขอของผู้ใช้ไม่ให้คำร้องขอไปอยู่ที่เครื่องแม่ข่ายเดียว หรือวิธีการนี้เป็นการแบ่งรายการยกเลิกใบรับรองออกเป็นส่วนย่อยๆ ทำให้ผู้ใช้ทำการดาวน์โหลดรายการยกเลิกใบรับรองได้เร็ว ในส่วนวิธีการออกใบรับรองเหลื่อมเวลาแบบแบ่งส่วนเป็นการกำหนดช่วงเวลาในการใช้รายการยกเลิกใบรับรองแต่ละไม่เท่ากันทำให้ผู้ใช้ที่รายการยกเลิกใบรับรองยังไม่หมดอายุก็จะไม่ทำการดาวน์โหลด อีกทั้งวิธีการนี้ทำการแบ่งส่วนรายการยกเลิกใบรับรอง สุดท้ายวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีจัดเก็บแบบกระจายมีปริมาณการใช้รายการยกเลิกใบรับรองน้อยที่สุด เนื่องจากวิธีการนี้ได้แบ่งส่วนรายการยกเลิกใบรับรองและกำหนดช่วงเวลาในการใช้รายการยกเลิกใบรับรองแต่ละส่วนไม่เท่ากัน อีกทั้งกระจายรายการยกเลิกใบรับรองไปยังหลายเครื่องแม่ข่าย จึงทำให้ผู้ใช้รายการยกเลิกใบรับรองยังไม่หมดอายุก็จะไม่ทำการดาวน์โหลดและผู้ใช้ที่ต้องการดาวน์โหลดทำการใช้ส่งคำร้องของไปยังเครื่องแม่ข่ายต่างๆ

- ขนาดของ CRL จากผลลัพธ์ที่ได้จะเห็นว่าวิธีการ base CRL และ delta-CRL นั้นไม่มีการแบ่งรายการยกเลิกใบรับรองออกเป็นส่วนย่อยๆ จึงทำให้มีขนาดของ CRL ใหญ่กว่าวิธีการที่มีการแบ่งส่วนรายการยกเลิกใบรับรอง คือ วิธีการออกรายการยกเลิกใบรับรองแบบแบ่งส่วน วิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบแบ่งส่วน และวิธีการออกรายการยกเลิกใบรับรอง

เหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย ซึ่งทำให้ขนาดของรายการยกเลิกใบรับรองมีขนาดเล็ก

- ขนาดของ delta-CRL จากผลลัพธ์ที่ได้จะเห็นว่าวิธีการ delta-CRL นั้น ไม่มีการแบ่งรายการยกเลิกใบรับรองออกเป็นส่วนย่อยๆ จึงทำให้มีขนาดของ CRL ใหญ่กว่าวิธีการที่มีการแบ่งส่วนรายการยกเลิกใบรับรอง คือ วิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย ซึ่งทำให้ขนาดของรายการยกเลิกใบรับรองมีขนาดเล็ก

จากรูปที่ 4.1 เป็นกราฟที่แสดงถึงการเปรียบเทียบอัตราการร้องขอรายการยกเลิกใบรับรองของสามวิธีการ จะเห็นได้ว่าอัตราการร้องขอของวิธีการ base CRL และวิธีการออกรายการยกเลิกใบรับรองแบบแบ่งส่วนนั้นมีอัตราการร้องของใกล้เคียงกันเนื่องจากทั้งสองวิธีการนี้รายการยกเลิกใบรับรองหมดอายุพร้อมกัน จึงทำให้ผู้ใช้ทุกคนทำการดาวน์โหลดรายการยกเลิกใบรับรองพร้อมกัน แต่วิธีออกรายการยกเลิกใบรับรองแบบแบ่งส่วนจะมีความชันของเส้นกราฟน้อยกว่า เนื่องจากวิธีการนี้ได้แบ่งการจัดเก็บรายการยกเลิกใบรับรองออกเป็นหลายเครื่องแม่ข่ายจึงทำให้มีการกระจายอัตราการร้องขอ ในส่วนของกราฟของวิธีการ over-issuing segmented CRL นั้นมีอัตราการร้องขอต่ำที่สุด เนื่องจากวิธีการนี้มีการแบ่งการจัดเก็บรายการยกเลิกใบรับรองออกเป็นหลายเครื่องแม่ข่ายและมีการกำหนดช่วงเวลาการใช้รายการยกเลิกใบรับรองให้หมดอายุไม่พร้อมกันจึงทำให้มีอัตราการร้องขอต่ำกว่าสองวิธีการข้างต้น

จากรูปที่ 4.2 เป็นกราฟที่แสดงถึงอัตราการร้องขอรายการยกเลิกใบรับรองของวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้า จะเห็นได้ว่าอัตราการ้องของรายการยกเลิกใบรับรองพื้นฐานและรายการยกเลิกใบรับรองแบบเดลต้าเท่ากันและหลังจากนั้นผู้ประกอบการรับรอง (CA) จะทำการออกรายการยกเลิกใบรับรองแบบเดลต้าอย่างต่อเนื่องและเมื่อรายการยกเลิกใบรับรองแบบเดลต้าที่ออกมานี้หมดอายุจึงค่อยทำการออกรายการยกเลิกใบรับรองแบบเดลต้าใหม่ ซึ่งรายการยกเลิกใบรับรองแบบเดลต้านี้จะหมดอายุพร้อมกัน จึงทำให้มีอัตราการร้องขอรายการยกเลิกใบรับรองแบบเดลต้าสูงอย่างต่อเนื่องตามช่วงเวลาที่รายการยกเลิกใบรับรองแบบเดลต้าออกมา

จากรูปที่ 4.3 เป็นกราฟที่แสดงถึงอัตราการร้องของรายการยกเลิกใบรับรองของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจายสามไดเร็กทอรี จะเห็นได้ว่าอัตราการร้องขอทั้งรายการยกเลิกใบรับรองพื้นฐานและรายการยกเลิกใบรับรองแบบเดลต้าต่ำกว่าอัตราการร้องขอของรูปที่ 4.1 และ 4.2 เนื่องจากวิธีการนี้ได้มีการกำหนดช่วงเวลาการใช้รายการยกเลิกใบรับรองให้แต่ละรายการหมดอายุไม่เท่ากันและมีการกระจายการจัดเก็บรายการยกเลิกใบรับรองไว้หลายเครื่องแม่ข่าย จึงทำให้อัตราการร้องขอต่ำกว่าทุกวิธีการที่ได้กล่าวมา

จากรูปที่ 4.4 เป็นกราฟที่แสดงถึงการเปรียบเทียบขนาดของรายการยกเลิกใบรับรองแบบเดลต้าระหว่างวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบ

กระจาย กับวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่ไม่มีการจัดเก็บแบบกระจาย จะเห็นได้ว่าถ้ากำหนดค่าขนาดช่วงเวลาของรายการยกเลิกใบรับรองแบบเดลต้า (window)ให้มากขึ้นขนาดของ delta-CRL ของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจายจะมีขนาดเล็กกว่าวิธีการออกที่ไม่มีการกระจายอย่างชัดเจน

จากรูปที่ 4.5 เป็นกราฟที่แสดงถึงการเปรียบเทียบปริมาณการใช้เครือข่ายระหว่างวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย กับวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่ไม่มีการจัดเก็บแบบกระจาย จะเห็นได้ว่าถ้ากำหนดค่าขนาดช่วงเวลาของรายการยกเลิกใบรับรองแบบเดลต้า (window) ให้มากขึ้นปริมาณการใช้เครือข่ายของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจายจะมีปริมาณการใช้น้อยกว่าวิธีการออกที่ไม่มีการกระจายเล็กน้อย

แต่อย่างไรก็ตามจากรูปที่ 4.6 เป็นกราฟที่แสดงถึงการเปรียบเทียบอัตราการร้องขอระหว่างวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย กับวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่ไม่มีการจัดเก็บแบบกระจาย จะเห็นได้ว่าถ้ากำหนดค่าขนาดช่วงเวลาของรายการยกเลิกใบรับรองแบบเดลต้า (window) ให้มากขึ้นอัตราการร้องขอของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจายจะมีอัตรการร้องขอมากกว่าวิธีการออกที่ไม่มีการกระจายเล็กน้อย

4.2 ระบบจำลองการออกรายการยกเลิกใบรับรอง

จากการแทนค่าทางคณิตศาสตร์ในเบื้องต้น โดยการกำหนดสภาพแวดล้อมให้เหมือนกันจะได้ผลลัพธ์จากแต่ละวิธีการออกรายการยกเลิกใบรับรองที่ได้แสดงในหัวข้อ 4.1 แล้วนั้น วิทยานิพนธ์ฉบับได้ทำการสร้างระบบจำลองการออกรายการยกเลิกใบรับรองเหลื่อมเวลาที่มีการจัดเก็บแบบกระจาย ซึ่งเหตุผลที่ต้องทำระบบจำลองนี้มีดังนี้

1. การทำระบบแบบจำลองเพื่อตรวจสอบผลลัพธ์ที่ได้และนำมาสนับสนุนผลลัพธ์จากการทำวิธีการทางคณิตศาสตร์นั้นถูกต้อง
2. การทำระบบแบบจำลองสามารถทำงานได้คล้ายหรือใกล้เคียงความจริงได้มากกว่าวิธีการทางคณิตศาสตร์
3. หาความสัมพันธ์บางอย่างที่ทางคณิตศาสตร์หาไม่ได้ เช่น ภาระระบบ (process overhead)

4.2.1 การออกแบบระบบจำลองการออกรายการยกเลิกใบรับรอง

ระบบจำลองนี้ได้อ้างอิงมาจากแอนเดรียน [12][13] โดยระบบจำลองจะทำกับการกำหนดเวลาที่ทำการควบคุมเหตุการณ์โดยการกำหนดเวลาในการเกิดเหตุการณ์ที่แน่นอน ซึ่งเหตุการณ์เหล่านี้จะทำการดำเนินงานบางอย่างบนหนึ่งเอนทิตี้หรือหลายเอนทิตี้ โดยระบบจำลองนี้ใช้สองเอนทิทีที่แตกต่างกัน คือ เครื่องแม่ข่ายที่ใช้ในการเก็บรายการยกเลิกใบรับรอง (Directory) และเอนทิทีปลายทาง นอกจากนี้ระบบจำลองยังมีเหตุการณ์หลักสามเหตุการณ์คือ การปรับปรุงข้อมูลยกเลิกใบรับรองบนเครื่องแม่ข่าย การปรับปรุงข้อมูลยกเลิกใบรับรองแบบเดลต้าบนเครื่องแม่ข่าย และการตรวจสอบใบรับรองหรือลายมือชื่อดิจิทัลในเอนทิทีปลายทาง

ระบบจำลองนี้จะเริ่มที่จำนวนเครื่องแม่ข่ายและเอนทิตีทีปลายทางตามพารามิเตอร์ทีรับเข้าเหตุการณ์ที่ได้กล่าวไปแล้วข้างต้นจะถูกการกระจายตามเวลาที่กำหนดและเอนทิทีที่เหมาะสม ซึ่งเครื่องแม่ข่ายจะถูกปรับปรุงตามเวลาที่กำหนด ในส่วนการพิสูจน์ความถูกต้องของใบรับรองในเอนทิทีจะปรากฏแบบสุ่ม เมื่อเหตุการณ์พิสูจน์ความถูกต้องของใบรับรองปรากฏขึ้นเอนทิทีจะถูกถามว่าข้อมูลยกเลิกใบรับรองปัจจุบันยังใช้ได้อยู่หรือไม่ ถ้าข้อมูลยกเลิกใบรับรองของเอนทิทีใช้ไม่ได้ เอนทิทีจะทำการร้องขอข้อมูลยกเลิกใบรับรองใหม่จากเครื่องแม่ข่าย

4.2.2 สภาพแวดล้อมของระบบจำลอง

ระบบแบบจำลองการออกรายการยกเลิกใบรับรองเป็นโปรแกรมระบบจำลองแบบออบเจ็กโอเร็นเต็ดในภาษาจาวา ประโยชน์ของการใช้ภาษาจาวาคือระบบจำลองสามารถทำการเข้าถึงและทำงานโดยใช้แอพเพล็ตได้ง่าย ซึ่งภาษาจาวามีลักษณะเด่นในการสร้างหน้าจอที่ติดต่อกับผู้ใช้ได้ง่าย

ระบบจำลองนำมาใช้ให้เป็นประโยชน์สำหรับโครงสร้างระบบจำลองที่เป็นพื้นฐานของภาษาจาวาซึ่งถูกเรียกว่าเจซิม (JSIM) โดยสภาพแวดล้อมของเจซิมครอบคลุมดีพอและเป็นส่วนที่ถูกใช้ในระบบจำลอง คลาสดังต่อไปนี้จะถูกเริ่มใช้ในระบบจำลองตามลำดับดังนี้

- การกำหนดเวลา (Scheduler) คลาสการกำหนดเวลานี้ใช้เก็บลำดับของเหตุการณ์ต่างๆ ในระบบจำลอง โดยเหตุการณ์ต่างๆ นี้มีทั้งเหตุการณ์ที่ถูกกำหนดล่วงหน้าหรือเหตุการณ์ที่เกิดในระหว่างการดำเนินงานของระบบจำลอง
- เหตุการณ์ (Event) คลาสเหตุการณ์เป็นคลาสเหตุการณ์ย่อยๆ ที่รับช่วงโดยคลาสที่แสดงเหตุการณ์ที่เกิดขึ้นอย่างชัดเจน
- เอนทิที (Entity) คลาสเหตุการณ์เป็นคลาสเหตุการณ์ย่อยๆ ที่รับช่วงโดยคลาสที่แสดงเอนทิทีในระบบจำลอง ซึ่งเหตุการณ์โดยปกติจะแสดงการกระทำบนหนึ่งเอนทิที

4.2.3 คลาสในระบบจำลอง

ในระบบจำลองมีคลาสที่สำคัญดังนี้

- SimulatorApplet เป็นคลาสให้ผู้ใช้ทำการดำเนินการระบบจำลองได้ง่ายขึ้น
- Simulator เป็นคลาสหลักในการควบคุมเหตุการณ์ในแบบจำลอง ซึ่งคลาสนี้ทำงานประกอบด้วยคลาสเอนทิทีและคลาสที่เป็นตัวกำหนดเวลา ซึ่งจะทำพร้อมกับการกำหนดจำนวนเหตุการณ์ที่รับช่วงจากคลาสเหตุการณ์ต่างๆ
- Repository เป็นคลาสที่รับข้อมูลจากคลาส Entity และการใช้เครื่องแม่ข่ายของข้อมูลรายการยกเลิกใบรับรอง
- End Entity เป็นคลาสที่รับข้อมูลมาจากคลาส Entity และกำหนดจำนวนเครื่องผู้ใช้ในระบบ
- RevocationInfo เป็นคลาสที่เก็บข้อมูลการยกเลิกสำหรับคลาส Repository หรือคลาส End Entity
- DeltaRevocationInfo เป็นคลาสที่รับช่วงจากคลาส RevocationInfo และเก็บข้อมูลรายการยกเลิกใบรับรองแบบเดลต้า
- Computer เป็นคลาสที่ใช้ในการคำนวณค่าต่างที่รับมาจากคลาส Simulator
- Statistic เป็นคลาสที่เก็บค่าต่างๆ ที่ได้จากการคำนวณในส่วนต่างๆ ไว้ในอาร์เรย์

