Solution for Network Management of Future Internet

Thipvanee Thiengtrong, Chirapa Somchai, Wasana Thiwongweang

545020141-4, 545020164-2 , 545020190-1

บทคัดย่อ - ปัจจุบันมีเครื่องคอมพิวเตอร์จำนวนมากเชื่อมต่อเข้าด้วยกันเป็นระบบเครือข่าย ไม่ว่าจะเป็นระบบเครือข่ายที่ใช้ตามองค์กรต่างๆ หรือที่ใช้ติดต่อสื่อสารกันระหว่างประเทศที่รู้จักกันดีในชื่ออินเตอร์เน็ตดังนั้นจึงมีความจำเป็นที่จะต้องมีเครื่องมือหรือวิธีการบางอย่างมาช่วยในการบริหารและดูแลระบบเครือข่ายเหล่านั้นให้ใช้งานได้อย่างมีประสิทธิภาพมากที่สุดและบางครั้งอาจจะใช้ในการค้นหาสาเหตุที่ทำให้ระบบเครือข่ายทำงานผิดพลาดด้วยก็ได้ความจำเป็นในการดูแลและบริหารระบบเครือข่ายคอมพิวเตอร์มีความสำคัญมากขึ้นทุกวันเพราะระบบเครือข่ายทุกวันนี้มีขนาดโตขึ้นอย่างรวดเร็วมาก เครื่องมือที่นิยมนำมาใช้ทุกวันนี้อยู่ในรูปของโปรแกรมบริหารระบบเครือข่ายที่ใช้โปรโตคอลSNMP (Simple Network Management Protocol) โดยเป็นโปรแกรมที่ทำการค้นหาอุปกรณ์เครือข่ายและแสดงการเชื่อมต่อของอุปกรณ์ที่ต่อกับระบบเครือข่าย การบริหารจัดการระบบเครือข่ายทำหน้าที่การตรวจสอบอุปกรณ์ต่าง ๆ ที่ทำงานอยู่ภายในระบบเครือข่าย ว่ามีการทำงานได้ถูกต้อง หรือไม่และหากมีข้อผิดพลาดเกิดขึ้นที่ส่วนใด ต้องทำการแก้ไข ให้สามารถทำงานได้หรือหาทางแก้ปัญหาเฉพาะหน้า เพื่อที่จะให้สามารถที่จะทำการสื่อสารได้อย่างต่อเนื่องต่อไป

Keyword: Network Management , SNMP, CIMP, NETCONF

I. บทนำ

อินเตอร์เน็ตในปัจจุบันเป็นหนึ่งในเทคโนโลยีที่ประสบผลสำเร็จมากที่สุดในประวัติศาสตร์ เป็นปรากฏการณ์ทางสังคมและส่งผลกระทบหลักว่าทำอย่างไรที่เราจะดำเนินธุรกิจและเปลี่ยนแปลงการติดต่อสื่อสารกับของผู้คนซึ่งติดต่อกันได้

อย่างไรก็ตาม ในปัจจุบันยังมีปัญหาอีกหลายประการในตัวของมันเอง รวมทั้งความปลอดภัย ความคล่องตัว QoS, Scalability และด้านการบริหารจัดการ ปัญหาเหล่านี้ได้รับการจัดการด้วย ad-hoc ในลักษณะที่ค่อนข้างห่างไกลความสำเร็จ แต่นักวิจัยพบบางปัญหาที่มาจากปัญหาขั้นพื้นฐานด้วยการออกแบบดั้งเดิมของนักวิจัยหลายคนเริ่มทำการออกแบบใหม่ ให้กับ (เรียกว่าในอนาคต, เครือข่ายในอนาคต หรือ เครือข่ายยุคใหม่) เป็นความพยายามที่จะแก้ไขปัญหาพื้นฐาน

มี 3 ขั้นตอนพื้นฐานที่แตกต่างสำหรับออกแบบในอนาคต อย่างแรกคือ การเพิ่มขึ้นหรือวิธีวิวัฒนาการและหลักฐานจากวิธีแก้ปัญหามากมาย จะถูกประยุกต์ใช้ในปัจจุบันที่ละเมิดหลักการของสถาปัตยกรรม เช่น การเปลี่ยนแปลงที่อยู่เครือข่าย Firewall และเครือข่ายเสมือนส่วนตัว มีเอกสารมากมายให้เหตุผลว่า ทำไมไม่มีในวิธีการแก้ปัญหาอย่างยั่งยืน อย่างที่สอง เรียกว่า “Clean Slate”[10] ซึ่งกำจัดข้อผูกพันที่มีอยู่, restraints,และข้อสันนิษฐานและเริ่มต้นด้วยความคิดใหม่ ๆ ในขณะที่วิธีแรก วิวัฒนาการจากระยะที่ 1 และค่อย ๆ เพิ่มขึ้น ระยะหลังเกิดการใช้งานการออกแบบรากฐานของสถาปัตยกรรมในปัจจุบัน

