Survey: Future Internet (September 2011)

Anant Thunyarat, Benyada Siriwallop, Chirapa Somchai, Kanokporn Udompongsuk, Khaengkai Compapong, Nopparat Pathiruk,
Patcharapan Somsrimee, Thipvanee Theingtrong, Utid Jitjong,Wassana Thiwongweang,
Department of Information technology, Faculty of Science, Khonkean University.

บทคัดย่อ—บทความนี้นำเสนอเนื้อหาหลักบางส่วนจากเอกสารสรุปผลการศึกษาวิจัยจากต่างๆ ซึ่งเกี่ยวข้องกับอินเตอร์ในอนาคต เมื่ออินเตอร์เน็ตมีความสำคัญต่อชีวิตผู้คนในโลกมากขึ้นเรื่อยๆเช่นนี้ จึงมีบรรดานักวิชาการผู้เชี่ยวชาญทางด้านเทคโนโลยีจากหลากหลายสถาบันที่มีชื่อเสียงทั่วโลกดำเนินการสำรวจศึกษาวิจัยเพื่อประเมินแนวโน้มและทำนายอนาคตของระบบอินเตอร์เน็ต ทั้งในด้านผลกระทบต่อการออกแบบโครงสร้างสถาปัตยกรรมของอินเตอร์เน็ต และผลกระทบจากอินเตอร์เน็ตต่อบริบทต่างๆในการใช้ชีวิตประจำวันของผู้คนในโลกอนาคต ในปัจจุบันนี้ พบว่า การติดต่อสื่อสารระหว่างคอมพิวเตอร์ ในระบบเครือข่ายอินเตอร์เน็ตควบคู่กับบรอดแบรนด์กลายเป็นพื้นฐานของสังคมยุคใหม่ในหลายๆประเทศ มีโปรแกรมคอมพิวเตอร์ใหม่ๆเกิดขึ้นทุกวัน และบางโปรแกรมได้กลายเป็นส่วนหนึ่งของวัฒนธรรมไปแล้ว เช่นยูทูป (YouTube) และเฟซบุ๊ค (Facebook) มีการใช้งานโปรแกรมคอมพิวเตอร์ต่างๆ อย่างแพร่หลายในทุกระดับ จากการใช้งานระหว่างประเทศ การใช้งานระดับชาติ ระดับเครือข่ายการศึกษา รวมถึงเครือข่ายสำหรับธุรกิจบ้าน รถยนต์ และส่วนบุคคล นอกจากนี้ อินเตอร์เน็ตยังสามารถเคลื่อนที่ได้ด้วยอุปกรณ์เครือข่ายเซลลูล่าซึ่งได้รับการพัฒนาศักยภาพสำหรับเป็นอินเตอร์เน็ตโปรโตคอล (Internet Protocol : IP)

อินเตอร์เน็ตโปรโคอล ซึ่งในขณะนี้มีการใช้งานในผู้ใช้ส่วนบุคคลหลายล้านคนแล้ว และมีแนวโน้มว่าจะสามารถพัฒนาศักยภาพของระบบเครือข่ายให้มีผู้ใช้งานเพิ่มอีกหลายพันล้านคนทั่วโลกในไม่ช้านี้

คำสำคัญ : อินเตอร์เน็ตในอนาคต, การจัดการเครือข่าย, การรักษาความปลอดภัย, สื่อมัลติมีเดียของอินเตอร์เน็ตในอานคต, ไอดี/แอลโอซี (ID/LOC), เราติ้ง (Routing)

I. บทนำ

ในโลกยุคใหม่ที่ไร้พรมแดน ไร้กาลเวลา ไร้เชื้อชาติ และไร้ชนชั้น ผู้คนในโลกยุคใหม่นี้สามารถเดินทางข้ามพรมแดนข้ามกาลเวลา ไปพบปะพูดคุยกับใครก็ได้ ที่ไหนก็ได้ เวลาใดก็ย่อมได้ เพียงแค่ปลายนิ้วสัมผัส อินเตอร์เน็ตสื่อสารมวลชนแขนงหนึ่งซึ่งถือกำเนิดมากว่าสิบปีแล้ว จัดเป็นสื่อดิจิทัลที่ได้รับการพัฒนาขึ้นอย่างต่อเนื่องในช่วงหลายปีที่ผ่านมา จนทุกวันนี้ สื่ออินเตอร์เน็ตกลายเป็นสื่อสารมวลชนหลักที่เข้าถึงกลุ่มเป้าหมายจำนวนมากทั่วทั้งโลก อาทิ เช่น ชุมชนออนไลน์มายสเปซ (www.myspace.com) ซึ่งมีขนาดใหญ่มาก จากข้อมูลเมื่อกลางปี 2007 มีผู้เข้าชมเว็บไซต์แห่งนี้ ประมาณไม่ต่ำกว่าเดือนละ 110 ล้านคน ตัวเลขนี้สูงกว่าจำนวนผู้อ่านหนังสือพิมพ์หรือนิตยสาร แม้แต่ไทม์แมกกาซีน (Time Magazine) นิตยสารยอดนิยมอันดับหนึ่งของสหรัฐอเมริกา ยังมีผู้อ่านเพียงสัปดาห์ละ 3.5 ล้านคนเท่านั้น [1] ผู้คนในยุคนี้จึงจำเป็นต้องมีความรู้เรื่อง

แนวโน้มของอินเตอร์เน็ตในอนาคต เพื่อช่วยลดปัญหาอันเกิดจากการรู้ไม่เท่าทันเทคโนโลยี ซึ่งอาจเป็นประเด็นให้เกิดความเลื่อมล้ำทางสังคม ที่ทำให้ผู้มีความรู้ทางด้านเทคโนโลยีสารสนเทศมากกว่าจะได้เปรียบกว่าและมีโอกาสทางสังคมในบริบทต่างๆมากกว่าผู้มีความรู้น้อยกว่า เพราะในปัจจุบันนี้เกมออนไลน์ เว็บบล็อก เว็บไซต์ไม่ได้เป็นเรื่องที่จำกัดอยู่แต่เฉพาะในกลุ่มวัยรุ่นที่มีเวลาว่างเหลือเฟืออีกต่อไปแล้ว สื่ออินเตอร์เน็ตเหล่านี้ มีกลุ่มเป้าหมายจำนวนมากทั้งชาย หญิง หลากหลายกลุ่มอายุ การงาน อาชีพ และที่อยู่ทางภูมิศาสตร์พบว่ามีผู้ใช้บริการอินเตอร์เน็ตที่อยู่ในพื้นที่ห่างไกลทั่วโลกเพิ่มจำนวนมากขึ้นตลอดเวลา Bob Metcalfe ผู้ค้นพบ 3Com และอีเธอร์เน็ต (Ethernet) ทำนายว่าภายในปี 2020 การใช้งานอินเตอร์เน็ตจะเป็นมากยิ่งกว่าการใช้เพียงเพื่อการสื่อสาร [2]

จะเห็นได้ว่าระบบอินเตอร์เน็ตได้มีการพัฒนาปรับปรุงเปลี่ยนแปลงมาอย่างต่อเนื่อง จนสามารถมีการบริการและโปรแกรมต่างๆที่ยืดหยุ่นในการใช้งานมากขึ้น ทำให้ยุคสมัยนี้เป็นยุคสมัยแห่งการแบ่งปันข้อมูล เนื่องจากมีการออกแบบโครงสร้างสถาปัตยกรรมของระบบการสื่อสารทางอินเตอร์เน็ต (Design and architecture of the Internet) ให้สะดวกต่อการรับส่งข้อมูลต่างๆมากขึ้น เช่น ไคลเอนต์เซิร์ฟเวอร์ (Client-server) [7] เป็นรูปแบบหนึ่งของเครือข่ายแบบเซิร์ฟเวอร์เบส (server-based) โดยจะมีคอมพิวเตอร์หลักเครื่องหนึ่งเป็นเซิร์ฟเวอร์ (server) ซึ่งจะไม่ได้ทำหน้าที่ประมวลผลทั้งหมดให้เครื่องลูกข่าย (client) แต่เซิร์ฟเวอร์ จะทำหน้าที่เสมือนเป็นที่เก็บข้อมูลระยะไกล (Remote disk) และประมวลผลบางอย่างให้กับเครื่องลูกข่ายเท่านั้น เช่นประมวลผลคำสั่งในการดึงข้อมูลจากเซิร์ฟเวอร์ฐานข้อมูล (database server)

เพียร์ทูเพียร์ (peer-to-peer) [8] ซึ่งเทคโนโลยีนี้ช่วยทำให้ผู้ใช้สามารถแลกเปลี่ยนข้อมูลบริการและทรัพยากรอื่นๆในเครื่องคอมพิวเตอร์ ที่อยู่บนเครือข่ายได้สะดวกมากยิ่งขึ้น ดังเช่น Napster, Gnutella และ Free net ซึ่งเป็นโปรแกรมประยุกต์ที่ยอมให้ผู้ใช้อินเตอร์เน็ตค้นหา และแลกเปลี่ยนไฟล์ข้อมูลต่าง ๆ ระหว่างคอมพิวเตอร์ ซึ่งกันและกันได้โดยไม่จำเป็นต้องมีศูนย์กลางคอมพิวเตอร์แม่ข่าย (Central Server) จะต่างจากระบบไคลเอนต์เซิร์ฟเวอร์ซึ่งต้องมีคอมพิวเตอร์แม่ข่ายคอยให้บริการตามคำขอของเครื่องลูกข่ายในการขอข้อมูลบริการและไฟล์ข้อมูล ส่วนใหญ่มักใช้เพียร์ทูเพียร์เพื่อดาวน์โหลดภาพยนตร์และเพลงแบบผิดกฎหมายอย่างไรก็ตามโปรแกรมดังกล่าวมานี้ล้วนถูกออกแบบไว้ ก่อนที่จะมีระบบ LANs แต่โปรแกรมเหล่านี้สามารถใช้งานได้

อย่างสะดวกสบายมากยิ่งขึ้น ในยุคที่มีเครือข่ายเทคโนโลยีก้าวหน้ากว่าดังเช่นปัจจุบันนี้ [6]

อนาคตอันใกล้เซ็นเซอร์ (Sensors) หรืออุปกรณ์รับส่งสัญญาณที่ไวต่อแสงหและอุณหภูมิที่จะถูกเพิ่มเติมในเครือข่าย ซึ่งพัฒนาระบบมาจากเทคโนโลยีอาร์เอฟไอดี (RFID : Radio Frequency Identification) เพื่อเพิ่มศักยภาพในการเป็นอินเตอร์เน็ตในสรรพสิ่งรอบตัวผู้คน (Internet of Things : IOT) โดยอุปกรณ์เครือข่ายส่วนใหญ่ได้จัดเตรียมโปรแกรมสำหรับ e-commerce, e-education, e-health รวมอยู่ในโปรแกรมอินเตอร์เน็ตสำหรับการบริการนี้ด้วย (Internet of Services : IOS) การใช้อินเตอร์เน็ตยังสามารถพัฒนาเพื่อควบคุมการใช้พลังงานการใช้พลังงานให้คุ้มค่าเต็มประสิทธิภาพจะช่วยลดการปลดปล่อยมลพิษซึ่งทำให้เกิดสภาวะเรือนกระจก ดังนั้นการใช้อินเตอร์เน็ตจึงเป็นการช่วยรักษาสิ่งแวดล้อมในทางอ้อมอีกด้วย

ขณะนี้ พบว่ามีความต้องการโปรแกรมคอมพิวเตอร์ใหม่ ๆ ซึ่งทั้งผู้ให้บริการและผู้ใช้ จะเป็นส่วนหนึ่งของระบบเครือข่ายพื้นฐานระหว่างประเทศที่เกี่ยวข้องกันอย่างต่อเนื่อง อาจมีการรับส่งข้อมูลอันมหาศาลในช่วงเวลาเดียวกันผู้สังเกตการณ์บางคนจึงมีคำถามว่าโครงสร้างสถาปัตยกรรมคอมพิวเตอร์ที่สำคัญที่ใช้กันอยู่นั้นมีความทนทานเพียงพอที่จะปรับเปลี่ยนให้เหมาะสมกับความต้องการใหม่ๆของผู้คนเกี่ยวกับการใช้งานอินเตอร์เน็ตในอนาคตหรือไม่ ทั้งยังมีการสนับสนุนให้เร่งพัฒนาระบบการรักษาความปลอดภัยเป็นแนวทางหลักในการพัฒนาโครงสร้างสถาปัตยกรรมคอมพิวเตอร์แบบใหม่

ดังนั้นผู้คนจึงไม่ควรให้ความสำคัญเพียงแต่การพัฒนาด้านเทคโนโลยีเพียงเท่านั้น จำเป็นต้องให้ความรู้แก่ประชาชนให้กว้างขวางยิ่งมีการแลกเปลี่ยนข้อมูลกันมากขึ้นจะช่วยประชาชนให้เกิดความเชื่อมั่นในเทคโนโลยีใหม่ๆ มากกว่าจะเพิ่มความหวาดระแวงในแต่บริบทของการนำเทคโนโลยีไปใช้ การเปิดประเด็นเพื่อการถกเถียงกันถึงคุณลักษณะของเทคโนโลยีระบบอินเตอร์เน็ตในอนาคตต่อสาธารณะชนทั่วไปจะเป็นปัจจัยพื้นฐานอย่างยิ่งสำหรับความสำเร็จในการพัฒนาเทคโนโลยีเพื่อยกระดับคุณภาพชีวิตของผู้คน และในอนาคตอินเตอร์เน็ตอาจสามารถช่วยลดผลกระทบต่อระบบนิเวศวิทยาของมนุษยชาติบนโลกใบนี้ได้อีกทางหนึ่งด้วย [18]

ทำให้อินเตอร์เน็ตสามารถเข้าถึงตัวผู้คนได้แทบทุกหนทุกแห่งโลกจะอยู่ในยุคที่คอมพิวเตอร์แทรกซึมอยู่เกือบทุกอณูในชีวิตและผู้คนจะใช้อินเตอร์เน็ตทำงานแทนหลายต่อหลายอย่างจนบางครั้งเราแทบไม่รู้สึกเลยว่ามีมันอยู่ อินเตอร์เน็ตเหมือนกระแสไฟฟ้าที่เรามองไม่เห็นสัมผัสไม่ได้ตราบที่มันยังทำงานเป็นปกติ จะสังเกตเห็นได้ก็เฉพาะตอนเสียตัวคอมพิวเตอร์เองก็เลือนรางเต็มที เมื่อมันถูกเชื่อมโยงกับอุปกรณ์สื่อสารแบบพกพา เช่นโทรศัพท์มือถือหรือเครื่องเล่นเกมอินเตอร์เน็ตจะแนบสนิทอยู่ในทุกสรรพสิ่งแวดล้อมรอบตัวผู้คนจนแยกกันไม่ออก

II. งานวิจัยที่เกี่ยวข้อง

A. การบริหารจัดการเครือข่าย (Network Management)

ในระบบการทำงานต่าง ๆ นั้นเพื่อที่จะทำให้เกิดประสิทธิภาพในการทำงานจึงต้องมีการควบคุมดูแล การทำงาน และผู้ที่ทำ หน้าที่ในการควบคุมการทำงานในองค์กรก็คือผู้จัดการ (MANAGER) นั่นเอง โดยผู้จัดการจะคอย ทำการสอดส่องดูแล การทำงานของพนักงานในแผนกว่ามีการทำงานเป็นอย่างไ มีข้อบกพร่องตรงไหน ควรจะปรับปรุงส่วนใ เพื่อที่จะให้การทำงาน เป็นไปอย่างมีประสิทธิภาพมากที่สุด

ในระบบเครือข่ายก็เช่นกันโดยเฉพาะระบบเครือข่ายขนาดใหญ่อย่างอินเตอร์เน็ตหากไม่มีการบริหารที่ดีก็จะทำให้การสื่อสารข้อมูลเกิดความผิดพลาดขึ้นได้ ระบบบริหารเครือข่าย (NETWORK MANAGEMENT SYSTEM) จึงเกิดขึ้นมาเพื่อที่จะคอยทำหน้าที่ในการดูแลบริหารระบบเครือข่าย คอยทำการตรวจสอบอุปกรณ์ต่าง ๆ ที่ทำงานอยู่ภายในระบบเครือข่ายว่ามีการทำงานได้ถูกต้องหรือไม่และหากมีข้อผิดพลาดเกิดขึ้นที่ส่วนใดก็ต้องคอยทำการแก้ไขให้มันสามารถทำงานได้หรือหาทางแก้ปัญหาเฉพาะหน้า เพื่อที่จะให้สามารถที่จะทำการสื่อสารได้อย่างต่อเนื่อง [1]

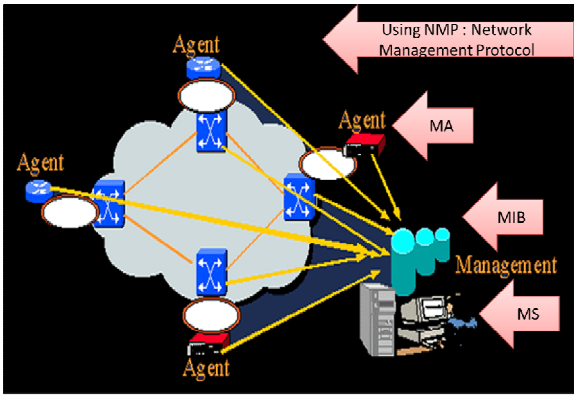
องค์ประกอบต่าง ๆ ภายในระบบบริหารเครือข่าย มีดังนี้

1) MANAGEMENT STATION (MS) จะทำหน้าที่เป็นสถานีส่วนกลาง ในการที่จะตรวจ สอบ สภาพของระบบ

2) MANAGEMENT AGENT (MA) เป็นซอฟแวร์ที่คอยเก็บข้อมูลและรายงานข้อผิดพลาด ในระบบให้แก่ MS

3) MANAGEMENT INFORMATION BASE (MIB) เป็นโครงสร้างของข้อมูลที่เก็บไว้

4) NETWORK MANAGEMENT PROTOCOL (NMP) เป็นโปรโตคอลที่ใช้ ในการสื่อสาร ภายใน ระบบ SNMP และ CMIP



รูปที่ 1 แสดงองค์ประกอบระบบบริหารเครือข่าย

SNMP: Simple Network Management Protocol

เป็นโปรโตคอลที่พัฒนาขึ้นเพื่อจัดการกับโหนด (เซิร์ฟเวอร์, เวิร์คสเตชั่น (Workstations), เราเตอร์, สวิตช์และฮับ ฯลฯ) บนเครือข่ายไอพี SNMP ทำให้ผู้ดูแลระบบเครือข่ายในการจัดการประสิทธิภาพของเครือข่ายการค้นหาและแก้ปัญหาเครือข่ายและวางแผนสำหรับการเจริญเติบโตของเครือข่าย ระบบการจัดการเรียนรู้เครือข่ายจากปัญหาที่เกิดขึ้นโดยได้รับการดักหรือข้อความแจ้งเตือนเปลี่ยนแปลงจากอุปกรณ์เครือข่ายการดำเนินการของ SNMP

เครือข่ายการจัดการ SNMP ประกอบด้วยสามองค์ประกอบสำคัญ : อุปกรณ์การจัดการ, ตัวแทน (Agent) และระบบเครือข่ายการจัดการ NMSs อุปกรณ์การ