4.2.4 รูปแบบของแบบจำลองรายการยกเลิกใบรับรอง

ระบบแบบจำลองการออกรายการยกเลิกใบรับรอง ถูกออกแบบให้ดำเนินการเป็นวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาที่มีการจัดเก็บแบบกระจายเท่านั้น โดยในระบบจำลองนี้ได้มีการกำหนดตัวแปรเข้าระบบดังนี้

- Simulation Timespan เป็นเวลาที่ใช้ในการดำเนินการของระบบแบบจำลอง
- System Size เป็นขนาดของผู้ใช้ที่อยู่ในระบบ
- Average Validation เป็นจำนวนการใช้รายการยกเลิกใบรับรองต่อวัน
- Revocation Rate เป็นอัตราการยกเลิกใบรับรอง
- Revocation information validity period เป็นช่วงเวลาที่ใช้รายการยกเลิกใบรับรองได้ (CRL)
- Number of distribution pointsเครื่องแม่ข่าย เป็นจำนวนเครื่องแม่ข่ายที่ใช้ในการกระจายการเก็บรายการยกเลิกใบรับรอง
- Window size เป็นขนาดของกรอบช่วงเวลาในการออกรายการยกเลิกใบรับรองแบบเดลต้า

- Issue Per Validity Period เป็นเวลาที่จะทำการออกรายการยกเลิกใบรับรองอย่างสม่ำเสมอ

และระบบจำลองนี้ได้กำหนดผลลัพธ์ที่ออกจากระบบดังนี้

- Max Request Rate เป็นอัตราการร้องของรายการยกเลิกใบรับรอง
- Max Delta CRL Request Rate เป็นอัตราการร้องของรายการยกเลิกใบรับรองแบบเดลต้า
- Max Network Load เป็นภาระในการใช้เครือข่าย
- Max Process Overhead เป็นภาระในการดำเนินงาน

4.2.5 ข้อกำหนดและค่าคงที่ที่ใช้ในระบบจำลอง

ในระบบจำลองการออกรายการยกเลิกใบรับรองนี้ได้มีข้อกำหนดและค่าคงที่ดังต่อไปนี้

- ช่วงเวลาที่ใบรับรองใช้ได้เท่ากับ 1 ปี
- อัตราการยกเลิกใบรับรองกำหนดเป็นเปอร์เซ็นต์ของใบรับรองที่ถูกยกเลิกซึ่งครอบคลุมหนึ่งปี
- กำหนดขนาดเส้นทางเครือข่ายของระบบเท่ากับ 10 เมกะบิตต่อวินาที
- ภาระการดำเนินงานหน่วยวัดเป็นยูนิต ดังนั้นหน่วยของระบบงานจะเท่ากันคือ 1 มิลลิวินาที ตัวอย่างเช่น ถ้าภาระระบบงานมีขนาดใหญ่กว่า 1,000 ยูนิตต่อวินาที ซึ่งการทำงานจะเป็นคิวจึงทำให้มีการเสียเวลา
- ลายมือชื่อดิจิทัลมีขนาด 128 ไบต์ ซึ่งหนึ่งการร้องขอรายการยกเลิกใบรับรองจะได้รายการยกเลิกใบรับรองที่มีส่วนหัวและส่วนข้อมูลขนาด 51ไบต์และ 9 ต่อใบรับรองและลายมือชื่อดิจิทัลตามลำดับ
- ระบบงานจะทำการร้องขอเมื่อรายการยกเลิกใบรับรองทำการลงลายมือชื่อแล้ว
- หน้าที่ของแต่ละเครื่องแม่ข่าย คือ จะทำการสุ่มโดยให้มีขนาดของรายการยกเลิกใบรับรองแต่ละส่วนเท่าๆ กันคล้ายกับเครื่องแม่ข่าย อื่นๆ ดังนั้นการร้องขอข้อมูลรายการยกเลิกใบรับรองใดๆ จะเท่ากับการร้องขอโดยตรงกับทุกๆเครื่องแม่ข่าย
- ช่วงของเวลาจะกำหนดเป็นนาที ความถี่ของการพิสูจน์ความถูกต้องกำหนดเป็นวัน อัตราการร้องขอวัดเป็นนาที และการเสียเวลา (delay) กำหนดเป็นมิลลิวินาที ซึ่งหน่วยในการกำหนดเหล่านี้เป็นค่ามาตรฐานในการวัดและให้ค่าตัวแปรในระบบแบบจำลองเสมือนจริงมากที่สุด
- ถ้าอัตราการใช้เครือข่ายมากที่สุดมีค่าสูงกว่าขนาดของช่องทางเครือข่ายที่ใช้เครือข่ายจะคับคั่ง ถ้าอัตราการใช้เครือข่ายโดยเฉลี่ยสูงกว่าขนาดของช่องทางเครือข่าย เครือข่าย

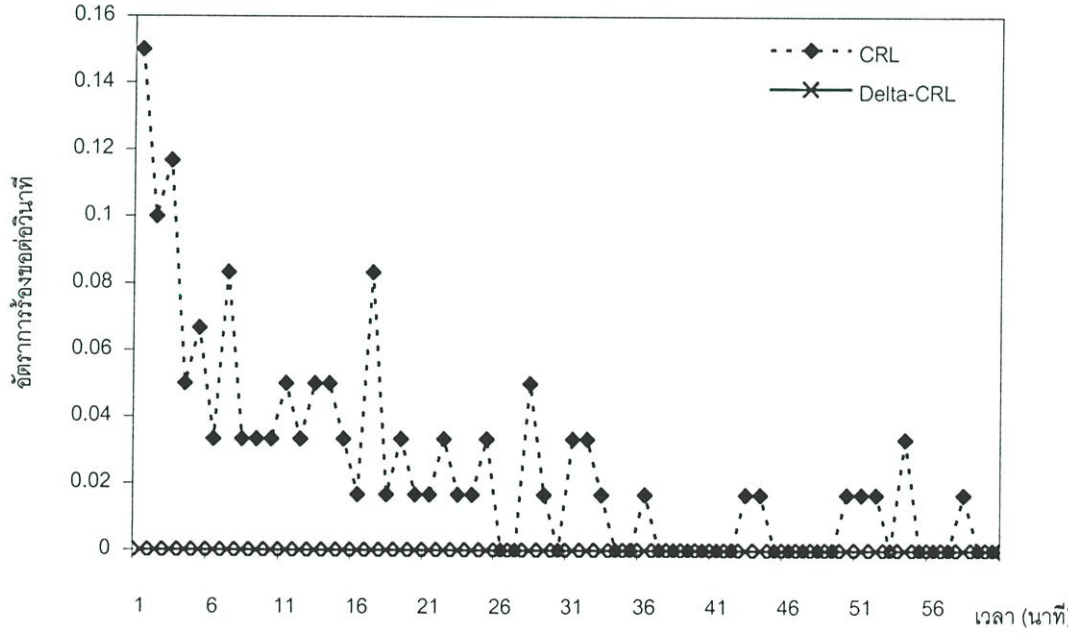
จะคับคั่ง และวิธีการออกใบรับรองวิธีต่างๆ จะทำงานไม่ดี ซึ่งคล้ายกับเวลาในการประมวลผลจริง ดังนั้นเวลาในการประมวลผลมากกว่า 1,000 แสดงว่าเครื่องแม่ข่ายเกิดการคับคั่ง

4.2.6 ผลลัพธ์จากระบบจำลอง

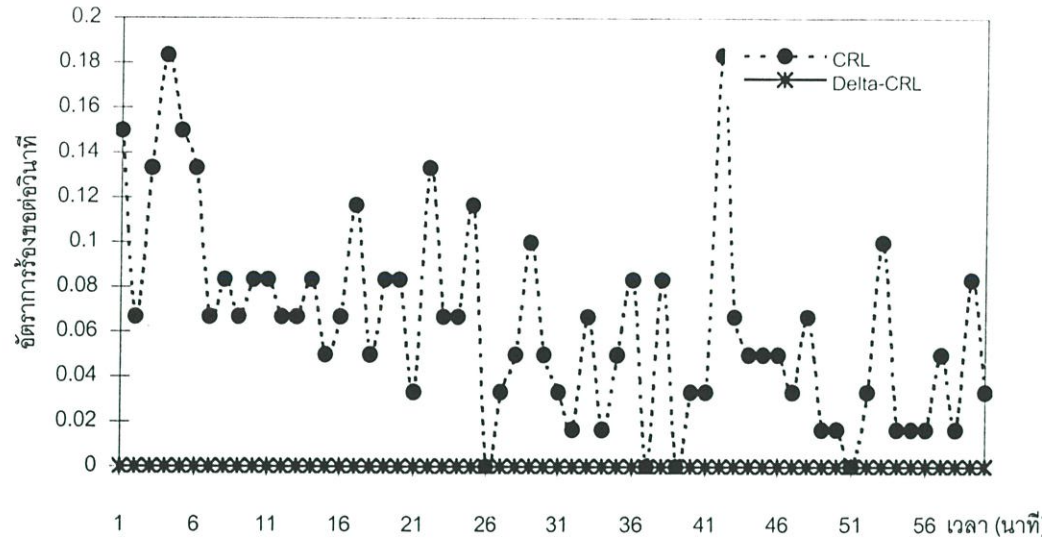
จากการประมวลระบบแบบจำลองนั้น จะได้ผลลัพธ์จากการรันระบบแบบจำลองวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้าที่มีการจัดเก็บแบบกระจายมาเปรียบเทียบกับผลลัพธ์จากการประมวลผลระบบจำลองการออกรายการยกเลิกใบรับแอนเดรียน [12][13] และดูแนวโน้มของกราฟว่าเป็นไปในแนวทางเดียวกับกราฟที่เป็นผลลัพธ์จากคณิตศาสตร์หรือไม่ โดยสมมติฐานให้ระบบจำลองของแอนเดรียน [12][13] นั้นถูกต้อง ระบบจำลองของแอนเดรียนนั้นมีวิธีการออกใบรับรองสี่วิธีคือ

1. วิธีการออกรายการยกเลิกใบรับรอง
2. วิธีการออกรายการยกเลิกใบรับรองที่มีการจัดเก็บแบบกระจาย
3. วิธีการออกรายการยกเลิกใบรับรองแบบเดลต้า
4. วิธีการออกรายการยกเลิกใบรับรองแบบเดลต้าที่มีการจัดเก็บแบบกระจาย

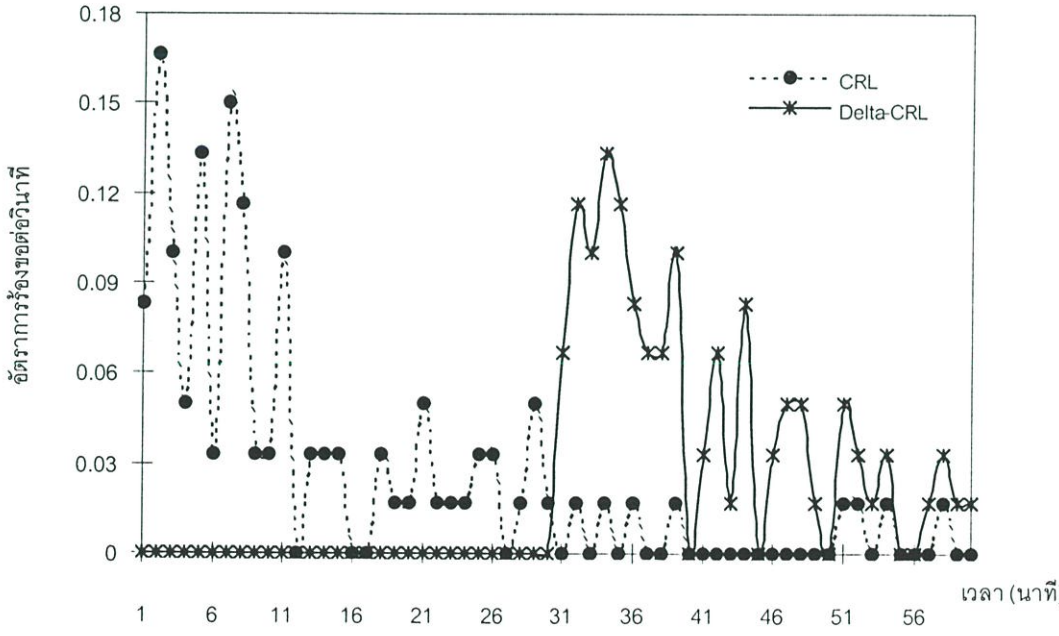
ซึ่งนำผลลัพธ์ที่ได้จากระบบแบบจำลองแสดงเป็นกราฟได้ดังนี้



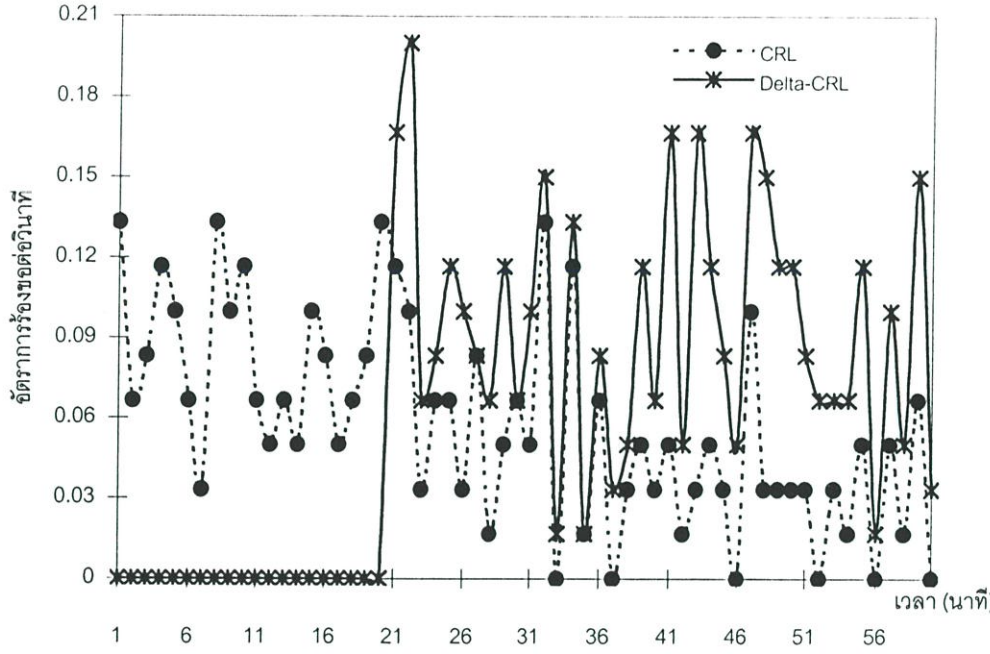
รูปที่ 4.7 กราฟแสดงอัตราการร้องขอรายการยกเลิกใบรับรอง



รูปที่ 4.8 กราฟแสดงอัตราการร้องขอของวิธีการออกรายการยกเลิกใบรับรองที่มีการจัดเก็บแบบกระจาย