อย่างไรก็ตามทางเลือกที่สามก็ยังมีอยู่ ซึ่งประนีประนอมทั้งสองวิธีที่กล่าวมา วิธีนี้เป็นความคิดใหม่ในวิวัฒนาการ ขณะที่สามารถใช้งานร่วมกันกับที่มีอยู่ ซึ่งสำคัญมากกับผู้ถือผลประโยชน์ร่วม เช่น ผู้ให้บริการ (ISPs) ผู้ซึ่งลงทุนหลายพันล้านในอุปกรณ์ของพวกเขาและต้องการผลกำไรที่เพิ่มขึ้นจากการลงทุน ซึ่งมีแรงบันดาลใจโดยความจริงของปัจจุบันและเครือข่ายในอนาคตและเครือข่ายประยุกต์มีความต้องการที่แตกต่างอย่างมาก นั่นหมายถึงสถาปัตยกรรมเดียวไม่สามารถตอบสนองความต้องการที่แตกต่าง ๆ ไปพร้อม ๆ กันได้

แต่ละสมาคมผู้วิจัยมีจุดสนใจของตัวเองในการออกแบบ น่าเสียดายที่มีแนวโน้มที่จะไม่สนใจลักษณะการบริหารจัดการในใน

อนาคต นักวิจัยบางกลุ่มพิจารณา Simple Network Manage Protocol (SNMP) หรืออินเตอร์เฟตของคำสั่งปัจจุบันที่เหมาะสมสำหรับการจัดการในปัจจุบัน แต่โปรโตคอลการบริหารจัดการนี้ไม่เหมาะสมกับในปัจจุบัน ตัวอย่าง SNMP ทำงานบนสุดของ Data Plane และจากนี้ไปการจัดการโปรโตคอลอาศัยการทำงานที่ถูกต้องของสิ่งสมมุตเพื่อบริหารจัดการ เมื่อไม่นานมานี้มุ่งไปที่ IETF ได้ยอมรับความจริงว่า SNMP และวิธีการที่เกี่ยวข้องก็ล้มเหลวในงานก่อนหน้านี้ ได้สรุปความต้องการด้านการจัดการสำหรับในอนาคตไว้แล้ว

ในการศึกษาครั้งนี้เรามุ่งสนใจอย่างไรก็ตามนี้ไม่ได้เป็นความพยายามด้านเทคนิคเพียงลำพัง สถาปัตยกรรมการจัดการเครือข่ายและลักษณะทางเศรษฐกิจควรจะพิจารณาที่จะพัฒนาเทคโนโลยีการจัดการใหม่ [1]

II. SNMP , CMIP และ NETCONF

SNMP (Simple Network Management Protocol) เป็นส่วนหนึ่งของชุดโปรโตคอล TCP/IP ที่ทำหน้าที่รายงานข้อมูลของอุปกรณ์เครือข่ายผ่านทางโปรโตคอล SNMP มายังระบบบริหารจัดการเครือข่าย (Network Management System) โดยการบริหารจัดการเครือข่ายบนจะกระทำร่วมกับ โปรโตคอล SNMP ซึ่งกำหนดในการอ้างอิง Object กำหนดประเภทของข้อมูลการเข้ารหัสและ MIB-2 จะเก็บ Object กับค่าของตัวแปรที่ Manager สามารถจัดการได้ ส่วนโปรโตคอล CMIP (Common Management Information Protocol) จะดำเนินการร่วมกับ ACSE (Association Control Service Element) ใช้ในการจัดการความสัมพันธ์ระหว่างโปรแกรมการจัดการและสามารถทำงานได้ในระยะเมื่อได้รับการร้องขอจะดำเนินการส่งผลไปยังองค์กร [2][9][11]

2.1 SNMP: Simple Network Management Protocol

เป็นโปรโตคอลที่พัฒนาขึ้นเพื่อจัดการกับโหนด (เซิร์ฟเวอร์, workstations, เราเตอร์, สวิตช์และฮับ ฯลฯ) บนเครือข่าย IP SNMP ทำให้ผู้ดูแลระบบเครือข่ายในการจัดการประสิทธิภาพของเครือข่ายการค้นหาและแก้ปัญหาเครือข่ายและวางแผนสำหรับการเจริญเติบโตของเครือข่าย ระบบการจัดการเรียนรู้เครือข่ายจากปัญหาที่เกิดขึ้นโดยได้รับการดักหรือข้อความแจ้งเตือนเปลี่ยนแปลงจากอุปกรณ์เครือข่ายการดำเนินการของ SNMP

เครือข่ายการจัดการ SNMP ประกอบด้วยสามองค์ประกอบสำคัญ : อุปกรณ์การจัดการ , Agent และระบบเครือข่ายการจัดการ (NMSs) อุปกรณ์การบริหารจัดการเป็นโหนดเครือข่ายที่มีตัวแทน SNMP และที่อยู่บนเครือข่ายการจัดการ อุปกรณ์การจัดการเก็บรวบรวมและจัดเก็บข้อมูลการจัดการและการให้ข้อมูลนี้ใช้ได้กับ NMSs ใช้ SNMP อุปกรณ์การจัดการบางครั้งเรียกว่าองค์ประกอบของเครือข่าย สามารถเป็นเราเตอร์และการเข้าถึงเซิร์ฟเวอร์, สวิทช์และสะพาน, ฮับ, โฮสต์คอมพิวเตอร์หรือเครื่องพิมพ์ [3]

