Department of Computer Science; Faculty of Science, KhonKaen University

CourseNo: cs322766

Course Name: Computer Networks

Delay Tolerant And Opportunistic Networking

Student Name/Last Name:

นายกษิดิศ วิจิตรโสภณ 555020116-4

นายจักรกฤษณ์ แก้วโยธา 555020118-0

นายฤทธิ์ ลาวพนม 555020128-7

นายสหรัถ หินกอง 555020130-0

นายธนกุล ปักกาเวสา 555020178-2

นายณัฐพล แก้วมาตย์ 555020174-0

นายวัชรพงษ์ ภูมาตย์ 555020196-0

Submission Date: 6/10/2011

Consent: -

Survey on OSPF Routing Protocol

สาขาเทคโนโลยีสารสนเทศ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

บทคัดย่อ—การกำหนดเส้นทาง Protocol คือ OSPF –Open Short Path Firstซึ่ง OSPF นี้ก็คือวิธีการบอกเส้นทางของเราเตอร์ที่เป็นพื้นฐานของ IGP (Internet Gateway Protocol) บน Internetนอกจากนี้ OSPF ยังถูกนำมาใช้สำหรับการแพร่กระจาย Router Node ของเครือข่ายอย่างกว้างขวาง การพัฒนาด้านเทคโนโลยีเครือข่ายทำให้มีการเปลี่ยนแปลงเกิดขึ้นทุกปี รูปแบบอันมากมายของ Protocol มีการใช้อย่างแพร่หลายรวมทั้งการมีปรับปรุงแก้ไขให้มีประสิทธิภาพดีขึ้นอยู่ตลอดซึ่งช่วยให้ขั้นตอนของการชี้เส้นทางทำได้ดีขึ้น โครงสร้างเส้นทางของ Domain มีการเปลี่ยนแปลงเพื่อให้ทันกับเหตุการณ์ปัจจุบัน ด้านการดูแลรักษาค่อนข้างมีความปลอดภัยสูง ดังนั้น OSPF จึงมีความรวดเร็วในการเปลี่ยนแปลงเส้นทางที่เกิดขึ้นใหม่หากOSPFไม่สามารถเปลี่ยนแปลงเส้นทางได้ก็ยังมีความยืดหยุ่นและอัตราการขยายเส้นทางเพื่อให้เกิดการสมดุลกันมากที่สุด

keyword-OSPF, OSPF Routing Protocol,

I.บทนำ

หากพูดถึงเส้นทางที่ดีที่สุดเราคงต้องพูดถึงเส้นทางที่สั้นที่สุดในการรับและส่งไฟล์ OSPF เป็นGateway เส้นทาง Protocol เช่น Protocolเส้นทางการทำงานในDomainซึ่งโดยทั่วไปแม้ว่าจะไม่จำเป็นต้องมีอยู่ในระบบ ในระบบเครือข่ายที่สมบรูณ์แต่ละเครือข่ายผู้ดูแลระบบต้องรู้เกี่ยวกับโครงสร้างของระบบเพื่อเพิ่มความยืดหยุ่นหรือการขยายตัวของเครือข่ายในอนาคต OSPF ช่วยให้การจัดการเรื่องการกำหนดเส้นทาง Domainที่จะแบ่งออกเป็นหลายเส้นทางซึ่ง Router ต้องรู้โครงสร้างที่สมบรูณ์ของเส้นทางเหล่านั้น และในส่วน Interface เป็นการเชื่อมโยงเส้นทาง Protocol เพื่อให้ครอบคลุมต่อการใช้งาน

การใช้งานInternet ทุกวันนี้ได้แพร่กระจายไปอย่างรวดเร็วและครอบคลุมในทั่วทุกที่ การหาเส้นทางการเชื่อมต่อของ Router ด้วยวิธีการแบบ OSPF จึงได้มีการนำมาใช้งานอย่างแพร่หลาย รวมทั้งมีการพัฒนาประสิทธิภาพของ OSPF อย่างต่อเนื่อง เช่น การปรับปรุงในส่วนของของการดำเนินการค้นหาเส้นทางและปริมาณการให้บริการการในด้านการตอบสนองของ Qosบนพื้นฐานโครงสร้างของการกำหนดเส้นทางรวมถึงการเปลี่ยนแปลงของเส้นทางเมื่อเวลาผ่านไป ในช่วงปีแรก OSPF มีการนำวัตถุประสงค์ในการกำหนดเส้นทางมาทำให้ OSPF สามารถขยายเส้นทางด้วยตนเองได้เป็นการเพิ่มขีดจำกัดของการประมวลผล ในการใช้ Internetเมื่อมีการร้องขอ Protocol จะมีความจำเป็นรองลงมาในเหตุการณ์ที่มีการล่มของสัญญาณชั่วขณะที่ให้บริการOSPFจะมีการกู้สัญญาณให้ใหม่อย่างทันท่วงที เป็นการให้บริการเครือข่ายตลอดเวลา การพัฒนาด้านอื่นๆ และการป้องกันปริมาณการใช้ Internet จึงเป็นการปรับปรุงความเร็วในการค้นหาเส้นทางที่ยังใช้งานได้อยู่ของOSPF

การทำงานของระบบ OSPF เมื่อการเปลี่ยนแปลงของ Topology มีการรวมตัวกันรวมทั้งข้อกำหนดที่สำคัญด้านโครงสร้างมีขีดจำกัดในด้านการประมวลผลหรือปริมาณการใช้ Internet เกินกว่าขีดจำกัดของเส้นทางProtocolนั้น OSPF สามารถทำได้ก่อนการร้องขอที่จะเกิดการกระจายของProtocol ได้ทันเวลา การดำเนินการ อื่นๆ เช่น การประมวลผลของPacket โดย Router เพื่อให้แน่ใจว่า Router ไม่ได้ทำงานหนักเกินหากมีการทำงานหนักเกินไปอาจทำให้เกิดการทำงานที่มากเกินกว่าหน้าที่ที่ Router จะต้องทำ Router สมัยใหม่ทุกวันนี้มีการกระจายโครงสร้างของการประมวลผลเส้นทางของProtocol และการจัดส่ง Protocol Packet การประมวลผลจะเริ่มจากการพิจารณาในส่วนหัวของ Packet และเส้นทางที่ระบุประเภทการขยายตัวของ Protocol พร้อมการให้ความสำคัญในเรื่องของขนาดเส้นทางDomain ถึงแม้ว่าCPU ของRouter จะมีความสามารถมากขนาดไหนก็ตาม การเพิ่มขนาดและเพิ่มความซับซ้อนของโครงสร้าง Domain ก็จะทำให้เกิดเหตุการณ์ที่CPU จะต้องทำงานหนักเกินความจำเป็นได้

ในPaper นี้เราเสนอเกี่ยวกับการสำรวจรายละเอียดของข้อเสนอแนะจากหลายๆ Paper เพื่อวิเคราะห์ความเหมาะสมในการใช้งานของเครือข่าย การลดขั้นตอนการประมวลผลของ CPU ในการทำงานของ OSPFRouter Protocol แบบไร้สายที่ระบบมีขนาดใหญ่ อย่างไรก็ตาม ทุกวันนี้โครงสร้างของเส้นทางมีการเพิ่มขึ้นจำนวนมาก ทั้งอุปกรณ์ และเรื่องของสัญญาญที่มีการขยายตัวมากขึ้น ไม่ว่า

ที่ไหนในตอนนี้ก็มีสัญญาณWireless การเรียกใช้งาน OSPFRouting Protocol ถึงแม้ว่าลำดับของเส้นทางจะถูกออกแบบมาในรูปของ MANETs การใช้งานที่แตกต่างกันของเส้นทางตามที่ MANETs ร้องขอมาเมื่อมีการแลกเปลี่ยนเส้นทางหรือข้อมูลที่ซับซ้อนระหว่าง OSPF และProtocol ซึ่งอาจไม่สามารถหลีกเลี่ยงเส้นทางที่จะช่วยลดปริมาณงานลงได้เพื่อให้ MANETs สามารถทำงานได้อย่างถูกต้อง ในPaper นี้นำเสนอข้อคิดเห็นที่จำเป็นอย่างยิ่งในการเพิ่มประสิทธิภาพให้กับOSPF เพื่อเพิ่มขีดความสามารถให้สามารถทำงานได้ดีขึ้น

Faster Failure Detection
Faster and Fewer Adjacency Establishments
Optimizing LSA Generation and Flooding
Optimizing Routing Table Calculations

รูปที่ 1 ขั้นตอนหลักในการปรับปรุงความสเถียรและความเร็วการค้นหาเส้นทางของOSPF:

รูปที่ 1 แสดงให้เห็นถึงขั้นตอนหลักที่กล่าวถึงในPaper นี้เกี่ยวกับการConvergence ของOSPF โดยได้ปรับปรุงและขยายขีดความสามารถ ในส่วนที่เหลือของPaper นี้มีการจัดระเบียบดังนี้ส่วนที่II. CONVERGENCE TO A TOPOLOGY CHANGE IN OSPF: AN OVERVIEWเป็นการแสดงภาพรวมของกระบวนการConvergenceในส่วนต่อมาเราอธิบายรายละเอียดแต่ละขั้นตอนในกระบวนการ Convergenceและยังกล่าวถึงข้อเสนอต่างๆเพื่อเพิ่มประสิทธิภาพการดำเนินการในแต่ละขั้นตอนส่วนที่III. FASTERFAILUREDETECTION IN OSPFอธิบายถึงความล้มเหลวและกลไกการตรวจสอบความแล้มเหลวที่ใช้ในเครือข่ายของOSPF: โดยที่การส่ง Hello Packet เป็นการเริ่มต้นการทำงานของ Protocol นำมาใช้ในการตรวจสอบความล้มเหลวของ Software ตลอดจนความล้มเหลวจากHardwareในการตรวจสอบกลไกที่พร้อมจะเชื่อมโยงบางเทคโนโลยีระดับLink-Layerในส่วนที่ III. FASTERFAILUREDETECTION IN OSPFนี้ยังอธิบายถึงการเชื่อมต่อแบบสองทิศทางด้วยการส่งต่อPacketและการตรวจสอบ (BFD) ซึ่งเป็นProtocolที่สามารถตรวจเจอข้อบกพร่องของเส้นทางผิดพลาดระหว่างอุปกรณ์เครือข่ายที่สองได้อย่างรวดเร็ว