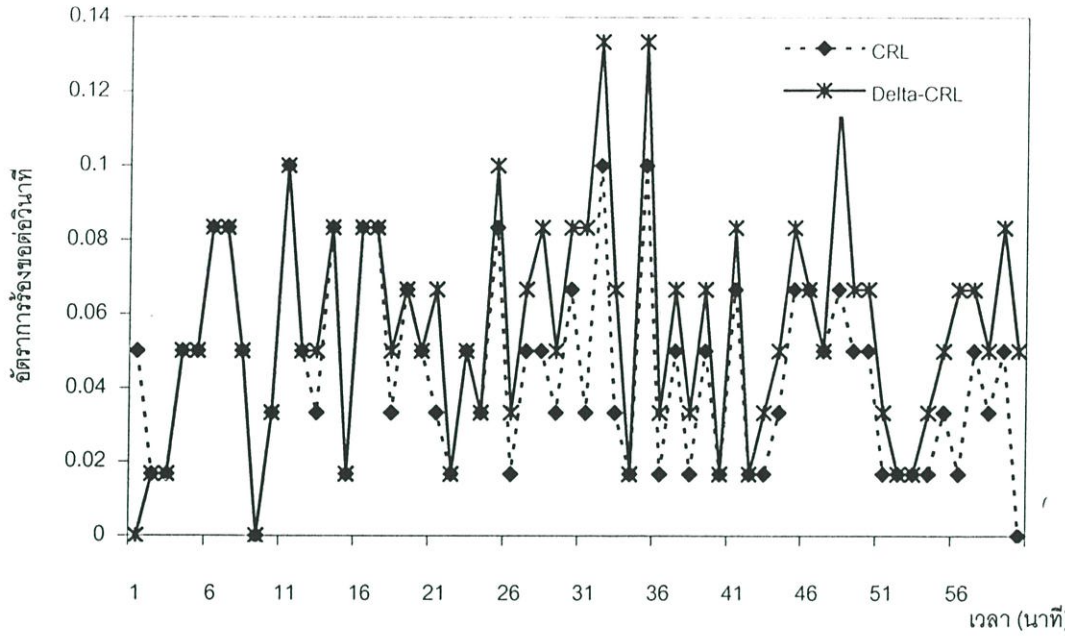


รูปที่ 4.9 กราฟแสดงอัตราการร้องขอของวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้า

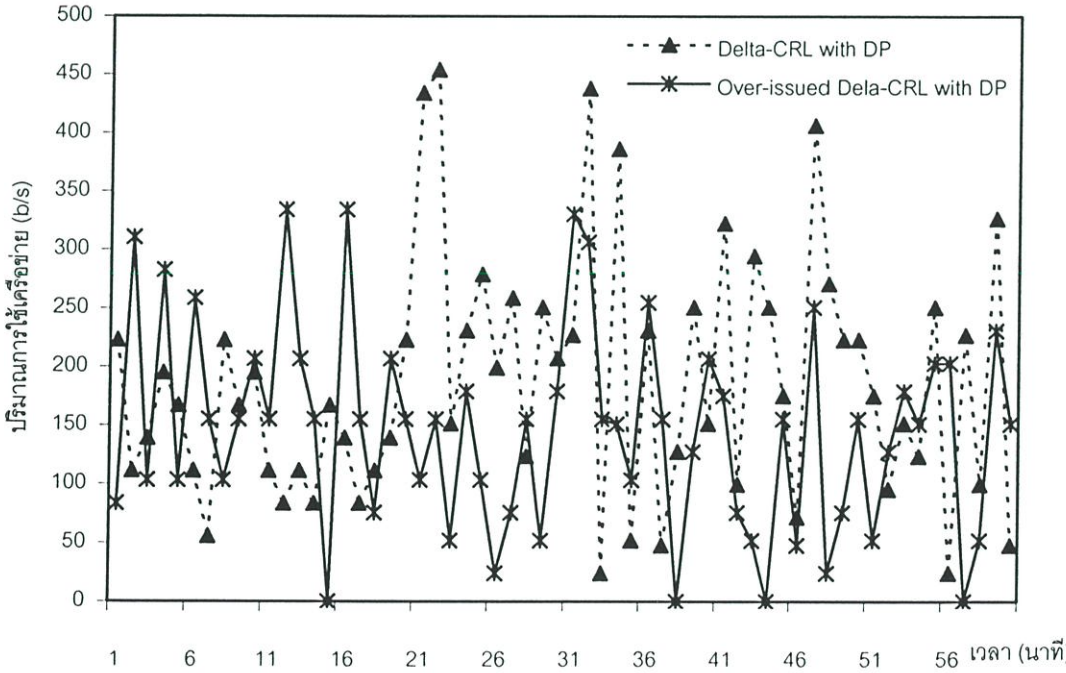


รูปที่ 4.10 กราฟแสดงอัตราการร้องขอของวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้าที่มีการจัดเก็บแบบกระจาย

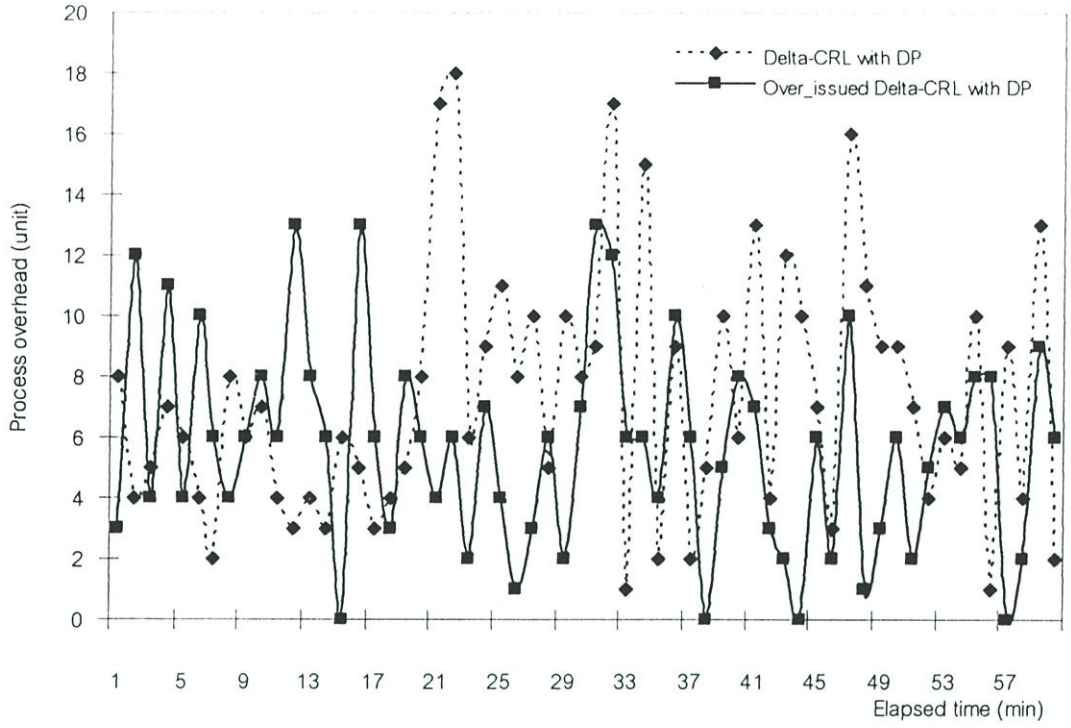
กราฟที่ 4.7-4.10 เป็นกราฟที่ได้จากระบบจำลองของแอนเดรียน [12][13] ซึ่งจะเห็นได้ว่ามีแนวโน้มของกราฟเป็นไปในทิศทางเดียวกับทางคณิตศาสตร์ จากนั้นจะนำอัตราการร้องขอสูงสุดที่ได้จากระบบจำลองของแอนเดรียนมาเปรียบเทียบกับอัตราการการร้องขอสูงสุดที่ได้จากระบบจำลองวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาที่มีการจัดเก็บแบบกระจาย ซึ่งแสดงในกราฟที่ 4.11 และกราฟแสดงการเปรียบเทียบปริมาณการใช้เครือข่ายระหว่างวิธีการออกใบรับรองแบบเดลต้าที่มีการจัดเก็บแบบกระจายกับวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย ซึ่งแสดงในกราฟที่ 4.12 และสองกราฟสุดท้ายจะเป็นกราฟแสดงการเปรียบเทียบภาระระบบงานระหว่างวิธีการออกใบรับรองแบบเดลต้าที่มีการจัดเก็บแบบกระจายกับวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย และกราฟแสดงการเปรียบเทียบอัตราการร้องขอรายการยกเลิกใบรับรองระหว่างระบบจำลองและวิธีการทางคณิตศาสตร์ ซึ่งแสดงในกราฟที่ 4.13 และ 4.14 ตามลำดับ



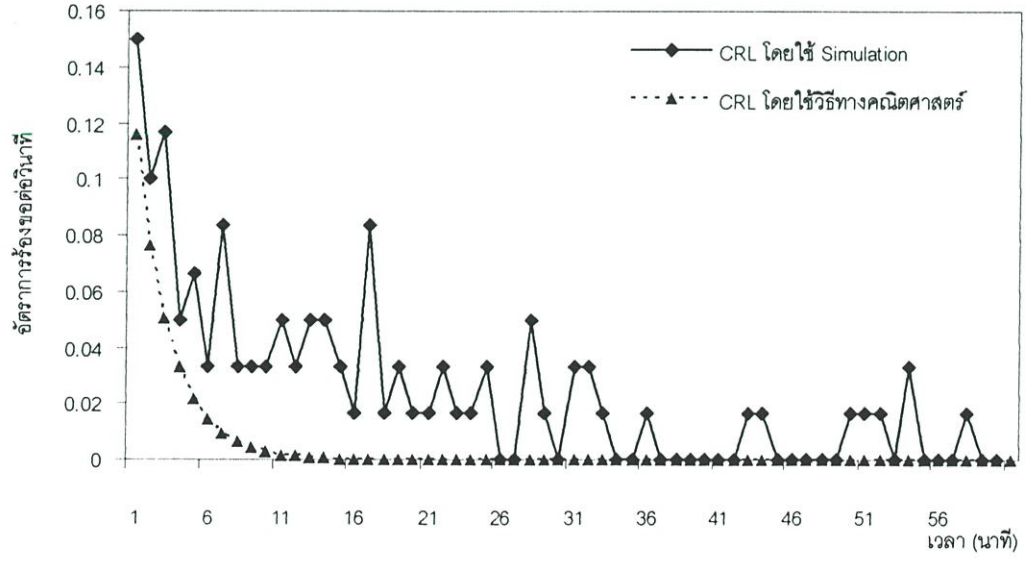
รูปที่ 4.11 กราฟแสดงอัตราการ้องขอของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย



รูปที่ 4.12 กราฟแสดงการเปรียบเทียบปริมาณการใช้เครือข่ายระหว่างวิธีการออกใบรับรองแบบเดลต้าที่มีการจัดเก็บแบบกระจายกับวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย



รูปที่ 4.13 กราฟแสดงการเปรียบเทียบภาระระบบงานระหว่างวิธีการออกใบรับรองแบบเดลต้าที่มีการจัดเก็บแบบกระจายกับวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย



รูปที่ 4.14 กราฟแสดงการเปรียบเทียบอัตราการร้องขอรายการยกเลิกใบรับรองระหว่างระบบจำลองและวิธีการทางคณิตศาสตร์

ตารางที่ 4.3 แสดงผลลัพธ์จากระบบจำลองวิธีการออกรายการยกเลิกใบรับรอง

Methods	Peak Request Rate of base CRL (req/s)	Peak Request Rate of Delta-CRL (req/s)	Peak Bandwidth Usage (bits/s)	Peak Processing Overhead (units)
CRL	0.17	-	358.67	0.17
CRL with DP	0.18	-	306.53	0.18
Delta-CRL	0.17	0.23	585.25	0.38
Delta-CRL with DP	0.13	0.20	453.87	0.30
Over-issuing Delta-CRL with DP	0.10	0.13	334.33	0.22

4.2.7 วิเคราะห์ผลการทดลองจากระบบแบบจำลอง

จากการดำเนินการของระบบแบบจำลองจะได้ผลลัพธ์คือ อัตราการร้องขอ CRL อัตราการร้องขอ Delta-CRL และ ปริมาณการใช้เครือข่าย ซึ่งได้นำผลลัพธ์ดังกล่าวนำเสนอเป็นกราฟดังรูปต่อไปนี้

- รูปที่ 4.7 เป็นกราฟที่แสดงอัตราการร้องขอรายการยกเลิกใบรับรองของวิธีการออกรายการยกเลิกรับรองแบบเดิม ซึ่งวิธีการนี้จะออก CRL อย่างเดียว ดังนี้แต่ละเอนทิทีจะทำการร้องขอ CRL เพียงครั้งเดียวเท่านั้นและจะขอใหม่เมื่อ CRL ใหม่ออกมา

- รูปที่ 4.8 เป็นกราฟที่แสดงอัตราการร้องขอรายการยกเลิกใบรับรองของวิธีการออกรายการยกเลิกรับรองที่มีการจัดเก็บแบบกระจาย เห็นว่าอัตราการร้องขอของวิธีการนี้ไม่ได้ลดลง แต่จะกระจายอัตราการร้องขอไปยังแต่ละเครื่องแม่ข่าย โดยวิธีการนี้จะทำการแบ่งรายการยกเลิกใบรับรองออกเป็นส่วนย่อยๆ ตามจำนวนเครื่องแม่ข่ายที่ใช้ในการจัดเก็บ ดังนั้นแต่ละเอนทิทีอาจต้องทำการร้องขอรายการยกเลิกใบรับรองไปยังหลายเครื่องแม่ข่าย ทำให้อัตราการร้องขอโดยรวมเพิ่มขึ้น แต่ทุกเอนทิทีจะไม่ทำการร้องขอไปยังเครื่องแม่ข่ายพร้อมๆ กัน ดังนั้นแต่ละเครื่องแม่ข่ายจะมีอัตราการ้องขอลดลง

- รูปที่ 4.9 เป็นกราฟที่แสดงอัตราการร้องขอรายการยกเลิกใบรับรองของวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้า จะเห็นว่าอัตราการร้องขอ CRL ต่ำกว่าวิธีการในรูปที่ 4.8 โดยวิธีการนี้จะทำการออกทั้ง CRL และ Delta-CRL ซึ่งผู้ใช้จะทำการร้องขอทั้ง CRL และ Delta-CRL โดยแต่ละเอนทิทีจะทำการร้องขอ CRL หรือ Delta-CRL หรือทั้งสองอย่าง ดังนั้นจึงมีอัตราการร้องขอมาที่เครื่องแม่ข่ายที่ทำการจัดเก็บเหล่านั้นน้อยกว่า

- รูปที่ 4.10 เป็นกราฟที่แสดงอัตราการร้องขอรายการยกเลิกใบรับรองของวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้าที่มีการจัดเก็บแบบกระจาย เห็นได้ว่ารูปนี้มีอัตราการร้องขอ CRL ต่ำกว่ารูปที่ 4.9 แต่อัตราการร้องขอ Delta-CRL สูงกว่ารูปที่ 4.9 เล็กน้อย โดยวิธีการนี้จะทำการออกรายการยกเลิกใบรับรองทั้ง CRL และ Delta-CRL แต่รายการที่ออกนั้นจะถูกแบ่งออกเป็นส่วนย่อยๆ ตามจำนวนเครื่องแม่ข่ายที่ใช้ในการจัดเก็บ ดังนั้นอัตราการร้องขอจะถูกกระจายไปยังเครื่องแม่ข่ายเหล่านั้น ทำให้แต่ละเครื่องแม่ข่ายมีอัตราการร้องขอลดลง