2.2 CMIP: Common Management Information Protocol

CMIP: Common Management information protocol เป็นโปรโตคอลในการจัดการเครือข่ายให้การดำเนินงานสำหรับการบริการที่กำหนดไว้โดย Common Management Information Service(CMIS)ช่วยให้การสื่อสารระหว่างโปรแกรมประยุกต์ในการจัดการเครือข่ายและตัวแทนการจัดการเครือข่ายแบบจำลองการจัดการข้อมูล CMIP ในแง่ของการจัดการวัตถุช่วยให้ปรับเปลี่ยนและดำเนินการเกี่ยวกับการจัดการวัตถุ มีการอธิบายการใช้ GDMO (Guidelines for the Definition of Managed Objects) และมีการระบุโดยใช้ชื่อที่แตกต่าง (DN) นอกจากนี้ CMIP ยังมีการรักษาความปลอดภัยที่ดีสนับสนุนการอนุญาต,การควบคุมการเข้าถึง,และการบันทึกการรักษาความปลอดภัยและการรายงานความยืดหยุ่นของเครือข่ายที่ผิดปกติ CMIP ถูกสร้างขึ้นเพื่อแข่งกับ SNMP และมีคุณสมบัติที่ดีกว่า เช่น SNMP กำหนดชุดการกระทำเพื่อเปลี่ยนสถานะอุปกรณ์ ในขณะที่ CMIP อนุญาตให้กำหนดทุกๆชนิดของการกระทำ อย่างไรก็ตามส่วนใหญ่อุปกรณ์ TCP/IP สนับสนุน SNMP เพราะความซับซ้อนและต้องการทรัพยากรที่มากกว่าของ CMIP. CMIP จึงเหมาะกับอุปกรณ์หลักๆของอุปกรณ์ในการติดต่อสื่อสาร

CMIP เป็นโปรโตคอลมาตรฐานที่ถูกกำหนดขึ้นโดยองค์การ ISO เพื่อใช้งานร่วมกับรูปแบบโปรโตคอลสื่อสารมาตรฐาน OSI โปรโตคอลเป็นคู่แข่งของโปรโตคอล SNMP มีข้อได้เปรียบคือ เป็นโปรโตคอลที่ใหม่กว่าและเป็นส่วนที่บังคับที่ใช้งานสำหรับเครื่องเซิร์ฟเวอร์ และเครื่องผู้ใช้ร่วมกับข้อบังคับอื่น ๆ โปรโตคอล CMIP

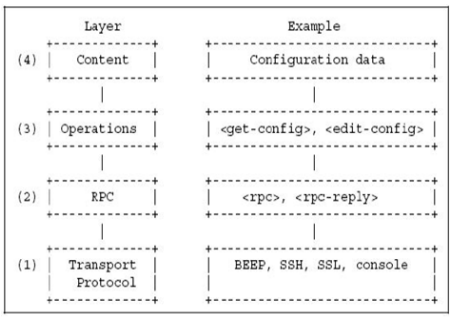
ยังให้ข้อมูลเกี่ยวกับระบบเครือข่ายที่ละเอียดกว่าและได้รับการพัฒนาให้มีความสมบูรณ์มากกว่าเนื่องจากต้องการนำมาใช้งานแทนโปรโตคอล SMNP

โปรโตคอล CMIP ยังมีการรักษาความปลอดภัยได้ดีกว่าเพราะได้รับเงินทุนสนับสนุนการวิจัยจากภาครัฐและเอกชน อย่างไรก็ตามโปรโตคอล มีความซับซ้อนมากจนระบบเครือข่ายส่วนใหญ่ไม่มีช่องสื่อสารที่มีขนาดใหญ่พอที่จะรองรับข้อมูลที่ส่งจากอุปกรณ์ CMIP มายังเซิร์ฟเวอร์ทำให้โปรโตคอลนี้ไม่ได้รับความนิยมในการมาใช้งาน [4]

2.3 NETCONFT: The Network Configuration Protocol

SNMP มีความสำคัญในด้านการจัดการเครือข่ายคอมพิวเตอร์ อย่างไรก็ตามการเติบโตของเครือข่ายในทุก ๆ นาที SMNP ได้ผลน้อยถึงน้อยมาก โดยเฉพาะอย่างยิ่งเมื่อมีการร้องขอการจัดการโครงสร้างมันจะ ทำงานหนัก The Network Configuration Protocol (NETCONFT) กำหนดใน RFC4741 จัดหาการคิดตั้งกลไกลใหม่ ๆ จัดการลบโครงสร้างของอุปกรณ์เครือข่าย NETCONF ใช้ XML-based ในการเปลี่ยนข้อมูลและส่งโครงสร้างข้อมูลถึงโปรโตคอล รักษาตรรกะระหว่างเซิร์ฟเวอร์และเครื่องลูกข่าย ใน NETCONF เซิร์ฟเวอร์ เป็นอุปกรณ์ในเครือข่ายปกติ เครื่องลูกข่ายบางทีเป็นการประยุกต์ใช้และ 2 อย่างนี้สนับสนุนติดต่อโปรโตคอลที่มีอยู่ เช่น BEEP,SSH,SSL และ SOAP [12]

NETCONF เป็นโปรโตคอลในการจัดการการตั้งค่าข้อมูลของอุปกรณ์เครือข่ายถูกออกแบบมาให้ครอบคลุม short-coming ของ Simple Network Management Protocol (SNMP) and Command-Line Interface (CLI) protocol ในฟังก์ชันของการตั้งค่าเครือข่าย NETCONF ให้กลไกในการติดตั้ง, จัดการและการลบ, การกำหนดค่าของอุปกรณ์เครือข่าย สามารถแบ่งแนวคิดออกเป็น 4 ชั้น ดังนี้ [5]



Basic Operation

<get>, <get-config>, <edit-config>, <copy-config>, <delete-config>, <lock>, <unlock>, <close-session>, <kill-session>.