บริหารจัดการเป็นโหนดเครือข่ายที่มีตัวแทน SNMP และที่อยู่บนเครือข่ายการจัดการอุปกรณ์การจัดการเก็บรวบรวมและจัดเก็บข้อมูลการจัดการและการให้ข้อมูลนี้ใช้ได้กับ NMSs ใช้ SNMP อุปกรณ์การจัดการบางครั้งเรียกว่าองค์ประกอบของเครือข่าย สามารถเป็นเราเตอร์และการเข้าถึงเซิร์ฟเวอร์, สวิตช์, บริดจ์, ฮับและโฮสต์คอมพิวเตอร์หรือเครื่องพิมพ์ [2]

CMIP: Common Management Information Protocol

CMIP: Common Management information protocol เป็นโปรโตคอลในการจัดการเครือข่ายให้การดำเนินงานสำหรับการบริการที่กำหนดไว้โดยซีเอ็มไอพี (Common Management Information Service : CMIS) ช่วยให้การสื่อสารระหว่างโปรแกรมประยุกต์ในการจัดการเครือข่ายและตัวแทนการจัดการเครือข่ายแบบจำลองการจัดการข้อมูลซีเอ็มไอพีในแง่ของการจัดการวัตถุช่วยให้ปรับเปลี่ยนและดำเนินการเกี่ยวกับการจัดการวัตถุ มีการอธิบายการใช้ GDMO (Guidelines for the Definition of Managed Objects) และมีการระบุโดยใช้ชื่อที่แตกต่าง (DN) นอกจากนี้ซีเอ็มไอพียังมีการรักษาความปลอดภัยที่ดีสนับสนุนการอนุญาต,การควบคุมการเข้าถึง,และการบันทึกการรักษาความปลอดภัยและการรายงานความยืดหยุ่นของเครือข่ายที่ผิดปกติซีเอ็มไอพีถูกสร้างขึ้นเพื่อแข่งกับ SNMP และมีคุณสมบัติที่ดีกว่า เช่น SNMP กำหนดชุดการกระทำเพื่อเปลี่ยนสถานะอุปกรณ์ ในขณะที่ซีเอ็มไอพีอนุญาตให้กำหนดทุกๆชนิดของการกระทำอย่างไรก็ตามส่วนใหญ่อุปกรณ์ทีซีพี/ไอพี (TCP/IP) สนับสนุน SNMP เพราะความซับซ้อนและต้องการทรัพยากรที่มากกว่าของซีเอ็มไอพี ซีเอ็มไอพีจึงเหมาะกับอุปกรณ์หลักๆของอุปกรณ์ในการติดต่อสื่อสาร

ซีเอ็มไอพีเป็นโปรโตคอลมาตรฐานที่ถูกกำหนดขึ้นโดยองค์การ ISO เพื่อใช้งานร่วมกับรูปแบบโปรโตคอลสื่อสารมาตรฐาน OSI โปรโตคอลเป็นคู่แข่งของโปรโตคอล SNMP มีข้อได้เปรียบคือ เป็นโปรโตคอลที่ใหม่กว่าและเป็นส่วนที่บังคับที่ใช้งานสำหรับเครื่องเซิร์ฟเวอร์ และเครื่องผู้ใช้ร่วมกับข้อบังคับอื่น ๆ โปรโตคอลซีเอ็มไอพียังให้ข้อมูลเกี่ยวกับระบบเครือข่ายที่ละเอียดกว่าและได้รับการพัฒนาให้มีความสมบูรณ์มากกว่าเนื่องจากต้องการนำมาใช้งานแทนโปรโตคอล SMNP

โปรโตคอลซีเอ็มไอพียังมีการรักษาความปลอดภัยได้ดีกว่าเพราะได้รับเงินทุนสนับสนุนการวิจัยจากภาครัฐและเอกชน อย่างไรก็ตามโปรโตคอลมีความซับซ้อนมากจนระบบเครือข่ายส่วนใหญ่ไม่มีช่องสื่อสารที่มีขนาดใหญ่พอที่จะรองรับข้อมูลที่ส่งจากอุปกรณ์ซีเอ็มไอพีมายังเซิร์ฟเวอร์ทำให้โปรโตคอลนี้ไม่ได้รับความนิยมในการมาใช้งาน [7]

NETCONFT: The Network Configuration Protocol

SNMP มีความสำคัญในด้านการจัดการเครือข่ายคอมพิวเตอร์ อย่างไรก็ตามการเติบโตของเครือข่ายในทุก ๆ นาที SMNP ได้ผลน้อยถึงน้อยมาก โดยเฉพาะอย่างยิ่งเมื่อมีการร้องขอการจัดการโครงสร้างมันจะทำงานหนัก (The Network Configuration Protocol :NETCONFT) กำหนดใน RFC4741 จัดหาการคิดตั้งกลไกลใหม่ ๆ จัดการลบโครงสร้างของอุปกรณ์เครือข่าย NETCONF ใช้ XML-based ในการเปลี่ยนข้อมูลและส่งโครงสร้างข้อมูลถึงโปรโตคอลรักษาตรรกะระหว่างเซิร์ฟเวอร์และเครื่องลูกข่ายใน NETCONF เซิร์ฟเวอร์ เป็นอุปกรณ์ในเครือข่ายปกติ เครื่องลูกข่ายบางทีเป็นการประยุกต์ใช้และ 2 อย่างนี้สนับสนุนติดต่อโปรโตคอลที่มีอยู่ เช่น BEEP,SSH,SSL และ SOAP

NETCONF เป็นโปรโตคอลในการจัดการการตั้งค่าข้อมูลของอุปกรณ์เครือข่ายถูกออกแบบมาให้ครอบคลุม short-coming ของ Simple Network Management Protocol (SNMP) and Command-Line Interface (CLI) protocol ในฟังก์ชันของการตั้งค่าเครือข่าย NETCONF ให้กลไกในการติดตั้ง, จัดการและการลบ, การกำหนดค่าของอุปกรณ์เครือข่าย สามารถแบ่งแนวคิดออกเป็น 4 ชั้น [3],[10]

ข้อดี

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

XMLP

XMLP เป็นโปรโตคอลขนาดเล็กซึ่งถูกกำหนดโดย W3C และใช้สำหรับแลกเปลี่ยนโครงสร้างการจัดการข้อมูลในสภาพแวดล้อมการกระจาย. ข้อได้เปรียบของ XMLP คือ :

1. ใช้ XML เป็นโปรโตคอลพื้นฐาน ซึ่งทำให้เป็นประโยชน์อย่างง่ายดายสำหรับตัวแปลง และการพัฒนาอื่นและการดำเนินงานชุดเครื่องมือ
2. การจัดการข้อมูลที่กำหนดไว้ค่อนข้างง่าย ยืดหยุ่นและมีประสิทธิภาพ
3. ความเป็นอิสระภายใต้โปรโตคอลที่ใช้ในการขนส่ง หนึ่งในความสำคัญของ XMLP WG เพื่อให้มั่นใจในความเป็นอิสระของโปรโตคอล XMLP ให้ข้อความที่สามารถแลกเปลี่ยนที่หลากหลายของโปรโตคอลพื้นฐานนี้จะทำให้ขยายสถานการณ์ที่โปรโตคอลในการขนส่งอาจจะเป็นที่ต้องการ
4. นับตั้งแต่ถูกออกแบบสำหรับสภาพแวดล้อมที่กระจาย มีกลไกสำหรับการใช้งานที่เกี่ยวกับการอ่านข้อมูลพร้อม ๆ กัน การเขียนข้อมูลหลาย ๆ คนและหน่วยงานควบคุม
5. การเชื่อมโยงระหว่างวัตถุที่มีความยืดหยุ่นของการบริหารจัดการวัตถุและการประยุกต์ใช้การจัดการเป็นอีกหนึ่งคุณลักษณะตามธรรมชาติของการกระจายของโปรโตคอล
6. มีการรักษาความปลอดภัยที่แข็งแกร่งในชุดโปรโตคอลที่มีความสามารถในการตรวจสอบโดยอัตโนมัติและการตรวจสอบส่วนกลาง

XMLP มีวัตถุประสงค์เพื่อเป็นรากฐานโปรโตคอล ความหมายของมันควรจะยังคงอยู่และเรียบง่าย มีเสถียรภาพในช่วงเวลา ที่ชัดเจนในการใช้ modularity และชั้นในการออกแบบที่เป็นผลลัพธ์จะช่วยรับประกันในระยะยาวเฟรมเวิร์ค (Framework) ดังกล่าวจะช่วยให้ขยายในการออกแบบในขณะที่ออกจากการออกแบบที่สมบูรณ์ [6],[9]

โดยเนื้อแท้ของ XMLP สนับสนุนดังต่อไปนี้

- ร้องขอการเข้ารหัสทั้งหมด รวมทั้งส่วนหัวของข้อความและทั้งหมด
- ส่วนที่ 3 ของการทำงาน การสื่อสารผ่านตัวกลางที่หลากหลาย

- การส่งข้อความแบบไม่เป็นจังหวะและแคชที่มีการกำหนดการหมดอายุ
- ส่งข้อมูลที่ไม่ใช่ XML ซึ่งอาจต้องใช้ในสถานการณ์แบบดั้งเดิมที่เฉพาะเจาะจง
- การตั้งค่าโปรโตคอล XMLP ประกอบด้วย 2 องค์ประกอบ

Viewpoint of the Network Management Paradigm for Future Internet Networks

มุมมอง การจัดการในอนาคต รูปแบบสถาปัตยกรรมที่พัฒนาโดยสมาคมสหภาพยุโรป **(EU IST Autonomic Internet : AUTOI)** การออกแบบการจัดการในอนาคต เป็นการบริการเครือข่ายที่รับการค้ำประกัน ในการสร้างความน่าเชื่อถือ ความทนทานและความคล่องตัว ในบริบทการเข้าถึง การรักษาความปลอดภัย การสนับสนุนการบริการและการจัดการตนเองในกาติดต่อสื่อสาร ทรัพยากรและบริการ การแก้ปัญหาในสถานการณ์อินเทอร์เน็ตในอนาคตและ

อินเตอร์เน็ตในอนาคตจะยึดเป็นเครือข่ายทั่วโลกที่จับความหลากหลายที่ครอบคลุมทั่วทั้งเทคโนโลยีเครือข่ายความสามารถในอุปกรณ์และความต้องการของผู้ใช้ เครือข่ายที่มีลักษณะแพร่หลายและสนับสนุนอุปกรณ์และการเคลื่อนย้ายทรัพยากรและการตอบสนองความต้องการของผู้ใช้ที่มีความหลากหลาย การจัดการความซับซ้อนของ อินเตอร์เน็ตในปัจจุบันควรจะลดลงโดยใช้เทคนิคการจัดการอัตโนมัติ ที่ดำเนินการถือปฏิบัติโดยไม่ต้องเสียเวลา กับการทำงานแทรกแซงของคน ตัวอย่างเช่นองค์กรเครือข่ายที่แตกต่างกัน สามารถปฏิบัติตามกฎระเบียบทั่วไปที่กำหนด โดยผู้ดูแลระบบในขณะที่การดำเนินงานการจัดการในระดับต่ำสามารถดำเนินการได้โดยอัตโนมัติในความสอดคล้องกับกฎเหล่านี้ [4]

กระบวนทัศน์ในการจัดการเครือข่ายสำหรับอนาคตอินเตอร์เน็ตความท้าทายที่สำคัญมาก :

- การจัดการการเกี่ยวฟังก์ชั่นทำงาน ควรจะฝังการรู้บริการในเครือข่าย
- การจัดงาน การจัดการตนเองเกี่ยวกับฟังก์ชัน โดยเฉพาะการเพิ่มประสิทธิภาพ ; องค์กร; การกำหนดค่า; การปรับตัว; การรักษา ; การป้องกัน
- ฟังก์ชั่นการควบคุมการจัดการตนเอง โดยการตั้งค่า และเจรจาร่วมกัน / เป้าหมายที่ตกลงกัน
- ความตระหนักและฟังก์ชั่นการตรวจสอบเครือข่ายของตัวเองและบริบทการดำเนินงาน เช่นเดียวกับการเนินงานเครือข่าย เพื่อที่จะประเมินว่าเครือข่ายในปัจจุบันมีพฤติกรรมตอบสนองวัตถุประสงค์ของบริการ
- การปรับตัวและฟังก์ชั่นการปรับตัวเองเรียกการเปลี่ยนแปลงในดำเนินงานเครือข่าย (การตั้งค่า ฟังก์ชั่น) ในฟังก์ชันของการเปลี่ยนแปลงในบริบทของเครือข่าย
- ฟังก์ชั่น อัตโนมัติด้วยตนเอง เป็นวิธีการเปิดใช้งาน การควบคุมโดยตนเองในการดำเนินงานเครือข่ายภายใน
- การเขียนโปรแกรม แบบไดนามิก ของฟังก์ชันการจัดการและการบริการที่อนุญาตให้เพิ่มฟังก์ชั่นใหม่โดยไม่ต้องรบกวนสิ่งที่อยู่ของระบบ คือ (UN) Plug และ เล่นฟังก์ชั่นการบริการการจัดการความเรียบง่ายในการการจัดการฟังก์ชันเพื่อลดวงจรระบบการดำเนินงาน ค่าใช้จ่ายในและการปล่อย พลังงาน

ความท้าทายของการจัดการเครือข่ายที่เกิดขึ้นอัตโนมัติของในอนาคต

วิวัฒนาการที่มีอยู่ในสถาปัตยกรรมในอนาคตหรือที่ปรากฏในขณะนี้การออกแบบบรอดแบนด์มีข้อตกลงในวงกว้างว่าจะต้องมีความสามารถในการจัดการเครือข่ายที่มีความสามารถในการจัดการเครือข่ายที่มีประสิทธิภาพและยังค่าใช้จ่ายต่ำวิธีการจัดการเครือข่ายที่มีอยู่มักจะมีการควบคุมจากส่วนกลาง แต่การประสานงานข้ามโดเมนและการบริหารจัดการค่อนข้างเป็นไปได้ยาก อย่างไรก็ตามธุรกิจและหน่วยงานด้านนี้ เพิ่มขึ้นอย่างรวดเร็ว วิธีการที่มีอยู่แล้วไม่สามารถป้องกันได้และซับซ้อนมากขึ้น ดังนั้นการเชื่อมโยงเครือข่ายที่แตกต่างกัน จึงไม่เหมาะที่จะเปิดกว้างและยังมองไม่เห็นถึงสภาพแวดล้อมที่ยืดหยุ่นสำหรับในอนาคต

เพราะฉะนั้นปัญหาจากการจัดการเครือข่ายระบบศูนย์กลางการ จะต้องค่อยๆ พัฒนาด้านความยืดหยุ่นและต้องปรับมูลค่าเครือข่ายให้เข้ากับในอนาคต วิธีการหนึ่งที่มีแนวโน้มที่เป็นการจัดการเครือข่ายอัตโนมัติ การจัดการเครือข่ายที่มีความยืดหยุ่นสูงกับสัญญา ระบบมีการยอมรับการค้นหาโดยอัตโนมัติตอบสนองข้อเสนอที่เหมาะสมหรือทรัพยากรที่ใช้หรือสภาพแวดล้อมที่เปลี่ยนแปลงและควบคุมหรือลดค่าใช้จ่ายที่จะเกิดขึ้น

อย่างไรก็ตามการจัดการโดยอัตโนมัติของงานที่กำหนดภายใต้สภาพแวดล้อมเดียว ปัจจุบันการออกแบบของการดำเนินงานและระบบสนับสนุนธุรกิจ เนื่องจากผู้ประกอบการส่วนใหญ่มีความต้องการที่จะรวมฟังก์ชั่นการทำงานที่ดีที่สุดในการจำลองแบบของในอนาคต ซึ่งผลในการประกอบการไม่สามารถจัดการได้อย่างมีประสิทธิภาพ เนื่องจากความซับซ้อนของระบบธุรกิจและการดำเนินงานที่เพิ่มขึ้น

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

ซึ่งการจัดการอัตโนมัติเหล่านี้สามารถแบ่งความท้าทายออกเป็น 3 คู่ และคู่การจัดการที่อยู่ในระดับสูงสุดที่เกี่ยวข้องกับสหพันธ์การบริหารจัดการ มีดังนี้ [5],[8]

- สหพันธ์หลังการจัดการ
- การแมปปิ้ง (Mapping) ความหมายของสหพันธ์

ความท้ายทายระดับกลาง เกี่ยวข้องกับการตรวจสอบการบริการและการกำหนดค่า มีดังนี้

- การตรวจสอบระดับการบริการแบบ end – to – end

- การกำหนดค่าการขับเคลื่อนธุรกิจเครือข่าย

ความท้าทายระดับล่าง เกี่ยวข้องกับโครงสร้างพื้นฐานของเครือข่ายและการประสานงานการจัดการตนเอง มีดังนี้

- การจัดการตนเองและการนำกลับมาใช้ใหม่
- การประสานการจัดการตนเอง

B. มัลติมีเดีย (Multimedia)

เนื่องจากเครือข่ายอินเทอร์เน็ตได้ขยายกว้างขวางออกไปอย่างรวดเร็ว โครงสร้างพื้นฐานทางด้านระบบสื่อสารโทรคมนาคมจึงต้องพัฒนาให้สามารถรองรับได้อย่างเหมะสมกับปริมาณการใช้ข้อมูลข่าวสาร

การประยุกต์ใช้งานอินเทอร์เน็ตได้รับการพัฒนาอย่างต่อเนื่อง มีการประยุกต์ใหม่ๆ เกิดขึ้นอยู่เสมอ เริ่มแรกจากการรับส่งข้อมูลข่าวสารด้วยตัวหนังสือ ต่อมาจึงมีการพัฒนาให้ใช้ข้อความและรูปภาพกราฟิก เมื่อระดับความสามารถของระบบคอมพิวเตอร์ดีขึ้น คือ สามารถประมวลผล รูปภาพ เสียง ภาพเคลื่อนไหว และวิดีโอได้เป็นอย่างดี ไมโครคอมพิวเตอร์ในปัจจุบันจึงเป็นเครื่องคอมพิวเตอร์ที่ทำงานกับสื่อประสมได้หลายสื่อ เราเรียกสื่อประสมหลายสื่อนี้ว่า มัลติมีเดีย

หากพิจารณาที่เครื่องคอมพิวเตอร์แบบมัลติมีเดียจะพบว่า คอมพิวเตอร์มีระดับความสามารถของซีพียูที่คำนวณได้รวดเร็วมากขึ้น มีหน่วยความจำซึ่งเก็บข้อมูลได้มาก รวมถึงหน่วยเก็บข้อมูลสำรอง เช่น ฮาร์ดดิสก์ และซีดีรอมที่มีความจุเพิ่มขึ้น การแสดงผลก็ได้ภาพที่ละเอียดและมีจำนวนสีมากขึ้นกว่าเดิม ด้วยเหตุนี้การประยุกต์ใช้งานอินเทอร์เน็ตจึงได้รับการพัฒนา เพื่อให้ใช้งานบนระบบเวิลด์ไวด์เว็บที่เก็บข้อมูลข่าวสารในรูปแบบมัลติมีเดีย คือ มีการเก็บภาพเสียงและข้อมูลแบบวิดีโอ ผู้ใช้สามารถเรียกภาพและวิดีโอเหล่านี้มาแสดงผลบนเครื่องของตนเองได้