- รูปที่ 4.11 เป็นกราฟที่แสดงอัตราการร้องขอรายการยกเลิกใบรับรองของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย จะเห็นว่า อัตราการร้องขอสูงสุดของวิธีการนี้จะน้อยกว่ารูปที่ 4.10 แสดงมา เนื่องจากวิธีการนี้จะทำการออกรายการยกเลิกใบรับรองโดยไม่ต้องรอให้รายการเก่าหมดอายุก่อน แต่จะออกรายการตามเวลาที่กำหนด เช่น ออกรายการยกเลิกใบรับรองทุกๆ 20 นาที เป็นต้น ดังนั้น ณ เวลาใดๆ จะมีรายการที่ยังไม่หมดอายุมากกว่า 1 รายการทำให้เอนทิทีที่มีรายการที่ยังไม่หมดอายุอยู่นั้นไม่จำเป็นต้องร้องขอรายการยกเลิกใบรับรอง ซึ่งทำให้อัตราการร้องขอต่ำกว่าวิธีการอื่น

- รูปที่ 4.12 เป็นกราฟที่แสดงการเปรียบเทียบปริมาณการใช้เครือข่ายระหว่างวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้าที่มีการจัดเก็บแบบกระจาย และวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาที่มีการจัดเก็บแบบกระจาย จะเห็นได้ว่าปริมาณการใช้เครือข่ายของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาที่มีการจัดเก็บแบบกระจายนั้นมีปริมาณการใช้เครือข่ายที่น้อยกว่าเนื่องจากวิธีการนี้นั้น ถ้าเอนทิทีที่มีรายการไม่หมดอายุก็ไม่จำเป็นต้องร้องขอรายการยกเลิกใบรับรอง จึงทำให้ปริมาณการใช้เครือน้อยกว่าวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้าที่มีการจัดเก็บแบบกระจาย

- รูปที่ 4.13 เป็นกราฟแสดงการเปรียบเทียบภาระระบบงานระหว่างวิธีการออกใบรับรองแบบเดลต้าที่มีการจัดเก็บแบบกระจายกับวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย จะเห็นว่าภาระของระบบของวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาที่มีการจัดเก็บแบบกระจายนั้นมีภาระของระบบน้อยกว่าเนื่องจากวิธีการนี้นั้น ถ้าเอนทิทีที่มีรายการไม่หมดอายุก็ไม่จำเป็นต้องร้องขอรายการยกเลิกใบรับรองทำให้อัตราการร้องขอของผู้ใช้ในระบบลดลง จึงทำให้ภาระของระบบน้อยกว่าวิธีการออกรายการยกเลิกใบรับรองแบบเดลต้าที่มีการจัดเก็บแบบกระจาย

- รูปที่ 4.14 เป็นกราฟแสดงการเปรียบเทียบอัตราการร้องขอรายการยกเลิกใบรับรองระหว่างระบบจำลองและวิธีการทางคณิตศาสตร์ ซึ่งจะเห็นว่าแนวโน้มของการที่ได้จากระบบจำลองมีแนวโน้มเดียวกับกราฟที่ได้จากการคำนวณทางคณิตศาสตร์

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

ในปัจจุบันนี้องค์กรต่างๆ ได้ตระหนักถึงการรักษาความปลอดภัยในการติดต่อสื่อสารผ่านระบบเครือข่ายมากขึ้น โครงสร้างพื้นฐานกุญแจสาธารณะเป็นโครงสร้างการรักษาความปลอดภัยที่เหมาะกับองค์กรที่มีระบบเครือข่ายขนาดใหญ่หรือพาณิชย์อิเล็กทรอนิกส์ ซึ่งมีใบรับรองที่ใช้ในการกระจายกุญแจสาธารณะและพิสูจน์ตัวบุคคล การยกเลิกใบรับรองกลไกหลักอย่างหนึ่งของโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI) ซึ่งกลไลการยกเลิกใบรับรองนี้เป็นการประกาศใบรับรองที่ถูกยกเลิกก่อนเวลาหมดอายุจริง ถ้าผู้ใช้ไม่ทราบว่าใบรับรองนั้นถูกยกเลิกแล้วนั้นอาจทำให้เกิดการแอบอ้างจากผู้ไม่ประสงค์ดีในการยืนยันตัวบุคคลได้ จึงได้มีการใช้กลไกการยกเลิกใบรับรองขึ้น โดยวิธีการออกรายการยกเลิกใบรับรองที่มีอยู่แล้วนั้น เป็นวิธีการที่ทำให้มีอัตราการร้องขอรายการยกเลิกใบรับรองที่เครื่องแม่ข่ายสูง มีปริมาณการใช้เครือข่ายมาก และขนาดของรายการยกเลิกใบรับรองมีขนาดใหญ่ ซึ่งทำให้เครื่องแม่ข่ายให้การตอบสนองต่อการร้องขอของผู้ใช้ได้ช้า และผู้ใช้ต้องใช้เวลานานในการดาวน์โหลดรายการยกเลิกใบรับรอง

จากปัญหาที่กล่าวไปแล้วนั้น ผู้วิจัยจึงได้เสนอรูปแบบวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจาย โดยวิธีการนี้ได้มีการแบ่งส่วนรายการยกเลิกใบรับรองตามจำนวนเครื่องแม่ข่ายที่ใช้ในการจัดเก็บ และกระจายแต่ละส่วนของรายการยกเลิกใบรับรองไปยังเครื่องแม่ข่ายเหล่านั้น เพื่อให้ผู้ใช้ส่งคำร้องขอไปยังเครื่องแม่ข่ายแต่ละเครื่อง และแต่ละรายการยกเลิกใบรับรองนั้นจะถูกกำหนดให้ออกเมื่อถึงเวลาที่กำหนด ซึ่งแตกต่างจากวิธีการที่มีอยู่เดิมที่รายการยกเลิกใบรับรองจะถูกออกเมื่อรายการที่มีอยู่หมดอายุ ดังนั้นผู้ใช้ที่มีรายการยกเลิกใบรับรองอยู่แต่ยังไม่หมดอายุก็ไม่จำเป็นต้องส่งคำร้องขอไปยังเครื่องแม่ข่าย จากรูปแบบที่นำเสนอนี้ได้นำมาทดลองทางคณิตศาสตร์และระบบจำลองการออกรายการยกเลิกใบรับรองโดยเปรียบเทียบกับวิธีการที่มีอยู่เดิม ผลลัพธ์ที่ได้จากการทดลองนั้นจะเห็นว่าอัตราการร้องขอปริมาณการใช้เครือข่ายและขนาดรายการยกเลิกใบรับรองนั้นต่ำกว่าผลลัพธ์ของวิธีอื่นๆ ซึ่งสามารถสรุปได้ว่ารูปแบบวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจายนั้นมีประสิทธิภาพดีกว่าวิธีการที่มีอยู่เดิม

ในส่วนข้อเสนอแนะ งานวิจัยนี้สามารถนำรูปแบบวิธีการออกรายการยกเลิกใบรับรองเหลื่อมเวลาแบบเดลต้าที่มีการจัดเก็บแบบกระจายไปประยุกต์ใช้งานจริง ซึ่งวิธีการนี้เหมาะสำหรับระบบที่มีผู้ใช้จำนวนมาก มีการยกเลิกใบรับรองบ่อย แต่ข้อจำกัดของวิธีการนี้คือการจัดการที่ซับซ้อนกว่าวิธีการที่มีอยู่เดิมเล็กน้อย

เอกสารอ้างอิง

[1] S. Berkovits, S. Chokhani, J. A. Furlong, A. Geiter and J. C. Guild. "Public Key Infrastructure Study: Final Report," **The MITRE Corporation for NIST**, April 1994.

[2] Ueli Maurer. "Modelling a Public-Key Infrastructure." **In Proceeding of The European Symposium on Research in Computer Security**, vol.1146, pp.325-350, 1996.

[3] Silvio Micali. "Efficient Certificate Revocation." **Technical Report, Massachusetts Institute of Technology**, March 1996.

[4] Marc Branchaud. "A Servey of Public-Key Infrastructures." **Master Thesis of Department of Computer Science McGill University**, March 1997.

[5] Carlisle A., Robert Z. "A General, Flexible Approach to Certificate Revocation," **Entrust Technologies White Paper**, June 1998.

[6] Moni N., Kobbi N. "Certificate Revocation and Certificate Update." **In Proceeding of The 7th USENIX Security Symposium**, 1998.

[7] Ronald Rivest. "Can We Eliminate Certificate Revocation Lists?," **In Rafael Hirschfeld, editor, Financial Cryptography**, volume 1465, February 1998, pp. 178-183.

[8] R. Housley, W. Ford, W. Polk, and D. Solo. "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," **IETF RFC 2459**, January 1999.

[9] D. A. Cooper: "A Model of Certificate Revocation," **In Proceedings of the Fifteenth Annual Computer Security Applications Conference**, pages 256-264, December 1999.

[10] D. A. Cooper: "A More Efficient use of Delta-CRLs," **In Proceedings of the 2000 IEEE Symposium on Security and Privacy**, pages 190-202, May 2000.

[11] Patrick McDaniel, Aviel Rubin. "A Response to "Can We Eliminate Certificate Revocation Lists?", " **Technical Report 99.8.1, At&T Labs**, February 2000.

[12] A. Årnes. "Public Key Certificate Revocation Schemes," **Thesis, Queen's University, Ontario, Canada**, 2000.

[13] A. Årnes, H. Meijer, S. Lloyd, M. Just, and S. J. Knapskog. "Selecting Revocation Solutions for PKI," **NORDSEC 2000, Reykjavik, Iceland**, 2000-10-12/13.

[14] Richard A. "Certificate Revocation Mechanisms." **Advanced Technical Concepts/Research Group at CertCo, Inc.**, URL: http://www.certco.com

[15] Åsa H., Christopher M., and David R. "Cryptographic Support for Certificate Revocation." Secure Telecommunication Systems, ECE 636/INFT 931, April 2001.

[16] R. Housley, W. Ford, W. Polk, and D. Solo. "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation list (CRL) Profile," **IETF RFC 3280**, April 2002.

[17] William Stallings. **Cryptography and Network Security Principles and Practice.** New Jersey : Prentice Hall, Inc. 1998.

[18] Carlisle Adams., Steve Lloyd. **Understanding Public-Key Infrastructure : Concepts, Standards and Deployment Consisderations.** U.S.A : Macmillan Technical Publishing, 1999.

[19] Russ Housley., Tim Polk. **Planning for PKI.** Canada : Wiley Computer Publishing, 2001.

[20] Charles Pfleeger. **Security in Computing.** New Jersey : Prentice Hall, 1997.

[21] A. Arsenault and S. Turner. PKIX Roadmap. IETF Internet, October 1999.

[22] Entrust Securing the Internet, "Trusted Public-Key Infrastructures", **White Paper Entrust, Inc.**, August 2000.

[23] Ray Hunt., Associate Professor, Department of Computer Science, University of Canterbury, New Zealand. "PKI and Digital Certification Infrastructure." **IEEE International Conference on Networks**, 2001.

[24] Jens Kaps. "Public Key Infrastructure EE 537." 1997.

[25] Victor-Valeriu PATRICIU., Marin BICA., and Ion BICA. "Implementation Issues of PKI Technology." **International Carpathian Control Conference ICCC' 2002**, May 2002, pp. 513-518.

[26] M. St Johns. "The PKIX UserGroupName GeneralName Type." **IETF ietf-pkix-usergroup-00**, July 2001.

[27] Gaurav Jain. "Certificate Revocation : A Survey."

[28] Hector Ho Fuentes. "Certification Revocation Survey." September 2002.

[29] Stuart Stubblebine. "Recent-Secure Authentication: Enforcing Revocation in Distributed Systems." In Proceeding 1995 IEEE Symposium on Research in Security and Privacy, May 1995, pp. 224-234.

[30] M. Myers., R. Ankney., A. Malpani., S. Galperin., and C. Adams. "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP." IETF RFC 2560, June 1999.

ภาคผนวก ก.

ผลงานที่ได้รับการตีพิมพ์

1. C. Sathitwiriyawong, A. Rojapasakorn, "A Certificate Revocation Method using Over-issuing Delta-CRLs with Distribution Points," In Proceeding of The 3rd International Symposium on Communications and Information Technologies (ISCIT2003), pp.750-754, September 2003.
2. A. Rojapasakorn, C. Sathitwiriyawong, "A Performance Study of Over-Issuing Delta-CRLs with Distribution Points," In Proceeding of The 7th National Computer Science and Engineering Conference (NCSEC2003), pp.91-96, October 2003.
3. A. Rojapasakorn, C. Sathitwiriyawong, "A Performance Study of Over-Issuing Delta-CRLs with Distribution Points," In Proceeding of The 18th International Conference on Advanced Information Networking and Applications (AINA 2004), March 2004.

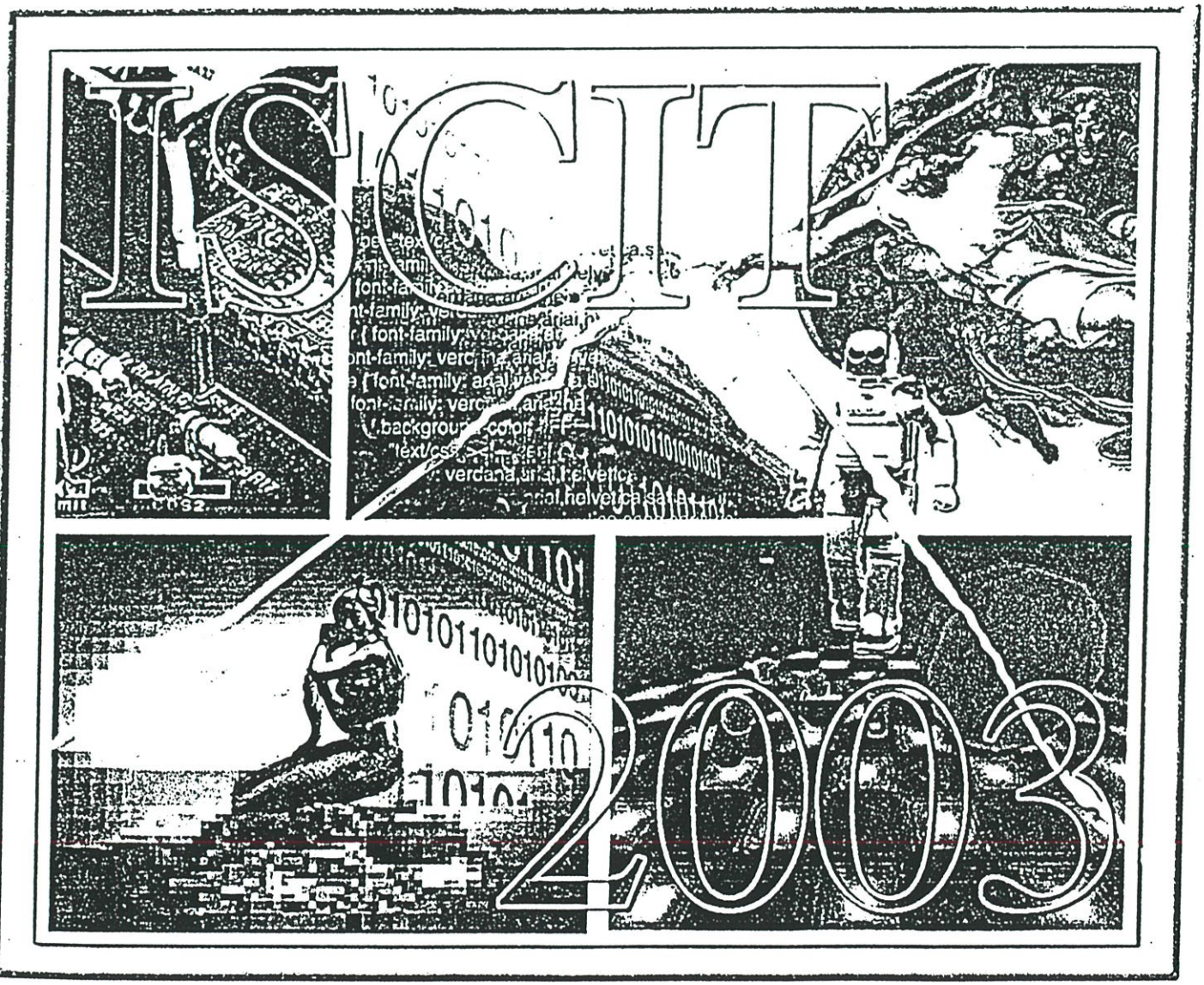
Volume II

Proceedings

The Third International Symposium
n Communications and Information Technologies

September 3-5, 2003

BP Samila Beach Hotel and Resort, Songkhla, Thailand



IT
C 2003
S
BN 974-644-437-9

A Certificate Revocation Method using Over-Issuing Delta-CRLS with Distribution Points