ข้อดี

- เป็นมิตรกับมนุษย์ (Base on XML)
- มีการแจ้งเตือน Notification
- ทำงานแบบ Client-Server

III. Viewpoint of the Network Management Paradigm for Future Internet Networks

มุมมอง การจัดการในอนาคต รูปแบบสถาปัตยกรรมที่พัฒนาโดย **EU IST Autonomic Internet – AUTOI** สมาคมสหภาพยุโรป การออกแบบการจัดการในอนาคต เป็นการบริการเครือข่ายที่รับการค้ำประกัน ในการสร้างความน่าเชื่อถือ ความทนทานและความคล่องตัว ในบริบท, การเข้าถึง การรักษาความปลอดภัย การสนับสนุนการบริการและการจัดการตนเองในกาติดต่อสื่อสาร ทรัพยากรและบริการ การแก้ปัญหาในสถานการณ์อินเทอร์เน็ตในอนาคตและ

อินเตอร์เน็ตในอนาคต จะยึดเป็นเครือข่ายทั่วโลกที่จับความหลากหลายที่ครอบคลุมทั่วทั้งเทคโนโลยีเครือข่าย ความสามารถในอุปกรณ์และความต้องการของผู้ใช้ เครือข่ายที่มีลักษณะแพร่หลายและสนับสนุน อุปกรณ์และการเคลื่อนย้าย ทรัพยากรและการตอบสนองความต้องการของผู้ใช้ที่มีความหลากหลาย การจัดการความซับซ้อนของ อินเตอร์เน็ตในปัจจุบันควรจะลดลงโดยใช้เทคนิคการจัดการอัตโนมัติ ที่ดำเนินการถือปฏิบัติโดยไม่ต้องเสียเวลา กับการทำงานแทรกแซงของคน ตัวอย่างเช่นองค์กรเครือข่ายที่แตกต่างกัน สามารถปฏิบัติตามกฎระเบียบทั่วไปที่กำหนด โดยผู้ดูแลระบบในขณะที่การดำเนินงานการจัดการ ในระดับต่ำสามารถดำเนินการได้ โดยอัตโนมัติในความสอดคล้องกับกฎเหล่านี้

กระบวนทัศน์ในการจัดการเครือข่ายสำหรับอนาคตอินเตอร์เน็ต ความท้าทาย ที่สำคัญมาก :

- การจัดการการเกี่ยวฟังก์ชั่นทำงาน ควรจะฝัง การรู้บริการในเครือข่าย

- การจัดงาน การจัดการตนเองเกี่ยวกับฟังก์ชัน โดยเฉพาะการเพิ่มประสิทธิภาพ ; องค์กร; การกำหนดค่า; การปรับตัว; การรักษา ; การป้องกัน
- ฟังก์ชั่นการควบคุมการจัดการตนเอง โดยการตั้งค่า และเจรจาร่วมกัน / เป้าหมายที่ตกลงกัน
- ความตระหนักและฟังก์ชั่นการตรวจสอบเครือข่ายของตัวเองและบริบทการดำเนินงาน เช่นเดียวกับการเนินงานเครือข่าย เพื่อที่จะ ประเมินว่าเครือข่ายในปัจจุบัน มีพฤติกรรมตอบสนองวัตถุประสงค์ของบริการ
- การปรับตัวและฟังก์ชั่นการปรับตัวเอง เรียก การเปลี่ยนแปลงในดำเนินงานเครือข่าย (state, การตั้งค่าฟังก์ชั่น) ในฟังก์ชันของการเปลี่ยนแปลงในบริบทของเครือข่าย
- ฟังก์ชั่น อัตโนมัติด้วยตนเอง เป็นวิธีการ เปิดใช้งาน การควบคุมโดยตนเอง (คือ Self - FCAPS) ของการดำเนินงานเครือข่ายภายใน
- การเขียนโปรแกรม แบบไดนามิก ของฟังก์ชันการจัดการ & บริการที่ อนุญาตให้เพิ่ม ฟังก์ชั่น ใหม่โดยไม่ต้อง รบกวนสิ่งที่อยู่ของระบบ คือ (UN) Plug และ เล่นฟังก์ชั่น การบริการการจัดการ
- ความเรียบง่ายใน การการจัดการฟังก์ชันเพื่อลดวงจรระบบการดำเนินงาน ค่าใช้จ่ายในและการปล่อย พลังงาน [6]