II. CONVERGENCE TO A TOPOLOGY CHANGE IN OSPF:AN OVERVIEW

OSPF เป็นProtocolในการค้นหาสถานะเส้นทางแต่ละ Interface แต่ละRouter เพื่อทำการเชื่อมโยงเครือข่ายเข้าด้วยกันอย่างสมบูรณ์ โดยที่OSPF ให้บริการในการแบ่งDomain เส้นทางได้หลายเครือข่าย ดังแสดงในรูปที่ 2, เครือข่ายในเส้นทางDomain ของOSPF จะจัดไว้ในศูนย์กลางที่เป็นเครือข่ายพิเศษที่เรียกว่าเครือข่ายที่ 0 หรือบริเวณ Backbone ทำหน้าที่เป็นศูนย์กลางและมีเครือข่ายอื่นๆที่เชื่อมต่อจากบริเวณBackbone ทุกเส้นทางจากเครือข่ายใดเครือข่ายหนึ่งไปยังปลายทางในเครือข่ายอื่นต้องผ่านบริเวณBackbone ดังแสดงในรูปที่ 2 Router อาจมี Interface ในหลายเครือข่ายRouter บางตัวเป็นที่รู้จักกันในชื่อ Area Border Routers (ABRs)และRouter บางตัวเป็นที่รู้จักกันในชื่อ Autonomous System Boundary Routers(ASBRs) ซึ่งอาจมีLink ไปยัง Router ในระบบอิสระอื่นๆในรูปที่ 2 มีการแยกเส้นทางแต่ละ Domain เข้าไปในเครือข่ายหลายจุด ช่วยให้Router ที่จะต้องขอข้อมูลโครงสร้างเส้นทางที่สมบูรณ์ของเครือข่ายเฉพาะเหล่านั้นที่เป็นเจ้าของ Interface ในต่อไปนี้เราจะอธิบายถึงเรื่องวิธีการของRouter อื่นๆในบริเวณใกล้เคียงและในท้ายที่สุดRouter (และการเชื่อมต่อภายในInterconnections) ในเครือข่ายที่เชื่อมต่อRouterสำหรับคำอธิบายรายละเอียดด้านต่างๆในการดำเนินงานของ OSPF ขอแนะนำให้ศึกษาต่อจาก *OSPF: Anatomy of an Internet Routing Protocol*[10] และ*OSPF Network Design Solutions, Second Edition*[11]

Router ที่ใช้งาน Protocol ในรูปแบบ OSPF ด้วยInterface ในการกระจายของระบบLANs หรือแบบPoint-To-Point บอกถึงRouter ที่อยู่ใกล้เคียงที่ผ่านการแลกเปลี่ยนข้อความโดยการส่งข้อความ HelloMulticastsOSPF Router เริ่มต้นทำงานโดยการส่งHello packet ที่บรรจุข้อมูลต่างๆไว้เช่นRouter ID, รายชื่อ Router ใกล้เคียง (Neighboring) ซึ่งจะไม่มีค่าใดๆเมื่อเริ่มต้นOSPF Router นอกจากจะส่งHello Packet แล้วยังคอยรับHello Packet จากRouter อื่นด้วยเมื่อฝ่ายส่งและรับทำงานได้สอดคล้องกันจะเป็นการสร้างเส้นทางการติดต่อกันRouterที่เป็นAdjacencyจะทำการส่งข้อมูลLSDB ไปกับ Database Description Packet ด้วยSequence ค่าหนึ่งการทำงานนี้จะเป็นการแลกเปลี่ยนข้อมูลด้วยความสัมพันธ์แบบMaster/Slave เมื่อ Router ได้รับข้อมูลจะนำข้อมูลที่ได้นั้นมาเปรียบเทียบกับข้อมูลเดิมที่มีอยู่และจะร้องขอเมื่อพบว่าตัวเองไม่มีข้อมูลใดหรือข้อมูลที่มีอยู่เก่าไปแล้วโดยการส่งLink State Request Packetซึ่ง Link State

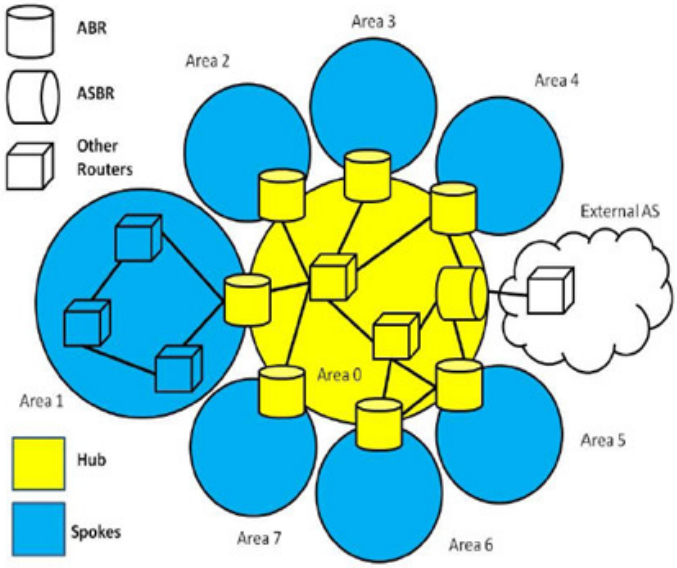
Update Packet จะเป็นResponse ของLink State Request Packet เพื่อเป็นการบอกข้อมูลล่าสุดเมื่อRouter ที่ได้รับทำการปรับปรุงข้อมูลตัวเองแล้วจะส่งLink State Acknowledge กลับไปหลังจากที่ได้สร้าง Adjacency แล้วแต่ละRouter จะยังคงส่งPeriodic Hello Packet อยู่เรื่อยๆเพื่อเป็นการตรวจสอบว่าRouter เพื่อนบ้านนั้นยังคงอยู่หรือไม่

การเริ่มต้นกระบวนการของการ Synchronizeฐานข้อมูลสถานะการเชื่อมโยงLSDBsระหว่าง Router ข้างเคียงความสมบูรณ์ของการ SynchronizeLSDB ผลลัพธ์ในRouter ของความต่อเนื่องกันการพิจารณากับเพื่อนบ้านB จนเต็มณจุดนี้ Router A สร้างLSAของ Router ใหม่พร้อมกับรายการสถานะความต่อเนื่องกันของ Interface ทั้งหมด

นั้นสำหรับRouter ที่อยู่ในเครือข่ายเดียวกัน (เป็นการเชื่อมโยงระหว่างตัวเองและ Router เพื่อนบ้านB)และส่งLSAออกจาก Interface เมื่อ Router เพื่อนบ้านได้รับLSA นี้มันจะส่งต่อ LSA ออกมาจากทุก Interface ในเครือข่ายยกเว้นจุดใดจุดหนึ่งที่LSA ได้รับดังนั้นLSA จะกระจายไปเต็มทั่วทั้งเครือข่ายกระบวนการรั่วไหลของข้อมูลและความน่าเชื่อถือโดยการกำหนดให้Router อื่นใช้รูปแบบLSAของการเป็นRouter ที่เชื่อมต่อที่อยู่ใกล้กันถ้ามันไม่ได้รับการรับรองของLSAจากRouter ข้างเคียงภายในบางช่วงเวลานั้น ดังนั้นแต่ละRouter ในเครือข่ายที่ได้รับการรับรอง LSAของ Router อื่นๆและได้รับข้อมูลเกี่ยวกับRouter ใกล้เคียง การที่RouterA ได้สร้างการเชื่อมต่อกับ Router อื่นๆอย่างต่อเนื่องจนเต็มเครือข่าย Router ทั้งสองที่อยู่ติดกันตราบใดที่ Router เหล่านั้นสามารถแลกเปลี่ยนข้อความHello เป็นระยะๆความต่อเนื่องในการติดต่อระหว่างกันจะลดลงเมื่อ Router เกิดการล้มเหลว ซึ่งจะต้องได้รับข้อความHello จาก Router ข้างเคียงภายในระยะเวลา RouterDeadIntervalที่เกิดขึ้นนี้หากการเชื่อมโยงระหว่างRouter นั้นๆกับ Router ข้างเคียงเกิดการล้มเหลวหรือหากRouter ข้างเคียงไม่สามารถทำงานได้ในบางกรณีProtocol Layer ของการเชื่อมโยงก็จะสามารถทำการแจ้งไปยัง Router อื่นๆเกี่ยวกับความล้มเหลวของการเชื่อมโยง

ดังนั้นRouter จึงอนุญาตให้ทำการยกเลิกการส่งข้อความ Hello สำหรับการสิ้นสุดความต่อเนื่องในการเชื่อมต่อกันโดยไม่ต้องรอให้ RouterDeadIntervalหมดอายุและการแบ่งรายละเอียดเพื่อสร้างLSA ของข้อความที่ต่อเนื่องกันทำให้RouterDeadInterval หมดอายุ

LSAของเราเตอร์รุ่นใหม่นี้เป็นการทำให้เกิดการรั่วไหลของข้อมูลตลอดจนเครือข่ายเพื่อแจ้งให้Router ทั้งหมดในเครือข่ายทราบเกี่ยวกับการแบ่งความต่อเนื่องกันเมื่อRouter ได้รับการรับรองLSA ใหม่จะมีการคำนวณตารางเส้นทางใหม่และทำการส่งต่อข้อมูล



รูปที่ 2 เครือข่าย Hub และ Spokes บนโครงสร้าง OSPF

พื้นฐานโดยรวมแล้วการConvergence และการเปลี่ยนTopology ในProtocolOSPFประกอบด้วย:

•การตรวจหาการเปลี่ยนTopology โดยRouter

•การตั้งค่าความต่อเนื่องกันหรือการแบ่งเส้นทางโดยRouter ได้รับผลกระทบจากการเปลี่ยนแปลงของTopology

•การสร้างLSAs ใหม่โดยRouter ที่ได้รับผลกระทบและการ Flooding ข้อความ HelloไปยังทุกๆNodeในเครือข่ายOSPF

•ตารางคำนวณเส้นทางของแต่ละRouter ในการรับการรับรอง LSAs ตามด้วยการแจกแจงของตารางเส้นทางการปรับปรุงการรับรองของ LSAs

การหน่วงเวลาConvergence โดยรวมขึ้นอยู่กับเวลาที่จำเป็นต้องทำให้เสร็จในแต่ละขั้นตอนที่ถูกกล่าวถึงในส่วนต่อไปนี้จะอธิบายแต่ละขั้นตอนเหล่าและจากการศึกษางานวิจัยที่ตีพิมพ์ล่าสุดในการลดความล่าช้าหรือการประมวลผลที่เกี่ยวข้องกับการปรับขั้นตอนให้เหมาะสม

III. FASTERFAILUREDETECTION IN OSPF

ในส่วนนี้เราอธิบายถึงความล้มเหลวที่เป็นไปตามธรรมชาติในเครือข่ายIP ซึ่งจะอธิบายถึงค่าเริ่มต้นของกลไกการตรวจสอบความล้มเหลวที่ใช้ในOSPF - The Hello Protocol และข้อเสนอที่ผ่านมาซึ่งสรุปไว้ในตารางที่ 1 เพื่อเพิ่มความรวดเร็วในกระบวนการตรวจสอบความล้มเหลวรวมทั้งการตรวจสอบการส่งต่อแบบสองทิศทาง

A.The Nature of Failures in IP Networks

ความล้มเหลวเป็นเหตุการณ์ปกติในเครือข่ายIP ความล้มเหลวที่ชั้นIPอาจเกิดขึ้นเนื่องจากการดำเนินงานการบำรุงรักษาเครือข่ายที่เกิดการล้มเหลวของHardware และ Software ในRouter ที่ผิดพลาดรวมถึงความผิดพลาดที่เกิดจากการกระทำของมนุษย์เช่นข้อผิดพลาดในการกำหนดค่าProtocol หรือความล้มเหลวในเครือข่ายพื้นฐานใยแก้วนำแสงความล้มเหลวอาจแสดงขึ้นที่ชั้นIP เป็นความล้มเหลวแบบเดี่ยวหรือหลายๆลิงค์ตัวอย่างเช่นFaulty Line Card จะทำให้เกิดความล้มเหลวของการเชื่อมโยงIP เดียวแต่การตัดสายเส้นใยแก้วนำแสงจะทำให้การเชื่อมต่อทั้งหมดทุกๆIP ที่อยู่บนสายFiber นั้นล้มเหลวในทำนองเดียวกันการรีบูตระบบปฏิบัติการในRouter จะส่งผลกระทบเพียงRouter เดียวแต่ถ้าไฟดับในPointof Presence(PoP) อาจจะทำให้เกิดผลกระทบต่อทุกๆRouter ที่อยู่ในนั้นบางครั้งความผิดพลาดของHardware และSoftwareอาจส่งผลให้Flapping Behavior จากหนึ่งการเชื่อมโยงหรือมากกว่านั้นในRouter เกิดการล้มเหลวอย่างต่อเนื่องสำหรับช่วงระยะเวลาที่มีการขยายเส้นทางซึ่งส่งผลกระทบอย่างรุนแรงในข้อมูลการจราจร (Traffic) [12], [13].