C. Sathitwiriyawong and A. Rojanapasakorn

Faculty of Information Technology, and Research Center for Communication and Information Technology, King Mongkut's Institute of Technology Ladkrabang Ladkrabang, Bangkok 10520, Thailand
Email: chanboon@it.kmitl.ac.th

Faculty of Information Technology, King Mongkut's Institute of Technology Ladkrabang, Ladkrabang, Bangkok 10520, Thailand
Email: pla_aradee@hotmail.com

Abstract

This paper presents a model for the segmentation of a certificate revocation list (CRL) issued by a certificate authority (CA). The model uses the combination of over-issuing segmented CRLs and delta-CRLs for distributed segmented CRLs to locate repositories. The results from the mathematical analyses show that the proposed certificate revocation system using over-issuing delta-CRLs with distribution points can significantly improve the system performance such as spreading out request rate, reducing the size of certification revocation information and reducing the average network load. This model is used to highlight inefficiencies in the traditional method of distributing certificate status information using CRLs.

1.Introduction

In 1994, the MITRE report [1] proposed several alternative revocation distribution mechnisms. In 2000, Cooper [2] presented models for the distribution of revocation information using certificate revocation lists (CRLs) and provided analyses of these models.

Public Key Infrastructure (PKI) is a prerequisite for security in large networks and distributed systems that certification authorities (CAs) will be interconnected. Each CA would periodically issues a certificate and a certificate revocation list (CRL) that is distributed to repository for each replying party downloading certificate status information.

The CRL is an account the serial numbers of all certificates issued by CA that have been revoked or invalid before CRL is expired. A relying party respects to use the information in the certificate that must be first validated. The relying party requires a recent CRL in order to perform validation and subsequently stores it in his cache. Delta-CRLs [3] is a base CRL that only contains information about the certificate status that has been changed in the revocation information to reference the base CRL. Delta-CRLs are periodically posted and updated to the last base CRL posting. Since the size of delta-CRLs is significantly smaller than the size of base CRLs and can be posted more frequently, the load on the repository can be reduced and the response time for the relying party can also be improved. However, the use of delta-CRL will not reduce the request rate for revocation information from the repository.

This paper presents a model of certificate revocation. The techniques that were developed previously [2][3] are applied to over-issuing delta-CRLs with distribution points model as the model were designed and the resulting model is shown the comparing with the over-issuing delta-CRLs. Finally, the new method of over-issuing delta-CRL with distribution points is presented.

2. Related works

The tradition method of distributing certificate status information concerns periodically issuing of a CRL that is posted to a repository. CA periodically issues a CRL listing all unexpired and revoked certificates [4]. In the traditional method of certificate revocation, each CRL includes a 'ThisUpdate' field that indicates the CRL issue time, while 'NextUpdate' indicates the next time of CRL issuance. When a CRL is issued, the relying party will obtain a CRL in order to perform validation. During the period of time in which a CRL is valid, each relying party will request the repository for revocation of information. Cooper [2] assumed that the certificate validation attempt time is independent of each other, so that an exponential interarrival probability density can be used to model the CRL scheme. So the probability that the relying party will perform the validation and request a CRL in the interval [t, t+dt] (in limit $dt \rightarrow 0$) is $ve^{-v}dt$. Where v represents the validation rate. The total number of requests for CRLs during interval [t, t+dt] is given by $ve^{-v}dt$ multiplied by

the number of relying parties (N): $T_{req}(t) = Nve^{-vt}dt$. Thus, the request rate for CRLs from the repository at time t is given by

$$R(t) = \frac{T_{req}(t)}{dt} = Nve^{-vt} \quad (1)$$

The problem with the traditional method of CRLs is that the CRLs cached by every relying party expire at the same time. When the CRL expires and a new CRL is issued, every relying party will request a CRL from the repository in order to perform a validation. As a result, there are high requests when a new CRL is issued. The over-issued CRL method can be distributed the requests in such a way that the peak request rate is always relatively smaller, but occurs more frequently.

Over-issuing [5] [7] is a method for spreading out requests for revocation information that the CRLs in the relying parties's cache will expire at different times. Thus, request rate for new CRLs will be spread out. It is possible to reduce the peak request rate by allowing multiple CRLs to have overlapping validity times. A relying party will request the fresh CRL, but the lifetime of that CRL is longer than the period to the next CRL issuance. Thus, the relying party will request a CRL from the repository during interval [t, t+dt] (in limit dt→0) that is the probability that the relying party performs its first validation attempt of the interval [t, t+dt] is

$$R_0(t) = \frac{Nve^{-vt}}{(O-1)(1-e^{-vt/O})+1} \quad (2)$$

Where O is the number of current valid CRLs and l is the validity time of a single CRL.

Another way to improve its performance over the tradition method of CRL is the use of segmented CRLs. However, segmenting CRLs may not reduce the peak request rate for CRLs, it will reduce the size of each CRL. So a repository can service request for CRL at a faster rate. The CRL is segmented and each segment is associated with a CRL distribution point that can be located on different repository. Each certificate has a pointer to the location of distribution points.

To simplify the analysis, the calculation that total request rate ($R_s(t)$) for all segments uses the following assumptions. The certificate revocation information has random distribution points, so any revocation information request equally refers to any distribution points. Finally, the CRL segments are issued at the same time. So Arnes [5] shows that the total request rate is

$$R_s(t) = Nve^{-vt/s} \quad (3)$$

Where s is the number of segments. Equation (3) shows the peak request rate in the system. Each relying party is likely to request more than one segment during a validity period. However, this method has no improvement in the request rate that is actually increased in average. There may be a significant improvement compared to the base CRL method in reducing the average network load and the size of revocation information since each single CRL segment is only a fraction of the base CRL.

As described above, the segmented CRLs method does not reduce the peak request rate compared to the base CRL posting since all CRLs expire at the same time. As a result, every relying party will request for revocation information from the repository. By taking the approach of over-issuing CRLs can be combined with the approach of segmented CRLs. When all CRL segments are issued at the same time and each CRL segment can be staggered relative to other segments. So the peak request occurs at the different time. Both methods can distribute and reduce the peak request rate on peak network load as over-issuing CRLs. Arnes [5] shows that the request rate during interval between staggered CRL segments issued at evenly separated interval is

$$R_{s,s}(t) = \frac{Nve^{-vt'/s}(1-e^{-vl/s})}{s(1-e^{-vl/s})} \quad (4)$$

Where $t' = t \bmod (\frac{l}{s})$ and l is the validity time of a CRL segment. The peak request rate can be reduced more by over-issuing the CRL segments. So the request rate during the interval is

$$R_{s,l}(t) = \frac{Nve^{-vt/s}}{(O-1)(1-e^{-vl/sO})+1} \quad (5)$$

Where t is the amount of time since the latest CRL segments were issued.

With the issuing delta-CRLs, the base CRL is issued periodically and each delta-CRLs collects all certificate revocation information since the last base CRL was issued [6]. In this method, base CRL posting is cached on the relying party and referred to as the base posting, while delta-CRLs are considered as incremental posting for a single base CRL. Whenever a base CRL is issued, the latest delta-CRL referencing the previously base CRL is also issued. Each validation will require access to the delta CRL and its corresponding base CRL. Therefore, the request rate for delta-CRLs will be the same as the request for base CRLs [4].

$$R_b(t) = Nve^{-vt} \quad (6)$$

Where t is the time passed since the issuance of the last base CRL. The request rate for the delta-CRL is identical, with a modification that t is the time passed since the last delta-CRL issuance [4].

$$R_\Delta(t) = Nve^{-vt} \quad (7)$$

This method can reduce the peak request rate of the base CRL. Each relying party requests a new delta-CRL rather than the new base CRL posting in the first validity period if the previous base CRL was required. The average size of the base CRL [3] is

$$S_f = S_H + \frac{S_E r L_c}{2} \quad (8)$$

Where S_H is the size of CRLs header, S_E is the size of CRL entry, r is the number of revoked certificate and L_c is the lifetime of CRL. The average size of a delta-CRL is

$$S_\Delta = S_H + S_E r w \quad (9)$$

Where w is the period of issued delta-CRL. Thus, the bandwidth for delta-CRL system can be computed as

$$B = S_f R_b(0) + S_\Delta \quad (10)$$

Next section describes the idea of over-issuing delta-CRLs with distribution points method that can improve performance of issued certificate revocation information.

3. Over-issuing delta-CRLs with distribution points

In this section, over-issuing delta-CRL with distribution points developed a mathematical model for certificate revocation models and applied this model by taking the approach of over-issuing segments CRLs [2] and delta-CRLs [3]. Both methods can distribute and reduce the peak request rates. Based on the similar analysis, if relying parties require to obtain a fresh certificate status information very frequently, then it may not be possible to significantly reduce the peak request rate for delta-CRL. But if the validity period of delta-CRL are long enough, then it may be possible to significantly reduce the request rate for delta-CRLs by over-issuing the delta-CRLs. The performance improvement can be done by the use of segmented CRLs that will usually reduce the size of each delta-CRLs.

In section 2, the request rate for over-issuing delta CRLs distribution points will be the same as the request rate for over-issued segmented CRLs that does not use delta-CRLs (equation (5)).

$$R_{sI}(t) = \frac{Nve^{-vt/s}}{(O-1)(1-e^{-vl/sO})+1}$$

Where l is the length of time that a delta-CRL is valid, O is the number of delta-CRL that are valid at any time, t is the amount of time since the most recent delta CRL was issued and s is the number of segments.

The request rate for CRLs can be determined by considering that a relying party will request a single CRL segment in the interval of delta-CRLs. The relying party that performs a validation in any interval will request CRL segment when the amount of time since the last received update certificate status information exceeds the window size of delta-CRLs. It is possible in either way that the relying party does not perform any validations during the window (the period of delta-CRL) or the relying party performs validations by using a segmented delta CRL that was obtained before the start of window (the period of currently delta-CRL). P_{val} is the probability that a relying party will perform a validation during the interval. So the probability that a relying party will perform no validation during interval is $1- P_{val}$. Since there are wO/l intervals in the period of delta-CRL : $(1-P_{val})^{wO/l}$. In order for a relying party to perform validation during the interval of current delta-CRL segment using the previous delta-CRL segment. The lifetime of the previous delta-CRL segment must overlap the window of the current delta-CRL segment as shown in figure 1.

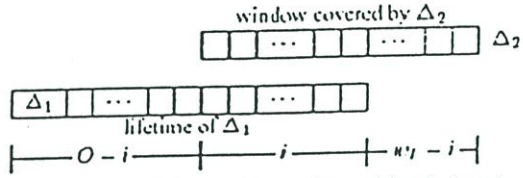


Figure 1. Lifetime Δ_1 overlaps with window Δ_2

The current delta-CRL segment (Δ_2) is issued at the beginning of interval (p) and has a window size of w_l. So, Δ_2 covers interval $[p-w_l, p-1]$. The last delta-CRL segment (Δ_1) is issued at the beginning of interval $p-w_l-O+i$ that is valid for O interval. So, the lifetime of Δ_1 and the window covered Δ_2 is overlap by i intervals. Obviously, the relying party must download a delta-CRL segment during interval $p-w_l-O+i$. So, the probability that the relying party will download a delta-CRL segment during $p-w_l-O+i$ is P_Δ. The probability that the relying party will perform no validation during interval $[p-w_l, p-w_l+i-1]$ is $(1-P_{val})^i$. The probability that the relying party will perform validations during interval $[p-w_l, p-w_l+i-1]$ is $1-(1-P_{val})^i$. Finally, the probability that the relying party will perform no validations during intervals $[p-w_l+1, p-1]$ is $(1-P_{val})^{w_l-i} = (1-P_{val})^{wO/l-i}$. The probability that the relying party will request a single CRL during interval is

$$P_b = P_{val}\left\{(1-P_{val})^{wO/l} + P_\Delta \sum_{i=1}^{O-1}[1-(1-P_{val})^i]\ (1-P_{val})^{wO/l-i}\right\} \quad (11)$$

The probability that the relying party will not perform validation during the interval is $e^{-vl/sO}$, so $P_{val} = 1-e^{-vl/sO}$. The probability that the relying party will request a delta CRL segment in any interval can be computed by equation (5) (giving N=1).

$$P_\Delta = \int_0^{l/O} \frac{ve^{-vt}\,dt}{(O-1)(1-e^{-vl/O})+1}$$

$$= \frac{1 - e^{-w/O}}{(O-1)(1-e^{-w/O}) + 1} \quad (12)$$

P_{val} and P_{Δ} (12) can be simplified to

$$P_{,} = \frac{(1 - e^{-w/sO})\ e^{-(w+l/O-t)v/s)}}{(O-1)(1-e^{-w/O}) + 1}$$

$$= P_{\Delta}\ e^{-(w+l/O-t)v/s)} \quad (13)$$

Equation (13) brings about computing the request rate for CRL segment that the relying party request a CRL segment at the first validation during interval [t...t+dt] (in limit dt→0) is $ve^{-w/s}dt$. So the probability that the relying party's validation during an interval will request a CRL segment during that interval can be computed by dividing equation (11) by P_{val} and multiplied by the number of relying party (N). The result of the request rate over the interval is

$$R_{sO}(t) = \frac{Nve^{-(t+w+l/O-t)v/s)}}{(O-1)(1-e^{-w/sO}) + 1}$$

$$= R_{sl}(t)\ e^{-(w+l/O-t)v/s)} \quad (14)$$

4. Analysis results

For the proposed revocation model, over-issuing delta-CRLs with distribution points, it is useful to define an environment. To simplify the analysis, it is assumed that the experimental environment has only one certificate revocation information issuer (CA) that serves all relying parties, and all revocations in the system are available to or delivered to each relying party.