IV. ความท้าทายของการจัดการเครือข่ายที่เกิดขึ้นอัตโนมัติของในอนาคต

วิวัฒนาการที่มีอยู่ในสถาปัตยกรรมในอนาคตหรือที่ปรากฏในขณะนี้ การออกแบบบอร์ดแบนมีข้อตกลงในวงกว้างว่าจะต้องมีความสามารถในการจัดการเครือข่ายที่มีความสามารถในการจัดการเครือข่ายที่มีประสิทธิภาพและยังค่าใช้จ่ายต่ำ วิธีการจัดการเครือข่ายที่มีอยู่มักจะมีการควบคุมจากส่วนกลาง แต่การประสานงานข้ามโดเมนและการบริหารจัดการค่อนข้างเป็นไปได้ยาก อย่างไรก็ตามธุรกิจและหน่วยงานด้านนี้ เพิ่มขึ้นอย่างรวดเร็ว วิธีการที่มีอยู่แล้วไม่สามารถป้องกันได้และซับซ้อนมากขึ้น ดังนั้นการเชื่อมโยงเครือข่ายที่แตกต่างกัน จึงไม่เหมาะที่จะเปิดกว้างและยังมองไม่เห็นถึงสภาพแวดล้อมที่ยืดหยุ่นสำหรับในอนาคต

เพราะฉะนั้นปัญหาจากการจัดการเครือข่ายระบบศูนย์กลางการ จะต้องค่อยๆ พัฒนาด้านความยืดหยุ่นและต้องปรับมูลค่าเครือข่ายให้เข้ากับในอนาคต วิธีการหนึ่งที่มีแนวโน้มที่เป็นการจัดการเครือข่ายอัตโนมัติ การจัดการเครือข่ายที่มีความยืดหยุ่นสูงกับสัญญา ระบบมีการยอมรับการค้นหาโดยอัตโนมัติ ตอบสนองข้อเสนอที่เหมาะสมหรือทรัพยากรที่ใช้หรือสภาพแวดล้อมที่เปลี่ยนแปลงและควบคุมหรือลดค่าใช้จ่ายที่จะเกิดขึ้น

อย่างไรก็ตามการจัดการโดยอัตโนมัติของงานที่กำหนดภายใต้สภาพแวดล้อมเดียว ปัจจุบันการออกแบบของการดำเนินงานและระบบสนับสนุนธุรกิจ เนื่องจากผู้ประกอบการส่วนใหญ่มีความต้องการที่จะรวมฟังก์ชั่นการทำงานที่ดีที่สุดในการจำลองแบบของในอนาคต ซึ่งผลในการประกอบการไม่สามารถจัดการได้อย่างมีประสิทธิภาพ เนื่องจากความซับซ้อนของระบบธุรกิจและการดำเนินงานที่เพิ่มขึ้น

ความท้าทายที่เราจะระบุมี 6 ทาง เป็นเทคนิคความท้าทายที่จะต้องตระหนักถึงวิสัยทัศน์ในการบริหารจัดการการสื่อสารอัตโนมัติ ทั้งนี้ต้องแน่ใจว่าการจัดการตนเองโดยอัตโนมัติมีการประสานงานข้ามขอบเขตของการจัดการและการตั้งค่าระบบการจัดการ ควรกำหนดทรัพยากรเครือข่ายในเป้าหมายให้สอดคล้องกันทางธุรกิจ การจัดการควรสนับสนุนการจัดส่งแบบ end – to – end ของบริการนั้น ๆ

ซึ่งการจัดการอัตโนมัติเหล่านี้สามารถแบ่งความท้าทายออกเป็น 3 คู่ และคู่การจัดการที่อยู่ในระดับสูงสุดที่เกี่ยวข้องกับสหพันธ์การบริหารจัดการ มีดังนี้

- สหพันธ์หลังการจัดการ
- Mapping ความหมายของสหพันธ์

ความท้ายทายระดับกลาง เกี่ยวข้องกับการตรวจสอบการบริการและการกำหนดค่า มีดังนี้

- การตรวจสอบระดับการบริการแบบ end – to – end
- การกำหนดค่าการขับเคลื่อนธุรกิจเครือข่าย

ความท้าทายระดับล่าง เกี่ยวข้องกับโครงสร้างพื้นฐานของเครือข่ายและการประสานงานการจัดการตนเอง มีดังนี้

- การจัดการตนเองและการนำกลับมาใช้ใหม่
- การประสานการจัดการตนเอง [7]

V. ความปลอดภัย

ความปลอดภัยที่จะกล่าวในที่นี้คือ การเข้ารหัส ซึ่งจะอธิบายดังต่อไปนี้

Conventional Encryption Algorithm

การเข้ารหัสแบบ Block Cipher นั้น มีอัลกอริทึมอยู่หลายตัวที่มีการออกแบบและใช้งานในปัจจุบัน โดยอัลกอริทึมที่มีความสำคัญ และใช้งานมากที่สุด คือ DES (Data Encryption Standard) และ 3DES (Triple Data Encryption Standard) ซึ่งถือว่าเป็นรากฐานของระบบเข้ารหัสที่ใช้ในปัจจุบัน อย่างไรก็ตาม เนื่องจาก DES และ 3DES ได้มีการใช้งานมาระยะหนึ่งแล้ว และเริ่มจะมีความปลอดภัยน้อยลง จึงได้มีความพยายามออกแบบอัลกอริทึมในการเข้ารหัสใหม่ในชื่อ AES (Advanced Encryption Standard)