ช่วงก่อนการกำหนดหรือดำเนินการบำรุงรักษาแบบเร่งด่วนเช่น Router Reconfigurations อัพเกรด Software และการแทนที่ Hardware ส่วนที่เก่าเกินไปLabovitzและคณะ [14]ตรวจสอบความล้มเหลวเมื่อขนาดของRegional IP Backbone ในปี 1998 และแสดงความล้มเหลวในการดำเนินงานบำรุงรักษาเครือข่ายMarkopoulou และคณะ [15] ศึกษาความล้มเหลวในSprint's IP Backbone ในปี 2002และพบเพียง 20% ของความล้มเหลวที่เกิดจากเหตุการณ์การบำรุงรักษาMedemและคณะ [16] ปี 2005-2007 วิเคราะห์ข้อมูลความล้มเหลวสำหรับInternet2 เครือข่ายจาก 11 Router และIP Backbone ขนาดใหญ่ประกอบด้วย Router จำนวนหลายร้อยตัวและพบว่า 72% ของความล้มเหลวในInternet2และ25%ความล้มเหลวในIP Backboneขนาดใหญ่เป็นเพราะการดำเนินงานบำรุงรักษาเครือข่าย

Mechanism	Advantage	Disadvantage
การตรวจสอบความล้มเหลวของ Hardware	พบความล้มเหลวภายใน 10 มิลลิวินาที	ไม่สามารถใช้ได้ตลอด
HelloIntervalลดลง	ปลอดภัยและจะลดลงไปครึ่งหนึ่งในช่วงที่สอง	ลดลงและอาจนำไปสู่เราเตอร์overloads และการเตือนภัยที่ผิดพลาด
การตรวจสอบการส่งต่อแบบสองทิศทาง	Protocol อิสระสามารถใช้ในการเชื่อมโยงกับการลดHelloIntervalเพื่อลดเวลาการตรวจสอบความล้มเหลว	ไม่สามารถตรวจสอบความล้มเหลวในการควบคุมให้เป็นไปตามแผน

ตารางที่ 1 การปรับปรุง OSPF ให้เร็วขึ้นและการจำแนกข้อมูลที่สร้างขึ้นเพียงเล็กน้อย

Hardware จำพวก Router ที่ได้รับรายงานความผิดพลาดเป็นแหล่งสำคัญของความล้มเหลวในเครือข่ายIP [12]-[16]ในปี 1998 การศึกษาโดยLabovitzและคณะ [14] เผยว่า 40% ของ Router Interfaceประสบความล้มเหลวเฉลี่ยภายใน40 วันกับ 5% ของ Interface ที่ล้มเหลวโดยเฉลี่ยภายใน 5 วันปี2002การศึกษาโดย Markopoulouและคณะ[15]พบว่าเกือบ 70% ของความล้มเหลวที่ไม่ได้วางแผนแก้ไขไว้นั้นเนื่องจาก Single Linkเกิดการล้มเหลวเป็นเพราะความผิดพลาดหรืออาจเป็นเพราะอายุของAgeing Interface Cards ข้อสังเกตเพิ่มเติมระบุว่าเพียง 2.5% ของการเชื่อมโยงเป็น

สัดส่วนกว่าครึ่งหนึ่งของความล้มเหลวเหล่านี้ปี2005-2007การศึกษาของMedemและคณะแสดงผลลัพท์ 8% ของความล้มเหลวโดยทันทีในInternet2 และพบเกือบ 47% ของความล้มเหลวที่ไม่ได้วางแผนแก้ไขในLarge IP Backbone ของ Hardware จำพวก Router ที่ผิดพลาด

ในปีล่าสุดSoftware ที่เกี่ยวข้องกับปัญหาการกำหนดค่าได้เป็นสาเหตุสำคัญของความล้มเหลวในเครือข่าย IPLabovitzและคณะแสดงให้เห็นผลลัพท์เพียง 1.3% ของความล้มเหลวที่ปัญหาจาก Software อย่างไรก็ตามMarkopoulouและคณะแสดงผลลัพท์ที่มากกว่าคือ 16.5% ของความล้มเหลวที่ไม่ได้วางแผนแก้ปัญหาที่จะเกิด Router Crashes ขึ้นMedemและคณะแสดงเกือบหนึ่งในสามของความล้มเหลวทั้งหมดจากSoftware ที่เกี่ยวข้องกับปัญหา

ความล้มเหลวในชั้นOptical Fiberเป็นสาเหตุสำคัญของความล้มเหลวอื่นๆในระดับ IPส่วนหนึ่งของความล้มเหลวที่ไม่ได้วางแผนแก้ปัญหาประกอบกับปัญหาเครือข่าย Optical ในช่วง 10ถึง 15% ในการศึกษาที่ตีพิมพ์ [14] [15] Ganjaliและคณะในปี 2003 ได้ทำการศึกษาเกี่ยวกับ Sprint's IP Backbone โดยตั้งข้อสังเกตว่า 84% ของความล้มเหลวของการเชื่อมโยงที่มีผลกระทบต่อประสิทธิภาพของเครือข่ายเกิดจากการมีปัญหาที่ OpticalLayer

B.The Hello Protocol

Hello Protocol ให้ค่าเริ่มต้นของกลไกที่ทำให้เกิดความล้มเหลวและมีการตรวจสอบในOSPF โดยที่ OSPF RouterจะรักษาInactivity Timer สำหรับแต่ละเครือข่ายข้างเคียงก็มีการจัดตั้งFull Adjacency ด้วย เมื่อเราเตอร์ได้รับข้อความHelloจาก Nodes ที่อยู่ข้างเคียงมันจะResetInactivityTimer ที่เกี่ยวข้องกับ Nodes ที่อยู่ข้างเคียงการจัดตารางการไล่ลบเส้นทางการเชื่อมต่อออกหลังจาก RouterDeadIntervalเกิดการหมดอายุRouterDeadIntervalโดยทั่วไปจะมีจำนวนการส่งข้อมูลสี่ครั้งในHelloIntervalเมื่อเครือข่ายข้างเคียงมีการเชื่อมโยงระหว่างRouterและ Router จะไม่ได้รับข้อความ Hello เป็นระยะๆจาก Nodes ที่อยู่ข้างเคียงดังนั้นInactivity Timer จะไล่RouterDeadIntervalออกหลังจากได้รับการส่งข้อความHello ล่าสุดจาก Nodes ที่อยู่ข้างเคียงการไล่ลบเส้นทางการเชื่อมต่อออกของ Inactivity Timer จะทำให้Router ที่อยู่ใกล้ชิดกันยุติการเชื่อมต่อกับ Nodes ที่อยู่ข้างเคียงและสร้างRouterLSA ใหม่ทั้งนี้ขึ้นอยู่กับความล้มเหลวเมื่อเกิดขึ้นหลังจากได้รับข้อความHello ล่าสุดจากเครือข่ายที่อยู่ข้างเคียงRouter อาจใช้เวลาใดก็ได้ระหว่าง 3-4HelloIntervalsที่จะหยุดการติดต่อกันและให้ทำการตรวจสอบความล้มเหลวค่าเริ่มต้น 10 วินาทีสำหรับ HelloIntervalและควรกำหนด RouterDeadInterval40 วินาทีและRouter จะใช้เวลาใดก็ได้ระหว่าง 30 และ 40 วินาทีสำหรับRouter ในการตรวจสอบความล้มเหลว

เทคโนโลยีบางHardware เช่น Packet บน SONET [19] ให้ตรวจสอบการเชื่อมโยงของความล้มเหลวภายในไม่กี่10มิลลิวินาทีโดยการส่ง Routerที่สุดท้ายของทั้งสองการเชื่อมโยงที่เกิดการสูญเสียของสัญญาณข้อความ Helloในการรับสัญญาณดังกล่าวRouterจะรอระยะเวลาCarrier Delayก่อนที่จะให้ทำที่OSPF Carrier Delay ช่วยให้ Routerหลีกเลี่ยงการเตือนภัยที่ผิดพลาดและช่วยระบุ Link Flapping อย่างไรก็ตามการตรวจสอบความล้มเหลวของ Hardware ที่ใช้ไม่สามารถทำได้ทุกครั้ง

มีหลายข้อเสนอเพื่อลด HelloIntervalและด้วยเหตุนี้ RouterDeadIntervalจะลดเวลาการตรวจสอบความล้มเหลว Alaettinogluและคณะ [20] เสนอลดHelloIntervalที่ช่วงมิลลิวินาทีเพื่อให้บรรลุการตรวจสอบความล้มเหลวมีความกังวลเกิดขึ้นในหลายกฎเกณฑ์ที่จะลดHelloIntervalที่มีค่าขนาดเล็กมากความกังวลแรกคือจำเป็นที่จะต้องทำการส่งและรับข้อความHello ทุกครั้งหลังจากไม่กี่มิลลิวินาทีซึ่งจะทำให้CPU ของRouter ตัวนั้นเกิดการโหลดงานเพิ่มมากขึ้นความกังวลนอกจากนั้นก็คือว่า RouterDeadIntervalที่มีขนาดเล็กมากอาจส่งผลให้มีการเตือนภัยที่ผิดพลาดบ่อยมากขึ้น เนื่องจาก HelloIntervalที่มีขนาดเล็กมีโอกาสที่จะไปเพิ่มความแออัดของเครือข่ายและจะนำไปสู่การสูญเสียหรือการประมวลผลของหลายๆข้อความHelloที่ล่าช้าทำให้มีการสร้างLSA ขึ้นเนื่องจากFalse Alarm Lead เพื่อคำนวณเส้นทางใหม่ของตาราง False Alarmคือการทำการแก้ไขทันทีที่มีการแลกเปลี่ยน–ข้อความ Helloที่ประสบความสำเร็จในการรับส่งระหว่างRouter ที่ได้รับผลกระทบซึ่งเป็นสาเหตุให้ Router เหล่านี้จะต้องสร้างการติดต่อซึ่งกันและกัน แล้วสร้างLSA ใหม่โดย LSAใหม่เหล่านี้จะบังคับให้ Router ทั้งหมดในเครือข่ายทำการคำนวณตารางเส้นทางอีกครั้งดังนั้นการเตือนที่ผิดพลาดทำให้เกิดการเปลี่ยนแปลงชั่วคราวในเส้นทางTraffic ของเครือข่ายรวมทั้งเกิดภาระการประมวลผลที่ไม่จำเป็นบนRouterการเปลี่ยนแปลงเส้นทางของ Traffic อาจมีผลกระทบรุนแรงในการรับส่งข้อมูลตั้งแต่QoSหากเส้นทางการเปลี่ยนแปลงอาจจะมีความล่าช้าอย่างมีนัยสำคัญและลักษณะการ

สูญเสียอาจจะเป็นเพราะความแออัดที่เกิดจากการเปลี่ยนแปลงของตัวเองมากกว่าเส้นทางเดิม