Let N represents the number of relying parties (300,000 relying parties), v represents the validation rate (10 certificates per day), O represents the number of CRLs (delta-CRLs) that are valid at any time (4 CRLs), w represents the window size of the current delta-CRLs (9 hr.), l represents the length of time that a delta-CRL is valid (4 hr.), t represent the amount of time since the most recent delta-CRL was issued and r represents the average of certificates that are revoked each day (1,000 certificates per day). In MITRE, it is estimated that the size of a CRL is 51 bytes plus 9 bytes for each certificate included on the CRL.

The analysis result that compares the request rate between the over-issuing delta-CRL method and the over-issuing delta-CRL method is shown in figure 2. We can make a conclusion from this graph that the over-issuing delta-CRL with distribution points method has no improvement in the request rate that actually increases in average, but the repository serves the requests for delta-CRL segment at a faster rate.

In figure 3, the comparison between the size of delta-CRL of the over-issuing delta-CRL with distribution point and without distribution points concludes that the over-issuing delta-CRL with distribution points method can reduce the size of delta-CRL. As a result, the traditional delta-CRL scheme can be improved since the bandwidth usage is reduced as shown in figure 4.

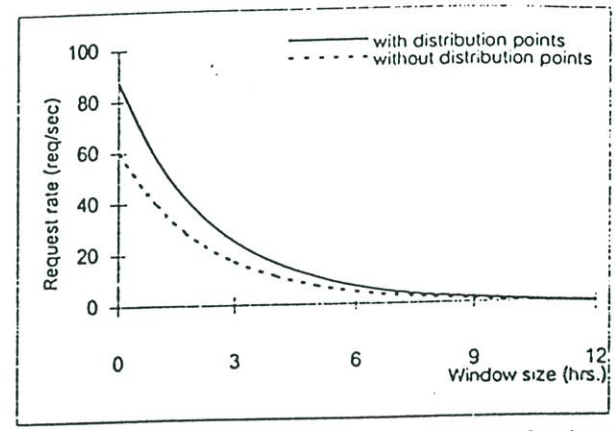


Figure 2. The effect of window size on request rate for three repositories

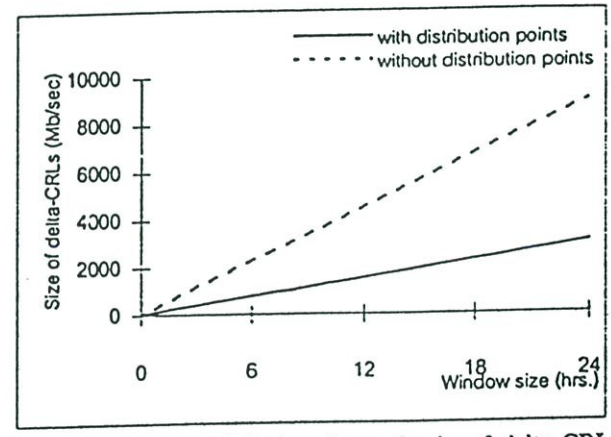


Figure 3. The effect of window size on the size of delta-CRL for three repositories

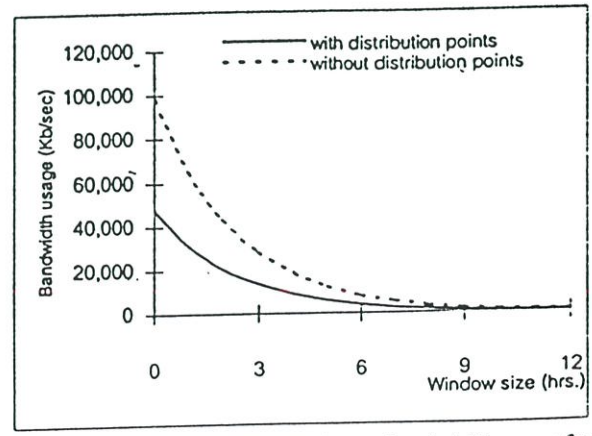


Figure 4. The effect of window size on bandwidth usage for three repositories

5. Conclusion

This paper has presented a model for over-issuing delta-CRL with distribution points using delta-CRLs together with over-issuing segmented CRLs. The proposed method can spread out the request rate and reduce the size of the delta-CRL. We compare the proposed model with the existing over-issuing delta-CRLs. It is demonstrated that the combination of both methods can improve the performance of the revocation system. The proposed model provides the performance benefits for which delta-CRLs and over-issuing delta-CRLs were originally designed.

6. References

[1] S. Berkovits, S. Chokhani, J. A. Furlong, A. Geiter and J. C. Guild, "Public Key Infrastructure Study: Final Report," the MITRE Corporation for NIST, April 1994.

[2] David A. Cooper, "A Model of Certificate Revocation," Proceedings of the Fifteenth Annual Computer Security Applications Conference, December 1999, pp. 256-264.

[3] David Cooper, "A More Efficient use of Delta-CRLs," IEEE Symposium on Security and Privacy, May 2000, pp. 190-202.

[4] Patrick McDaniel and Aviel Rubin, "A Response to "Can We Elimininate Certificate Revocation List?"," Technical Report 99.8.1, AT&T Labs, February 2000.

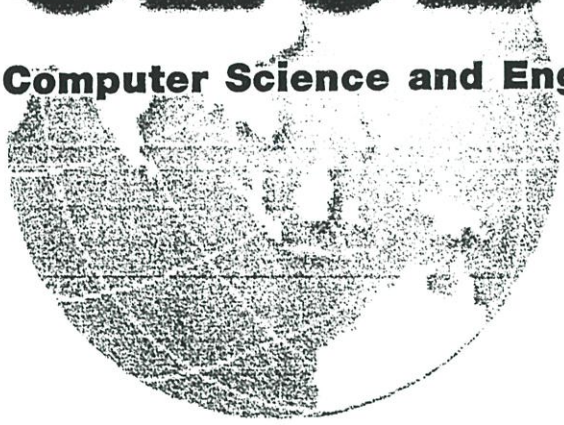
[5] André Årnes, "Public Key Certificate Revocation Schemes," Thesis, Queen's University, Ontario, Canada, 2000.

[6] André Årnes et al., "Selecting Revocation Solutions for PKI," Proceedings of NORDSEC 2000, Fifth Nordic Workshop on Secure IT Systems, Reykjavik, Iceland, September 2000.

[7] Åsa Hagström, Christopher J. Michelsen and David Rowe, "Cryptographic Support for Certificate Revocation," Secure Telecommunication Systems, ECE 636/INFT 931, April 2001.

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

A Comparative Analyzes of Over-Issuing Delta-CRLs with Distribution Points with Existing Certificate Revocation Methods

Aradee Rojanapasakorn
Faculty of Information Technology,
King Mongkut's Institute of Technology Ladkrabang
Ladkrabang, Bangkok 10520, Thailand
Email: pla_aradee@hotmail.com

Chanboon Sathitwiriyawong
Faculty of Information Technology, and
Research Center for Communication and Information Technology,
King Mongkut's Institute of Technology Ladkrabang
Ladkrabang, Bangkok 10520, Thailand
Email: chanboon@it.kmitl.ac.th

Abstract

PKI' s certificates is a basis that allows entities to trust each other. Due to different constraints, a certificate is only valid within a specific period of time. Coming from several threats, there are important reasons why its validity must be terminated sooner than assigned, the certificate needs to be revoked. This paper presents a model for the certificate revocation list (CRL) issued by a certificate authority (CA). The model uses the combination of over-issuing segmented CRLs and delta-CRLs for distributed segmented CRLs to locate repositories. The results from the comparative analyzes show that the proposed certificate revocation system using over-issuing delta-CRLs with distribution points can significantly improve the system performance such as spreading out request rate, reducing the size of certification revocation information and reducing the average network load.. This model is used to highlight inefficiencies in the traditional method of distributing certificate status information using CRLs.

Key-Words: Certificate Revocation List (CRL), Delta-CRLs, segmented CRL, over-issuing CRLs, Distribution Points

1. Introduction

Public Key Infrastructure (PKI) is a prerequisite for security in large networks and distributed systems that certification authorities (CAs) will be interconnected. Each CA would periodically issues a certificate and a certificate revocation list (CRL) that is distributed to repository for each replying party downloading certificate status information.

A CRL contains a list of serial numbers of revoked certificates together with their date of revocation, and also a date of its generation and a latest date of the next issue. A relying party respects to use the information in the certificate that must be first validated. The relying party requires a recent CRL in order to perform validation and subsequently stores it in his cache.

Delta-CRLs is a base CRL that only contains information about the certificate status has been changed in the revocation information to refer the base CRL. Delta-CRLs are periodically posted and updated to the last base CRL posting. Since the size of delta-CRLs is significantly smaller than the size of base CRLs and can be posted more frequently, the load on the repository can be reduced and the response time for the relying party can also be improved. However, the use of delta-CRL will not reduce the request rate for revocation information from the repository.

This paper presents a model of certificate revocation. The techniques that were developed previously are applied to over-issuing delta-CRLs with distribution points method as the method were designed and the resulting model is shown the comparative methods of certificate revocation. Finally, the new method of over-issuing delta-CRLs with distribution points is presented.

2. Related Works

In 1994, The National Institute of Standards and Technology (NIST) cooperated The MITRE Corporation [1] to study the alternatives for automated management of public keys and management of the associated public key certificates. This Public Key Infrastructure (PKI) study focuses on the policy and legal that issues relates to the operation and the management of the PKI. Architectural and implementation alternatives for the PKI are developed. In addition, a methodology to determine the cost of the PKI is presented. This report presented the result of the PKI study, the information and techniques

In 1998, Carlisle A. and Robert Z. [2] presented a framework that allows CRLs to be small, to provide timely information when needed, to scale and to be flexible. It also has the advantage that it can be engineered at the outset to provide a reliable service meeting certain space, timeliness and scale requirements and can be modified later if these requirements change. This framework is based on established standards and requires only the definition of one additional certificate extension and one additional CRL extension.

About the same time, Ronald Rivest [3] proposed the idea of without CRL's. CA can organize a certificate infrastructure so that a signer can present just a collection of certificates to the acceptor as evidence a support of signature and the signed message. The acceptor and signer might negotiate about the recency of some of the certificate, in which case it is the signer's responsibility to get more recent replacement. But in 2001, Patrick McDaniel and Aviel Rubin [4] disputed the idea's Rivest that mechanism was without CRLs. They assert that the need for real-time revocation state is not present in the vast majority of Internet transactions. CRLs are most suited to tightly coupled environments where reference locality can be observed. The requirement of timeliness can be met with short, achievable, periods using any number of revocation techniques.

In 1999, The Internet X.509 PKI Certificate and CRL Profile [5] is documented specifies an Internet Standard track protocol for the Internet community, and requests discussion and suggestion for improvements. The X.509 v2 CRL format is described in detail, with additional information regarding the format and semantics of Internet name forms. And David Cooper [6] [7] presented a model of the distribution of revocation information using certificate revocation list (CRLs). This model is used to highlight inefficiencies in the base CRL method. Several alternative CRL-based revocation distribution mechanisms, over-issued CRLs, segmented CRLs and delta-CRL was presented

In 2000, Andre Arnes's thesis [8] provided a survey and an analysis of existing schemes for public key certificate revocation. The analysis includes the traditional certificate revocation lists, protocols that provide on-line certificate revocation, as well as revocation systems with reduced data structures, Some techniques for improving the existing schemes are suggested. Based on the analysis, the different schemes are compared in order to highlight advantages. A guideline for using this information in selecting a revocation solution is developed and applied to different example scenarios. Next paper [9] presented a survey, a comparative analysis of available revocation schemes for PKI certificates and performance simulations on some revocations schemes. As a conclusion, the schemes are evaluated with respect to combining different schemes in order to achieve better performance.

In 2002, The Internet X.509 PKI certificate and CRL profile [10] is document that an overview of this approach and model are provided as an introduction. The X.509 v3 certificate and the X.509 v2 CRL format is described in detail, with additional information regarding the format and semantics of Internet name forms. Standard certificate extensions are described and two Internet-specific extensions and a set of required certificate extensions.

This paper is base on the work with the paper "A Certificate Revocation method of Over-Issuing Delta-CRLs with Distribution Points" [11] submitted to the 3rd International Symposium on Communications and Information Technologies September 2003. The paper presented a model over-issuing delta-CRLs with distribution points. The result model is shown the comparing with the over-issuing delta-CRLs from the mathematical analyses show that the proposed model can significantly improve the system performance such as spreading out request rate, reducing the size of certification revocation information and reducing the bandwidth usage. This paper provides a comparative analysis of available revocation model. The result of the mathematical analysis are also presented.

Next section describes the idea of over-issuing delta-CRLs with distribution points method that can improve performance of issued certificate revocation information.

3. Over-Issuing Delta-CRLs with Distribution Points

In this section, over-issuing delta-CRL with distribution points developed a mathematical model for certificate revocation models and applied this model by taking the approach of over-issuing segments CRLs [6] and delta-CRLs [7]. Both methods can distribute and reduce the peak request

rates. Based on the similar analysis, if relying parties require to obtain a fresh certificate status information very frequently, then it may not be possible to significantly reduce the peak request rate for delta-CRL. But if the validity period of delta-CRL are long enough, then it may be possible to significantly reduce the request rate for delta-CRLs by over-issuing the delta-CRLs. The performance improvement can be done by the use of segmented CRLs that will usually reduce the size of each delta-CRLs.

The request rate for over-issuing delta CRLs distribution points will be the same as the request rate for over-issued segmented CRLs that does not use delta-CRLs [7].

$$R_{sI}(t) = \frac{Nve^{-vt/s}}{(O-1)(1-e^{-vl/sO})+1} \quad (1)$$

Where l is the length of time that a delta-CRL is valid, O is the number of delta-CRL that are valid at any time, t is the amount of time since the most recent delta CRL was issued, and s is the number of segments.

The request rate for CRLs can be determined by considering that a relying party will request a single CRL segment in the interval of delta-CRLs. The relying party that performs a validation in any interval will request CRL segment when the amount of time since the last received update certificate status information exceeds the window size of delta-CRLs. It is possible in either way that the relying party does not perform any validation during the window (the period of delta-CRL) or the relying party performs validations by using a segmented delta CRL that was obtained before the start of window (the period of currently delta-CRL). P_{val} is the probability that a relying party will perform a validation during the interval. So the probability that a relying party will perform no validation during interval is $1-P_{val}$. Since there are wO/l intervals in the period of delta-CRL: $(1-P_{val})^{wO/l}$. In order for a relying party perform validation during the interval of current delta-CRL segment using the previous delta-CRL segment. The lifetime of the previous delta-CRL segment must overlap the window of the current delta-CRL segment as shown in Figure 1.