5.1 Data Encryption Standard

DES เป็นอัลกอริทึมแบบ Block Cipher ที่มีการใช้งานมากที่สุด โดย DES เป็นมาตรฐานของ NIST (National Institute of Standard and Technology) โดยประกาศใช้งานเมื่อปี 1977 โดยใช้ชื่อรหัสว่า FIPSP UB 64 (Federal Information Processing Standard 46) และในปี 1994 ได้ปรับปรุงมาตรฐานเป็น FIPS PUB 46-2 โดยอัลกอริทึมที่ใช้รู้จักกันในชื่อของ DEA (Data Encryption Algorithm)

อัลกอริทึมการทำงานของ DES จะใช้บล็อกข้อมูลขนาด 64 บิต และใช้คีย์ขนาด 56 บิต โดยหากข้อมูลมีขนาดใหญ่กว่า 64 บิต ก็จะแบ่งออกเป็นบล็อกละ 64 บิต

The Strength of DES

ในการพิจารณาถึงความแข็งแกร่งของ DES นั้น เราจะพิจารณากันใน 2 ด้าน คือ ด้านของตัวอัลกอริทึมเอง และด้านความยาวของคีย์ สำหรับเรื่องของอัลกอริทึมนั้น หลังจากที่ DES ได้ประกาศใช้ออกมา ก็ได้มีผู้พยายามจะหาจุดอ่อนของ DES อยู่มาก จนอาจกล่าวได้ว่า DES เป็นอัลกอริทึมการเข้ารหัสที่มีผู้ศึกษาค้นคว้ามากที่สุดในโลกก็ว่าได้ แต่จนถึงบัดนี้ก็ยังไม่มีผู้ที่ค้นหาจุดอ่อนของ DES ได้เลย ดังนั้นจึงอาจถือได้ว่ายังเป็นอัลกอริทึมที่ยังไม่มีจุดอ่อน

แต่จุดที่น่าสนใจมากกว่า คือ ความยาว 56 บิต ของ DES เพียงพอหรือไม่ เนื่องจาก DES เกิดมาในช่วงที่คอมพิวเตอร์ยังไม่มีความเร็วมากนัก แต่หลังจากนั้นก็ได้มีการพัฒนาความสามารถของคอมพิวเตอร์อย่างรวดเร็ว ทำให้ความเป็นไปได้ในการแกะคีย์ขนาด 56 บิตมีความเป็นไปได้มากขึ้น ในปี 1998 มีเหตุการณ์หนึ่งที่ต้องบันทึกไว้ และถือได้ว่าเป็นเหตุการณ์ที่ทำให้อัลกอริทึม DES ถึงจุดจบอย่างเป็นทางการ เหตุการณ์ที่ว่านั้นเกิดจากหน่วยงานหนึ่งที่ชื่อว่า EFF (Electronics Frontier Foundation) ได้สร้างเครื่องคอมพิวเตอร์ขึ้นมาเครื่องหนึ่งเพื่อทำหน้าที่ในการแกะรหัส DES โดยเฉพาะ โดยใช้ชื่อว่า “DES Cracker” โดยใช้เงินทุนไม่ถึง 250,000 เหรียญ โดยสามารถแกะคีย์ขนาด 56 บิตได้ในเวลา 3 วันเท่านั้น ยิ่งไปกว่านั้น EFF ได้เผยแพร่ผลงานของตนเองสู่สาธารณะ ทำให้ทุกคนสามารถสร้างได้

อย่างไรก็ตาม ในการแกะรหัสนั้นจะเริ่มจากการใส่ Cipher text เข้าไปจากนั้นก็ใส่ คีย์ เข้าไปทีละตัวอย่าง ซึ่งจะทำให้เกิดเป็น Plaintext ออกมาแต่ Plaintext จะเป็น Plaintext ที่ถูกต้อง คือ ตรงกับต้นฉบับก็ต่อเมื่อ คีย์ ที่ใส่เข้าไปเป็นคีย์ที่ถูกต้อง คราวนี้จะรู้ได้อย่างไรว่า Plaintext ที่ได้เป็น Plaintext ที่ถูกต้อง ซึ่งหมายถึง คีย์ ที่ถูกต้องด้วย นั่นก็คือ การพิจารณาดูเนื้อความ เช่น หากต้นฉบับเป็นภาษาอังกฤษ Plaintext ที่ถูกต้องก็ต้องเป็นภาษาอังกฤษด้วย ดังนั้นก็จะใช้วิธีดูไปเรื่อย ๆ ว่าหากผลลัพธ์ที่แกะได้ออกมาเป็นภาษาที่อ่านได้ ก็หมายความว่า คีย์ ที่ใช้เป็น คีย์ ที่ถูกต้องแล้ว แต่หากไฟล์ที่เข้ารหัสเป็นไฟล์แบบอื่น เช่น ไฟล์ที่มีตัวเลขอย่างเดียว หรือ ไฟล์ที่ผ่านการบีบข้อมูลมาแล้ว ก็จะยิ่งหา คีย์ ที่ถูกต้องได้ยากยิ่งขึ้น หรืออาจทำไม่ได้เลยก็ได้