การประยุกต์แบบมัลติมีเดียบนอินเทอร์เน็ตมีมากมาย ตั้งแต่การใช้ในระบบสื่อสารระหว่างกัน เช่น การส่งข้อความและเสียงในรูปแบบเมล์เสียง (Voice mail) การโต้ตอบพูดคุยผ่านอินเทอร์เน็ตที่เรียกว่า อินเทอร์เน็ตโฟน การประชุมบนเครือข่ายอินเทอร์เน็ต (Net Meeting) การประยุกต์ในเรื่องการกระจายสัญญาณบนเครือข่าย เช่น การตั้งสถานีวิทยุ สถานีโทรทัศน์ และกำลังพัฒนาเป็นเว็บทีวี กล่าวคือ สามารถส่งทีวีไปบนเครือข่าย โดยผู้ชมได้บราวเซอร์เรียกชมได้

อินเตอร์เน็ตอนาคต สามารถที่จะส่งมัลติมีเดียแพ็คเกจในบนเครือข่ายแบบเดี่ยวได้และจะมีการตรวจสอบข้อผิดพลาดได้ในเครือข่าย ซึ่งสามารถที่จะทำการ balance traffic load ได้บนเครือข่ายขนาดใหญ่เป็นบรอดแบรนด์สวิตช์ซึ่งเราเตอร์ มีการออกแบบสำหรับการเชื่อมต่อของมัลติมีเดียจะเป็นการเชื่อมต่อแบบการกำหนดการเชื่อมต่อ (Connection Oriented) การเชื่อมต่อนั้นจะเป็นในลักษณะแบบเครือข่ายขนาดใหญ่ ซึ่ง MPEG2 และ MPEG4 และจะมีการนำเทคโนโลยี VRML virtual มาหาค่าเฉลี่ยของแพ็คเกจบนอินเตอร์เนตที่เดินทางไปถึงยังปลายทาง โดยที่มีเราเตอร์ค้นหาเส้นทางที่ดีที่สุดด้วยเราเตอร์จะเป็นเทคโนโลยีใหม่ที่ต้องการความเชื่อมั่นในการให้บริการด้วยคุณภาพของการให้บริการ (Quality of Service : QoS)

บนอินเตอร์เน็ตจะมีความแตกต่างกันของแต่ละเครือข่ายจะมีอุปกรณ์ในการค้นเส้นทาง 2 อย่าง คือเอทีเอ็มสวิตช์จะเชื่อมต่อแบบการกำหนดการเชื่อมต่อสวิตช์และการเชื่อมต่อแบบไม่มีการเชื่อมต่อ (connectionless) จะเป็นเราเตอร์ การเชื่อมต่อกำหนดการเชื่อมต่อสวิตช์จะรับรองแบนด์วิดธ์ได้และมีระยะเวลาการส่งที่สั้นเพราะจะมีการค้นหาเส้นทาง การเชื่อมต่อจะเป็นในลักษณะกำหนดการเชื่อมต่อสวิตช์ เช่น สามารถที่จะส่งแบบแพ็คเกจมัลติมีเดียเบส (multimedia-based packets) ซึ่งการวิเคราะห์ประสิทธิภาพของเครือข่ายจะมีการแบ่งเป็น 4 ส่วนคือ input queuing, dedicated internal queuing, shared internal queueing และ output queueing ทั้งนี้ในเครือข่ายของเอทีเอ็มสวิตช์ไม่มีการบล็อคเครือข่ายจากเครือข่ายภายในสถาปัตยกรรมการกำหนดการเชื่อมต่อสวิตช์และแบบไม่มีการเชื่อมต่อ ทั้งสองแบบนี้จะมีความแตกต่างกันบรอดแบรนด์ในอนาคตจะมีทั้งแบบมีการเชื่อมต่อและไม่มีการเชื่อมต่อในการวิเคราะห์ประสิทธิภาพจะวิเคราะห์ได้ดังนี้

1) ความแตกต่างด้านเวลา

2) ความสำเร็จที่ส่งแพ็คเกจถึงปลายทางจะมีความแตกต่างด้านสถาปัตยกรรม เป็นการจำลองโครงสร้างของเครือและบริการต่างๆ ที่ใช้ควบคุมเครือข่าย VINI จะทำงานอยู่เป็นเครื่องมือช่วยในด้านประสิทธิภาพและมีการออกแบบมาให้ควบคุมเครือข่ายให้มีประสิทธิภาพ ทั้งยังควบคุมโปรโตคอล การวัดประสิทธิภาพจะเป็นในลักษณะของ end – to –end โดยจะมีการแบ่งเป็นซับเน็ตในการใช้เครื่องมือยังการควบคุมการทำงานของเราเตอร์รวมไปถึงดูแลแพ็คเกจในการรับส่งเป็นการวัดประสิทธิภาพของเครือข่ายผ่านตัวแบบในเครือข่ายไอพีจะมีการออกแบบมาให้ควบคุมกับควบคุมดูแลเครือข่ายและยังควบคุมรวมถึงโปรโตคอลโดยที่จะแบ่งไอพีเป็นระดับซึ่ง NIST จะเป็นตัวแบบโดยจะมีการส่งข้อมูลแบบ end-to-end พร้อมทั้งวัดประสิทธิภาพของเครือข่าย เช่น มีการสูญเสียมากหรือน้อย ช้าหรือเร็วเป็นสถาปัตยกรรมในการจำกัดการค้นหาเส้นทางของเราเตอร์ที่ทำการส่งแพ็คเกจไปยังเครือข่ายโดยที่เราเตอร์จะมีการตั้งค่าของเครือข่าย

C. การรักษาความปลอดภัย (Security)

ระบบคอมพิวเตอร์ส่วนใหญ่ในอินเตอร์เน็ตที่ทำหน้าที่เป็นตัวให้บริการข้อมูล การรักษาความปลอดภัยเป็นความกังวลหลักสำหรับผู้ใช้อินเตอร์เน็ตและผู้ดูแลระบบ ไม่ว่าจะการป้องข้อมูลที่เป็นความลับและข้อมูลในแต่ละไฟล์ การล็อคระบบคอมพิวเตอร์ให้กับผู้ใช้ที่ไม่ได้รับอนุญาตให้ควบคุมการเข้าถึงอินทราเน็ตหรือเอ็กซ์ทราเน็ตหรือการดำเนินธุรกิจบนอินเตอร์เน็ตที่จะกำหนดเป็นระดับที่เหมาะสมของความปลอดภัยและประสิทธิภาพทางด้านความปลอดภัยของเครือข่ายที่มีประสิทธิภาพเพื่อให้บรรลุวัตถุประสงค์ต่อภัยคุกคามความปลอดภัยของอินเตอร์เน็ตเป็นหนึ่งในอุปสรรคหลักวิกฤตการศักยภาพเป็นที่มุ่งเน้นการประยุกต์ใช้อินเตอร์เน็ตในประเทศและแม้กระทั่งในโลกในอนาคต การวิเคราะห์ความเสี่ยงด้านความปลอดภัยของอินเตอร์เน็ต และหนึ่งในปัญหาที่สำคัญที่สุดเกี่ยวกับอินเตอร์เน็ตในปัจจุบันคือการขาดการรักษาความปลอดภัยที่รัดกุม ก่อให้เกิดปัญหามากมายและมีวิธีการแก้ไขที่แตกต่างกันซึ่งในการรักษาความลับและความซื่อสัตย์ของข้อมูลจะถูกบุกรุก ดังนั้นเมื่อการออกแบบ

อินเตอร์เน็ตในอนาคตก็เป็นที่ชัดเจนว่าการรักษาความปลอดภัยจะต้องมีการพิจารณาการออกแบบเป็นสิ่งแรก เพื่อให้สามารถออกแบบการรักษาความปลอดภัยสำหรับอินเตอร์เน็ตในอนาคตนั้นจำเป็นต้องทำความเข้าใจอย่างละเอียดถึงการคุกคามของศัตรูว่าระบบจะต้องป้องกันอะไร การแนะนำจำนวนของภัยคุกคามใหม่ ๆ การรักษาความปลอดภัยที่จำเป็น

Addressing Security Issues in the Autonomic Future Internet [13] จากงานวิจัยนี้เราได้นำเสนอเรื่องความมั่นคงปลอดภัยข้อมูลกลายเป็นเรื่องสำคัญสำหรับการบริหารจัดการระบบสารสนเทศที่ดีและมีประสิทธิภาพ ระบบสารสนเทศที่มีความเสถียรภาพสูงควรสามารถป้องกันการโจมตีจากแฮกเกอร์หรือมัลแวร์ต่างๆ ได้เป็นอย่างดี วัตถุประสงค์หลักขององค์กรก็คือการรักษาความลับ,การรักษาความสมบูรณ์,ความพร้อมใช้งาน (CIA : Confidentiality, Integrity และ Availability) ให้กับระบบสารสนเทศขององค์กร ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และ การทำให้ระบบมีความมั่นคงและมีเสถียรภาพในการให้บริการอย่างต่อเนื่อง (Availability)

ดังนั้นในงานวิจัยนี้จะมีความเกี่ยวข้องกับเรื่องการบริหารจัดการระบบความมั่นคงปลอดภัยข้อมูลจึงเป็นเรื่องที่ผู้บริหารทุกองค์กรไม่สามารถหลีกเลี่ยงได้ ในปัจจุบันองค์กรขนาดใหญ่ได้แยกแผนกรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศออกจากแผนกเทคโนโลยีสารสนเทศ เพื่อความคล่องตัวในการบริหารและการแบ่งแยกอำนาจหน้าที่รับผิดชอบให้เกิดความชัดเจน รวมทั้งในอนาคตองค์กรควรจะต้องมีแผนกอย่างน้อย 3 แผนกคือ แผนกไอที (Information Technology : IT) หรือระบบสารสนเทศเพื่อการบริหาร (MIS : Management Information System) แผนกการรักษาความปลอดภัยในเทคโนโลยีสารสนเทศ (IS) และแผนกผู้ตรวจสอบภายในไอที (IT Internal Audit) ร่วมมือกันทำงานและตรวจสอบซึ่งกันและกัน นโยบายด้านความปลอดภัยมีความสำคัญในป้องกันการละเมิดการรักษาความปลอดภัยของเครือข่ายและภัยคุกคามที่มีผลต่อการสื่อสารคอมพิวเตอร์ในระบบรักษาความปลอดภัย ที่เกิดช่องโหว่ในระบบเครือข่ายคอมพิวเตอร์จะมีการระบุในแง่ของการหาประโยชน์ในการปรับใช้เทคโนโลยีสามารถแสกนเพื่อหาช่องโหว่เหล่านี้ได้และมีผลต่อความสมบูรณ์ของข้อมูลของการแลกเปลี่ยนข้อมูลการใช้บริการ โดยข้อความนี้บ่งชี้ว่าควรศึกษาอินเตอร์เน็ตในปัจจุบันเพื่อหลีกเลี่ยงการการเจอปัญหาและหนึ่งในปัญหาที่สำคัญที่สุดสำหรับอินเตอร์เน็ตในปัจจุบันคือมีการขาดการรักษาความปลอดภัยที่รัดกุมในความเป็นจริงความซุกของมัลแวร์ที่เพิ่มขึ้นการโจมตี [3] การบุกรุกของเครือข่ายโดยการเข้ารหัส [5, 12] และภัยคุกคาม [2,6] ที่จะเกิดขึ้นเห็นได้ชัดเจนว่าโครงสร้างพื้นฐานด้านอินเตอร์เน็ตในปัจจุบันไม่มีพื้นฐานโครงสร้างที่แข็งแกร่ง ซึ่งโซลูชั่นรักษาความปลอดภัยที่มีประสิทธิภาพสามารถสร้างขึ้นได้

ในขณะที่มันได้รับการยอมรับอย่างกว้างขวางว่าอินเตอร์เน็ตในอนาคตจำเป็นต้องมีในตัวกลไกการรักษาความปลอดภัยการทำงานของกลไกเหล่านี้มีความชัดเจนน้อยลงนอกจากนี้และมีปัญหาพอ ๆ กันรูปแบบการ Adversarial จะไม่เข้าใจกันดีนั่นคือในขณะที่ปัญหาในปัจจุบันเป็นที่รู้จักกันจะไม่ชัดเจนซึ่งภัยคุกคามอินเตอร์เน็ตในอนาคตจะต้องมีการติดอาวุธต่อต้าน แต่ระบุรูปแบบและการคาดการณ์ adversarial ภัยคุกคามเป็นขั้นตอนแรกที่จำเป็นในการสร้างที่มีความปลอดภัยอินเตอร์เน็ตในอนาคต เฉพาะเมื่อชุมชนมีความเข้าใจที่มั่นคงของการคุกคามที่ว่าอินเตอร์เน็ตในอนาคตอาจเผชิญ การตอบโต้ที่เหมาะสมสามารถออกแบบได้

ในงานวิจัยฉบับนี้เราจะเริ่มต้นในการสร้างรูปแบบการ adversarial สำหรับอินเตอร์เน็ตในอนาคต เหตุนี้เราแนะนำจำนวนของภัยคุกคามที่ควรจะนำเข้าบัญชีเมื่อมีการพัฒนาออกแบบของอินเตอร์เน็ตในอนาคตภัยคุกคามเหล่านี้และความท้าทายที่มีการระบุถึงความพยายามรวมของทั้งสามกลุ่มทำงานที่ทำงานภายใต้กรอบของสหภาพยุโรป F7 โครงการทั้งสามกลุ่มทำงานโครงการลักษณะที่แตกต่างกันของวิธีการที่เราคาดหวังว่าอินเตอร์เน็ตในอนาคตจะนำไปใช้และภัยคุกคามที่เป็นอันตรายต่อกรณีการใช้งานเหล่านี้ ดังนั้นภัยคุกคามที่จะมีการระบุโดยกลุ่มที่มีการพัฒนาโดยทั่วไปว่าการออกแบบอินเตอร์เน็ตในอนาคตมีแนวโน้มที่ต้องยังคงมีอยู่

กลุ่มที่ทำงานครั้งแรกมุ่งเน้นไปที่มัลแวร์และการฉ้อโกง เหตุผลในการเลือกพื้นที่ปัญหานี้เกิดจากความเชื่อว่าอินเตอร์เน็ตในอนาคตจะยังคงใช้สำหรับการพาณิชย์อิเล็กทรอนิกส์และการทำธุรกรรมทางการเงินได้มากขึ้นเพื่อรวมกับความจริงที่เราเป็นพยานการก่อตัวของเศรษฐกิจใต้ดินเจริญรุ่งเรืองที่เราคาดว่าโอกาสที่สำคัญสำหรับโค้ดที่เป็นอันตรายและการดำเนินการหลอกลวงที่ตกเป็นเหยื่อการหลอกลวงเพื่อหวังผลกำไรทางการเงิน คณะทำงานที่สองมุ่งเน้นภัยคุกคามที่เกิดจากการเปลี่ยนแปลงของเครือข่ายปกติในสภาพแวดล้อมสมาร์ทด้วยวิธีนี้เราหมายถึงจำนวนเพิ่มมากขึ้นของอุปกรณ์ขนาดเล็กที่มีการเพิ่มอำนาจการใช้คอมพิวเตอร์อุปกรณ์เหล่านี้มีขนาดเล็กเร็ว ๆ นี้จะนำเสนอทุกที่และเชื่อมต่ออย่างถาวรกับอินเตอร์เน็ต ดังนั้นการออกแบบอินเตอร์เน็ตในอนาคตได้ไปยังที่อยู่ภัยคุกคามที่เกิดจากการระเบิดของอุปกรณ์ขนาดเล็กที่แพร่หลายของสุดท้ายเราคาดการณ์ว่าอินเตอร์เน็ตจะใช้มากขึ้นในการควบคุมระบบที่สำคัญ ขณะนี้มักจะหมายถึงการควบคุมของโรงงานอุตสาหกรรมและโครงสร้างพื้นฐานที่สำคัญนี้เป็นเพียงส่วนหนึ่งของภาพ เหตุผลก็คือระบบซอฟต์แวร์ที่ยังสามารถดำเนินงานภารกิจที่สำคัญและการสูญเสียหรือเหตุขัดข้องของความล้มเหลวในการเชื่อมต่อหรือซอฟต์แวร์ที่สามารถทำให้เกิดความเสียหายทางเศรษฐกิจอย่างรุนแรงหรือคุกคามชีวิต ดังนั้นอินเตอร์เน็ตในอนาคตได้ไปยังที่อยู่ภัยคุกคามที่มาพร้อมกับความเชื่อมั่นที่เพิ่มขึ้นเกี่ยวกับการทำงานที่อยู่ภายใต้โครงสร้างพื้นฐานเครือข่าย

ในส่วนต่อไปนี้เราจะกล่าวถึงภัยคุกคามที่สำคัญที่ได้รับการระบุโดยทั้งสามกลุ่มการทำงานและยืนยันว่าพวกเขามีความเกี่ยวข้องในการออกแบบที่มีความปลอดภัยอินเตอร์เน็ตในอนาคต

ไฟร์วอล (Firewall)

ไฟร์วอลใช้สำหรับป้องกันผู้บุกรุกบนอินเทอร์เน็ต ซึ่งเป็นบุคคลที่ไม่มีสิทธิ์ในการเข้าถึงระบบเครือข่ายส่วนบุคคล แต่ต้องการมุ่งโจมตีหรือประสงค์ร้ายต่อระบบอุปกรณ์ไฟนอลอาจเป็นเร้าเตอร์ เกตเวย์ หรือคอมพิวเตอร์ที่ติดตั้งซอฟต์แวร์ไฟร์วอลซึ่งทำหน้าที่ตรวจสอบติดตามแพ็คเกจที่เข้าออกระบบ เพื่อป้องกันการเข้าถึงเครือข่าย หน้าที่ของไฟร์วอลจะอนุญาตให้ผู้มีสิทธิ์หรือมีบัตรผ่านเท่านั้นที่จะเข้าถึงเครือข่ายทั้งสองฝั่ง โดยจะมีการป้องกันบุคคลภายนอกที่

ไม่ต้องการให้เข้าถึงระบบ รวมถึงการป้องกันบุคคลภายในไม่ ให้เข้าไปยังบางเว็บไซต์ที่ ไม่ต้องการอีกด้วย

• **การป้องกันไฟร์วอล (Protect Firewall)** เป็นเครื่องมือที่ใช้ในการป้องกันโดยข้อมูลที่มีการรับหรือส่งผ่านระบบเครือข่ายโดยจะถูกกำหนดเป็นกฎเกณฑ์หรือข้อบังคับ (Rule) เพื่อใช้บังคับในการสื่อสารภายในเครือข่าย (ข้อมูลที่มีการรับส่งภายในหรือภายนอกระบบเครือข่ายเราเรียกว่าแพ็คเกจ)

• **บ้อบังคับพื้นฐาน (Rule Base)** ข้อกำหนดในการควบคุมการรับ-ส่งข้อมูลภายในระบบเครือข่าย ดังนั้นการติดตั้งไฟร์วอลจะต้องมีการกำหนดกฎเกณฑ์ในการควบคุมการทำงานในระบบเครือข่าย