BasuและRiecke [21] ดำเนินการจำลองการวิเคราะห์ตามผลกระทบของการแบ่งหรือการSub Second ค่าของ HelloInterval และรายงานว่าการลดHelloInterval500msหรือ 250msไม่ก่อให้เกิดการโหลดเพิ่มขึ้นของCPU อย่างไรก็ตามพวกเขาไม่สังเกตเห็นการเพิ่มขึ้นเป็นหกเท่าในจำนวนของRoute Flaps ที่เกิดจากการเตือนภัยที่ผิดพลาดในขณะที่HelloIntervalจะลดลงจาก 500msกับ 250msChoudhuryและคณะ [22], [23] ตั้งข้อสังเกตว่าการลดHelloIntervallowersThreshold(ในแง่ของจำนวนLSAs) ที่LSA ออกมาจะนำไปสู่การสร้างการเตือนภัยที่มีความผิดพลาดLarge LSA Burst Scan จะเกิดจากจำนวนปัจจัยเช่นการฟื้นฟูโดยพร้อมเพรียงกันของLSAsจำนวนมากๆGoyalและคณะ[24] ตั้งข้อสังเกตว่าความถี่ของการเตือนภัยที่มีความผิดพลาดในเครือข่ายที่เพิ่มขึ้นจนถึงระดับที่เกิดความแออัดของเครือข่ายและการเพิ่มขึ้นในจำนวนของการเชื่อมโยงในเครือข่ายดังนั้นทางออกที่ดีที่สุดสำหรับการรับและส่งHelloIntervalในเครือข่ายขึ้นอยู่กับความทนทานของเครือข่ายสำหรับความถี่ในการเตือนภัยที่ผิดพลาดโดยที่จะไม่เกินระดับความแออัดที่คาดหวังและจำนวนของการเชื่อมโยงในโครงสร้างเครือข่าย

C.Bidirectional Forwarding Detection (BFD)

การตรวจสอบการสูญเสียของการเชื่อมต่อระหว่างสองอุปกรณ์ที่อยู่ภายในเครือข่ายเดียวกันได้อย่างรวดเร็วคือข้อกำหนดทั่วไปสำหรับระบบเครือข่ายหลาย Protocol [25] บ่อยครั้ง Protocol ไม่ได้มีกลไกในระดับ Native Mechanism สำหรับวัตถุประสงค์นี้ Native Mechanism ไม่สามารถตรวจสอบความล้มเหลวได้อย่างรวดเร็วพอยกตัวอย่างเช่นในกรณีของOSPF Native Mechanism (Hello protocol) ไม่สามารถทำให้ช่วงมิลลิวินาทีตรวจหาความล้มเหลวพบอีกตัวอย่างหนึ่งคือการใช้LSP-Ping [26] Mechanism ในการตรวจสอบความผิดพลาดในLabel Switched Path (LSP)ในMulti-Protocol Label Switching(MPLS) จำนวน 4เครือข่ายการประมวลผลที่จำเป็นสำหรับLSP-Ping Messages ถือว่ามีความสำคัญมากและด้วยเหตุผลนี้ความถี่ของการรับส่งข้อความดังกล่าวไม่สามารถเพิ่มกฎเกณฑ์เพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบให้ได้พบความล้มเหลวของเครือข่ายอย่างรวดเร็ว

การตรวจสอบการส่งต่อแบบสองทิศทาง (BFD) วัตถุประสงค์ทั่วไปของ Light Weight Protocol คือการตรวจสอบความผิดพลาดของเส้นทางการเชื่อมต่อแบบสองทิศทางระหว่างอุปกรณ์สองอุปกรณ์บนเครือข่ายที่อาจเกิดขึ้นอย่างรวดเร็ว [29] BFD ทำงานเป็นอิสระจาก Protocol อื่นๆและตรวจสอบความผิดพลาดในการดำเนินการของฟังก์ชันการส่งPacket ฟังก์ชั่นการส่งต่อแพ็คเก็ตจะดำเนินการส่งต่อตามปกติโดยProcessor ใน Line Cardsเพื่อหลีกเลี่ยงการใช้งานร่วมกันกับการแผนการควบคุมที่ทำงานบนRouting Protocols BFD มีวัตถุประสงค์ที่จะนำมาใช้ในข้อมูลการส่งข้อมูลให้มากที่สุดความสามารถของBFD คือตรวจสอบความผิดพลาดการส่งข้อมูลได้รวดเร็วสามารถใช้ร่วมกับความสามารถในProtocol's Nativeเมื่อทำการตรวจสอบข้อมูลหรือทำการควบคุมความผิดพลาดในการส่งข้อความ ตัวอย่างเช่นRouter ที่ใช้วิธีการกำหนดเส้นทางOSPF สามารถเริ่มต้น SessionBFD กับRouter เพื่อนบ้านและใช้ร่วมกับHello Protocol เพื่อทำการตรวจสอบการสูญเสียของการเชื่อมต่อกับRouter เพื่อนบ้านได้อย่างรวดเร็ว [30]

Session BFD ระหว่างสองอุปกรณ์สามารถทำงานในสองโหมดที่แตกต่างกันในโหมด Asynchronous อุปกรณ์จะคำนวณระยะเวลาการส่ง Packet เพื่อควบคุมBFD กับแต่ละอุปกรณ์ โดยอุปกรณ์เหล่านั้นจะทำการแจ้งให้ทราบถึงความล้มเหลวในการเชื่อมต่อเมื่อมันไม่ได้รับPacket BFD จากอุปกรณ์อื่นๆบางเวลาที่มีการกำหนดไว้ล่วงหน้าในโหมดความต้องการ (Demand Mode) หากไม่มีการแลกเปลี่ยนระยะเวลาของการส่งข้อความระหว่างอุปกรณ์ในSession BFD BFDก็จะยังมี FunctionEcho คอยสนับสนุนเพื่อที่จะส่งอุปกรณ์Packet ควบคุมที่จ่าหน้าผู้รับถึงตัวเองไปยังอุปกรณ์อื่นๆ ดังนั้นFunctionEcho จึงช่วยให้อุปกรณ์ในการทดสอบเพียงเส้นทางการส่งต่อบนเครื่องระยะไกลสามารถกำหนดว่าเกิดความล้มเหลวขึ้นได้อย่างรวดเร็ว [29]

BFD ช่วยให้ทั้งสองอุปกรณ์ที่เชื่อมต่อกันทำการสร้างSessionBFD เพื่อที่จะเจรจาช่วงเวลารับส่งข้อมูลระหว่าง Router เนื่องจาก PacketควบคุมBFDที่รับส่งนั้นอาจจะเกิดความล้มเหลว ดังนั้นเวลาการตรวจสอบจะสามารถทำได้อย่างรวดเร็ว (ประมาณ 50 ms [32]) ถ้าอุปกรณ์ในSession BFDสามารถรับ Packet ควบคุมที่ส่งไปอย่างรวดเร็วในช่วงเวลาระหว่างที่Packet ควบคุมถูกส่งออกไปอย่างต่อเนื่องจะสามารถปรับแบบDynamic Protocol BFD ได้จึงเหมาะสำหรับการดำเนินงานในHardware ของ Line Card หรือ Firmware ที่เป็นอุปกรณ์ใน Session BFD ที่คาดว่าจะส่งข้อมูล

V. LSA GENERATION AND FLOODING

ข้อมูลโครงสร้างของOSPFจะดำเนินการอยู่ในLSAs โดย Router LSA จะอธิบายสภาพของInterface ของ Router ไปยังพื้นที่เครือข่าย LSA ที่แสดงการส่งออกข้อมูลและอธิบายชุดของRouter ที่เชื่อมต่อกับระบบLANนอกจากนี้Area Border Routers (ABRs) คือเราเตอร์ที่มีInterface เชื่อมต่อไปยังหลายพื้นที่อาจเกิดขึ้นในเครือข่าย LSAs แต่ภายใน ASสุดท้ายจะเป็นAutonomous System Boundary Routers(ASBRs) คือRouter ที่มีการเชื่อมโยงไป Router ในภายนอก ASทั้งนี้ASอาจเกิดอยู่ภายนอก (ASE)ตารางที่ 4ให้ภาพรวมคร่าวๆที่แตกต่างกันของLSAs ที่ใช้ในเครือข่าย OSPF

IV. การสร้างการเชื่อมต่อที่เร็วขึ้นและลดความสัมพันธ์ที่ต้องเชื่อมต่อระหว่างกันของเร้าเตอร์เพื่อนบ้าน

ความสัมพันธ์ระหว่างกันของ Router นั้นเกิดขึ้นเมื่อ Router เกิดการแลกเปลี่ยนข้อความ Hello Message ระหว่างกันหรือที่รู้จักกันดีว่าสถานะการสื่อสารแบบสองทาง (Bidirectional Status) ซึ่งจะถูกติดตามด้วยการแลกเปลี่ยนDD Packet แล้วDD นี้จะเป็นตัวอธิบายเซ็ทของLSA ใน Router ที่มีเก็บอยู่ใน LSDBการรวบรวม LSDBทำได้โดยการแลกเปลี่ยน LSAระหว่าง Router ข้างเคียง Router ทุกตัวจะพยายามทำให้ LSDBของมันมีข้อมูลที่เหมือนกับRouter ข้างเคียงในArea Network การเชื่อมต่อทั้งหมดคงที่Router ทั้งหมดจะมีข้อมูลเดียวกันในLSDB

ในหัวข้อย่อยต่อไปนี้จะอธิบายเกี่ยวกับการปรับปรุงวิธีการในการสร้างความสัมพันธ์ระหว่างกันของสอง Router ซึ่งการปรับปรุงนี้ลดจำนวนการสร้างความสัมพันธ์ระหว่างกันที่ถูกร้องขอในBroadcast/NBMA, LANs, Mobile AdhocNetwork หรือที่เรียกว่า MANETsตารางที่ 2 แสดงภาพรวมของกระบวนการปรับปรุงต่างๆ

A. การปรับปรุง DatabaseExchange Process

Ogierได้นำเสนอ Database Exchange Summary List Optimization ว่าการที่ต่อเพิ่มการทำงานไปยังOSPF v2/v3 ทำให้เพิ่มความเร็วในกระบวนการแลกเปลี่ยนฐานข้อมูล (DB Exchange Process) เป็นการลด Payload ของDD Packet ลงมาที่กระบวนการรับDD Packet จาก Router เพื่อนบ้าน Router จะส่งDD packet ของตัวเองไปเป็นเสมือน Response ในมาตรฐานของOSPF นั้นในDD Packet ก็ประกอบไปด้วย Header ที่มีข้อมูลของการตอบสนองLSA ซึ่งกันไว้ในLSDB การแผ่ขยายช่วงการทำงานของOSPF นั้น Router จะดูว่าLSA ในDD Packet ที่รับมานั้นมีกระบวนการแบบเดิมที่มีอยู่แล้วในLSDB หรือไม่หรือมีอันใหม่เข้ามาถ้าหากมีอยู่แล้วก็จะไม่ถูกส่งออกไปจะส่งข้อมูลเป็น Response ที่มีอยู่แล้วให้ไปแทน

Baccelliได้นำเสนออีกวิธีการในการแลกเปลี่ยนฐานข้อมูลไว้โดยมันเป็นหลักการที่ค่อนข้างจะง่ายและได้แรงบันดาลใจมาจากลูกจ้างคนหนึ่งใน ISISคือการแลกเปลี่ยน CompactSignature