5.2 Triple DES

อัลกอริทึม 3DES ได้รับการเสนอครั้งแรกโดย Tuchman โดยเริ่มแรกเป็นมาตรฐานของ ANSI หมายเลข X9.17 ในปี 1985 จากนั้น NIST ได้นำมาเป็นส่วนหนึ่งของมาตรฐานหมายเลข FIPS PUB 46-3 ใน

ปี 1999 โดย 3DES จะใช้อัลกอริทึมเดียวกับ DES แต่จะใช้คีย์จำนวน 3 คีย์และทำ DES จำนวน 3 ครั้ง

ดังนั้นคีย์ทั้งหมดจะมีความยาวเท่ากับ 168 บิต อย่างไรก็ตาม FIPS PUB 46-3 ยอมให้ใช้คีย์เพียง 2 คีย์ คือ กำหนดให้คีย์ K1 เท่ากับ K3 ได้ ดังนั้นความยาวคีย์จะเหลือเท่ากับ 112 บิต กล่าวโดยสรุป 3DES เป็นการปรับปรุง DES ให้มีความปลอดภัยมากขึ้น สามารถใช้งานร่วมกับ DES ได้ อย่างไรก็ตามการทำ DES จำนวน 3 ครั้ง ถือได้ว่ามีความปลอดภัยมากพอสำหรับช่วงเวลาที่จะมีการพัฒนาอัลกอริทึมในการเข้ารหัสตัวต่อไป นั่นก็คือ AES

5.3 Advanced Encryption Standard

แม้ว่า 3DES เป็นอัลกอริทึมที่มีความปลอดภัย เพราะใช้คีย์ที่มีความยาวถึง 168 บิต ทำให้ยากต่อการแกะรหัส และใช้ อัลกอริทึมเดียวกับ DES ซึ่งรู้จักกันทั่วไป ดังนั้นจึงถือว่ามีความปลอดภัยมากที่สุดในปัจจุบัน ซึ่งจนถึงปัจจุบันก็ยังไม่มีใครแกะ3DES ได้สำเร็จ ดังนั้นหากจะพิจารณาในด้านความปลอดภัยเพียงอย่างเดียว 3DES ถือเป็นตัวเลือกที่เหมาะสม แต่เนื่องจากรูปแบบอัลกอริทึมเป็นอัลกอริทึมที่ออกแบบมาให้ง่ายต่อการสร้างด้วยฮาร์ดแวร์มากกว่าซอฟต์แวร์ ประกอบกับการทำ DES ถึง 3 ครั้ง ทำให้การเข้ารหัสข้อมูลจำนวนมาก ๆ มีความล่าช้า อีกประการหนึ่งคือ บล็อกข้อมูลขนาด 64 บิต ถือว่าเล็กเกินไปหน่อยในปัจจุบัน

ด้วยเหตุดังกล่าวในระยะยาว จึงมีความต้องการอัลกอริทึมใหม่ ที่มีความเหมาะสมมากขึ้น โดยในปี 1997 ได้มีการประกาศให้นักพัฒนาเสนออัลกอริทึมเข้ามาให้ NIST พิจารณา โดยได้ตั้งชื่ออัลกอริทึมใหม่นี้ว่า AES ซึ่งมีข้อกำหนดเบื้องต้นว่า จะต้องมีความปลอดภัยอย่างน้อยเท่ากับ 3DES มีการใช้บล็อกข้อมูลขนาด 128 บิต และสามารถใช้ความยาวคีย์ได้ตั้งแต่ 128 บิต 192 บิต และ 256 บิต โดยมีความเร็วในการทำงานที่ดี และใช้หน่วยความจำในการทำงานน้อย โดยในรอบแรกมีผู้เสนอเข้ามา 15 อัลกอริทึม และได้คัดเหลือ 5 อัลกอริทึมในรอบที่ 2 คือ MARS, RC6™, Rijndael, Serpent, Twofish และล่าสุดในเดือนตุลาคม 2543 ที่ผ่านมานี่เอง ทาง NIST ก็ได้ประกาศผู้ชนะ ออกมา

อัลกอริทึม AES ที่ได้รับการตัดสินให้ชนะเลิศนี้ สร้างขึ้นโดย Joan Daemen และ Vincent Rijmen ซึ่งเป็นนักวิจัยชาวเบลเยี่ยม โดยอัลกอริทึมนี้เดิมทีใช้ชื่อว่า Rijndael (Rijmen & Daemen) อัลกอริทึมนี้จะยังคงเป็นแบบ Block Cipher โดยใช้บล็อกข้อมูลขนาด 128 บิต 196 บิต และ 256 บิต โดยสามารถใช้คีย์ได้ยาวถึง 128 บิต 196 บิต และ 256 บิต โดยอัลกอริทึมนี้ได้รับการออกแบบให้มีการทำงานที่เหมาะสมกับโพรเซสเซอร์รุ่นใหม่ ๆ และสามารถใช้งานกับ Smart Card ได้ เพราะใช้หน่วยความจำน้อย