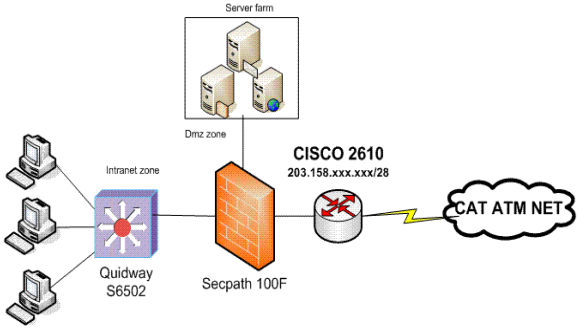
• **การควบคุมการเข้าถึง (Access Control)** หมายถึง การควบคุมระดับการเข้าถึงการรับ-ส่งข้อมูล

ไฟร์วอลเป็นระบบควบคุมการเข้า-ออกเครือข่ายซึ่งใช้สำหรับปกป้องเครือข่ายภายในขององค์กรจากการโจมตีจากภายนอกได้ โดยปกติแล้วไฟร์วอลล์จะติดตั้งขวางกั้นระหว่างสองเครือข่ายอินเตอร์เน็ตและอินทราเน็ต อย่างไรก็ตามไฟร์วอลไม่สามารถที่จะปกป้องการโจมตีที่ใช้ช่องทางปกติที่เปิดไว้โดยไฟร์วอลได้ กล่าวคือไม่สามารถป้องกันการโจมตีที่มาจากเครื่องภายในเครือข่ายได้เนื่องจากเครื่องดังกล่าวไม่ต้องผ่านไฟร์วอลหรือถ้ามาจากภายนอกก็ไม่สามารถป้องกันการโจมตีในโซน DMZ ที่ให้บริการเว็บเซิร์ฟเวอร์ได้ถ้าโซนดังกล่าวมีช่องโหว่และจุดอ่อน

เหตุผลหลักของการนำไฟร์วอลมาใช้ก็เพื่อต้องการให้ผู้ใช้ภายในเครือข่ายสามารถใช้บริการได้อย่างเต็มที่และยังสามารถใช้บริการเครือข่ายภายนอก เช่น อินเตอร์เน็ตได้ ในทางกลับกันไฟร์วอลจะป้องกันการเข้ามาใช้บริการเครือข่ายภายในด้วย โดยไฟร์วอลจะควบคุมการผ่านเข้าออกของแพ็คเกจได้โดยอนุญาตหรือไม่อนุญาตผ่านได้ ซึ่งจะต้องขึ้นอยู่กับนโยบายการรักษาความปลอดภัยขององค์กรนั้นๆ

ในการแก้ไขปัญหานำเสนอขั้นตอนวิธีการเส้นทาง PGBR ซึ่งเป็นการลาดกระจายตามเส้นทางโปรโตคอลเทคนิคการค้นพบเส้นทาง PGBR เส้นทางโดยการผ่านทางเครือข่ายโดยฮ็อป (Hop) จนกว่าจะถึงปลายทางเขตข้อมูลความลาดชันในเครือข่ายจะขึ้นอยู่กับโหนดในท้องถิ่นเพื่อการปฏิสัมพันธ์ของโหนดที่มีการเปลี่ยนแปลงแบบไดนามิคเป็นภาระในการเปลี่ยนแปลงเครือข่ายขึ้นอยู่กับโหลดในเครือข่ายของการค้นพบเส้นทางที่จะหลีกเลี่ยงส่วนของเครือข่ายที่มีความแออัดสูงและผ่านเส้นทางที่แออัดต่ำของเครือข่ายที่นำไปสู่การเป็นเครือข่ายที่สมดุลที่ดีในเวลาเดียวกันขั้นตอนวิธีการเส้นทาง PGBR นี้ยังเหมาะมากสำหรับอินเตอร์เน็ตในอนาคตควรเป็นสถาปัตยกรรมที่จะต้องใช้กลไกการกำหนดเส้นทางแบบไดนามิคสูงเพื่อสนับสนุนการบริการหลากหลายประเภท เช่นเดียวกับรูปแบบการจราจรแบบไดนามิคความยืดหยุ่นในพารามิเตอร์เลือกยังสามารถช่วยให้แต่ละเส้นทางที่จะค้นพบเกี่ยวกับการระบุความต้องการคุณภาพของการให้บริการ การจำลองการทำงานนอกจากนี้ยังมีการนำเสนอเพื่อแสดงให้เห็นประโยชน์ของขั้นตอนวิธีการ PGBR มากกว่าการกระจายขั้นตอนวิธีการกำหนดเส้นทางเช่นเดียวกับขั้นตอนวิธีเส้นทางที่สั้นที่สุด แบบจำลองที่มีการแสดงวิธีการ PGBR มีประสิทธิภาพดีกว่าเทคนิคอื่น ๆ สำหรับการกำหนดเส้นทางสี่ขนาดโครงสร้างแตกต่างกันและโหลดเครือข่ายที่แตกต่างกัน การทำงานการจำลองยังได้รับการดำเนินการเกี่ยวกับค่าพารามิเตอร์ที่แตกต่างกันของขั้นตอนวิธีการ PGBR เส้นทางและวิธีการนี้มีผลต่อขนาดโครงสร้างที่แตกต่างกันและโหลดในเครือข่าย[5],[3]

แนวโน้มงานวิจัยในยุคอินเตอร์เน็ตในอนาคตจะมุ่งเน้นไปในทิศทางการแก้ไขข้อจำกัดด้านความแออัดของการจราจรของเครือข่าย เพื่อการค้นหาเส้นทางที่มีประสิทธิภาพ



รูปที่ 1 การทำงานของระบบไฟร์วอล

จุดประสงค์หลักของความปลอดภัยทางข้อมูล

1. การรักษาความลับ (Confidentiality) [9] คือการรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ และผู้มีสิทธิ์เท่านั้นจึงจะเข้าถึงข้อมูลนั้นได้

2. การรักษาความสมบูรณ์ (Integrity) คือการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา

3. ความพร้อมใช้ (Availability) คือการรับรองว่าข้อมูลและบริการการสื่อสารต่าง ๆ พร้อมที่จะใช้ได้ในเวลาที่ต้องการใช้งาน

4. การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) คือวิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

กำหนดลักษณะของการควบคุมความมั่นคงปลอดภัย (Security Controls) ได้ 3 ระดับ

1. การเข้ารหัส (Encryption)

การเข้ารหัส คือการเก็บข้อมูลให้เป็นส่วนบุคคลจากบุคคลอื่นที่ไม่ได้รับอนุญาต ส่วนประกอบ 2 ส่วนที่สำคัญที่จะช่วยทำให้ข้อมูลนั้นเป็นความลับได้ก็คือ การกำหนดสิทธิ์และการพิสูจน์ตัวตนเพราะว่าก่อนการอนุญาตให้บุคคลที่กล่าวอ้างเข้าถึงข้อมูลหรือถอดรหัสข้อมูลนั้นต้องสามารถแน่ใจได้ว่าบุคคลที่กล่าวอ้างนั้นเป็นใครและได้รับอนุญาตให้สามารถเข้ามาดูข้อมูลได้หรือไม่ ในการเข้ารหัสนั้นวิธีการหนึ่งที่ทำได้คือการเข้ารหัสในรูปแบบของกุญแจลับ (Secret key) ซึ่งในการใช้คีย์รูปแบบนี้ต้องเฉพาะผู้ที่มีกุญแจลับนี้เท่านั้นที่สามารถรับข้อมูลที่เข้ารหัสแล้วได้

2. การอนุญาต การอนุมัติ (Authorization)

การกำหนดสิทธิ์ คือขั้นตอนในการอนุญาตให้แต่ละบุคคลสามารถเข้าถึงข้อมูลหรือระบบใดได้บ้าง ก่อนอื่นต้องทราบก่อนว่าบุคคลที่กล่าวอ้างนั้นคือใครตามขั้นตอนการพิสูจน์ตัวตนและต้องให้แน่ใจด้วยว่าการพิสูจน์ตัวตนนั้นถูกต้อง

3. การตรวจสอบบุคคล (Authentication)

การตรวจสอบ คือการตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ ซึ่งสามารถใช้ในการติดตามการดำเนินการเพื่อตรวจสอบความถูกต้องและแม่นยำ ตัวอย่างเช่น การตรวจสอบบัญชีชื่อผู้ใช้ โดยผู้ตรวจบัญชี ซึ่งการตรวจสอบความถูกต้องของการดำเนินการเพื่อให้แน่ใจว่าหลักฐานทางอิเล็กทรอนิกส์นั้นได้ถูกสร้างและสั่งให้ทำงานโดยบุคคลที่ได้รับอนุญาต และในการเชื่อมต่อเหตุการณ์เข้ากับบุคคลจะต้องทำการตรวจสอบหลักฐานของบุคคลนั้นด้วย ซึ่งถือเป็นหลักการพื้นฐานของขั้นตอนการทำงานของการพิสูจน์ตัวตนด้วยการพิสูจน์ตัวตนจัดเป็นการตรวจสอบหลักฐานขั้นพื้นฐานที่สำคัญที่สุดใน 5 ระดับชั้นของการควบคุมความปลอดภัย ดังนั้นการพิสูจน์ตัวตนดีจะช่วยเพิ่มความมั่นคงปลอดภัยขั้นพื้นฐานให้กับระบบมากยิ่งขึ้น

ประเภทของการพิสูจน์ตัวตน (Authentication Types)

ส่วนประกอบพื้นฐานของการพิสูจน์ตัวตนสมบูรณ์แบ่งได้เป็น 3 ส่วน คือ

- การพิสูจน์ตัวตน (Authentication) คือส่วนที่สำคัญที่สุดเพราะเป็นขั้นตอนแรกของการเข้าใช้ระบบ ผู้เข้าใช้ระบบต้องถูกยอมรับจากระบบว่าสามารถเข้าสู่ระบบได้ การพิสูจน์ตัวตนปั่นการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลนั้นจริง
- การกำหนดสิทธิ์ (Authorization) คือข้อจำกัดของบุคคลที่เข้ามาในระบบ ว่าบุคคลคนนั้นสามารถทำอะไรกับระบบได้บ้าง
- การบันทึกการใช้งาน (Accountability) คือการบันทึกรายละเอียดของการใช้ระบบและรวมถึงข้อมูลต่างๆที่ผู้ใช้กระทำลงไปในระบบ เพื่อผู้ตรวจสอบจะได้ตรวจสอบได้ว่า ผู้ใช้ที่เข้ามาใช้บริการได้เปลี่ยนแปลงหรือแก้ไขข้อมูลในส่วนใดบ้าง

จากที่ได้กล่าวไปข้างต้นว่าการพิสูจน์ตัวตนมีความสำคัญที่สุดกับการเข้าใช้ระบบ จึงแจกแจงชนิดของการพิสูจน์ตัวตนใช้กันอยู่ในปัจจุบันว่ามีอะไรบ้างและแต่ละชนิดมีลักษณะอย่างไร ดังนี้

A. ไม่มีการพิสูจน์ตัวตน
B. การพิสูจน์ตัวตนโดยใช้รหัสผ่าน
C. การพิสูจน์ตัวตนโดยใช้ PIN
D. การพิสูจน์ตัวตนโดยใช้ password authenticators หรือ tokens
E. การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล
F. การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว
G. การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ
H. การพิสูจน์ตัวตนโดยการใช้ลายเซ็นดิจิตอล
I. การพิสูจน์ตัวตนโดยใช้การถาม – ตอบ
J. ตารางเปรียบเทียบข้อดีข้อเสียของการพิสูจน์ตัวตนแต่ละชนิด

ความปลอดภัยของสภาพแวดล้อม

การรักษาความปลอดภัย คือการป้องกันปัญหาทั้งหมดแต่การป้องกันจะอ้างถึงกลไกเฉพาะด้านของโปรแกรมระบบที่ใช้ป้องกันข้อมูลสำหรับการรักษาความปลอดภัย มีประเด็นอยู่ 3 ด้านคือ

1. ภัยคุกคาม (Threat)

1.1 นำความลับไปเปิดเผย (Data confidentiality)
1.2 เปลี่ยนแปลงข้อมูล (Data integrity)
1.3 ทำให้หยุดบริการ (System availability)

2. ผู้ประสงค์ร้าย (Intruder)

2.1 พวกชอบสอดรู้สอดเห็น
2.2 พวกชอบทดลอง
2.3 พวกพยายามหารายได้ให้ตนเอง
2.4 พวกจารกรรมข้อมูล

3. ข้อมูลสูญหายโดยเหตุสุดวิสัย (Accidental data loss)

3.1 ปรากฏการณ์ทางธรรมชาติ
3.2 ฮาร์ดแวร์หรือซอฟแวร์ที่ทำงานผิดพลาด
3.3 ความผิดพลาดของมนุษย์

ตัวอย่างของภัยคุกคาม

การสอดแนม (Snooping or Sniffing or Eavesdropping)

หมายถึง การดักเพื่อแอบดูข้อมูล ซึ่งจัดอยู่ในประเภทเปิดเผย การสอดแนมเป็นการโจมตีแบบพาสซีฟ (Passive) คือเป็นการกระทำที่ไม่มีการเปลี่ยนแปลงหรือการแก้ไขข้อมูล เช่น การดักอ่านข้อมูลระหว่างการส่งผ่านเครือข่ายการอ่านไฟล์ที่จัดเก็บอยู่ในระบบการแท็ปสายข้อมูล (Wiretapping) เป็นวิธีการหนึ่งของการสนูพปิ้ง (Snooping) เพื่อเฝ้าดูข้อมูลที่วิ่งบนเครือข่าย การปกป้องรักษาความลับของข้อมูลคือการเข้ารหัสข้อมูลนั่นเอง

แพ็คเกจสนิฟเฟอร์ (Packet Sniffer) เป็นรูปแบบหนึ่งของการโจมตีแบบสอดแนมข้อมูลที่ส่งผ่านเครือข่ายนั้นจะถูกแบ่งย่อยเป็นชุดเล็ก ๆ ซึ่งเรียกว่าแพ็คเกจแอพพลิเคชั่น (Application Packet) บางชนิดส่งข้อมูลแบบไม่ได้เข้ารหัสหรือแบบเคลียร์เท็กซ์ (Clear Text) ดังนั้นข้อมูลอาจถูกคัดลอกและโพรเซส (Process) โดยเครื่องอื่นที่มิใช่เครื่องปลายทางได้

การเปลี่ยนแปลงข้อมูล (Modification)

หมายถึง การแก้ไขข้อมูลโดยที่ไม่ได้รับอนุญาต ซึ่งอาจถือเป็นการหลอกลวง (Deception) ถ้าฝ่ายรับต้องใช้ข้อมูลที่ถูกเปลี่ยนแปลงแล้ว เช่นการโจมตีแบบคนกลางหรือการแทรกแซงการสื่อสาร (Man in the Middle Attack : MITM) การรักษาความคงสภาพจะช่วยปกป้องการโจมตีแบบนี้

การปลอมตัว (Spoofing)

หมายถึงการทำให้อีกฝ่ายหนึ่งเข้าใจว่าตัวเองเป็นอีกบุคคลหนึ่ง การโจมตีแบบนี้จัดอยู่ในประเภทหลอกลวงและควบคุมระบบ การปลอมตัวเป็นการหลอกให้คู่สนทนาเชื่อว่าตนกำลังสนทนากับอีกฝ่ายหรือบุคคลที่ต้องการ

สนทนาจริงๆ ดังนั้นการรักษาความคงสภาพโดยตรวจสอบบุคล การแสดงตัวตน ซึ่งจะเป็นวิธีการป้องกันการโจมตีในลักษณะนี้ได้

ไอพีสปูฟิง (IP Spoofing) หมายถึงการที่ผู้บุกรุกอยู่นอกเครือข่าย แล้วแสร้งทำเป็นว่าคอมพิวเตอร์ที่เชื่อถือได้ หรืออาจจะใช้ไอพีแอดเดรสเหมือนกับที่ใช้ในเครือข่ายหรืออาจใช้ไอพีแอดเดรสข้างนอกที่เครือข่ายเชื่อว่าเป็นคอมพิวเตอร์ที่เชื่อได้หรืออนุญาตให้เข้าใช้ทรัพยากรในเครือข่ายได้ การโจมตีแบบนี้โดยมากมักเป็นการเปลี่ยนแปลงหรือเพิ่มข้อมูลเข้าไปในแพ็คเกจที่รับส่งระหว่างไคลเอนท์และเซิร์ฟเวอร์หรือคอมพิวเตอร์ที่สื่อสารกันในเครือข่าย

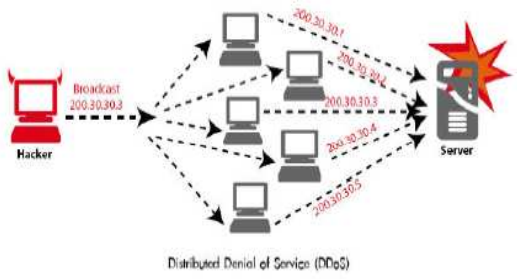
การปฏิเสธการให้บริการ (Denial of Service)

หมายถึงการขัดขวางการให้บริการของเซอร์ฟเวอร์เป็นเวลานาน การใช้ทรัพยากรจนหมดหรือถึงขีดจำกัดของเซิร์ฟเวอร์ การขัดขวางช่องทางสื่อสารไปยังเซิร์ฟเวอร์ การส่งแพ็คเกจเข้าไปในเครือข่ายจำนวนมาก ซึ่งจะทำให้ประสิทธิภาพของเครือข่ายลดลง หรืออาจเกิดระหว่างทางโดยการละทิ้งแพ็กคเกจข้อมูลที่รับส่งระหว่างเซิร์ฟเวอร์ ดังนั้นการรักษาความพร้อมใช้จะช่วยแก้ไขปัญหาการโจมตีในลักษณะนี้

ภัยคุกคาม หรือการสร้างความเสียหายในระบบคอมพิวเตอร์ มี 3 ประการคือ นำความลับไปเปิดเผย (Data confidentiality) การเปลี่ยนแปลงข้อมูล (Data integrity) และทำให้หยุดบริการ (System availability) เปรียบเทียบเป้าหมายการป้องกันและการสร้างความเสียหาย [6]

ความท้าทายสำคัญที่จะพัฒนาประสิทธิภาพของการออกแบบโครงสร้างสถาปัตยกรรมของระบบการสื่อสารทางอินเตอร์เน็ตยุคใหม่ (Design and architecture of the Internet) มีดังต่อไปนี้คือ:

- **Security and privacy :** ต้องมีความปลอดภัยและเป็นส่วนตัว
- **Resistance to Distribute Denial of Service (DDoS) attacks :** ต้องสามารถต้านทานการโจมตีแบบ Distributed Denial of Service (DDoS) ได้ซึ่งการโจมตีแบบ Distributed Denial of Service (DDoS) [10] คือการนำเครื่องมือที่จะใช้ในการโจมตีไปติดตั้งบนเครื่องคอมพิวเตอร์ที่ถูกเจาะไว้แล้วซึ่งมีจำนวนพอสมควร จากนั้นจึงจะระดมส่งข้อมูลในรูปแบบที่ควบคุมได้ โดยผู้ ควบคุมการโจมตีไปยังเหยื่อหรือเป้าหมายที่ต้องการ ซึ่งการโจมตีรูปแบบนี้ มักจะก่อให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่จนผู้อื่นไม่สามารถใช้งานได้ตามปกติ หรือทำให้ระบบที่ถูกโจมตีไม่มีทรัพยากรเหลือพอที่จะให้บริการผู้ใช้ทั่วไปได้จนทำให้เกิดปัญหาที่เซิร์ฟเวอร์