(การทำ Hashing ใน Partition ของLSDB) ระหว่างกันของ Router ข้างเคียงแทนที่วิธีการข้างต้นที่จะไม่ส่งDD packet ไปหากว่าดูแล้วว่าHeader มีข้อมูลของ LSAResponse ที่ซ้ำกันเพื่อทำการตรวจสอบว่ามีความแตกต่างกันหรือไม่ระหว่างข้อมูลที่ถูกส่งมาใหม่กับ Packet เดิมที่อยู่ในLSDB เมื่อความแตกต่างกันระหว่างสองสิ่งที่ควรจะเหมือนกันเกิดขึ้นในสอง Signatures Bit ที่ใช้ในการรับส่งข้อมูลจะมีการร้องขอให้สร้างการทำงานที่สอดคล้องกันในLSDB ระหว่าง Router ที่เกี่ยวข้องกันในขณะนั้นแล้วจึงทำการระบุและเกิดการแลกเปลี่ยนLSDB ซึ่งกันและกัน

B. การลดจำนวนการสร้างความสัมพันธ์ในการเชื่อมต่อระหว่างกันของRouterข้างเคียงในBroadcast/NBMA และ LANs

ในขั้นตอนการเริ่มต้นOSPF Router ที่เชื่อมต่อด้วย Interface สำหรับ Broadcast หรือNBMA และLANs จะสร้างการสื่อสารระหว่างกันแบบสองทิศทางกับ Router เพื่อนบ้านโดยการส่งและรับ Hello Massage ในสภาวะแบบนี้ไม่ว่า Router ตัวใดก็จะถูกมองว่าเป็นเพื่อนบ้านของกันและกันการสร้างการเชื่อมต่อความสัมพันธ์กับเร้าเตอร์ข้างเคียงในเครือข่ายสภาวะเช่นนั้นอาจเป็นการเพิ่มภาระการทำงานให้ Router มากเกินไปดังนั้นในการทำงานของOSPF Protocol เช่นนี้จะเลือก Router ที่เป็นเสมือนผู้นำมาหนึ่ง Router ซึ่งเรียกว่า Designed Router หรือDR และตัวที่เป็นตัวสำรองข้อมูลไว้หนึ่ง Router เรียกว่า Backup Designed Router โดย Router ทั้งสองนี้จะสร้างความสัมพันธ์แบบเต็มรูปแบบกับ Router ทุกตัวในวงแลน

C.กลยุทธ์ให้เหมาะสมสร้างความต่อเนื่องกันบนMANETs

ในเครือข่ายแบบ Ad Hoc (ยังเรียกว่าMANETs), Router มีความสามารถในการทำงานแบบ Dynamic ร่วมกันได้หรือมีการหลุดออกจากเครือข่ายบ่อยซึ่งทำให้เป็นมาตรฐานOSPF เพื่อความต่อเนื่องกันและเพื่อสร้างวิธีการใหม่ๆจึงมีการนำเสนอวิธีในการลดจำนวนของความต่อเนื่องกันโดยOSPF Internet Engineering Task

Force (IETF) ได้พัฒนาข้อเสนอOSPF สำหรับผลกระทบในการดำเนินการบนMANETs:

• OSPF MPR [36] และOSPF-OR[37], โดยยึดหลักการถ่ายทอดข้อมูลแบบจุด (MPR)

•ลดความซ้ำซ้อนในการส่งข้อความHello: แทนที่จะส่งข้อมูลทั้งหมดก็เลือกข้อมูลข้อความHelloพื้นที่ใกล้เคียงบางรายงานที่มีการเปลี่ยนแปลงเฉพาะในพื้นที่ใกล้เคียงของRouter

วิธี	คำอธิบาย	Pros/Cons
การใช้ฐานข้อมูลรวมให้เหมาะสม	แพ็คแก็คDDไม่ได้รวมอยู่ในHeaderของ LSAที่อยู่ใกล้เคียง	จากตัวอย่างสามารถเรียกคืนค่าที่เกินไปของ DD ได้ประมาณ 50 %ในระบบครือข่ายและ IETF ก็ยอมรับ
การเปลี่ยนจาก LSDB เป็น LSA		การพัฒนาฐานข้อมูลให้ไม่ใหญ่มากนัก เพิ่มได้กับทุกฐานข้อมูล
การปรับค่าของ OSPF		การเรียกคืนค่าเวลาและการประมวลผลที่ร้องขอใน DR/BDR เพื่อเลือกการทำงาน
การเพิ่มขึ้นของ OSPF-MANET	ดูรายละเอียดในตารางที่3	ภาพรวมของ MANETs กับการติดต่อระบบเครือข่าย เพื่อเรียกคืนค่าที่ใกล้เคียงหมายเลขและ การร้องขอที่ใกล้เคียง,ขนาดของข้อความและส่วนของ LSAทีแกว่งไปมา ใน MANETs
การตอบสนองที่รวดเร็วใน OSPF	ความต่อเนื่องในการส่งผ่านข้อมูล คล้ายกับ OSPF	การใช้สายแบบเดิมอยู่ทำให้จะเข้าถึงได้ง่ายกว่า

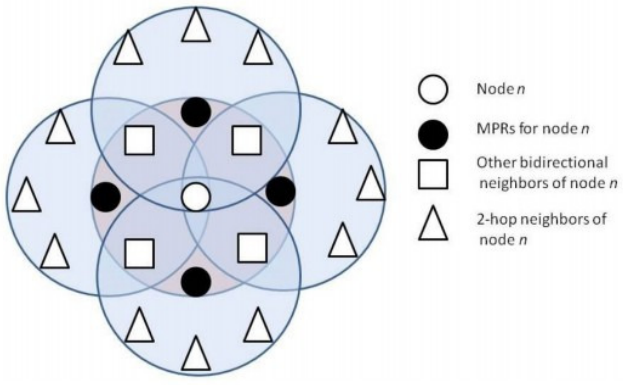
ตารางที่ 2แสดงภาพรวมของส่วนขยายของOSPF ที่แตกต่างกันMANET ในส่วนนี้กล่าวถึงการเลือกความต่อเนื่องกันของกลไกในส่วนขยายเหล่านี้กลไกประเภทอื่นๆที่กล่าวถึงข้างต้นจะกล่าวถึงในภายหลังในPaper นี้

•*OSPF-MDR* [38], ตามหลักMANETตามหลักการ Router (MDR) โดยทั่วๆไปแล้วระหว่างนามสกุลOSPF มีความแตกต่างกันสำหรับ MANET คือOSPF นำเสนอประเภท Interface ใหม่OSPF เหมาะสำหรับลักษณะของเครือข่ายไร้สายหลาย Multi-hop, ในขณะที่ OSPF วิ่งเปลี่ยนแปลงเส้นทางบนเครือข่ายและการเชื่อมต่อปกติที่มีอยู่OSPF ใช้กลไกทางเลือกที่จะลดค่าใช้จ่ายและเพิ่มความเร็วในเวลา Convergence ซึ่งสามารถแบ่งได้เป็นหมวดหมู่ดังต่อไปนี้ [40]:

•การเลือกความต่อเนื่องกัน: แทนที่จะสร้างความต่อเนื่องกันด้วย Router ทั้งหมดที่อยู่ติดกันกับRouter ข้างเคียงที่เลือกให้เหมาะเท่านั้น

•การเพิ่มประสิทธิภาพในการลดการเกิดRetransmissions Flooding ซ้ำซ้อน

•ลดโครงสร้าง Topology: แทนที่จะส่งรายการ Router ที่อยู่ติดกันทั้งหมดก็ให้ Router เพื่อนบ้านรายงานเพียงส่วนย่อยของ Adjacencies ในLSAs



รูปที่ 3 Multi-point กลุ่ม MPR โหนด N เลือก MPRs ครอบคลุมถึงวงกลมรอบข้าง 2 หน่วยการแสดงระยะห่าง ระหว่าง Node-Node

OSPF-MPR[36] ใช้การเชื่อมต่อแบบหลายจุดในการถ่ายทอดเทคนิค (MPR) สำหรับการแนะนำให้รู้จักกับ MANET

Routing Protocol ที่เรียกว่า Optimized Link State โดยกำหนดเส้นทาง (OLSR) [41] ใน OSPF-MPR ซึ่งแต่ละ Router จะเลือกจำนวน Relay หลายจุดจากชุดของRouter เพื่อนบ้านแบบสองทิศทางของเพื่อนบ้าน MPR และจะถูกเลือกโดย Router เพื่อที่ Router เพื่อนบ้าน อีก 2 hops ที่อยู่ห่างออกไปสามารถเข้าถึงได้อย่างน้อยหนึ่ง Router ผ่าน MPR (รูปที่ 3) แต่ละRouter จึงรักษาการตั้งรายชื่อเพื่อนบ้านที่จะเลือกไว้ในปัจจุบันเป็นMPR เช่นเดียวกับการตั้งค่ารายชื่อ Router เพื่อนบ้านที่มีในขณะนี้เป็น MPR ของตนเอง (Router เพื่อนบ้านเหล่านี้จะถูกเรียกว่าSelectors MPR) Router กำหนดถ้อยคำเฉพาะเต็มMPRs และ Selectors MPR ของตัว Router เองซึ่งจะช่วยลดจำนวนAdjacencyที่ไม่จำเป็นใน MANET เพื่อที่จะรับมือกับกรณีการเกิดข้อมูลที่ไม่เป็นประโยชน์ในสภาพที่หาได้ยากส่งผลให้การตั้งค่านี้ทำให้Adjacencies ไม่ได้เชื่อมต่อเครือข่ายแม้แต่หนึ่ง Router ในเครือข่าย (The Sync Router) กำหนดถ้อยคำกับทุก Router เพื่อนบ้าน การวิเคราะห์พฤติกรรมเพื่อเลือกMPRs และThe Sync Router สามารถพบได้ใน [36]

IV อธิบายกระบวนการของการเกิดความต่อเนื่องในการเชื่อมต่อกันระหว่างสอง Router OSPF และการปรับปรุงที่สำคัญ

สำหรับกระบวนการนี้ในส่วนนี้ยังอธิบายถึงการนำเสนอ Protocol ที่มีการปรับปรุงการลดจำนวนของความต่อเนื่องกันในการเชื่อมต่อPacket ที่กระทำข้อมูล Topology ภายหลังส่วนนี้อธิบายถึงปัจจัยที่มีผลกระทบต่อกระบวนการสร้างและการรั่วไหลLSAของ Parameter ติดต่อที่ล่าช้าอันเนื่องมาจากกลไกชอบLSAs และเครือข่ายย่อยแบบรวมและการปรับปรุงต่างๆที่ออกแบบมาเพื่อลดค่าใช้จ่ายที่เกิดขึ้นในการรั่วไหลโดยเฉพาะอย่างยิ่งในสิ่งแวดล้อมของMANETส่วนVI อธิบายกระบวนการของการคำนวณการสร้างตารางเส้นทางต่อไปนี้อาทิเช่น กลไกของการรับรองLSA ใหม่ใช้เพื่อหลีกเลี่ยงการคำนวณการสร้างตารางเส้นทางบ่อยๆครั้งและอัลกอริทึมที่ใช้ในการสร้างเครือข่ายต้นไม้เส้นทางที่สั้นที่สุด

ตารางการคำนวณส่วนที่ 7อธิบายการเริ่มการทำงานที่ดี กลไกที่ช่วยให้ควบคุมได้ตามแผนควบคุมการเริ่มระบบใหม่ในการทำให้ Router ดำเนินการต่อไปได้โดยไม่ต้องมีการเผยแพร่ของข้อมูลเกี่ยวกับเส้นทางไปทั่วทั้งเครือข่ายการเริ่มต้นส่วนVIIIอธิบายว่า OSPF ไม่ใช่วิธีเชิงรุกในการกู้คืนความล้มเหลวอย่างรวดเร็วขั้นตอนสุดท้ายส่วนMPLSและRerouteเส้นทางIP อย่างรวดเร็ว