The current delta-CRL segment (Δ_2) is issued at the beginning of interval (p) and has a window size of w_I. So, Δ_2 covers interval $[p-w_I, p-1]$. The last delta-CRL segment (Δ_1) is issued at the beginning of interval $p-w_I-O+i$ that is valid for O interval. So, the lifetime of Δ_1 and the window covered Δ_2 is overlap by i intervals. Obviously, the

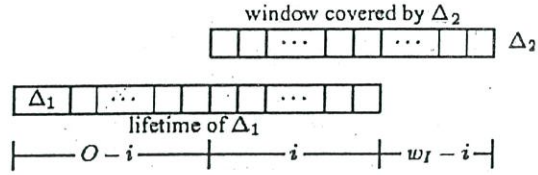


Figure 1. Lifetime Δ_1 overlaps with window Δ_2

relying party must download a delta-CRL segment during interval $p-w_I-O+i$. So, the probability that the relying party will download a delta-CRL segment during $p-w_I-O+i$ is P_Δ. The probability that the relying party will perform no validation during interval $[p-w_I, p-w_I+i-1]$ is $(1-P_{val})^i$. So, the probability that the relying party will perform validations during interval $[p-w_I, p-w_I+i-1]$ is $1-(1-P_{val})^i$. Finally, the probability that the relying party will perform no validations during intervals $[p-w_I+1, p-1]$ is $(1-P_{val})^{w_I-l} = (1-P_{val})^{wO/l-l}$. The probability that the relying party will request a single CRL during interval is

$$P_b = P_{val}\{(1-P_{val})^{wO/l} + P_\Delta \sum_{i=1}^{O-1}[1-(1-P_{val})^i]\ (1-P_{val})^{wO/l-i}\} \quad (2)$$

The probability that the relying party will not perform validation during the interval is $e^{-vl/sO}$, So $P_{val} = 1-e^{-vl/sO}$. The probability that the relying party will request a delta CRL segment in any interval can be computed by equation (5) (giving N=1).

$$P_\Delta = \int_0^{l/O} \frac{ve^{-vt}dt}{(O-1)(1-e^{-vl/O})+1} = \frac{1-e^{-vl/O}}{(O-1)(1-e^{-vl/O})+1} \quad (3)$$

P_{val} and P_Δ in equation (8) can be simplified to

$$P_s = \frac{(1-e^{-vl/sO})\ e^{-(w+l/O-l)(v/s)}}{(O-1)(1-e^{-vl/O})+1} = P_\Delta\ e^{-(w+l/O-l)(v/s)} \quad (4)$$

Equation (4) brings about computing the request rate for CRL segment that the relying party request a CRL segment at the first validation during interval [t...t+dt] (in limit dt→0) is $ve^{-vt/s}dt$. So the probability that the relying party's validation during an interval will request a CRL segment during that interval can be computed by dividing equation (2) by P_{val} and multiplied by the number of relying party (N). The result of the request rate over the interval is

$$R_{sO}(t) = \frac{Nve^{-(t+w+l/O-l)(v/s)}}{(O-1)(1-e^{-w/sO})+1}$$
$$= R_{sI}(t) \quad e^{-(w+l/O-l)(v/s)} \qquad (5)$$

4. Analysis Results

In this section, we present the graph in order to compare over-issuing delta-CRLs with distribution points with several CRL-based methods. For the proposed revocation model, it is useful to define an environment. To simplify the analysis, it is assumed that the experimental environment has only one certificate revocation information issuer (CA) that serves all relying parties, and all revocations in the system are available or delivered to each relying party.

An environment for demonstration, let N represents the number of relying parties (300,000 relying parties), v represents the validation rate (10 certificates per day), O represents the number of CRLs (delta-CRLs) that are valid at any time (4 CRLs), w represents the window size of the current delta-CRLs (9 hr.), l represents the length of time that a delta-CRL is valid (4 hr.), t represent the amount of time since the most recent delta-CRL was issued and r represents the average of certificates that are revoked each day (1,000 certificates per day), In MITRE [1], it is estimated that the size of a CRL is 51 bytes plus 9 bytes for each certificate included on the CRL.

An observation from the traditional CRL model is that the peak request rate for CRLs will occur at the time of the CRL issuance. At this time, there will be a rush to obtain the newest CRL. After that, the request rate is exponentially decreasing, as each relying party caches the CRL and only has to obtain a CRL at most once each interval as depicted in figure 2. The CRL distribution points can spread out peak request rate to several repository. The over-issuing segmented CRL can reduce the peak load on the repository for base CRL. In figure 3, the delta-CRLs method bring about the increase validity period of base CRLs, since the delta CRL ensure higher timeliness with significantly smaller postings. In figure 4, the over-issuing delta-CRLs with distribution points can reduce the peak request rate by allowing multiple CRLs and delta-CRLs to have overlapping validity times. So, there are multiple valid CRLs available, each with a different expiration time.

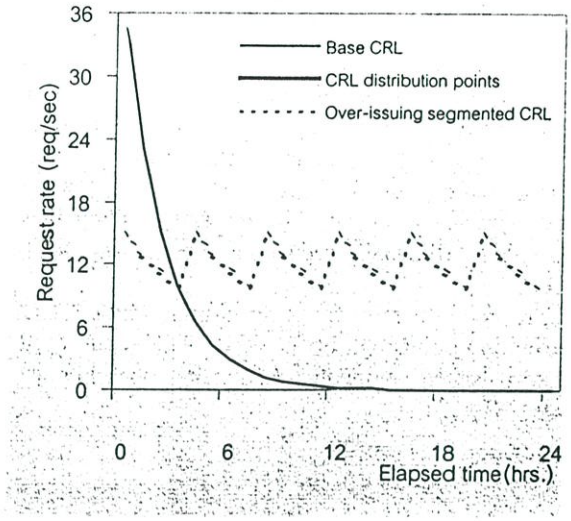


Figure 2. The comparative methods of CRLs

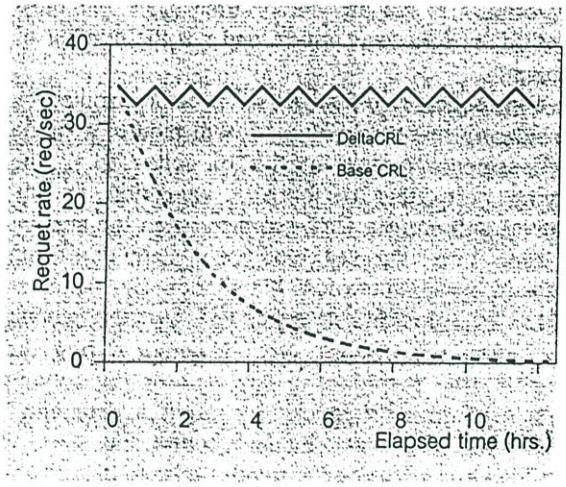


Figure 3. The request rate for delta-CRL

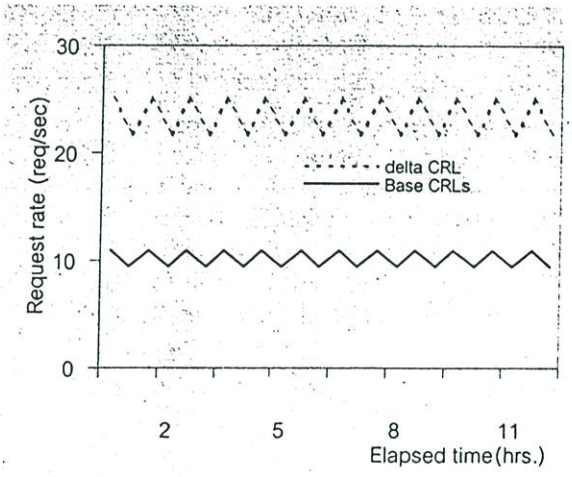


Figure 4. The request rate for over-issuing delta-CRL with three distribution points

The analysis result that compares the request rate with based CRLs, CRL distribution points, over-issuing CRL, delta-CRL and over-issuing delta-CRL method. The demonstration is shown in figure 2, 3, 4. We can make a conclusion from this graph that the peak request rate for CRL is maximum at the time of CRL issuance. For CRL distribution points, the peak request rate is unchanged, but the graph decreases slower that demonstrate to spread out the peak request rate to several repository. For over-issuing segmented CRL, it is possible to reduce the peak request rate for base CRL. For delta-CRL, the peak request rate is unchanged, but the validity period of base CRLs increased. For the over-issuing delta-CRL with distribution points method has an improvement in the request rate that decreases in average, and the repository serves the requests for delta-CRL segment at a faster rate.

We computed the mathematic of several CRLs methods for each method using peak bandwidth and the size of CRLs (see table 1).

Table 1. Comparison of several certificate revocation methods

Method	Reqest rate for base CRL (req/sec)	Reqest rate for delta-CRL (req/sec)	Peak bandwidth (Kbytes/sec)	size CRLs (Kbytes)	size delta-CRL (Kbytes)
CRL	34.72	0.00	57.03	1,642.55	0.00
CRL distribution points	34.72	0.00	57.03	1,642.55	0.00
Over-issuing segmented CRL	25.95	0.00	42.62	1,642.55	0.00
Delta-CRL	34.72	34.70	57.15	1,642.55	3.43
Over-issuing Delta-CRL with distributrion points	2.05	25.00	1.15	547.55	1.18

It compares the different certificate revocation methods base on the previous analysis and highlights and the weaknesses and strengths of the different methods. The peak request rate for several certificate revocation methods vary slightly except the over-issuing delta-CRLs with distribution points method that the request rate is lowest. The bandwidth usage varies widely that base CRLs and delta-CRLs have similar maximum bandwidth usage. Since base CRLs and delta-CRLs have a large size of CRLs and high request rate. The size of CRLs and size of delta-CRLs varies widely. These variations most likely occur due to the separate CRLs method. Obviously, the size of delta-CRLs for base CRLs, CRLs distribution points and over-issuing segmented CRLs are zero. As can be seen in the tables, The over-issuing delta-CRL with distribution points method can be improve performance the certificate revocation method, since it can be spread out request for CRLs and reduce the size of each CRL and the CRLs in relying parties' caches do not all expire at the same time.

For a sufficient number of certificate revocations (as in environment), these graphs qualitatively confirmed Cooper's model [6] [7]. In particular, the peak request rate for CRL occur at time zero, and it decrease exponentially. As, the graph for the CRLs distribution points method is similar to the graph for base CRLs but it decreases slower. Each delta-CRLs period demonstrates the same properties as a base CRLs period. Finally, the request rate for over-issuing delta-CRLs with distribution points is swing as a result of staggering the issuance of segmented CRLs and delta-CRLs

5. Conclusions

This paper describes the idea of over-issuing delta-CRLs with distribution points method that can improve performance of issued certificate revocation information. The method developed a mathematical model for certificate revocation models and applied this model by taking the approach of over-issuing segmented CRLs and delta-CRLs. The proposed method can spread out the request rate and reduce the size of the delta-CRL. We compare the proposed model with the existing certificate revocation methods. the mathematical analyze demonstrated that the other methods have performance lower than the over-issuing delta-CRL with distribution points using delta-CRLs in the same environment.

6. References

[1] S. Berkovits, S. Chokhani, J. A. Furlong, A. Geiter and J. C. Guild, "Public Key Infrastructure Study: Final Report," the MITRE Corporation for NIST, April 1994.

[2] C. Adams, R. Zuccherato, "A General, Flexible Approach to Certificate Revocation," Entrust Technologies White Paper, June 10, 1998.

[3] Ronald Rivest, "Can We Eliminate Certificate Revocation Lists?," In Rafael Hirschfeld, editor, Financial Cryptography, Volume 1465, February 1998, pp. 178-183.

[4] Patrick McDaniel, Aviel Rubin, "A Response to "Can We Eliminate Certificate Revocation Lists?"," Technical Report 99.8.1, AT&T Labs, February 2000.

[5] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," IETF RFC 2459, January 1999.

A Performance Study of Over-Issuing Delta-CRLs with Distribution Points

Aradee Rojanapasakorn and Chanboon Sathitwiriyawong
Faculty of Information Technology,
King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand
Email: pla_aradee@hotmail.com, chanboon@it.kmitl.ac.th

Abstract

Digital certificates have been used to prove the identities of entities. Due to different constraints, they are only valid within a specific time. Confronting many threats is an important reason why their validities must be terminated sooner than assigned. Therefore, a certificate revocation is essential. This paper presents a new method of issuing certificate revocation lists (CRLs) by over-issuing delta-CRL with distribution points. The combination of over-issuing segmented CRLs and delta-CRLs is used to distribute CRL segments over several directories. The results from the comparative analyzes show that the proposed certificate revocation method can significantly improve the system performance such as spreading out the request rate, and reducing the size of certification revocation information and the average network usage. It also highlights inefficiencies of the traditional method of distributing certificate status information using CRLs.

1. Introduction

Public key cryptography requires the ability to verify the authenticity of public keys. Public key infrastructure (PKI) is a security basis for distributed systems that many certification authorities (CAs) are interconnected. Each CA issues a certificate and a certificate revocation list (CRL) periodically. The CRL is distributed to a directory where each relying party downloads the certificate status information. It contains a list of serial numbers of revoked certificates, date of revocation, date of its generation, and the latest date of the next issue. A relying party respects to use the information in the certificate that must be first validated. A recent CRL is required in order to perform validation and subsequently stored in the cache. Many CRL methods are standardized and widely used. The CRL-based methods are viewed by many experts as a suitable basis for most certificate revocation systems.

Delta-CRL is a base CRL that contains the certificate status that has been changed in the revocation information to refer to the base CRL. Delta-CRLs are periodically posted and updated to the last base CRL posting. Since the size of delta-CRLs is much smaller than that of base CRLs and they can be posted more frequently, the workload on the directories and the response time experienced by the relying parties can be reduced. However, the use of delta-CRLs will not reduce the request rate for the revocation information.

Sliding window delta-CRL is an issuance of delta-CRL that setting a large fixed window size rather than allowing various window sizes. It allows a new base CRL created locally to be based on a valid base CRL and delta-CRL. In this way, most relying parties will request a delta-CRL before the cached certificate revocation information expires. The peak request rate for the base CRL is therefore reduced. However, the request rate of delta-CRLs is not reduced due to its large window size.

This paper presents a new method of issuing CRLs using the combination of over-issuing segmented CRLs and delta-CRLs to distribute CRL segments over several directories. Its performance is analytically evaluated and compared with existing revocation methods.

2. Related works

PKI was initiated by the NIST [1] to study the alternatives for automated management of public keys and management of the associated public key certificates. The study focused on the policy and legal issues that relate to the operation and management of the PKI. Architectural and implementation alternatives for the PKI were developed. Carlisle and Robert [2] presented a framework using small CRLs to provide reliable services, timeliness, scalability, and flexibility. The framework was based on established standards and required only the definition of one additional certificate extension and one additional CRL extension.

Rivest [3] proposed another idea that did not need CRLs. CA can organize a certificate infrastructure so that a signer can present just a collection of certificates to the acceptor as evidence a support of signature and the signed message. The acceptor and signer might negotiate about the recency of some certificates, in which case it is the signer's responsibility to get more recent replacement.

ceedings of the 18th International Conference on Advanced Information Networking and Application (AINA'04)
695-2051-0/04 $ 20.00 © 2004 IEEE

However, McDaniel and Rubin [4] disputed Rivest's idea. They asserted that real-time revocation states are needed in the vast majority of Internet transactions. CRLs are most suitable for tightly coupled environments where reference locality can be observed. The requirement of timeliness can be met using any number of revocation techniques.

Internet X.509 PKI certificate and CRL profile [5][10] specifies X.509v3 certificate, X.509v2 CRL format, and the format and semantics of Internet name forms. Standard certificate extensions are described together with two Internet-specific extensions and a set of required certificate extensions.

Cooper [6][7] presented a model of the distribution of revocation information using CRLs to highlight the inefficiency of the base CRL method. Several alternatives such as over-issuing CRLs, segmented CRLs, and delta-CRLs were presented.

Arnes [8] provided a survey and an analysis of existing schemes including traditional CRLs, protocols that provide the on-line certificate revocation, and revocation systems with reduced data structures. Some techniques for improving the existing schemes were suggested. Different schemes were compared in order to highlight their advantages. The next paper [9] presented a survey, a comparative analysis of available revocation schemes, and simulation study on some revocation schemes. They were evaluated with respect to the combination of different schemes in order to achieve better performance.