รูปที่ 2 แสดงรูปแบบการโจมตี

D. เราติ้ง (Routing)

เราติ้งเป็นโปรโตคอลที่ใช้ในการแลกเปลี่ยนตารางเราติ้งระหว่างอุปกรณ์เครือข่ายต่าง ๆ ที่ทำงานในระดับเน็ตเวิร์คเลเยอร์ (เลเยอร์ 3) เช่นเราเตอร์เพื่อให้อุปกรณ์เหล่านี้สามารถส่งข้อมูลไอพีแพ็คเกจ (IP packet) ไปยังคอมพิวเตอร์ปลายทางได้อย่างถูกต้อง โดยที่ผู้ดูแลเครือข่ายไม่ต้องแก้ไขข้อมูลตารางเราติ้งของอุปกรณ์ต่าง ๆ ตลอดเวลาเรียกว่าการทำงานของเราติ้งโปรโตคอลทำให้เกิดการใช้งานไดนามิคเราติ้งต่อระบบเครือข่ายข้อจำกัดของการขนส่งและการสื่อสารด้วยการค้นหาเส้นทางจากจุดเริ่มต้นไปสู่จุดหมาย โดยมีเส้นทางหลาย ๆ เส้นทางจะใช้แบบเราติ้งโมเดลเพื่อวิเคราะห์เส้นทางที่เหมาะสมที่สุด นอกจากนี้ยังสามารถนำหลักการเดียวกันไปใช้สำหรับการตัดสินใจในการค้นหาเส้นทาง การออกแบบสำหรับเส้นทางสถาปัตยกรรมใหม่ที่ทำให้อินเตอร์เน็ตเส้นทางเพิ่มเติมสามารถปรับขนาดได้ เพื่อค้นหาตำแหน่งของโฮสต์ที่จะต้องมีการทำแผนที่ ระบบที่ส่งตัวระบุตำแหน่งที่เหมาะสมในการตอบสนองต่อการร้องขอแผนที่ (map requests) สำหรับตัวระบุเฉพาะเจาะจงของเส้นทางของเราติ้ง [1] ข้อจำกัดที่เกิดขึ้นเกี่ยวกับการค้นหาเส้นทางที่มักจะพบบ่อยคือ การขาดความคล่องตัวในการจราจรของการค้นหาเส้นทางซึ่งจะทำให้ผู้ให้บริการเครือข่ายประสบกับปัญหา แนวความคิดพิจารณาเป็นวิธีที่มีแนวโน้มเพื่อแก้ปัญหาที่กล่าวถึงแต่วิธีการออกแบบกรอบการทำงานที่เหมาะสมสำหรับการระบุตามเส้นทางในที่ตั้ง / ตัวบ่งชี้บริบทแยกยังคงเป็นปัญหาที่เกิดขึ้นในการระบุข้อมูลพื้นฐาน (Identifier-Based) เป็นระบบการกำหนดเส้นทางของเราเตอร์ที่มีการนำเสนอโดยการใช้หลักการในการค้นหาเส้นทางแบบไดนามิค [2] อีกทั้งยังมีปัญหาพื้นฐานหลายอย่างสำหรับการพัฒนาโดเมนระหว่างเส้นทางโปรโตคอลในเครือข่ายแสงเราอธิบายวิธีการคำนวณได้รับการสนับสนุนคุณภาพของการให้บริการใด ๆ ระหว่างสองโหนดและในโดเมนที่ต่างกัน [5] กล่าวถึงแล้ววิธีการเลือกเส้นทางระหว่างโดเมนสำหรับได้รับการขอเชื่อมต่อระหว่างโดเมนกับความต้องการคุณภาพของการให้บริการเพื่อแก้ไขปัญหาและข้อจำกัดของการเราติ้งที่เกิดขึ้นในปัจจุบันนำไปสู่ยุคใหม่ของยุคอินเตอร์ในอนาคต

E. ไอดี/แอลโอซี (ID/LOC)

การสนับสนุนการเคลื่อนย้ายผ่านสถาปัตยกรรมแบบแยกไอดี/แอลโอซี [34]

ในบทความนี้เสนอระบบการตั้งชื่อใหม่และการค้นหาสถาปัตยกรรมเครือข่ายบนพื้นฐานของแนวคิดการตั้งชื่อในลำดับชั้นที่มีความคล่องตัวและการสนับสนุนการสื่อสาร นอกจากนี้ยังแก้ปัญหาความยืดหยุ่นในการควบคุมการจราจรภายใต้เงื่อนไขแบบมัลติไปยังจุดหมายปลายทางในวิธีการแก้ปัญหาประกอบไปด้วย 3 แนวคิดหลักๆ

1. นำเสนอแนวความคิดเกี่ยวกับสถานที่ตั้งของระบบบริหารจัดการเพื่อสนับสนุนการเคลื่อนที่

2. นำเสนอแนวความคิดเกี่ยวกับสถาปัตยกรรมที่ใช้แนวคิดหลักการของคอร์เอดจ์ (core-edge) ของการกำหนดเส้นทางและที่อยู่

3. นำเสนอแนวความคิดเพื่อปรับปรุงประสิทธิภาพของระบบการทำแผนที่ระดับการจัดการการระบุตำแหน่งที่จะแสดงข้อดีของสถาปัตยกรรมการจำลองแม่ข่ายขนาดใหญ่และการวิเคราะห์ประสิทธิภาพการทำงานของสถาปัตยกรรม

ในงานวิจัยฉบับนี้ได้แนะนำเครือข่ายแบบใหม่ การแยกไอดี / การระบุตำแหน่ง สถาปัตยกรรมที่มีความสามารถในการสนับสนุนการเคลื่อนไหวและการแก้ปัญหาการขยายเส้นทาง และรูปแบบที่อยู่บนพื้นฐานของแนวคิด “8 + 8” มีความสามารถในการจัดเก็บ การระบุและการค้นหาข้อมูลในเวลาเดียวกันและการเปลี่ยนแปลงตำแหน่งได้อย่างง่าย และมีประสิทธิภาพเพิ่มความยืดหยุ่นของการกำหนดเส้นทางในระบบเครือข่ายทั่วโลก โดยเฉพาะแนวคิดของเซิร์ฟเวอร์เพื่อจัดการกับตัวเลขที่เติบโตอย่างรวดเร็วของ MHS และการเคลื่อนไหวแบบไดนามิค

การเคลื่อนที่แบบจัดการความปลอดภัยสำหรับ 6LoWPAN ไอดี / การระบุตำแหน่ง สถาปัตยกรรมแบบแยกส่วน [25]

ในการเคลื่อนที่ในการสนับสนุน 6LoWPAN การเชื่อมต่อช่วยให้การขยายและปรับเครือข่ายการเปลี่ยนแปลงของตำแหน่งและโครงสร้างพื้นฐาน คุณสมบัติเหล่านี้เป็นสิ่งที่จำเป็นเพื่อตอบสนองความเชื่อถือและวัดได้ของเครือข่ายของโลกในอนาคต การพัฒนาเพื่อรองรับการเคลื่อนย้าย แต่ส่วนใหญ่ในปัจจุบันมีข้อจำกัดที่เกิดจากบทบาทของที่อยู่ไอพีเป็นไอดีของโหนดทั้งสองสำหรับการใช้งาน สถาปัตยกรรม 6LoWPAN ซึ่งสนับสนุนการกำหนดขนาดและการส่งสัญญาณการเคลื่อนไหว วิธีการดังกล่าวนำเสนอด้านความปลอดภัยเนื่องจากไอดี/ การระบุตำแหน่งจัดการข้อความที่อาจเป็นอันตรายเช่นโฮสต์ที่เป็นอันตราย

ด้วยเหตุผลที่ว่าในบทความนี้จะดำเนินการรักษาความปลอดภัยการวิเคราะห์และเสนอความคล่องตัวในการจัดการรักษาความปลอดภัยรูปแบบใหม่การพิจารณาความต้องการและข้อจำกัดของอินเตอร์เน็ตในอนาคตของเครือข่ายกิจกรรมโครงการที่เสนอคือขึ้นอยู่กับส่วนขยายของกระบวนการ Routability ที่มีการตรวจจับและแก้ไขความผิดพลาด (Error Checking and Correction : ECC) ที่ใช้อ่านรหัสไม่สมมาตรเพื่อจะดำเนินการตรวจสอบโดเมนระหว่างปรับขนาดได้สำหรับทุกฝ่ายที่เกี่ยวข้องในการปรับปรุงตำแหน่งที่จดทะเบียนการถ่ายโอนและมีผลผูกพัน

รูปแบบงานวิจัยฉบับนี้ได้นำเสนอวิธีการแก้ปัญหาเรื่องภัยคุกคามและช่องโหว่ที่พบในสถาปัตยกรรมเพื่อการสนับสนุนการเคลื่อนไหวในสถาปัตยกรรม 6LoWPAN แยกไอดี/ การระบุตำแหน่งโครงการที่เสนอความปลอดภัยและขยายขีดความสามารถให้การสนับสนุนการเคลื่อนย้ายขึ้นอยู่กับส่วนขยายของห่วงโซ่ความน่าเชื่อถือมีการกำหนดของคีย์ที่ใช้ร่วมกันระหว่างหน่วยงานที่จำเป็นต้องมีการแลกเปลี่ยนโดยตรงของข้อมูลนี้อยู่บนพื้นฐานการตรวจจับและแก้ไขความผิดพลาด การแลกเปลี่ยนคีย์และ Routability การย้อนกลับการทำงานในอนาคตคือมุ่งเน้นไปที่การสร้างแบบจำลองการเคลื่อนไหวและการประเมินผลการตรวจสอบโครงการที่เสนอและการเปรียบเทียบเกินพิกัดของโครงการใหม่นี้ที่เกี่ยวกับต้นฉบับ ท้ายที่สุดการดำเนินงานของโครงการที่เป็นไปจะดำเนินการวิเคราะห์ความยืดหยุ่นของสถาปัตยกรรม

นิยามของกลไกการจัดการการไอดี / การระบุตำแหน่งอย่างมีประสิทธิภาพ [28]

ในงานวิจัยฉบับนี้เสนอพื้นฐานของการเพิ่มประสิทธิภาพและขยายขีดความสามารถของไอดี / การระบุตำแหน่งแบบสถาปัตยกรรมการแยกส่วน (LIDS) การจัดการการเคลื่อนไหวถูกออกแบบกลไก จากนั้นวิเคราะห์ประสิทธิภาพการทำงานที่โดดเด่นการจัดการการเคลื่อนไหวของเครือข่ายที่ใช้กับเส้นทางสนับสนุนการเพิ่มประสิทธิภาพเมื่อเทียบกับวิธีการตามที่ไอพี (Mobile IPv6 and Proxy Mobile IPv6)

ในงานวิจัยนี้ได้นำเสนอไอดี / การระบุตำแหน่งที่มีประสิทธิภาพตามโครงการกลไกการแยกการเคลื่อนไหวตามการจัดการหลังจากที่นำเสนอประสิทธิภาพการทำงานที่มีการศึกษาและเมื่อเทียบกับไอพีอื่น ๆ โปรโตคอลการจัดการการเคลื่อนย้ายตามผลที่เป็นตัวเลขแสดงให้เห็นว่างานวิจัยที่เสนอสามารถให้ความคล่องตัวดีมาก และไม่มีค่าใช้จ่ายในการส่งแพ็คเกจทั้งในแนวนอนและแนวตั้ง

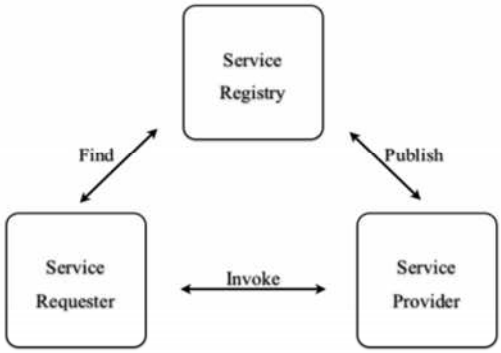
F. สถาปัตยกรรม (Architecture)

ระบบอินเตอร์เน็ตได้มีการพัฒนาปรับปรุงเปลี่ยนแปลงมาอย่างต่อเนื่อง จนสามารถมีการบริการและโปรแกรมต่างๆ ที่ยืดหยุ่นในการใช้งานมากขึ้น ทำให้ยุคสมัยนี้เป็นยุคสมัยแห่งการแบ่งปันข้อมูล เนื่องจากมีการออกแบบโครงสร้างสถาปัตยกรรมของระบบการสื่อสารทางอินเตอร์เน็ต (design and architecture of the Internet) ให้สะดวกต่อการรับส่งข้อมูลต่างๆมากขึ้น อินเตอร์เน็ตในปัจจุบันถูกออกแบบมาแล้วกว่า 40 ปี จะเห็นได้ว่ามีบทบาทมากมายในหลายๆ ด้าน อาทิ เช่น เชิงพาณิชย์ เชิงสังคมและวัฒนธรรม ฯลฯ ประกอบกับความต้องการในด้านการใช้งานก็ยังเพิ่มสูงขึ้นเรื่อยๆ การรักษาความปลอดภัย การเคลื่อนย้าย การกระจายเนื้อหา เป็นต้น การออกแบบสถาปัตยกรรมใหม่จึงมีความจำเป็นเพื่อรองรับความต้องการของผู้ใช้งานอินเตอร์เน็ตในอนาคต

Future Internet Architecture: A Service-Oriented Approach [37]

ความหมายของสถาปัตยกรรมการบริการ (Service-Oriented Architecture : สถาปัตยกรรมการบริการ)

ความหมายของการบริการ (Service) คือเป็นการรวมฟังก์ชั่นจากระบบสนับสนุนงานธุรกิจทั้งที่มีอยู่หรือที่สร้างใหม่ให้เป็นหน่วยเดียวตามมาตรฐานที่กำหนด และประกาศฟังก์ชันที่รวมขึ้นเป็นหนึ่งเดียวนั้นซึ่งจะทำให้ระบบอื่นสามารถค้นหาเซอร์วิส (Service Discovery) และเรียกใช้งานเซอร์วิสได้ง่ายขึ้น และสถาปัตยกรรมการบริการหมายถึงโมเดลของการพัฒนาซอฟต์แวร์ที่สร้างฟังก์ชันต่างๆ ให้เป็นบริการซึ่งสามารถนำมาใช้ทำงานร่วมกันได้ผ่านอินเตอร์เฟส (Interface) ที่เป็นมาตรฐานที่นิยามอย่างชัดเจน และมีการกำหนดเงื่อนไขรายละเอียดของบริการไว้



รูปที่ 3 แสดงโมเดลของสถาปัตยกรรมการบริการ

องค์ประกอบที่สำคัญของสถาปัตยกรรมการบริการ

คุณลักษณะสำคัญหลักๆ ดังนี้

1. สถาปัตยกรรมการบริการจะมีตัวเชื่อมต่ออินเตอร์เฟซที่อธิบายเซอร์วิส ซึ่งเป็นไฟล์ XML ที่ไม่ขึ้นกับแฟลตฟอร์มและเทคโนโลยี โดยมากมักจะใช้มาตรฐาน WSDL : Web Service Description Language) ในการอธิบายการให้บริการ

2. สถาปัตยกรรมการบริการจะมีการลงทะเบียน (Registry) ในการเก็บการบริการต่างๆที่มีอยู่ซึ่ง การลงทะเบียนจะทำหน้าที่เหมือนไดเร็กทอรี่ของโปรแกรมการให้บริการหรือการประมวลทางธุรกิจ (Business Process) ต่างๆจะค้นหาและเรียกใช้การบริการจากลงทะเบียนนี้ มาตรฐานที่ใช้ในการเก็บการลงทะเบียนที่นิยมใช้คือยูดีดีไอ (UDDI : Universal Description Definition and Integration)

3. การส่งข้อมูลระหว่างการบริการ สถาปัตยกรรมการบริการ จะใช้เอกสารที่เป็น XML ที่นิยามผ่าน XML Schema (ไฟล์ XSD) การสื่อสารระหว่างเซอร์วิสเหล่านี้สามารถทำได้ในระบบที่หลากหลายโดยไม่จำเป็นต้องทราบรายละเอียดของแฟลตฟอร์มและเทคโนโลยีที่เซอร์วิสนั้นใช้อยู่

4. สถาปัตยกรรมการบริการสามารถพัฒนาโปรแกรมหรือการประมวลทางธุรกิจโดยการประกอบสถาปัตยกรรมการบริการที่มีอยู่โดยใช้คำสั่งที่เป็น XML ซึ่งมาตรฐานที่นิยมใช้คือ WS-BPEL (Web Service-Business Process Execution Language)

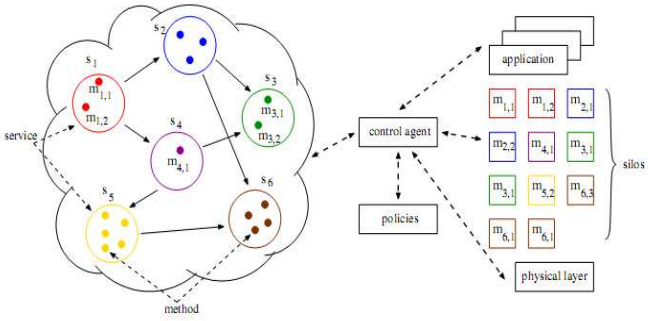
5. การบริการสถาปัตยกรรมการบริการแต่ละตัวจะมีส่วนการควบคุมคุณรูปที่เป็นการให้คุณภาพในการบริการ อาทิเช่นการควบคุมความปลอดภัยในด้านการตรวจสอบบุคคล, การอนุญาต การอนุมัติ, ข้อความที่น่าเชื่อถือได้และนโยบาย

ข้อดีของการพัฒนาสถาปัตยกรรมการบริการ

โครงสร้างของระบบไอทีขององค์กรขนาดใหญ่จะประกอบไปด้วยระบบที่หลากหลายทั้งในด้านระบบปฏิบัติการ โปรแกรมประยุกต์และระบบซอฟต์แวร์ ซึ่งโปรแกรมประยุกต์บางโปรแกรมอาจใช้ในการทำงานกับกระบวนการทางธุรกิจ (Business Process) บางอย่างที่อาจทำงานภายใต้ระบบโครงสร้างไอทีเดิม เช่นพัฒนาโดยใช้เครื่องเมนเฟรม ดังนั้นเมื่อมีความจำเป็นต้องเปลี่ยนแปลงกระบวนการทางธุรกิจจะทำให้การเปลี่ยนแปลงโดยใช้โครงสร้างไอทีเดิมทำได้ยากจนอาจมีความต้องการที่จะยกเลิกระบบเดิมและพึ่งพาเทคโนโลยีใหม่ระบบสถาปัตยกรรมการบริการจะช่วยคุ้มครองการลงทุนขององค์กรเพื่อให้สามารถนำระบบโครงสร้างไอทีเดิมมาใช้ต่อไปได้ โดยการพัฒนาระบบโปรแกรมเดิมให้เป็นการบริการ สถาปัตยกรรมการบริการและเราจะสามารถพัฒนากระบวนการทางธุรกิจจากบริการต่าง ๆ ที่มีอยู่จึงทำให้องค์กรสามารถเปลี่ยนกระบวนการทางธุรกิจได้อย่างรวดเร็ว โดยใช้โปรแกรมประยุกต์เดิมและโครงสร้างไอทีเดิมที่มีอยู่