Packet ที่จะถูกส่งต่อไปยัง Router ข้างเคียงนี้ Packet เหล่านี้จะถูกส่งต่อโดยใช้ค่าการติดตั้งที่เชื่อมโยง Router ที่ล้มเหลวOSPF สนับสนุนอยู่หลายการตั้งค่าที่เรียกว่าเครือข่ายMulti-Technology[96]

XI และChao [97] นำเสนอการเขียนโปรแกรมเชิงเส้นโดยใช้จำนวนเต็มFormulation (ILP) เป็นการค้นหาลำดับที่ตามอัลกอริทึมสำหรับปัญหาถัดไปของการค้นหาในการสำรองข้อมูลจะใช้โดย Router ในกรณีของความล้มเหลวของการเชื่อมโยง Router ตามเส้นทางหลักซึ่งเลขของ Router โดยใช้การสำรองข้อมูล ซึ่งข้อมูลจะถูกย่อให้เล็กที่สุดในข้อเสนอนี้Router จะตัดสินใจว่าความล้มเหลวได้เกิดขึ้นไปตามเส้นทางหลักเมื่อได้รับPacket จาก Hop ถัดไปของเส้นทางหลักสำหรับปลายทางของPacket Bryant และคณะ [90] แนะนำว่าบนความล้มเหลวในการตรวจหาเมื่อถึง Hop ถัดไปสำหรับ Packet Router ควรส่งสัญญาณ Packet ไปยัง Router จากที่สามารถต่อไปยังปลายทางของการส่งต่อผ่านIP ปกติใดๆการไหลเวียนภายในกลไกเช่นIP ในIP [98] หรือGRE [99],สามารถใช้สำหรับวัตถุประสงค์นี้เพื่อซ่อมแซมตารางเส้นทางMulti-Hop มีความยากในการกำหนดตลอดจนเรียกใช้อย่างไรก็ตามเป็นที่คาดหวังที่ในการจะต้องใช้เส้นทางดังกล่าวซ่อมแซมเพียงส่วนเล็กๆของจุดหมายปลายทางของเครือข่ายIP โดยทั่วไปซ่อมแซมเส้นทางที่ใช้ชั่วคราวเท่านั้นในขณะที่ทำการ Convergence ที่IGP (OSPF)เมื่อIGP Convergence แล้วนั้น Packet สุดท้ายจะถูกส่งต่อโดยใช้กระบวนการสร้างขึ้นมาใหม่โดยIGP

เปลี่ยนเส้นทางของทราฟฟิกที่ได้รับผลกระทบตามแนวเส้นทางอื่นตาม ING มีความล้มเหลวในการเชื่อมโยงอาจเนื่องมาจากการสร้างเกินพิกัดตามความสำคัญในบางส่วนของเครือข่าย จึงต้องระวังเรื่องการกำหนดน้ำหนักของการเชื่อมโยง ซึ่งอาจช่วยให้หลีกเลี่ยงสถานการณ์นี้ไปได้ อย่างไรก็ตามการเปลี่ยนน้ำหนักการเชื่อมโยงตลอดทั้งเครือข่ายหลังจากเกิดความล้มเหลวจะไม่สามารถเป็นไปได้ถ้าความล้มเหลวไม่ได้เป็นการชั่วคราวโดยทั่วๆไป ดังนั้นNucciและคณะ [100]แนะนำว่าควรเปลี่ยนแปลงชุดของน้ำหนักเชื่อมโยงเครือข่าย โดยกำหนดในลักษณะที่เชื่อมโยงแบบรับภาระให้สามารถหลีกเลี่ยงได้ทั้งในระหว่างการดำเนินการแบบปกติและในระหว่างที่เกิดความล้มเหลวในการเชื่อมโยงเชิงเดี่ยว นอกจากนี้ Nucciและคณะ ยังนำเสนอแบบวิเคราะห์พฤติกรรมการค้นหาไฟล์ชุดที่มีน้ำหนักเชื่อมโยงที่ดีโดยการประเมินจากผลการกระทบของความล้มเหลวที่เป็นไปได้ในการเชื่อมโยงเครือข่ายทั้งหมดสำหรับแต่ละ

ตัวอย่างน้ำหนักของชุดเชื่อมโยงสำหรับเครือข่ายขนาดใหญ่มีการคำนวณปริมาณมากและเกิดความซับซ้อนของงานสูง สามารถเป็นจุดที่มีความสำคัญในการทำให้ลดลงโดยต้องประเมินกับผลกระทบของการเชื่อมโยงที่สำคัญเท่านั้นSridharanและGuerin [103]แนะนำเทคนิคสำหรับการระบุชุดน้ำหนักดังกล่าวโดยเชื่อมโยงส่วนที่จำเป็นในการรายงานโดยลดความสำคัญของเครือข่ายและต้องใช้ในเวลาการตรวจสอบน้ำหนักการเชื่อมโยงที่ดีโดยเฉพาะสำหรับเครือข่ายขนาดใหญ่

นอกจากนี้มีข้อเสนออื่นอีกหลายแนวทางเพื่อป้องกันการเกิดการทำงานแบบวนซ้ำชั่วคราวFrancois และคณะ [104] แนะนำการเพิ่มจำนวนต้นทุนของการเชื่อมโยงที่ล้มเหลวในขั้นตอนต่อไปภายในสายงานการรับส่งข้อมูลแทนรูปแบบการรับส่งข้อมูลอย่างทันทีเพื่อป้องกันไม่ให้เกิดการวนรอบชั่วคราวการตรวจสอบที่อยู่ภายใต้เงื่อนไขที่เพิ่มขึ้นสำหรับการเชื่อมโยงที่ล้มเหลวสามารถสร้างรอบการประมวลผลที่ทำให้เกิดการวนซ้ำในเฉพาะขอบเขตของเครือข่ายที่มีข้อมูลของทุกรอบน้อยกว่าหรือเท่ากับเนื่องจากจะเกิดการวนซ้ำที่เกิดจากการใกล้ชิดกับ Router ที่มีการเชื่อมโยงล้มเหลวRouter เหล่านั้นจะทำการปรับปรุงเส้นทางหลอกๆก่อนRouter ห่างไกลป้องกันได้โดยต้องกำหนด Router เพื่อปรับปรุงFIB เท่านั้นหลังจาก Router เด็กๆในต้นไม้เส้นทางที่สั้นที่สุดที่ฝังรากตรวจพบอุปกรณ์ล้มเหลว [105] อีกวิธีที่คล้ายกันที่ใช้บังคับในสถานการณ์ที่การปรับปรุงครั้งFIB มีความสำคัญคือการที่จำเป็นต้องให้Router ทั้งหมดสลับไปFIB ใหม่ที่สอดคล้องกันเพื่อกำหนดโครงสร้างใหม่ในเวลาเดียวกันเมื่อRouter ทั้งหมดได้คำนวณFIB ใหม่ [106] วิธีการดังกล่าวต้องใช้การประสานเวลาที่แม่นยำในหมู่เราเตอร์ทั้งหมดในเครือข่าย

V. LSA GENERATION AND FLOODING

ใน OSPF ข้อมูลโครงสร้างจะเก็บเอาไว้ภายใน LSAsโดย RouterLSA อธิบายสภาพของInterface ของ Router ไปยังพื้นที่เครือข่าย และ LSA ส่งข้อมูล Broadcast/NBMALAN และอธิบายชุดของ Router ที่เชื่อมต่ออยู่ภายในระบบ LANนอกจากนี้ Area Border Routers (ABRs) คือ Router ที่มี Interface เชื่อมต่อไปยังพื้นที่หลายเครือข่ายอาจเกิดเฉพาะในพื้นที่ของ LSAs สรุปที่อธิบายที่มา ABR เพื่อจุดหมายอยู่นอกพื้นที่ แต่ภายใน AS สุดท้ายเป็น AS Border Routers (ASBRs) กล่าวคือเราเตอร์ที่มีการเชื่อมโยงไปยัง Router ภายนอก AS หรือ AS อาจเกิดภายนอก (ASE) นั้น LSAs ที่อธิบายผลกระทบที่เกิดขึ้นจาก ASBR ไปยังจุดหมายปลายทางนอก AS คือตารางที่4แสดงให้เห็นภาพรวมคร่าวๆที่แตกต่างกันของLSAs ที่ใช้ในเครือข่าย OSPFการเปลี่ยนแปลงโครงสร้างภายในส่งผลไปถึงพื้นที่ในกรณีใหม่ของLSAs Router / เครือข่าย LSA โดยได้รับผลกระทบRouterในทำนองเดียวกันโครงสร้างกิจกรรมที่มีการเปลี่ยนแปลงที่อยู่นอกเครือข่ายอาจส่งผลให้ในLSAs สรุปASE ใหม่เราเตอร์เครือข่ายใหม่หรือข้อมูลที่เป็นการสรุปของLSA ถูกส่งออกไปแบบ Flood ตลอดทั่วทั้งเครือข่ายที่มันเป็นในขณะที่ASE LSA ใหม่อาจถูกFlood ตลอดASในคำอื่นๆขอบเขตการ Floodจาก Router เครือข่ายหรือสรุปLSA ประกอบด้วยพื้นที่เดียวในขณะที่ของASE LSA อาจประกอบด้วยพื้นที่ทั้งหมด

เร้าเตอร์ที่รับLSA ใหม่แต่ละคนใช้เวลาส่วนหนึ่งในการ Flood การประมวลผลโดยการส่งLSA ใหม่ระหว่างInterfaces ทั้งหมดภายในขอบเขตการ Flood ยกเว้นหนึ่งที่คือLSA arrived7ในที่สุด Router ทั้งหมดในขอบเขตการ Flood ของLSA จะได้รับLSA ใหม่เพื่อทำการปรับปรุงLSDB ของRouter เหล่านั้นและการดำเนินการคำนวณตารางเส้นทางใหม่ของRouter เหล่านั้นสะท้อนให้เห็นถึงโครงสร้างปัจจุบันRouter นอกจากนี้ยังสร้างตัวอย่างใหม่ของLSA เมื่อถึงอายุที่กำหนดโดยพารามิเตอร์LSRefreshTime (30)

รุ่นของLSA และการไหลของOSPF ข้อมูล Topology ได้ดำเนินการในLSAs โดย LSAของ Router อธิบายถึงสถานะของ Interface ของ Router ไปยังพื้นที่Lsaของเครือข่ายแทนการออกสู่ Internet/NBMA LANและคำอธิบายของ Router ที่เชื่อมต่อกับLAN นอกจากนี้ Area Border Routers (ABRs), เช่น Router ที่มีInterface ไปยังหลายพื้นที่บนเครือข่ายอาจสรุปLSAs และสามารถอธิบายค่าเริ่มต้นABR ในการไปยังจุดหมายปลายทางที่อยู่นอกพื้นที่แต่อยู่ภายในการDownload สุดท้ายไปยังAS Border Routers (ASBRs), เช่น Router ที่มีการเชื่อมโยงไปยัง Router ในการเป็นที่ภายนอกอาจเป็นภายนอก (ASE)หรือ LSAs ที่อธิบายถึงค่าเริ่มต้นของASBR ไปยังจุดหมายปลายทางนอกการDownload ตารางที่ 4แสดงภาพรวมโดยย่อของความแตกต่างกันในการใช้เครือข่ายของOSPF LSAs