อัลกอริทึม Rijndael จะใช้ฟังก์ชัน Round ที่สามารถเลือกได้ว่าจะทำ 10,12 หรือ 14 ครั้ง โดยมีการทำงานอยู่ 4 การทำงานย่อย คือ Byte Sub ก็คือการใช้ S-Boxes ในการสลับข้อมูลระหว่าง 2 บล็อก ShiftRow คือการสลับข้อมูลระหว่างแถว Mix Column คือการ Shift ข้อมูลในแต่ละ Column และสุดท้ายคือ Key Addition คือการนำมาบวกกับคีย์ ซึ่งการทำงานทั้งหมด เป็นการทำงานที่ง่าย มีจำนวนครั้งของการทำงานน้อย ทำงานได้เร็ว และใช้หน่วยความจำน้อย[9]

ตารางเปรียบเทียบ Network Management Protocol

	SNMP	CMIP	NETCONF
Feature	Manage simple network well	Solution to the problem on overall network and system management	Base on XML , Do not depend on the type of transmission, Include a notification
Managed Object	Object Identifier	Distinguished Name	-
Specification format of managed object	Object-Type notation	GDMO (Guideline of Definition Managed Object) notation	-
Protocol	Connectionless Protocol	Connection-oriented	Connection-Oriented

		Protocol	Protocol
	SNMP	CMIP	NETCONF
Operation	GET, SET,GET-NEXT, TRAP	M-Get, M-Cancel-GET, M-Event-Report, M-Set, M-Action, M-Create, M-Delete	<get>, <get-config>, <edit-config>, <copy-config>, <delete-config>, <lock>, <unlock>, <close-session>, <kill-session>
Security	v1: Easy for an Attacker v2 : weak security v3 : DESC Encryption	Good security	-

VI. สรุปผลการศึกษา

แนวโน้มของเทคโนโลยีโปรโตคอลจะมีการเพิ่มคุณสมบัติทางด้านความปลอดภัยให้มากยิ่งขึ้นโดยการเข้ารหัสข้อความซึ่งจะทำให้เกิดข้อผิดพลาดกับข้อมูลน้อยลงในการรับส่งข้อมูล

ในระบบเครือข่ายเพื่อพัฒนาโปรโตคอลในการจัดการเครือข่ายให้มีประสิทธิภาพมากยิ่งขึ้น จะส่งผลให้การพัฒนาโปรแกรมประยุกต์ที่ใช้ในการควบคุมอุปกรณ์ในเครือข่าย เช่น

เราเตอร์, เซิร์ฟเวอร์ และเครื่องคอมพิวเตอร์ให้สามารถตรวจสอบได้อย่างทันที เพื่อสะดวกในการควบคุม และตรวจสอบอุปกรณ์ภายในเครือข่าย

REFERENCES

[1] Sung-Su Kim, Young J. Won,and and John Strassner ," **Towards Management of the Future Internet**" 2009 IFIP/IEEE Integrated Network Management-Workshops, p 81 – 86,2009.

[2] http://www.javvin.com/protocolSNMP.html สืบค้นวันที่ 10 กันยายน 2554

Du Jiangyi and Niu Yan, "**The Design and**

[3] **Implementation of Multifunction Probe Based on SNMP**", 2009 IITA International Conference on Control, Automation and Systems Engineering, p 434-436, 2005.

[4] http://en.wikipedia.org/wiki/Common_management_interface_protocol สืบค้นวันที่ 10 กันยายน 2554 เรื่อง CIMP

[5] Ji Huang, Bin Zhang, and Yan Li, "**Challenges to the New Network Management Protocol:NETCONF**", First International Workshop on Education Technology and Computer Science, p 832 – 836,2009.

[6] Javier Rubio-Loyola,Joan Serrat and Giannis Koumoutsos, "**A Viewpoint of the Network Management Paradigm for Future Internet Networks**", 2009 IFIP/IEEE Integrated Network Management-Workshops, p 93–100,2009.

[7] Brendan Jenning, Rob Brennan, William Donnelly, Simon N. Foley, Dave Lewis, Declan O'Sullivan, John Streassner, Sven van der Meer, "**Challenges for Federated, Autonomic Network Management in the Future Internet**", 2009 IFIP/IEEE Intl. Symposium on Integrated Network Management – Workshops, p 87 – 92.

[8] http://www.msit.mut.ac.th/member/filemanager/share_file/bon/security/Secret%20Key.doc สืบค้นวันที่ 10 กันยายน 2554 เรื่อง Encryption

[9] http://cpe.rsu.ac.th/students/u501796/nana.pdf สืบค้นวันที่ 10 กันยายน 2554 เรื่อง Network Management

[10] C. Mingardi, G. Nunzi, D. Dudkowski, and M. Brunner, "**Event Handling in Clean – Slate Future Internet Management**", 2009 IFIP/IEEE International Symposium on Integrated Network Management (IM 2009), P 275 – 278.

[11] Jithesh Sathyan and Naveen Unni. "**Defining an Optimized Management Protocol for Next Generation Packet Networks**", in Wireless Pervasive Computing, 2006 1st International Symposium, pp. 1-6 , 2006.

[12] Yaun Chang,Debao Xiao and Limiao Chen, "**Design and Implementation of NETCONF-Base Network Management System**", 2008 Second International Conference of Future Generation Communication and Network,2008,p 256-259.