สถาปัตยกรรมการบริการเป็นแนวคิดในการพัฒนาสถาปัตยกรรมไอทีขององค์กรให้เป็นแบบเชิงบริการ เพื่อที่จะทำให้ระบบไอทีในองค์กรสามารถเชื่อมโยงกันได้ การพัฒนาสถาปัตยกรรมการบริการสามารถทำได้หลายวิธีและเว็บเซอร์วิส (Web Service) เป็นวิธีหนึ่งที่เหมาะสมในการพัฒนาระบบสถาปัตยกรรมการบริการจำเป็นที่จะต้องมีผลิตภัณฑ์และเครื่องมือในการพัฒนาที่สำคัญที่สุดคือต้องมีอีเอสบี (An enterprise service bus : ESB) เพื่อเชื่อมโยงระบบไอทีต่าง ๆ โดยผ่านอะแดปเตอร์ซึ่งจะเห็นได้ว่าการเชื่อมโยงที่ดีอาจไม่จำเป็นต้องแปลงระบบเดิมมาสู่เว็บเซอร์วิสทั้งหมดทั้งนี้เพราะอะแดปเตอร์ที่ยังสามารถติดต่อกับโมดูลเดิมที่อาจใช้โปรโตคอลอื่นได้ การพัฒนาสถาปัตยกรรมการบริการมีต้นทุนที่ค่อนข้างสูง และจำเป็นต้องมีทีมงานที่เข้าใจธุรกิจเฉพาะนั้น ๆ แต่ผลตอบแทนระยะยาวจะคุ้มค่ามาก

The SILO Architecture for Services Integration control and optimization for the Future Internet [39]



รูปที่ 4 แสดงสถาปัตยกรรม SILO

ข้อดีของการพัฒนา SILO

สถาปัตยกรรม SILO มีความยืดหยุ่นสูงและขยายต่ออย่างไร้ข้อจำกัด สนับสนุนสถาปัตยกรรมแบบครบวงจรที่ปรับขนาดได้ และยังเชื่อมต่อข้ามเซอร์วิส (cross-service) ที่ชัดเจนเพื่อเพิ่มประสิทธิภาพ

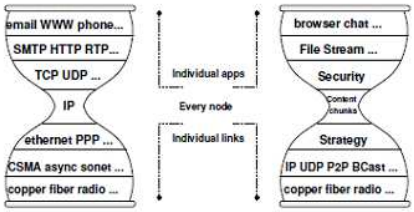
ข้อจำกัด

- ไม่มีเลเยอร์มากไปกว่านี้
- ป้องกันการเกิดกระบวนการแบ่งคู่ต่อสู้ (balkanization)

Architectures for Future Media Internet [40]

สถาปัตยกรรมซีซีเอ็น (CCN :Content-Centric Network)

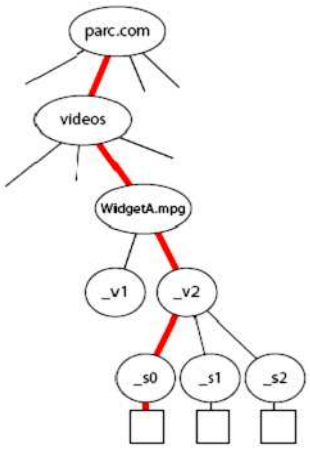
สถาปัตยกรรมนี้มีจุดมุ่งหมายคือใช้งานได้ตลอดเวลาแทนที่จะเป็นตลอดการใช้งาน ตัวอย่างเช่น multiply-to-multiply มากกว่าแบบเดิมคือพ้อยทูพ้อย (point-to- point)



รูปที่ 5 แสดงซีซีเอ็นทำการเคลื่อนย้ายขององค์ประกอบทั่วไปของเครือข่ายจากไอพีไปยังกลุ่มของเนื้อหา

นอกจากนี้ยังมีสถาปัตยกรรมซีซีเอ็นแนะนำสามโครงสร้างข้อมูลหลัก

- ฐานข้อมูลการส่งต่อ (Forwarding Information Base: FIB) : ใช้เพื่อส่งความสนใจไปยังแหล่งของข้อมูลที่ตรงกัน
- ตัวเก็บเนื้อหา (Content Store) ทำหน้าที่คล้ายกับบัฟเฟอร์ (buffer) ของเร้าท์เตอร์ไอพีแต่ต่างกันตรงที่การทับซ้อนความเป็นส่วนตัว แพ็คเก็ตไอพีขึ้นกับการติดต่อสื่อสารแบบพ้อยทูพ้อย ดังนั้นการส่งต่อหนึ่งครั้งจึงไม่มีประโยชน์นักอีกด้านหนึ่งแพ็คเกจซีซีเอ็นทั้งหมดที่อาจเป็นประโยชน์มากกว่าเนื่องจากมีมากกว่าหนึ่ง
- พีไอที (PIT : Pending Interest Table) : เก็บแทร็คของการส่งความสนใจไปยังแหล่งข้อมูล โดยที่โครงสร้างเหล่านี้อนุญาตให้แพ็คเกจข้อมูลย้อนกลับไปตามผู้ร้องขอ (คล้ายกับการระบุเส้นทางยูอาร์แอล (URL) ดังที่เห็นในโครงสร้างลำดับชั้น) ชื่อแต่ละตัวจะถูกแปลงเป็นหมายเลขของส่วนประกอบที่สามารถเข้ารหัสเพื่อความเป็นส่วนตัว



รูปที่ 6 แสดงการแปลงชื่อเป็นหมายเลข

สถาปัตยกรรมซีซีเอ็นรวมทั้งวิวัฒนาการกลไกความแตกต่างเช่นเดียวกับในเครือข่ายไอพีราวกับว่าเป็นกระแสและการควบคุมโดเมนภายนอกและโดเมนภายใน เส้นทาง ฯลฯ คุณสมบัติอื่น ๆ ของซีซีเอ็นคือความปลอดภัยอยู่ในข้อมูลของมันเองไม่ได้อยู่ในช่องของเครือข่ายดังเช่นอินเตอร์เน็ตในยุคปัจจุบันนี้ แทนที่จะเน้นไปทางด้านความปลอดภัยในโฮสต์และในการเชื่อมต่อการสื่อสารมันกลับเน้นด้านความปลอดภัยการเข้ารหัสในตัวเนื้อหาของมันเองเครือข่ายเท่านั้นที่เกี่ยวข้องกับวิธีการกระจายข้อมูลและการเผยแพร่การควบคุมความปลอดภัยของข้อมูล ผลที่ตามมาก็เล็งเห็นถึงเครือข่ายอินเตอร์เน็ตในอนาคตเป็นแหล่งจัดเก็บข้อมูลขนาดใหญ่รับรองความถูกต้อง

III. ผลการศึกษา

มุมมองการจัดการในอนาคตรูปแบบสถาปัตยกรรมที่พัฒนาโดยสมาคมสหภาพยุโรป (EU IST Autonomic Internet – AUTOI) การออกแบบการจัดการในอนาคต เป็นการบริการเครือข่ายที่รับการค้ำประกันในการสร้างความน่าเชื่อถือ ความทนทานและความคล่องตัว ในบริบทการเข้าถึง การรักษาความปลอดภัย การสนับสนุนการบริการและการจัดการตนเองในการติดต่อสื่อสารทรัพยากรและบริการการแก้ปัญหาในสถานการณ์อินเตอร์เน็ตในอนาคต

อินเตอร์เน็ตในอนาคตจะยึดเป็นเครือข่ายทั่วโลกที่จับความหลากหลายที่ครอบคลุมทั่วทั้งเทคโนโลยีเครือข่าย ความสามารถในอุปกรณ์และความต้องการของผู้ใช้ เครือข่ายที่มีลักษณะแพร่หลายและสนับสนุนอุปกรณ์และการเคลื่อนย้ายทรัพยากรและการตอบสนองความต้องการของผู้ใช้ที่มีความหลากหลาย การจัดการความซับซ้อนของ อินเตอร์เน็ตในปัจจุบันควรจะลดลงโดยใช้เทคนิคการจัดการอัตโนมัติ ที่ดำเนินการถือปฏิบัติโดยไม่ต้องเสียเวลา กับการทำงานแทรกแซงของคน ตัวอย่างเช่นองค์กรเครือข่ายที่แตกต่างกันสามารถปฏิบัติตามกฎระเบียบทั่วไปที่กำหนดโดยผู้ดูแลระบบในขณะที่การดำเนินงานการจัดการในระดับต่ำสามารถดำเนินการได้โดยอัตโนมัติในความสอดคล้องกับกฎเหล่านี้

กระบวนทัศน์ในการจัดการเครือข่ายสำหรับอนาคตอินเตอร์เน็ต ความท้าทายที่สำคัญมาก :

- การจัดการการเกี่ยวฟังก์ชั่นทำงานควรจะฝังการรู้บริการในเครือข่าย
- การจัดงานการจัดการตนเองเกี่ยวกับฟังก์ชัน โดยเฉพาะการเพิ่มประสิทธิภาพ องค์กร การกำหนดค่า การปรับตัว การรักษา การป้องกัน
- ฟังก์ชั่นการควบคุมการจัดการตนเอง โดยการตั้งค่าและเจรจาร่วมกัน / เป้าหมายที่ตกลงกัน
- ความตระหนักและฟังก์ชั่นการตรวจสอบเครือข่ายของตัวเองและบริบทการดำเนินงาน เช่นเดียวกับการเนินงานเครือข่ายเพื่อที่จะประเมินว่าเครือข่ายในปัจจุบันมีพฤติกรรมตอบสนองวัตถุประสงค์ของบริการ
- การปรับตัวและฟังก์ชั่นการปรับตัวเองเรียกการเปลี่ยนแปลงในดำเนินงานเครือข่าย (สถานะการตั้งค่าฟังก์ชั่น) ในฟังก์ชันของการเปลี่ยนแปลงในบริบทของเครือข่าย

- ฟังก์ชั่นอัตโนมัติด้วยตนเองเป็นวิธีการเปิดใช้งานการควบคุมโดยตนเอง (คือ Self - FCAPS) ของการดำเนินงานเครือข่ายภายใน
- การเขียนโปรแกรมแบบไดนามิคของฟังก์ชั่นการจัดการและการบริการที่อนุญาตให้เพิ่มฟังก์ชั่นใหม่โดยไม่ต้องรบกวนสิ่งที่อยู่ของระบบ คือ (UN) Plug และเล่นฟังก์ชั่นการบริการการจัดการความเรียบง่ายในการการจัดการฟังก์ชันเพื่อลดวงจรระบบการดำเนินงาน ค่าใช้จ่ายในและการปล่อยพลังงาน

วิวัฒนาการที่มีอยู่ในสถาปัตยกรรมในอนาคตหรือที่ปรากฏในขณะนี้การออกแบบบรอดแบนด์มีข้อตกลงในวงกว้างว่าจะต้องมีความสามารถในการจัดการเครือข่ายที่มีความสามารถในการจัดการเครือข่ายที่มีประสิทธิภาพและยังค่าใช้จ่ายต่ำ มีวิธีการจัดการเครือข่ายที่มีอยู่มักจะมีการควบคุมจากส่วนกลาง แต่การประสานงานข้ามโดเมนและการบริหารจัดการค่อนข้างเป็นไปได้ยาก อย่างไรก็ตามธุรกิจและหน่วยงานด้านนี้มีการเพิ่มขึ้นอย่างรวดเร็ว วิธีการที่มีอยู่แล้วไม่สามารถป้องกันได้และมีความซับซ้อนมากขึ้น ดังนั้นการเชื่อมโยงเครือข่ายที่แตกต่างกันจึงไม่เหมาะที่จะเปิดกว้างและยังมองไม่เห็นถึงสภาพแวดล้อมที่ยืดหยุ่นสำหรับในอนาคต

เพราะฉะนั้นปัญหาจากการจัดการเครือข่ายระบบศูนย์กลางการจะต้องค่อยๆ พัฒนาด้านความยืดหยุ่นและต้องปรับมูลค่าเครือข่ายให้เข้ากับในอนาคต วิธีการหนึ่งที่มีแนวโน้มที่เป็นการจัดการเครือข่ายอัตโนมัติ การจัดการเครือข่ายที่มีความยืดหยุ่นสูงกับสัญญาณระบบมีการยอมรับการค้นหาโดยอัตโนมัติตอบสนองข้อเสนอที่เหมาะสมหรือทรัพยากรที่ใช้หรือสภาพแวดล้อมที่เปลี่ยนแปลงและควบคุมหรือลดค่าใช้จ่ายที่จะเกิดขึ้น

อย่างไรก็ตามการจัดการโดยอัตโนมัติของงานที่กำหนดภายใต้สภาพแวดล้อมเดียว ในปัจจุบันการออกแบบของการดำเนินงานและระบบงานการสนับสนุนธุรกิจ เนื่องจากผู้ประกอบการส่วนใหญ่มีความต้องการที่จะรวมฟังก์ชั่นการทำงานที่ดีที่สุดในการจำลองแบบของในอนาคต ซึ่งผลในการประกอบการไม่สามารถจัดการได้อย่างมีประสิทธิภาพ เนื่องจากมีความซับซ้อนของระบบธุรกิจและการดำเนินงานที่เพิ่มขึ้น

ความท้าทายที่เราจะระบุมี 6 ทิศทางเป็นเทคนิคความท้าทายที่จะต้องตระหนักถึงวิสัยทัศน์ในการบริหารจัดการการสื่อสารอัตโนมัติ ทั้งนี้ต้องให้แน่ใจว่าการจัดการตนเองโดยอัตโนมัติมีการประสานงานข้ามขอบเขตของการจัดการการตั้งค่าระบบการจัดการควรกำหนดทรัพยากรเครือข่ายในเป้าหมายให้สอดคล้องกันทางธุรกิจ การจัดการควรสนับสนุนการจัดส่งแบบ end – to – end ของบริการนั้น ๆ

ซึ่งการจัดการอัตโนมัติเหล่านี้สามารถแบ่งความท้าทายออกเป็น 3 คู่และคู่การจัดการที่อยู่ในระดับสูงสุดที่เกี่ยวข้องกับสหพันธ์การบริหารจัดการ มีดังนี้

- สหพันธ์หลังการจัดการ
- การแมปปิ้ง (Mapping) ความหมายของสหพันธ์

ความท้าทายระดับกลางที่เกี่ยวข้องกับการตรวจสอบการบริการและการกำหนดค่า มีดังนี้

- การตรวจสอบระดับการบริการแบบ end – to – end
- การกำหนดค่าการขับเคลื่อนธุรกิจของเครือข่าย

ความท้าทายระดับล่างที่เกี่ยวข้องกับโครงสร้างพื้นฐานของเครือข่ายและการประสานงานการจัดการตนเอง มีดังนี้

- การจัดการตนเองและการนำกลับมาใช้ใหม่
- การประสานการจัดการตนเอง

ตารางที่ 1 เปรียบเทียบโปรโตคอลของระบบเครือข่าย (Network Protocols)

	SNMP	**CMIP**	**NETCONF**	**XMLP**
คุณลักษณะ	เครือข่ายดี	วิธีการแก้ปัญหาเกี่ยวกับปัญหาบนเครือข่ายโดยรวมและการจัดการระบบ	XML พื้นฐานไม่ได้ขึ้นอยู่กับชนิดของการส่งรวมถึงการแจ้งเตือน	XML พื้นฐานการแลกเปลี่ยนการจัดการโครงสร้าง
การจัดการวัตถุ	ตัวระบุวัตถุ	ความแตกต่างของชื่อ	-	การเชื่อมโยงมีความยืดหยุ่น
รูปแบบรายละเอียดของการจัดการวัตถุ	สัญลักษณ์ประเภทของวัตถุ	แนวทางในการนิยามการจัดการวัตถุ (GDMO)	-	-
โปรโตคอล	โปรโตคอลแบบไม่มีการสื่อสาร	โปรโตคอลการกำหนดการเชื่อม ต่อ	โปรโตคอลการกำหนดการเชื่อม ต่อ	โปรโตคอลแบบไม่มีการสื่อสาร
การทำงาน	GET,SET, GET-Next, TRAP	M-get, M-cancle-get, M-even-report, M-set, M-action, M-create, M-report	<get>, <get-config>, <edit-config>, <copy-config>, <delete-config>, <lock>, <unlock>, <close-session>, <kill-session>	GET, GET-Next, SET , Get-respons, TRAP

	SNMP	CMIP	NETCONF	XMLP
ความปลอดภัย	V1 : ง่ายต่อการโจมตี V2 : การรักษาความปลอดภัยที่อ่อนแอ V3 : รายละเอียดการเข้ารหัส	มีการรักษาความปลอดภัยที่ดี	-	มีการเข้ารหัส

ตารางที่ 2 ตารางการเปรียบเทียบข้อจำกัดของมัลติมีเดีย

ชื่อเรื่อง	ข้อดี	ข้อจำกัด
Deploying IP Multimedia Subsystem (IMS) Services in Future Mobile Networks[11]	บูรณาการระหว่าง IMS และ LTE / SAEได้รับการสำรวจและดู สามตัวเลือกสำหรับการให้บริการเสียงผ่าน LTE มีการทดลองเปรียบเทียบคุณภาพของการให้บริการ	-
Designing Networking Service for Multimedia Service Composition over Programmable Network Substrate[12]	การควบคุมในแนวราบแยกอัตโนมัติ แนวราบควบคุมนี้ประกอบด้วยสามส่วน i) ระบบปฏิบัติการเครือข่าย (เช่น NOX) ตั้งอยู่ในการควบคุมซอฟแวร์หลากหลาย ii) การประยุกต์ใช้เครือข่ายที่ทำงานบนระบบปฏิบัติการเครือข่าย iii) โปรโตคอล OpenFlow ที่ให้การเข้าถึงข้อมูลที่สวิทช์พื้นผิวเรียบและตารางการไหลภายในของพวกเขาตั้งค่าและสถิติ	-
Future U.S. Wireless Landscape and IMS Rollout[14]	มีการเปรียบเทียบตลาดระบบเครือข่ายไร้สายในสหรัฐอเมริกา	เป็นทฤษฎีการทดลองมากกว่าการนำมาใช้จริง และขาดมาตรฐาน IMS ในการใช้งาน

ชื่อเรื่อง	ข้อดี	ข้อจำกัด
A Novel Scalable Architecture for Efficient QoS to cater IMS Services for Handheld Devices based on Android[15]	มีการออกแบบที่มีประสิทธิภาพวิธีการทำงานภายในสถาปัตยกรรมเพื่อให้มั่นใจได้ง่ายขึ้น การขยายสำหรับสเปกตรัมกว้างของการใช้งาน จุดของผู้อื่นมุ่งเน้นการรักษาความปลอดภัยแบบ end - to - end เป็นเครื่องรักษาความปลอดภัยโทรศัพท์มือถือ	-
ENHANCED IP MULTIMEDIA SUBSYSTEM (IMS) FOR FUTURISTIC TACTICAL NETWORKS[16] FOR FUTURISTIC TACTICAL NETWORKS[16]	R - IMS จะมีความน่าเชื่อถือของระบบที่ดีกว่ามาตรฐานอย่างอื่น	-