การเปลี่ยนแปลงของ Topology ภายในพื้นที่ผลลัพธ์ในการสร้างรูปแบบใหม่ของ Router/ระบบเครือข่ายแบบLSAs ที่ได้รับผลกระทบ Router เมื่อมีการเปลี่ยนแปลงเหตุการณ์จากภายนอกพื้นที่โดย Topology อาจส่งผลในการสร้างใหม่ได้คือASE LSAs Router ใหม่รวมทั้งระบบเครือข่ายหรือผลรวมของLsaที่เกิดการไม่คงที่โดย

	Multi-point Relays (MPR)	**MANET Designated Routers (MDR)**	**Overlapping Relays (OR)**
เงื่อนไขที่สำคัญ	ชุด MPRชุดของเพื่อน : บ้านของเราเตอร์ที่ให้การเชื่อมไปยังเพื่อนบ้าน -2 ทั้งหมดhop ของ เลือก MPRเพื่อนบ้านที่ : เลือกเราเตอร์ที่เป็นMPR	MDRs: ชุดของเราเตอร์ฟอร์มหลักที่เชื่อมต่อและให้การเชื่อมต่อเราเตอร์อื่น ๆ ใน เครือข่าย	SmartPeering: สองเราเตอร์ต้องไม่สร้างความต่อเนื่องกันถ้าสามารถเข้าถึงกันแล้วใน SPT. OR: เพื่อนบ้านที่ให้เชื่อมต่อหนึ่งหรือมากกว่า -2hop ของเราเตอร์ Active ORs ชุดของเพื่อนบ้านของเราเตอร์ที่ : ให้reachability ออกทั้งหมด ฮอป 2
การเลือกความต่อเนื่องกัน	การจัดตั้ง adj เฉพาะกับ MPRs และ selectors MPR	การจัดตั้ง adj เฉพาะกับ MDR และสำรอง MDR เพื่อนบ้าน	ไม่จำเป็นต้องสร้าง adj ที่มีเพื่อนบ้านสามารถเข้าถึงใน SPT. เรียบร้อยแล้ว
เพิ่มประสิทธิภาพ Flooding	เฉพาะของเราเตอร์ MPRs relay หลังlsaได้รับจากเราเตอร์ บนอินเทอร์เฟซ MANET	MDR การสำรอง relays หลัง lsa ที่ได้รับบนอินเทอร์เฟซของ MANET เท่านั้นถ้าจำเป็น	An active OR: ของเราเตอร์ทุกๆรีเลย์หลัง LSA ที่ได้รับจากเราเตอร์ในอินเตอร์เฟซของ MANET A non-active OR:จากรีเลย์เตอร์หลัง LSA ที่ได้รับจากเราเตอร์ที่เชื่อมต่อ MANET ที่จำเป็นเท่านั้น
ลดโครงสร้าง	LSAs แจ้ง adjacencies ระหว่าง MPRs และ ที่ selectors MPR	ค่า LSAFullness เป็นตัวกำหนดขอบเขตของโทโพโลยีในการรายงานใน LSAs	นอกจากนี้ LSAs จะรายงานเฉพาะ adjacencies ที่สร้างผ่านสมาร์ท peering
การสนับสนุนสำหรับ hellos เดลต้า	ไม่	ใช่	ใช่

ตารางที่3ภาพโดยรวมส่วนเพิ่มเติมของ 3 OSPF-MANET

ประเภทของ LSA	Originating Router	ข้อมูลในการดำเนินการ	ขอบเขตการ flooding
เราเตอร์ LSA	เราเตอร์ต่างๆ	สถานะความต่อเนื่องกันบนอินเทอร์เฟซของเราเตอร์ในพื้นที่	พื้นที่กว้าง
เครือข่าย LSA	Designated Router (DR)	อธิบายชุดของเราเตอร์บน broadcast/NBMA	พื้นที่กว้าง
สรุป 3 ประเภท ของ LSA (OSPFv2 [1]) / พื้นที่อินเตอร์เราเตอร์ LSA (OSPFv3 [2])	พื้นที่ Border Router	อธิบายเครือข่าย IP หรือช่วงของที่อยู่ IP ใน ASแต่อยู่ภายนอกพื้นที่ที่ LSA ถูก flooded	พื้นที่กว้าง

โดยการส่งการLsaอีกรอบผ่าน Interface ทั้งหมดภายในรวมทั้งส่ง

ประเภทของ LSA	Originating Router	ข้อมูลในการดำเนินการ	ขอบเขตการ flooding
สรุป 4 ประเภท ของ LSA (OSPFv2) / พื้นที่อินเตอร์นำหน้า LSA (OSPFv3	พื้นที่ Border Router	อธิบาย ASBR ภายนอกพื้นที่ที่ LSA ถูก flooded	พื้นที่กว้าง
LSA ภายนอก	เป็น Boundary Router	อธิบายหัวข้อภายนอก AS	AS กว้างยกเว้นในพื้นที่stub และพื้นที่ not-so-stubby) NSSA) [[42
กลุ่มสมาชิก LSA	เราเตอร์ต่างๆ	อธิบายที่มาของเราเตอร์โดยตรงที่อยู่ในเครือข่ายโดยเฉพาะที่มีสมาชิกของกลุ่ม multicast]43]	พื้นที่กว้าง
NSSA Lsa 7ชนิด	NSSA ที่เป็น Boundary Router	อธิบายหัวข้อภายนอก AS	ภายในที่มาของNSSA
การเชื่อมโยง LSA (OSPFv3)	เราเตอร์ต่างๆ	แจ้งเราเตอร์อื่น ๆเกี่ยวกับการเชื่อมโยงของแหล่งกำเนิดเราเตอร์ที่มีที่อยู่เป็น link-local และ IPvที่เชื่อมโยงกับลิงก์ 6	การเชื่อมโยงท้องถิ่น, i.e, ไม่ flooded อีกโดยเราเตอร์ได้รับ LSA
พื้นที่ภายใน LSA(OSPFv3)	เราเตอร์ต่างๆ	เชื่อมโยงรายการของหมายเลขที่อยู่หน้า IPv6 กับเราเตอร์หรือผ่านเครือข่ายที่เราเตอร์ DR	พื้นที่กว้าง
Opaque LSA	เราเตอร์ต่างๆ	แสดงกลไกทั่วไปในการกระจายข้อมูลผ่านทาง OSPF	การเชื่อมโยงภายในเครื่องสำหรับสำหรับ 9 ชนิดของ opaque LSAs พื้นที่กว้างสำหรับ ชนิดของ 10 opaque LSAs AS กว้างสำหรับ ชนิด 11ของ opaque LSAsยกเว้นในพื้นที่ Stub และ NSSA

ตารางที่ 4OSPF LINK STATE ADVERTISEMENTS [1], [2]

ภาพรวมของ Router สรุปได้ว่าLSA หากอยู่ในLSAนั้นจะไม่เกิดการรั่วไหลของข้อมูลแต่ASELSA อาจมีการไม่คงที่ของข้อมูล

Router ระบบเครือข่ายหรือLsaประกอบด้วยพื้นที่เดียวกันขณะที่ของASELSA อาจประกอบด้วยการ Load ของข้อมูลทั้งหมดใน Router แต่ละตัวที่รับLsaมาใหม่ในส่วนหนึ่งเรื่องการประมวลผลในที่สุด Router ทั้งหมดที่อยู่ในการ Flood Lsaอีกรอบนั้นจะปรับปรุง LSDB และทำการคำนวณใหม่

ตารางสายงานสะท้อนให้เห็น Topology ปัจจุบันของ Router นอกจากนี้การสร้างค่าใหม่ของLsaกรณีเดิมเคือเมื่อถึงอายุที่กำหนดโดยParameter ชื่อ LSRefreshTime (30 นาทีจะกลับสู่ค่าค่าเริ่มต้น)

กระบวนการนี้เรียกว่ากระบวนการช่วยฟื้นฟูLsaเพื่อกระตุ้นการทำงาน Protocol ในส่วนแรกนี้อธิบายการกำหนดค่าต่างๆ Parameter ที่มีผลต่อกระบวนการสร้าง/Flooding ของLsaนี้ตามด้วยคำอธิบายของDoNotAge LSAs และ Subnet Aggregation ที่กลไกนั่นอย่างมากลดการผิดพลาด

ข้อเสนอต่างๆที่มุ่งไปสู่กระบวนการFlooding ที่ปรับให้เหมาะสมของการLsaทั่วทั้งขอบเขตของ Flooding สุดท้ายเราอธิบายกลไกของการลดค่า packet ที่ไม่จำเป็นออกโดยใช้OSPFส่วนขยายสำหรับสภาพโดยรวมของตารางที่ 5ให้เป็นบทสรุป

สรุปปรับปรุงOSPF ที่อธิบายไว้ในส่วนนี้

รุ่นของLsaและการกระจายของข้อมูลกระบวนการ:

•Parameter ต่ำสุดหรือค่าเริ่มต้นของ5 วินาทีจำกัดความถี่ที่ Router สามารถฟื้นคืนมาใหม่LSAs ของ Router สามารถนำมาเป็นตัวอย่างใหม่อีกรอบLsaดังเช่นตัวอย่างก่อนหน้านี้ที่มีค่าน้อยจากภายใน

• Parameter minLSArrivalกับค่าเริ่มต้นที่สองโดยจำกัดความถี่เป็น 1ซึ่งสามารถใช้Router ที่ยอมรับLSAs ใหม่และส่งโดยRouter อื่นๆทีเป็นตัวอย่างของLsaการมาถึงที่Router จะถูกละทิ้งถ้าอินสแตนซ์ก่อนหน้าได้รับน้อยกว่าเวลามาแล้ว

กลไกการทำงาน	คำอธิบาย	ข้อดี / ข้อเสีย
Dynamic minLSInterval [44], [45]	minLSIntervalเพิ่มตามความถี่การสร้าง LSA ใน Router ที่มีจำหน่ายในเชิงพาณิชย์[46].	ความเร็วConvergence สูงสุดสำหรับการเปลี่ยนแปลงTopology อย่างมาก
Dynamic RxmtInterval and pacing delay [22]	รูปแบบDynamic เพิ่ม RxmtInterval และความล่าช้าช่วงเว้นจังหวะที่ Router ข้างเคียงมีความหนาแน่น	ช่วยให้หลีกเลี่ยงความแออัด
Group pacing delay [47]	รีเฟรช LSA ในกลุ่มเพื่อลดจำนวนของ LS ที่ปรับปรุง Packet และหลีกเลี่ยงการรับส่ง LSA ปริมาณมหาศาล ใน Router ที่มีจำหน่ายในเชิงพาณิชย์[47].	
Setting DoNoAge bit in LSAs to avoid periodic refresh [48].		ลดความสำคัญของ LSA ที่ Router ประมวลผลแล้ว Overhead และ IETF ยอมรับ
Algorithms for smart subnet aggregation [49], [50]	การรวม Subet ที่อ้างถึงการสร้าง ABR ประเภทเดี่ยว 3 ประเภท และ LSA ที่เป็นผลรวมของเครือข่ายย่อย	ช่วยลดจำนวนของ LSAs ในขณะที่ลด suboptimality ในการเลือกเส้นทาง
Extended reverse path forwarding [51]–[53]	LSA ถูกส่งต่อพร้อม Spanning Tree Rootedที่มาจาก LSA	สามารถลด Flooding Overhead ของ LSA อย่างมีนัยสำคัญ
OSPF-MANET extensions for topology reduction and flooding optimization [36]–[38]	LSAs เท่านั้นที่ส่ง subgraph ทั่วๆไปโดยไม่คำนึงถึงแหล่งที่มา ดูตารางที่3	ลดความสำคัญของ LSA Flooding Overheadใน MANETs