Our previous work [11] proved that the over-issuing delta-CRLs with distribution points method can greatly improve the system performance such as spreading out the request rate, reducing the size of the certification revocation information and the bandwidth usage.

3. Proposed certificate revocation method

Based on analytical models of over-issuing segmented CRLs [6] and delta-CRLs [7], we developed a certificate revocation model for over-issuing delta-CRLs with distribution points. Based on the similar analysis, if relying parties require certificate status information very frequently, then it may not be possible to significantly reduce the peak request rate for delta-CRLs. If the validity period of delta-CRL is long enough, then it may be possible to significantly reduce the request rate for delta-CRLs by over-issuing the delta-CRLs. The performance improvement can be achieved by the use of segmented CRLs that will usually reduce the size of each delta-CRL. The request rate for the proposed method is the same as that for over-issuing segmented CRLs [7] as follows.

$$R_{sl}(t) = \frac{Nve^{-vt/s}}{(O-1)(1-e^{-vl/sO})+1} \qquad (1)$$

Where N is the number of relying parties, v is the validation rate, l is the length of time that a delta-CRL is valid, O is the number of delta-CRLs that are valid at any given time, t is the amount of time since the most recent delta CRL was issued, and s is the number of segments.

The request rate for CRLs can be determined by considering that a relying party will request a single CRL segment in the interval of delta-CRLs. The relying party that performs a validation in a given interval will request a base CRL in that interval if the amount of time since the last received update certificate status information exceeds the window size of delta-CRLs (w). It is possible in either way that the relying party does not perform any validation during the window (the period of delta-CRL) or the relying party performs a validation by using a segmented delta CRL that was obtained before the start of the window (the period of currently delta-CRL). P_{val} is the probability that a relying party will perform a validation during the interval. Since there are wO/l intervals in the period covered by a delta-CRL, the probability that a relying party will perform no validation during that period is $(1-P_{val})^{wO/l}$. In order for a relying party to perform validation during the interval of current delta-CRL segment using the previous delta-CRL segment, the lifetime of the previous delta-CRL segment must overlap the window of the current delta-CRL segment [11].

The current delta-CRL segment (Δ_2) is issued at the beginning of the interval (p) and has a window size of w_l. So, Δ_2 covers interval $[p-w_l, p-1]$. The last delta-CRL segment (Δ_1) is issued at the beginning of the interval $p-w_l-O+i$ that is valid for O interval. So, the lifetime of Δ_1 and the window covered Δ_2 is overlapped by i intervals. Obviously, the relying party must download a delta-CRL segment during the interval $p-w_l-O+i$. So, the probability that the relying party will download a delta-CRL segment during $p-w_l-O+i$ is P_Δ. The probability that the relying party will perform no validation during interval $[p-w_l, p-w_l+i-1]$ is $(1-P_{val})^i$. So, the probability that the relying party will perform a validation during interval $[p-w_l, p-w_l+i-1]$ is $1-(1-P_{val})^i$. Finally, the probability that the relying party will perform no validation during interval $[p-w_l+1, p-1]$ is $(1-P_{val})^{w_l-i} = (1-P_{val})^{wO/l-i}$. The probability that the relying party will request a single CRL during the interval is

$$P_b = P_{val}\left\{(1-P_{val})^{wO/l} + P_\Delta \sum_{i=1}^{O-1}[1-(1-P_{val})^i]\ (1-P_{val})^{wO/l-i}\right\} \qquad (2)$$

ceedings of the 18th International Conference on Advanced Information Networking and Application (AINA'04)
695-2051-0/04 $ 20.00 © 2004 IEEE

The probability that the relying party will not perform any validation during the interval is $e^{-vl/sO}$, So $P_{val} = 1 - e^{-vl/sO}$. The probability that the relying party will request a delta CRL segment in any interval can be computed by equation (1) (giving N=1).

$$P_{\Delta} = \int_0^{l/O} \frac{ve^{-vt}dt}{(O-1)(1-e^{-vl/O})+1} = \frac{1-e^{-vl/O}}{(O-1)(1-e^{-vl/O})+1} \quad (3)$$

P_{val} and P_{Δ} in equation (2) can be simplified to

$$P_s = \frac{(1-e^{-vl/sO})\ e^{-(w+1/O-1)(v/s)}}{(O-1)(1-e^{-vl/O})+1} = P_{\Delta}\ e^{-(w+1/O-1)(v/s)} \quad (4)$$

Equation (4) brings about the computation of the request rate for the CRL segment requested by the relying party at the first validation during interval [t...t+dt] (in limit dt→0) that is equal to $ve^{-vt/s}dt$. So the probability of requesting a CRL segment for validation during an interval can be computed by dividing equation (4) by P_{val} and multiplied by the number of relying parties (N). The result of the request rate over the interval is

$$R_{sO}(t) = \frac{Nve^{-(t+w+1/O-1)(v/s)}}{(O-1)(1-e^{-vl/sO})+1} = R_{sl}(t)\ e^{-(w+1/O-1)(v/s)} \quad (5)$$

4. Analysis results

We compared the performance of the proposed method with several existing CRL-based methods. To simplify the analysis, it is assumed that there is only one certificate revocation information issuer (CA) that serves all relying parties, and all revocations in the system are available and delivered to each relying party.

Using the same parameter values as Cooper's work [6][7] where N=300,000, v=10, O=4, w=9, *and* l=4. It is estimated that the size of a CRL is 51 bytes plus 9 bytes for each certificate included on the CRL [1].

As shown in figure 1, the peak request rate for either the base CRL method or the CRL distribution points method is equal and occurs at the time of CRL issuance. After that, the request rate is exponentially decreasing, as each relying party caches the CRL and only has to obtain a CRL at most once each interval. For the latter, the request rate is decreased slower because of the spreading out of CRL requests to several repositories. The over-issuing segmented CRL can reduce the peak load on the repository for base CRL. As depicted in figure 2, the peak request rate of delta-CRL method is unchanged, but the validity period of base CRLs is increased to ensure higher timeliness. For the sliding window delta-CRL method shown in figure 3, the peak request rate for base CRL is reduced but that for delta-CRL is unchanged due to the setting of large window size and the its frequent issuance. So the relying parties do not download the base CRL, if they have the previous delta-CRL that does not expire. In figure 4, the over-issuing delta-CRLs with distribution points can reduce the peak request rate by allowing multiple CRLs and delta-CRLs to overlap their validity times. Therefore, multiple valid CRLs are available, each with a different expiration time.

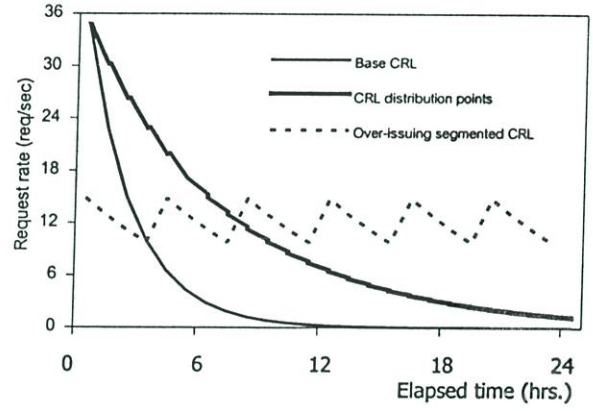


Figure 1. Comparison of various CRL methods

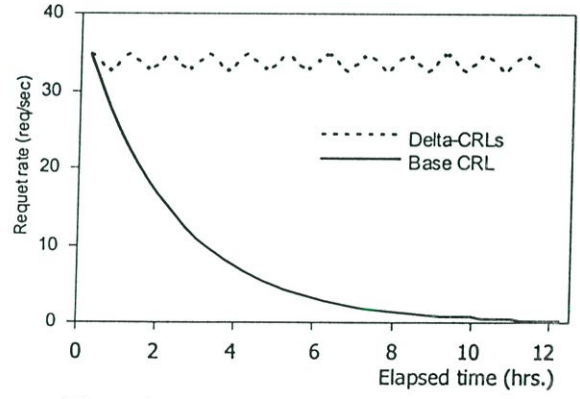


Figure 2. Request rate for delta-CRL method

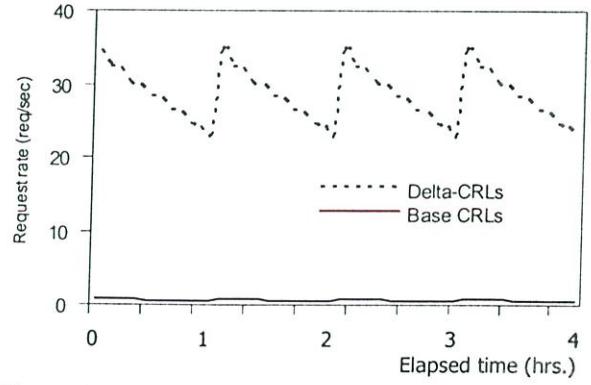


Figure 3. Request rate for sliding window delta-CRL method

ceedings of the 18th International Conference on Advanced Information Networking and Application (AINA'04)
695-2051-0/04 $ 20.00 © 2004 IEEE

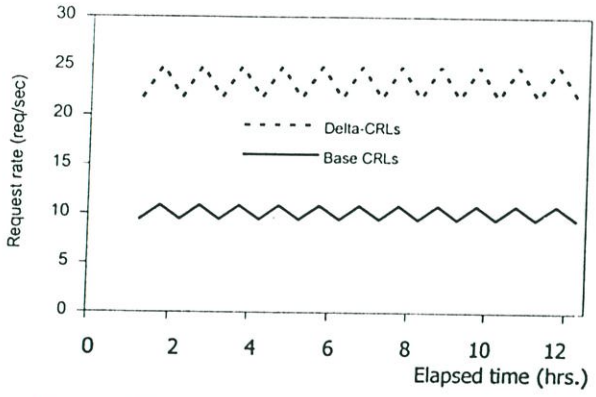


Figure 4. Request rate for over-issuing delta-CRL with distribution points method

In table 1, we compares several certificate revocation methods in terms of the request rate, the bandwidth usage and the size of CRLs.

Table 1. Comparison of several certificate revocation methods

Method	Reqest rate for base CRL (req/sec)	Reqest rate for delta-CRL (req/sec)	Bandwidth usage (Mbytes/sec)	Size of base CRL (Kbytes)	Size of delta-CRL (Kbytes)
CRL	34.72	-	57.03	1,642.55	-
CRL distribution points	34.72	-	57.03	1,642.55	-
Over-issuing segmented CRL	25.95	-	42.62	1,642.55	-
Delta-CRL	34.72	34.70	57.15	1,642.55	3.43
Sliding window delta-CRL	0.82	32.38	1.46	1,642.55	3.43
Over-issuing delta-CRL with distribution points	2.05	25.00	1.15	547.55	1.18

The peak request rate for base CRL of most certificate revocation methods is similar and relatively high, except the sliding window delta-CRL method and the proposed method. The request rate for delta-CRL is in the vicinity but the proposed method is the lowest. The bandwidth usage of both methods is also relatively low because of their small request rate. The proposed method has the smallest size of both base CRLs and delta-CRLs. It can improve the performance of the certificate revocation method since it can spread out the requests for CRLs and reduce the size of each CRL, and the CRLs in relying parties' caches do not expire at the same time.

Each delta-CRLs period demonstrates the same properties as a base CRLs period. Finally, the request rate of the proposed method is swing as a result of staggering the issuance of segmented CRLs and delta-CRLs.

5. Conclusions

It can be concluded that the over-issuing delta-CRLs with distribution points method can improve the performance of issuing certificate revocation information. Mathematical models for certificate revocation methods were developed by employing over-issuing segmented CRLs and delta-CRLs approaches. The proposed method can spread out the request rate and reduce the size of the base CRL and the delta-CRL. We compared the proposed model with the existing certificate revocation methods. The analyses demonstrated that the proposed method gains higher performance than the other methods since it can distribute CRL segments to several directories and each CRL segment has different expiration time. As a result, the relying parties do not need to download a new CRL from the directory if they have the valid CRL. Since the security of the proposed method is not reduced and the performance of issuing CRLs is significantly improved, we can conclude that the proposed method is the best issuing certificate revocation method.

6. References

[1] S. Berkovits, S. Chokhani, J.A. Furlong, A. Geiter, and J.C. Guild, *Public Key Infrastructure Study : Final Report*, the MITRE Corporation for NIST, April 1994.

[2] C. Adams, and R. Zuccherato, "A General, Flexible Approach to Certificate Revocation," Entrust Technologies White Paper, June 10, 1998.

[3] R. Rivest, "Can We Eliminate Certificate Revocation Lists?," *Financial Cryptography, Volume 1465*, February 1998, pp. 178-183.

[4] P. McDaniel, and A. Rubin, "A Response to "Can We Eliminate Certificate Revocation Lists?"," *Technical Report 99.8.1*, AT&T Labs, February 2000.

[5] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," *IETF RFC 2459*, January 1999.

[6] D.A. Cooper, "A Model of Certificate Revocation," *Proceedings of the Fifteenth Annual Computer Security Applications Conference*, December 1999, pp. 256-264.

[7] D.A. Cooper, "A More Efficient use of Delta-CRLs," *Proceedings of the 2000 IEEE Symposium on Security and Privacy*, May 2000, pp. 190-202.

[8] A. Arnes, "Public Key Certificate Revocation Schemes," *Thesis*, Queen's University, Ontario, Canada, 2000.

[9] A. Årnes, H. Meijer, S. Lloyd, M. Just, and S.J. Knapskog, "Selecting Revocation Solutions for PKI," *Proceedings of the Fifth Nordic Workshop on Secure IT Systems (NORDSEC 2000)*, Reykjavik, Iceland.

[10] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," *IETF RFC 3280*, April 2002.

[11] C. Sathitwiriyawong, and A.Rojanapasakorn, "A Certificate Revocation Method using Over-issuing Delta-CRLs with Distribution Points," *Proceedings of the Third International Symposium on Communications and Information Technologies (ISCIT 2003)*, September 2003, pp. 750-754.

ประวัติผู้เขียน

ชื่อ-นามสกุล	นางสาวอารดี โรจนภาสกร
วัน เดือน ปีเกิด	6 พฤศจิกายน 2518 ที่กรุงเทพ
ที่อยู่	940/155 ซ.เชลียง 7 ถ.บางนา-ตราด แขวงบางนา เขตบางนา กรุงเทพฯ 10260 โทร.0-2393-8958
ประวัติการศึกษา	พ.ศ. 2540 สำเร็จการศึกษาปริญญาตรีวิทยาศาสตร์บัณฑิต สาขาคณิตศาสตร์ประยุกต์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ความชำนาญเฉพาะด้าน	1.) ระบบการรักษาความปลอดภัยทางคอมพิวเตอร์ 2.) การจัดการระบบฐานข้อมูล
ประสบการณ์การทำงาน	
พ.ศ. 2542-พ.ศ.2546	เข้าเป็นพนักงานรัฐวิสาหกิจในตำแหน่งพนักงานโปรแกรมคอมพิวเตอร์ 4 สังกัดการสื่อสารแห่งประเทศไทย
พ.ศ. 2546-ปัจจุบัน	ดำรงตำแหน่งพนักงานโปรแกรมคอมพิวเตอร์ 5 สังกัดบริษัท ไปรษณีย์ไทย จำกัด