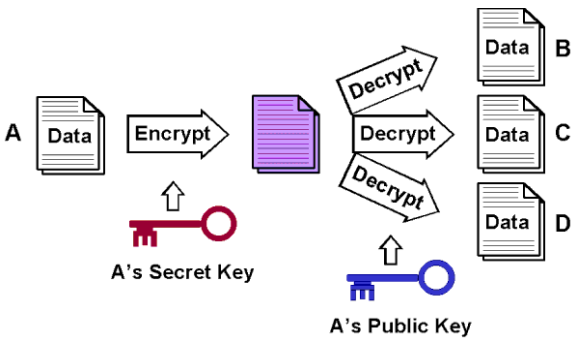
ตารางที่ 3 ตารางเปรียบเทียบงานวิจัยเกี่ยวกับมัลติมีเดีย

ชื่องานวิจัย	End to end	คุณภาพการให้บริการ	การจัดการด้านเวลา	การให้บริการในอนาคต
Deploying IP Multimedia Subsystem (IMS) Services in Future Mobile Networks[11]	✓	✓	✓	✓
Designing Networking Service for Multimedia Service Composition over Programmable Network Substrate[12]	✓	✓	-	✓
Future U.S. Wireless Landscape and IMS Rollout[14]	-	✓	-	
A Novel Scalable Architecture for Efficient QoS to cater IMS Services for Handheld Devices based on Android[15]	✓	✓	-	✓

ชื่องานวิจัย	End to end	คุณภาพการให้บริการ	การจัดการด้านเวลา	การให้บริการในอนาคต
ENHANCED IP MULTIMEDIA SUBSYSTEM (IMS) FOR FUTURISTIC TACTICAL NETWORKS[16]	✓	✓	-	✓

การเข้ารหัสข้อมูลหรือเอ็นคริพชั่น (Encryption) เป็นกลไกหลักสำหรับป้องกันข้อมูลที่มีอยู่ระหว่างการสื่อสาร ถ้ามีการเข้ารหัสที่ดีข้อมูลก็จะถูกป้องกันไม่ให้สามารถอ่านได้จากผู้ที่ไม่ประสงค์ดี อย่างไรก็ตามผู้ใช้ที่ส่งและรับจะต้องสามารถเข้าและถอดรหัสข้อมูลนั้นได้ สิ่งที่สำคัญของการเข้ารหัสก็คือคีย์ (Key) สำหรับการถอดรหัส

อย่างที่กล่าวไว้ในตอนต้นแล้วว่าโดยปกติข้อมูลที่รับส่งผ่านเครือข่ายนั้นจะอยู่ในรูปเคลียร์เท็กซ์ (Clear Text) ซึ่งข้อมูลนี้อาจถูกอ่านหรือคัดลอกโดยใช้เทคนิคที่เรียกว่าสนิฟเฟอริง (Sniffering) ดังนั้นเพื่อป้องกันข้อมูลที่รับส่งผ่านเครือข่ายจำเป็นต้องมีการเข้ารหัส การเข้ารหัสข้อมูลคือวิธีที่ใช้สำหรับแปลงเคลียร์เท็กซ์ให้มาอยู่ในรูปของไซเฟอร์เท็กซ์ (Cipher Text) หรือข้อมูลที่เข้ารหัสแล้ว ซึ่งข้อมูลนี้จะถูกส่งไปให้ผู้รับเมื่อผู้รับได้รับก็จะถอดรหัสข้อมูล (Decryption) เพื่อให้ได้ข้อมูลเดิม การเข้ารหัสและถอดรหัสข้อมูลเรียกว่า คริพโตกราฟี (Cryptography)



รูปที่ 7 ระบบการทำงานการเข้ารหัสข้อมูล

ปัญหาพื้นฐานหลายอย่างสำหรับการพัฒนาโดเมนระหว่างคุณภาพของการให้บริการเส้นทางโปรโตคอลในเครือข่ายแสงเราอธิบายวิธีการคำนวณได้รับการสนับสนุนคุณภาพของการให้บริการใด ๆ ระหว่างสองโหนดและในโดเมนที่ต่างกัน [5] กล่าวถึงแล้ววิธีการเลือกเส้นทางระหว่างโดเมนสำหรับได้รับการขอเชื่อมต่อระหว่างโดเมนกับความต้องการคุณภาพของการให้บริการเพื่อแก้ไขปัญหาและข้อจำกัดของเราติ้งที่เกิดขึ้นในปัจจุบัน นำไปสู่ยุคใหม่ของยุค อินเตอร์เน็ตในอนาคตโดยจะมีการนำเสนอแนวทางการแก้ไขปัญหาเราติ้งแบ่งแยกเป็นหัวข้อหลัก จากการศึกษางานวิจัยจำนวน 5 งานวิจัยแบ่งแยกออกเป็นตารางดังนี้

ตารางที่ 4 ตารางการเปรียบเทียบข้อจำกัดของงานวิจัย

ชื่องานวิจัย	ข้อดี	ข้อจำกัด
FIRMS: A Mapping System for Future Internet Routing. [36]	อธิบายแนวคิดใหม่ของการรักษาความปลอดภัยและประเมินความยืดหยุ่นของการค้นหาเส้นทางระบุเป็นหลักการออกแบบสำหรับเส้นทางสถาปัตยกรรมใหม่ที่ทำให้อินเตอร์เน็ตเส้นทางเพิ่มเติม สามารถปรับขนาดได้เพื่อค้นหาตำแหน่งของโฮสต์	มีการอ้างอิงผลการทดลองจากงานวิจัยอื่นไว้ในสรุป แต่ในงานวิจัย นี้ไม่มีการแสดงข้อมูลของการทดลองเพื่อเปรียบเทียบ
A Framework for Identifier-Based Routing for Future Internet[37]	มีการนำเสนอกรอบหลักการการกำหนดเส้นทางสำหรับอินเตอร์เน็ตในอนาคตรวมทั้งรูปแบบการออกแบบของส่วนประกอบหลักประการที่สามที่เรานำวิธีการบางอย่างเพื่อเพิ่มการรักษาความปลอดภัยและปรับปรุงประสิทธิภาพการเราติ้ง	ความยืดหยุดของการค้นหาเส้นทางและรูปแบบการจราจรแบบไดนามิค
Parameterized Gradient Based Routing (PGBR) for Future Internet[38]	ได้นำเสนอพีจีบีอาร์เส้นทางขั้นตอนวิธีการซึ่งเป็นลาดกระจายตามเส้นทางโปรโตคอลเทคนิคการค้นพบเส้นทางพีจีบีอาร์	ไม่ได้กล่าวถึงความน่าเชื่อถือทางด้านการแก้ปัญหาการดีเลย์ (Delay) ของการเราติ้ง
Towards a Scalable Routing Architecture For Future Internet. [39]	แสดงให้เห็นว่าสถาปัตยกรรมที่นำมาเสนอมีความยืดหยุ่นที่มากและความน่าเชื่อถือกว่าอินเตอร์เน็ตในปัจจุบัน	-

ชื่องานวิจัย	ข้อดี	ข้อจำกัด
Hierarchical QoS Routing in Next Generation Optical Networks[40]	กล่าวถึง มาตรฐานคุณภาพการให้บริการ ใน hierarchical optical ของการขอเชื่อมต่อและการค้นหาเส้นทางในลักษณะการแปลงความยาวคลื่นสัญญาณรวมทั้งการวิเคราะห์อย่างเป็นทางการและการทดลองแบบจำลองของเราแสดงให้เห็นว่าการกำหนดเส้นทางโปรโตคอลของเรามีประสิทธิภาพดีกว่าที่มีอยู่โปรโตคอลและเป็นสัญญาณสำหรับรุ่นต่อไปออปติคอลเครือข่ายรวมถึงการกล่าวถึงสุตรการคำนวน	-

ตารางที่ 5 ตารางเปรียบเทียบงานวิจัยเกี่ยวกับเราติ้งในอนาคต

ชื่องานวิจัย	การรักษาความปลอดภัย	การเพิ่มประสิทธิภาพของการเราติ้ง	การเสนอแนวทางด้านสถาปัตยกรรม	การนำเสนอมีความยืดหยุ่นของเราติ้ง
FIRMS: A Mapping System for Future Internet Routing.[36]	✓	✓	✓	✓
A Framework for Identifier-Based Routing for Future Internet[37]	✓	✓	✓	-
Parameterised Gradient Based Routing (PGBR) for Future Internet[38]	-	✓	✓	✓
Towards a Scalable Routing Architecture For Future Internet[39]	-	-	✓	✓
Hierarchical QoS Routing in Next Generation Optical Networks[40]	-	✓	-	-

สถาปัตยกรรมไซโล (SILO) มีความยืดหยุ่นสูงและขยายต่ออย่างไร้ข้อจำกัด สนับสนุนสถาปัตยกรรมแบบครบวงจรที่ปรับขนาดได้ และยังเชื่อมต่อข้ามเซอร์วิส (cross-service) ที่ชัดเจนเพื่อเพิ่มประสิทธิภาพ นอกจากนั้นยังสนับสนุนการเพิ่มประสิทธิภาพผ่านการเลือกฮาร์ดแวร์

สถาปัตยกรรมการบริการเป็นแนวคิดในการพัฒนาสถาปัตยกรรมไอทีขององค์กรให้เป็นแบบเชิงบริการ เพื่อที่จะทำให้ระบบไอทีในองค์กรสามารถเชื่อมโยงกันได้การพัฒนาสถาปัตยกรรมการบริการสามารถทำได้หลายวิธีและเว็บเซอร์วิสเป็นวิธีหนึ่งที่เหมาะสม การพัฒนาระบบสถาปัตยกรรมการบริการจำเป็นที่จะต้องมีเครื่องมือในการพัฒนาที่สำคัญที่สุดคือต้องมีอีเอสบีเพื่อเชื่อมโยงระบบไอทีต่างๆโดยผ่านอะแดปเตอร์ ซึ่งจะเห็นได้ว่าการเชื่อมโยงที่ดีอาจไม่จำเป็นต้องแปลงระบบเดิมมาสู่เว็บเซอร์วิสทั้งหมดทั้งนี้เพราะอะแดปเตอร์สามารถติดต่อกับโมดูลเดิมที่อาจใช้โปรโตคอลอื่นได้ การพัฒนาสถาปัตยกรรมการบริการมีต้นทุนที่ค่อนข้างสูงและจำเป็นต้องมีทีมงานที่เข้าใจธุรกิจเฉพาะนั้น ๆ แต่ผลตอบแทนระยะยาวจะคุ้มค่ามาก

สถาปัตยกรรมซีซีเอ็นรวมทั้งวิวัฒนาการกลไกความแตกต่างเช่นเดียวกับในเครือข่ายไอพีราวกับว่าเป็นกระแสและการควบคุมเส้นทางโดเมนภายนอกและโดเมนภายใน ฯลฯ คุณสมบัติอื่นๆของซีซีเอ็นคือความปลอดภัยอยู่ในข้อมูลของมันเองไม่ได้อยู่ในช่องของเครือข่ายดังเช่นอินเตอร์เน็ตในยุคปัจจุบันนี้ แทนที่จะเน้นไปทางด้านความปลอดภัยในโฮสต์และในการเชื่อมต่อการสื่อสารมันกลับเน้นด้านความปลอดภัยการเข้ารหัสของในตัวเนื้อหามันเอง

เครือข่ายเท่านั้นที่เกี่ยวข้องกับวิธีการกระจายข้อมูลและการเผยแพร่การควบคุมความปลอดภัยของข้อมูล ผลที่ตามมาก็เล็งเห็นถึงเครือข่ายอินเตอร์เน็ตในอนาคตเป็นแหล่งจัดเก็บข้อมูลขนาดใหญ่รับรองความถูกต้อง ดังตารางที่ 4

ตารางที่ 6 ตารางเปรียบเทียบซีซีเอ็น ไซโลและสถาปัตยกรรมการบริการ

	CCNx	SILO	SOA
การจัดสรรทรัพยากรที่มีความยืดหยุ่น	สูง	สูง	สูง
การรักษาความปลอดภัยและความเป็นส่วนตัว	สูง(การเข้ารหัสข้อมูลของตัวเอง)	ดี, โดยรวมราบรื่น	ต่ำ
ความคุ้มค่า	-	-	สูง
คุณภาพการให้บริการแบบ End-to-End	-	✓	✓
ความคล่องตัว	-	✓	-
ความเชื่อถือได้	-	-	✓
การเชื่อมต่อออกจากเครือข่าย	✓	✓	✓
การสนับสนุนการเพิ่มประเภทของบริการ	✓	✓	✓
การขยายขนาดของเครือข่าย	เล็ก	เล็ก,ใหญ่	เล็ก

เปรียบเทียบความแตกต่างและวิวัฒนาการของอินเตอร์เน็ต [19]

สาระสำคัญเรื่องการออกแบบโครงสร้างสถาปัตยกรรมของระบบการสื่อสารทางอินเตอร์เน็ต (Design and architecture of the Internet) เป็นเรื่องที่ผู้คนสนใจอภิปรายกันตลอดหลายปีที่ผ่านมาซึ่งมักจะมีวัตถุประสงค์ดังนี้

- **Connection of existing networks :** เพื่อเชื่อมต่อกับเครือข่ายที่มีอยู่แล้วได้
- **Survivability :** เพื่อให้สามารถดำรงอยู่ได้

- **Support of multiply types of services :** เพื่อสนับสนุนการบริการที่หลากหลาย

- **Accommodation of a variety of physical networks :** เพื่อปรับตัวเครือข่ายเข้ากับกายรูปที่หลากหลาย

- **To allow distributed management :** เพื่อให้เกิดการบริหารจัดการเผยแพร่แบ่งปัน

- **Cost-effecttiveness :** เพื่อให้มีค่าใช้จ่ายสมเหตุสมผล

- **To allow for host attachment with a low level of effort :** เพื่อให้เกิดแม่ข่ายคอมพิวเตอร์ได้ง่ายขึ้นโดยไม่ต้องใช้ความพยายามมากนัก

- **To allow for resource accountability :** เพื่อให้เกิดแหล่งข้อมูลที่ตรวจสอบได้เพื่อให้บรรลุเป้าประสงค์ดังกล่าว องค์ประกอบที่สำคัญของการออกแบบโครงสร้างสถาปัตยกรรมของระบบการสื่อสารทางอินเตอร์เน็ตระหว่างคอมพิวเตอร์ ดังที่เคยใช้กันมาคือ

- **Layering :** การจัดเรียงลำดับชั้นของภาพดิจิทัล

ผลกระทบต่อการออกแบบโครงสร้างสถาปัตยกรรมทางอินเตอร์เน็ตในอนาคต [32]

- **The Commercial Internet :** ในอนาคตจะมีการใช้อินเตอร์เน็ตในเชิงธุรกิจการค้าอย่างเข้มข้นมากยิ่งขึ้น โดยการลงทุนในเครือข่ายการค้าทางอินเตอร์เน็ตจะมีมูลค่าสูงถึงหลายร้อยล้านดอลล่าต่อปีทีเดียว จะมีการให้บริการลูกค้าหรือการทำธุรกิจในรูปแบบต่าง ๆ ผ่านทางอินเตอร์เน็ตมากยิ่งขึ้น จึงจำเป็นต้องมีการเพิ่มความเร็วของการรับส่งข้อมูลทำให้ผู้คนต้องการการออกแบบโครงสร้างสถาปัตยกรรมทางอินเตอร์เน็ตยุคใหม่ที่มีความเหมาะสมทันต่อการเปลี่ยนแปลงและเพิ่มประสิทธิภาพในการทำธุรกิจการค้าทางอินเตอร์เน็ตได้มากขึ้น

-**The Mobile Internet :** ในอนาคตจะมีการเติบโตอย่างรวดเร็วของระบบโทรศัพท์เคลื่อนที่ โดยโทรศัพท์เคลื่อนที่จะมาแทนที่คอมพิวเตอร์ส่วนบุคคล (PC : Personal Computer) ในการเข้าถึงหรือเชื่อมต่อระบบเพื่อใช้งานอินเตอร์เน็ตในประเทศที่เจริญแล้วผู้คนจะนิยมใช้โทรศัพท์เคลื่อนที่เป็นหลักในการเข้าถึงสิ่งที่พวกเข้าต้องการในอินเตอร์เน็ต เทคโนโลยีของโทรศัพท์เคลื่อนที่จึงมีการเปลี่ยนแปลงเร็วมาจาก 2 ไปยัง 2.5G และจาก 3G ไปยัง 3.5G และกำลังจะไปถึง 4G การออกแบบโครงสร้างสถาปัตยกรรมทางอินเตอร์เน็ตยุคใหม่ต้องมีความเหมาะสม เพื่อให้การรับส่งข้อมูลระหว่างกันเป็นไปได้อย่างรวดเร็วมากยิ่งขึ้น

บนอินเตอร์เน็ตจะมีความแตกต่างกันของแต่ละเครือข่ายจะมีอุปกรณ์ในการค้นเส้นทาง 2 อย่าง คือเอทีเอ็มสวิตช์จะเชื่อมต่อแบบการกำหนดการเชื่อมต่อสวิตช์และการเชื่อมต่อแบบไม่มีการเชื่อมต่อจะเป็นเราเตอร์ การเชื่อมต่อแบบกำหนดการเชื่อมต่อสวิตช์จะรับรองแบนด์วิดธ์ได้และมีระยะเวลาการส่งที่สั้นเพราะจะมีการค้นหาเส้นทาง การเชื่อมต่อจะเป็นในลักษณะกำหนดการเชื่อมต่อสวิตช์ เช่นสามารถที่จะส่งแบบแพ็คเกจมัลติมีเดียเบส (multimedia-based packets)

ตารางที่ 7 ตารางเปรียบแต่ละงานวิจัย

ชื่องานวิจัย	ข้อดี	ขีดจำกัด
An Overlap Virtual Networks Testbed for Future Real-Time Multimedia Transmission	1. สามารถตรวจสอบการจราจรบนเครือข่ายได้ 2. สามารถตรวจสอบเส้นทางเดินได้และเส้นทางเดินที่สั้นที่สุด 3. สามารถที่จะตรวจสอบหาเส้นทางแบบ load balance	1. ในการทำ load balance จะช้าตอนค้นหา 2. บางครั้งอาจจะเกิดความล่าช้าในการส่งแพ็คเกจ 3. ต้นทุนสูง
Next - Generation Broadband Switching Router System Architecture for Future Multimedia-oriented Internet: Design and Analysis	1. มีการส่งการกำหนดการเชื่อมต่อสวิตช์และการเชื่อมต่อแบบไม่มีการเชื่อมต่อ 2. MPEG2 และ MPEG4 และจะมีการนำเทคโนโลยี VRML virtual มาใช้ 3. การเชื่อมต่อทางโทรศัพท์จะเป็นแบบ demand-oriented	1. เอทีเอ็มสวิตช์ไม่มีการบล็อคเครือข่ายจากเครือข่ายภายใน 2. หากมีเราเตอร์หลายตัวจะมีการเดินทางหลาย ๆ ฮ็อปอาจจะมีความผิดพลาด 3. เครื่องแม่ข่ายต้องมีความจุมาก
The Flexibility of ATM: Supporting Future Multimedia and Mobile Communications	1. การรองรับเครือข่ายบรอดแบรนด์ 2. การเชื่อมต่อลักษณะเครือข่ายโทรศัพท์เป็นอัตโนมัติ 3. ส่งได้ทั้งภาพและเสียงที่รวดเร็ว	1. ต้องการความเร็วในการส่งสูง 2. สายต้องที่เชื่อมต่อต้องรองรับ 3. มีการควบคุมที่ซับซ้อน
Multimedia: Future and Impact for Semiconductor Technology	1. เครือข่ายมีประสิทธิภาพที่สูงขึ้น2. มีการนำเทคโนโลยี leading-edge เข้ามาใช้ 3. ประสิทธิภาพของมัลติมีเดียสูงขึ้น	1.บางครั้งใช้เวลาในการประมวลผลที่นาน 2. อัลกอริทึมมีความซับซ้อน 3. มีการประมวลผลเป็น signal processing
WCDMA-The Radio Interface for Future Mobile Multimedia Communications	1. รองรับย่านความถี่สูงๆ ได้ 2. WCDMA radio รองรับ higher rate services 3. มีการประมวลที่รวดเร็ว 4. รองรับเทคโนโลยี capacity improving	1. มีการลงทุนที่สูง 2. โทรศัพท์มือถือต้องรองรับกับระบบ 3. มีปัญหาในย่านความถี่

การแยกสามารถสนับสนุนบริการข้ามแดนอัตโนมัติทั่วโลก ผู้ให้บริการที่ไร้พรมแดน และผู้ให้บริการการพกพาที่มีการระบุสถานที่อิสระที่สำคัญความท้าทายในงานสถาปัตยกรรมการแยกนี้ไอดี/แอลโอซีนี้เป็นวิธีการการออกแบบระบบการทำแผนที่เป็นผู้จัดการสถานที่ซึ่ง จัดเก็บและรักษาความผูกพันระหว่างการระบุ MNS และการระบุตำแหน่งปัจจุบันของพวกเขา บทความนี้เสนอปรับขนาดได้ และมีประสิทธิภาพสูงผ่าน ระบบการทำแผนที่ การทำแผนที่ การกระจาย ที่นำเสนอระบบ ประกอบด้วยจำนวนของต้นไม้สามระดับ ระบบย่อยบนเซิร์ฟเวอร์

เพื่อประเมินประสิทธิภาพของการทำแผนที่ที่เสนอระบบในแง่ของการสนับสนุน การเคลื่อนไหวของการเสนอโครงการการจัดการสถานที่ รวมถึงสถานที่ปรับปรุง การเรียกการส่งมอบ และสร้างการวิเคราะห์ แบบที่ได้ผลลัพธ์ที่เป็นตัวเลขแสดงให้เห็นว่าระบบการทำแผนที่ที่นำเสนอมีประสิทธิภาพสามารถลดค่าใช้จ่ายในการส่งสัญญาณ และการสนับสนุนผู้ใช้สูงมาก ความหนาแน่น เมื่อเทียบกับที่มีอยู่สถาปัตยกรรม LISP - DNS

IV. สรุปผลการศึกษา

เมื่อประเมินแนวโน้มของอินเตอร์เน็ตในอนาคต ทั้งในด้านการออกแบบโครงสร้างสถาปัตยกรรมของอินเตอร์เน็ตและผลกระทบจากอินเทอร์เนตในอนาคตต่อบริบทต่างๆ เช่น สังคม การเมืองและเศรษฐกิจ จากเนื้อหาบทความข้างต้นสามารถอนุมานได้ว่าอินเตอร์เน็ตในอนาคต คือสรรพสิ่งอัจฉริยะ (Internet of Things) เทคโนโลยีอาร์เอฟไอดีจะสาและมารถรับระบบตัวเลขที่ไม่ซ้ำกัน เช่นไอพีเวอร์ชั่น 6 ซึ่งจะทำให้วัตถุแต่ละชิ้นมีลักษณะเฉพาะและมีที่อยู่ส่วนตัว ชิ้นส่วนอัจฉริยะจะสามารถดำเนินชุดของกิจกรรมที่แตกต่างกัน โดยขึ้นอยู่กับสภาวะแวดล้อม และขึ้นอยู่กับภาระงานที่พวกมันถูกออกแบบขึ้นมาเพื่อกระทำการนั้นๆ ซึ่งไม่มีขีดจำกัดของกิจกรรม และสามารถควบคุมวัตถุอัจฉริยะนี้ได้อย่างมีประสิทธิภาพ อาทิเช่นวัตถุเหล่านี้สามารถที่จะถูกติดตามการเคลื่อนย้ายได้โดยตรง สามารถปรับตัวเชื่อมต่อกันเป็นเครือข่ายกับสิ่งแวดล้อมด้วยตัวเองได้ ดูบำรุงรักษาตนเองได้ ซ่อมแซมด้วยตนเองได้และกำจัดตนเองได้อีกด้วย [18] ทำให้อินเตอร์เน็ตสามารถเข้าถึงตัวผู้คนได้แทบทุกหนทุกแห่งโลกจะอยู่ในยุคที่คอมพิวเตอร์แทรกซึมอยู่เกือบทุกอณูในชีวิตและผู้คนจะใช้อินเตอร์เน็ตทำงานแทนหลายต่อหลายอย่าง จนบางครั้งเราแทบไม่รู้สึกเลยว่ามีมันอยู่อินเตอร์เน็ตเหมือนกระแสไฟฟ้าที่เรามองไม่เห็นสัมผัสไม่ได้ตราบที่มันยังทำงานเป็นปกติจะสังเกตเห็นได้ก็เฉพาะตอนเสียตัวคอมพิวเตอร์เองก็เลือนรางเต็มที เมื่อมันถูกเชื่อมโยงกับอุปกรณ์สื่อสารแบบพกพา เช่น โทรศัพท์มือถือหรือเครื่องเล่นเกมอินเตอร์เน็ตจะแนบสนิทอยู่ในทุกสรรพสิ่งแวดล้อม รอบตัวผู้คนจนแยกกันไม่ออกตัวอย่างระบบสิ่งแวดล้อมอัจฉริยะ[1] อาทิเช่น หากมีใครคนหนึ่งกำลังลดน้ำหนักเครื่องชั่งน้ำหนักตู้เย็นและเตาไมโครเวฟภายในบ้านซึ่งเชื่อมต่อกันด้วยระบบเครือข่ายไร้สาย สรรพสิ่งที่อยู่รอบตัวคนที่จะสื่อสารเชื่อมโยงถึงกัน เช่นเตาไมโครเวฟจะไม่ยอมทำงานหรือบางทีบริษัทประกันสุขภาพอาจยื่นจดหมายพร้อมคำขาดให้ลดอาหารหรือเฝ้าติดตามดูอยู่ห่างๆ ว่าเจ้าของกรมธรรม์ ประกันสุขภาพนั้นได้ปฏิบัติตามข้อบังคับของกรมธรรม์หรือไม่จะเห็นได้ว่าความเป็นส่วนตัวกับความต้องการเฉพาะตัวส่อเค้ามีความขัดแย้งกันให้เห็นเพื่อให้การพัฒนา เทคโนโลยีไปไกลถึงในระดับที่คำว่า “อินเตอร์เน็ตในสรรพสิ่ง” จะสื่อความหมายถึงสิ่งแวดล้อมอัจฉริยะ เทคโนโลยีหรือนวัตกรรมที่เกี่ยวข้องต้องได้รับการบริหารจัดการ สร้างมาตรฐานและพัฒนาศักยภาพในด้านต่างๆ เพื่อให้เกิดการแลกเปลี่ยนข้อมูลระหว่างวัตถุได้ การแพร่หลายของเครือข่าย (The Ubiquitous Network) ถือเป็นสิ่งที่จำเป็นอย่างยิ่งต่อการพัฒนาในแนวทางนี้ [18]

เรื่องความมั่นคงปลอดภัยข้อมูล กลายเป็นเรื่องสำคัญสำหรับการบริหารจัดการระบบสารสนเทศที่ดีและมีประสิทธิภาพ ระบบสารสนเทศที่มีเสถียรภาพสูงควรสามารถป้องกันการโจมตีจากแฮกเกอร์หรือมัลแวร์ต่างๆ ได้เป็นอย่างดี วัตถุประสงค์หลักขององค์กรก็การรักษา ความลับ,การรักษาความสมบูรณ์,ความพร้อมใช้งาน (CIA : Confidentiality, Integrity และ Availability) ให้กับระบบสารสนเทศขององค์กร ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และ การทำให้ระบบมีความมั่นคงและมีเสถียรภาพในการให้บริการอย่างต่อเนื่อง (Availability)

ดังนั้นความเกี่ยวข้องกับเรื่อง การบริหารจัดการระบบความมั่นคงปลอดภัยข้อมูล จึงเป็นเรื่องที่ผู้บริหารทุกองค์กรไม่สามารถหลีกเลี่ยงได้ ในปัจจุบันองค์กรขนาดใหญ่ได้แยกแผนกรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศออกจากแผนกเทคโนโลยีสารสนเทศ เพื่อความคล่องตัวในการบริหารและการแบ่งแยกอำนาจหน้าที่รับผิดชอบให้เกิดความชัดเจน รวมทั้งในอนาคตองค์กรควรจะต้องมีแผนกอย่างน้อย 3 แผนกคือ แผนกไอที (Information Technology : IT) หรือระบบสารสนเทศเพื่อการบริหาร (MIS : Management Information System) แผนกการรักษาความปลอดภัยในเทคโนโลยีสารสนเทศ (IS) และแผนกผู้ตรวจสอบภายในไอที (IT Internal Audit) ร่วมมือกันทำงานและ ตรวจสอบซึ่งกันและกัน

ซึ่งในอนาคตของวงการความปลอดภัยข้อมูล คุณสมบัติและข้อกำหนดทั้งฮาร์ดแวร์ ซอฟแวร์และบุคลากร (People ware) ที่เกี่ยวกับเรื่อง "การรักษาความปลอดภัยในสารสนเทศ" นั้นอาจจะถูกบรรจุไว้ในผลิตภัณฑ์ และ ถูกรวมเข้ากับบริการของผู้ให้บริการ (Service Provider) ไปโดยปริยาย เพราะในอนาคตจะมองว่า การรักษาความปลอดภัยในสารสนเทศก็คือโครงสร้างพื้นฐาน เช่น เมื่อซื้อรถยนต์มาก็ควรมีระบบเบรค ABS และ ระบบ AIRBAG ติดมากับรถยนต์โดยลูกค้าไม่ต้องจ่ายเพิ่มโดยลูกค้าในอนาคตจะไม่อยากจ่ายเพิ่มในเรื่อง "การรักษาความปลอดภัยในสารสนเทศ" ที่ลูกค้าเองมองว่าควรจะฟรีมีอยู่แล้วในการให้บริการของ Service Provider ในอนาคตเราอาจจะเห็นการรวมกันของบริษัทเทคโนโลยีสื่อสารคมนาคมกับบริษัทผู้เชี่ยวชาญด้านความปลอดภัยข้อมูลอีกหลายราย

จากค่านิยม ที่เปลี่ยนไปดังกล่าว ทำให้ผู้ให้บริการเกี่ยวกับระบบเทคโลยีสารสนเทศและผู้ให้บริการด้านอินเตอร์เน็ตทั่วไป จำเป็นต้องมีคุณลักษณะด้านความปลอดภัยของข้อมูล (Information Security Feature) ที่ภายใน (Built-In) ถูกรวมเข้าไว้ในระบบและบริการของผู้ให้บริการ หรือ Service Provider โดยอัตโนมัติ ซึ่งจะทำให้มีข้อได้เปรียบเหนือคู่แข่งที่ไม่มีคุณลักษณะด้านความปลอดภัยของข้อมูล ดังกล่าวตลอดจนยังรักษาฐานลูกค้าให้เกิดความ Royalty กับบริการของผู้ให้บริการอีกด้วย

REFERENCES

[1] Sung-Su Kim, Young J. Won,and and John Strassner," Towards Management of the Future Internet", 2009.

[2] Du Jiangyi and Niu Yan, "The Design and Implementation of Multifunction Probe Based on SNMP", 2009 IITA International Conference on Control, Automation and Systems Engineering, pp 434-436, 2009.

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

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

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

[6] 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.

[7] Jürgen Schönwälder, Marc Fouquet, Gabi Dreo Rodosek and Iris C. Hochstatter, "Future Internet = Content + services + Management", 2009 IEEE Communications Magazine, 2009, p. 27 – 33.

[8] 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.

[9] 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.

[10] 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.

[11] Keyurkumar J. Patel, S. Vijay Anand, Suman Kumar S.P. A Novel Scalable Architecture for Efficient QoS to cater IMS Services for Handheld Devices based on Android Fourth International Conference on Next Generation Mobile Applications, Services and Technologies, 2010.

[12] A. Oredope, V. Pham, B. Evans, Deploying IP Multimedia Subsystem (IMS) Services in Future Mobile Networks, Centre for Communications Systems Research (CCSR), University of Surrey, Guildford, 2011.

[13] Zhiwei Van, Huachun Zhou, Hongke Zhang, Sidong Zhang. A Novel Mobility Management Mechanism Based On an Efficient Locator/ID Separation Scheme. Beijing Jiaotong University, China, 2009.

[14] Namgon Kim and JongWon Kim, Designing Networking Service for Multimedia Service Composition over Programmable Network Substrate, International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2010.

[15] Sherry Wang and Harold Zheng, ENHANCED IP MULTIMEDIA SUBSYSTEM (IMS) FOR FUTURISTIC TACTICAL NETWORKS, The Johns Hopkins University /Applied Physics Laboratory, 2008.

[16] Fuchun Joseph Lin, Future U.S. Wireless Landscape and IMS Rollout, Mobile Networking Research Telcordia Technologies Piscataway, NJ 08854, 2009.

[17] Feng Qiu,Miao Xue and Homgke Zhang,'A DISTRIBUTED MAPPING SYSTEM TO SUPPORT MOBILITY IN IDENTIFIER/LOCATOR SEPARATION ARCHITECTURE" on Proceeding of IC-NIDC 2009,pp. 280- 285.

[18] Jie Hou,Yaping Lui and Zhenghu Gong, "Support Mobility for Future Internet",Telecommunication Network Strategy and Planing Sympsium (Network),2010 14th International, 27-30 Sep 2010.

[19] Ved P.Kafel,Hideki Ostuki and Masugi Inoue, "AN ID/LOCATOR SPLIT ARCHITECTURE OF FUTURE NETWORKS" Innovation for Digital Inclusion,2009 ITU,pp.1-8.

[20] Jaeyong Choi,Chulhyun Park and Yanghee Choi, "Addressing in Future Internet: Problems, Issues and Approaches".

[21] Rebahi Y, Tcholtchev N, Chaparadza R, Merekoulias V.N, "Addressing Security Issues in the Autonomic Future Internet.", Inst for Open Commun Syst, FOKUS Fraunhofer, Berlin, Germany, 12 May 2011,pp. 517-518.

[22] H. Bos E. Jonsson, "Anticipating Security Threats to a Future Internet", Chalmers University, 2008.

[23] Dijiang Huang, Shingo Ata, and Deep Medhi, "Establishing Secure Virtual Trust Routing and Provisioning Domains for Future Internet", Arizona State University, USA, Osaka City University, Japan, University of Missouri–Kansas City, USA, 6 Dec 2010, pp.1-6.

[24] GAN Gang, LU Zeyong, JIANG Jun,"Internet of Things Security Analysis", School of Computer Science, Chengdu University of Information Technology, Chengdu 610225, P.R. China, 30 Aug 2011, pp. 1-4.

[25] Sampigethaya K, Poovendran R, "Security, Privacy and Trust in the Future Internet", Networked Syst Technol (NST), Boeing Res & Technol, Bellevue, WA, USA,4 Jan 2011, pp. 1-6.

[26] Meland P.H, Guerenabarrena J.B, Liewellyn-Jones D, "The Challenges of Secure and Trustworthy Service Composition in the Future Internet ", Software Eng, Safety & Security, SINTEF ICT, Trondheim, Norway, 27 June 2011, pp. 329-334.

[27] Sandra Dominikus, Manfred Aigner, Stefan Kraxberger, "Passive RFID Technology for the Internet of Things", Institute for Applied Information Processing and Communications, Graz University of Technology, 2009.

[28] Jianqing Zhang1, Nikita Borisov1, William Yurcik2, Adam J. Slagell2, and Matthew Smith3, "Future Internet Security Services Enabled by Sharing of Anonymized Logs", 1 University of Illinois at Urbana-Champaign, 2 National Center for Supercomputing Applications, 3 University of Marburg, 2009.

[29] Krishna Sampigethaya 1, Radha Poovendran 2, "Security and Privacy of Future Aircraft Wireless Communications with Offboard Systems", 1Networked Systems Technology (NST), Boeing Research & Technology, Bellevue, USA, 2 Network Security Lab (NSL), EE Department, University of Washington, Seattle, USA, 2008.

[30] Hayriye Altunbasak1, Henry Owen2, "Security Inter-layering for Evolving and Future Network Architectures", 1Scientific Atlanta (A Cisco Company, 5030 Sugarloaf ParkwayLawrenceville, GA, 2 School of Electrical and Computer Eng.Georgia Institute of Technology Atlanta, Georgia.

[31] Mario Golling and Björn Stelte, "Requirements for a Future EWS - Cyber Defence in the I", Universität der Bundeswehr, Faculty of Computer Science, D-85577 Neubiberg, Germany, 2011.

[32] María Alduán1, Federico Álvarez, Theodore Zahariadis, N. Nikolakis, F. Chatzipapadopoulos, David Jiménez and José Manuel Menéndez, "Architectures for Future Media Internet", Industrial and Information Systems, 2008, p.3.

[33] Rudra Dutta, George N. Rouskas Ilia Baldine Arnold Bragg, Dan Stevenson, "The SILO Architecture for Services Integration, controL, and Optimization for the Future Internet", ICC, 2007, pp.1-6.

[34] Paul Mueller, Bernd Reuther, Markus Hillenbrand, "Future Internet Architecture: A Service-Oriented Approach".

[35] Huhns, M.N., Singh, M.P., "Service-oriented computing: key concepts and principles ", Internet Computing, 2005, pp.75-81

[36] Michael Menth, Matthias Hartmann, and Michael Höfling,"Mapping System for Future Internet Routing", University of Würzburg, Institute of Computer Science Germany,page(s) : 1326 - 1331, October 2010.

[37] Jie Hou, Yaping Liu, Zhenghu Gong, "A Framework for Identifier-Based Routing for Future Internet",China, page(s): 579 – 584,2009.

[38] Sasitharan Balasubramaniam, Dmitri Botvich, Julien Mineraud, William Donnelly Balasubramaniam, S., Botvich, D., Mineraud, J., Donnelly, W.,"Parameterised Gradient Based Routing (PGBR) for Future Internet" Ireland, Page(s): 58 – 65,2009.

[39] Huaming Guo, Shuai Gao, Hongke Zhang,"Towards a Scalable Routing Architecture For Future Internet" China, Page(s): 261 – 265 ,2009.

[40] Ronghui Hou, King-Shan Lui, Fred Baker and Jiandong Li ,"Hierarchical QoS Routing in Next Generation Optical Networks", China, page(s): 2129 – 2138, 1 Aug 2010.