ตารางที่ 5การปรับปรุง OSPFเพื่อเพิ่มประสิทธิภาพการสร้าง LSA และการ Flood

A. การกำหนดค่าพารามิเตอร์ที่ส่งผลกระทบต่อการสร้าง Lsa และการ Flood

การไหลของข้อมูลจะอธิบายค่ามาตรฐานและลดค่าไม่จำเป็นต่างๆออกและกำหนดค่าพารามิเตอร์ที่มีผลกระทบที่สำคัญ

•RxmtIntervalค่าเริ่มต้นคือ 5 วินาทีระบุ Parameter ทีแตกต่างจากตัวอื่นช่วงเวลาหลังจากที่ Router ส่งข้อมูลใหม่อีกรอบของLsaถ้าRouterไม่รับรองหรือได้รับสำหรับการส่งผ่านก่อนหน้านี้

•เพิ่มอายุของLSAs ในฐานข้อมูลของตนเองที่ Router A ปกติการฟื้นฟู Self-Originatedของ Lsa(Lsaเช่นการอยู่กำเนิดโดยRouter

ตัวเอง)เมื่อมาถึงอายุที่กำหนดโดย Parameter(30 นาทีโดยค่าเริ่มต้น) ถ้า Router ต้นล้มเหลวไปและจะทำการเรียกค่าLSA ใหม่อีกครั้งต้องเรียก Protocol อีกรอบเพื่อให้สามารถใช้งานLsaได้อีกครั้งเมื่อ Router กำหนดค่า LsaSelf-Originated หรือMaxAge (ค่าเริ่มต้น: 1 ชั่วโมง)จะทำการกระจายข้อมูลอีกครั้งโดยทั่วไปพื้นที่รอบข้างจะมีการรับของLsaของMaxAgeทำให้เห็นถึงตัวอย่างทั้งหมดของLsaนี้จะลบออกจากLSDB Routerรับดังนั้นLsaที่มีการเข้าถึงMaxAgeใน Router เป็นไปอย่างรวดเร็วจะทำการลบออกจากLSDBs ของ Router ทั้งหมดในเครือข่ายลบLSAs ในลักษณะนี้ช่วยให้OSPF สามารถเก็บข้อมูลที่ไม่จำเป็นในLSAs ของ Router ที่ตาย

•ความล่าช้าของข้อมูลLsaคือ Parameter ที่เป็นมาตรฐานในการระบุช่วงเวลาที่ต่ำสุดระหว่างการส่ง Packet อย่างต่อเนื่องเพื่อทำการปรับปรุงสถานะการเชื่อมโยงโดยRouter หน่วงเวลานี้จำกัดกำลังการเชื่อมโยงที่ใช้งานโดยLsaของการดำเนินการ Flooding/Retransmission และสาเหตุ BatchingของLSAs ที่อาจมาโดย Router แตกต่างกันแบ่งออกเป็นสถานะเชื่อมโยงโปรแกรมปรับปรุงค่าPacket ขนาดใหญ่ (เช่นค่าเริ่มต้น 5 วินาที) สำหรับการจำกัดการเกิด minLSInterval ที่เป็น Parameter ของ Lsaโดยการ Routing และการทำงานเป็น Stabilizing Factor เมื่อการเปลี่ยนแปลง Topology มีสถานที่ขนาดใหญ่ (เช่น Router ระดับPoPReboots)หรือ In Face of Pathological เงื่อนไขดังกล่าวเป็นการเชื่อมโยงFlaps บนมืออื่นๆminLSIntervalขนาดใหญ่มีสาเหตุจากความล่าช้าใน การสร้างของ Lsaและการหน่วงเวลาดังนั้นในการบรรจบกันใน Topology การเปลี่ยนแปลงดังนั้นKatz [44] ที่แนะนำที่สำคัญLSAs(เช่นLSAs อธิบายความล้มเหลว) อาจถูกน้ำท่วมโดยไม่บังคับใช้ minLSArrival, minLSIntervalหรือLsaของ Pacing ความล่าช้า Choudhury [45] ได้รายงานสำคัญเกี่ยวกับการ Speedup เวลาในการ Convergence ถ้า Parameter minLSIntervalถูกตั้งค่าเป็นขนาดเล็ก(1 วินาที) แต่ได้รับอนุญาตให้มีเป็นคู่ (มีค่าสูงสุดราวๆ 5 วินาที) เมื่อใดก็ตามที่ Router พยายามเข้ามาใหม่ Instance ของLsaก่อนการหมดอายุของminLSIntervalปัจจุบันจะส่งกลับ Parameter ขนาดเล็กไปยังการเริ่มต้นค่าของ Router

การไม่พยายามมาใหม่ของ Lsaที่อยู่ภายในปัจจุบันค่า minLSIntervalเช่นการปรับปรุงแบบDynamic ในminLSIntervalมีการนำมาใช้ในCisco IOS (SBC รุ่น 12.2 (27)เป็นต้นไป) และเรียกว่าการควบคุมปริมาณ [46] LsaของCisco IOS (Release 12.2 (14) S เป็นต้นไป) ที่ให้สามชนิดของLsaของ Pacing มีความล่าช้าเนื่องจากการส่งซ้ำRetransmission Pacing แบบ Floodและกลุ่ม pacing [47] Retransmission การหน่วงเวลาเป็นชื่ออื่นสำหรับ RxmtIntervalในขณะที่Flood Pacingมีหน่วงเวลาเหมือนLsaของการหน่วงเวลาที่อธิบายไว้ข้างต้นเช่น Pacingเป็นช่วงเวลาที่ต่ำสุดที่ต้องรอระหว่างการส่งข้อมูลของPacket เพื่อทำการปรับปรุงสถานะของการเชื่อมโยงโดยสองเราเตอร์ที่มีค่าเริ่มต้นของFlood Pacing ที่มีการหน่วงเวลาเป็นมิลลิวินาทีที่ 33แม้ว่าจะสามารถกำหนดค่าต่างๆ เพื่อให้ครอบคลุม ในช่วงเวลาจาก 5มิลลิวินาทีและแบ่งจาก 100 มิลลิวินาทีความล่าช้าของ Pacing ต่อการเชื่อมโยงสามารถเพิ่มขึ้นอย่างรวดเร็วดังนั้นกระบวนการConvergence และCausing ที่มีขนาดใหญ่จะมีความแปรปรวนในระยะเวลาการมาถึงของLSAs ใน Router ที่มีความแตกต่างกันในเครือข่ายนี้อาจทำให้เกิดการวนซ้ำชั่วคราวและเปลี่ยนTopology สุดท้ายไปในPacingอื่นๆ

ความล่าช้าของการออกข้อบังคับตามวัตถุประสงค์ที่สำคัญของ Lsaสามารถตรวจจับจากการส่ง Flooding ข้อมูลให้กับเพื่อนบ้าน'congested' Choudhuryet al. [22] จะบ่งบอกว่าเราเตอร์ควรปรับปรุงแบบ Dynamic

ความล่าช้าสำหรับการรับส่งข้อมูลกับ Router เพื่อนบ้านในการการRxmtIntervalและpacing

B. การยกเลิกจำกัดเวลาการหมดอายุของ LSAs

ความเข้าใจว่าเพื่อนบ้านถูกcongestion หรือไม่เพื่อหลีกเลี่ยงการ Exasperating Congestion ที่ Router ใกล้เคียงของ Router เหล่านั้นโดยRouter ควรเพิ่มค่าRxmtIntervalสำหรับการLsaของเพื่อนบ้านถ้าพบว่าล้มเหลวซ้ำๆLsa จะรู้ (โดยการสันนิษฐานจากCongestion) นอกจากนี้การที่ Router ควรพยายามลดCongestion ที่ Router ใกล้เคียงโดยการปรับการหน่วงเวลาของPacing ตามจำนวนของ LSAs ที่ไม่ได้รับหมายเลขโดย Router เพื่อนบ้านถ้าพบว่า Unacknowledged LSAs มีปริมาณสูงมากกว่าการหน่วงเวลาของ Pacing แล้ว Router เพื่อนบ้านควรจะทำ Multiplicativelyเพิ่มขึ้น (บางอย่างมีปริมาณที่สูงใกล้เคียงกัน) กับเวลาPacingทำให้การหน่วงเวลาของ Router เพื่อนบ้านลดลงจนเป็นไปได้อย่างรวดเร็วหมายเลขของUnacknowledged LSAs ที่อยู่ใต้ระดับต่ำจะทำการอนุญาตให้กลุ่มของCisco Pacing หน่วงการฟื้นฟู[47] Lsaมีการจัดกลุ่มเข้าด้วยกันในลักษณะที่ต้องการพิจารณา Router ที่เกิดหลายLSAs เช่น พื้นที่ที่เป็นอยู่บริเวณขอบของเครือข่าย Router ทั้งหมด

สรุปคือ LSAs สามารถนำมาใช้ในการลดปริมาณการ Flooding จากLsaเมื่อต้องการฟื้นฟูเส้นทางสิ่งที่สำคัญคือการPackLSAs ใน Packet เดียวที่เชื่อมโยงการปรับปรุงที่เป็นไปได้อย่างไรก็ตาม Router ไม่ควรฟื้นฟูLSAs ทั้งหมดพร้อมกันในขณะที่ Lsaกำลังทำงานอยู่ โดยเฉพาะอย่างยิ่งถ้า Router มี LSAs จำนวนมากดังนั้นจำนวนLSAs ที่ฟื้นฟูร่วมกันควรจะไม่น้อยเกินไปหรือไม่ใหญ่เกินไปเมื่อเก็บเวลา กลุ่ม Pacing Delayfires การที่ Router เพิ่มเวลาของLSAs ใน ฐานข้อมูลและถ้าบางกรณีที่ Self-Originated LSAs เพิ่มมากขึ้นจนถึง LSRefreshTimeดังนั้นการที่ Router ฟื้นฟูจนได้กลุ่มPacing Delay ที่ จะระบุเวลาให้มีระดับความละเอียดมากจนถึงระดับที่Router กำหนด อายุLSAs ในฐานข้อมูลและช่วงเวลาที่ต่ำสุดระหว่างสองชุดของLsa

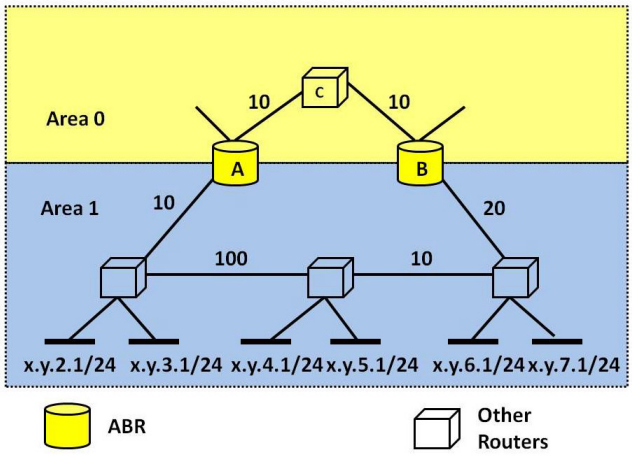
OSPF ช่วยให้การเชื่อมโยงประเภทวงจรเป็นไปตามความ ต้องการ [54], ซึ่งหมายความว่าการดำเนินงานต้นทุนของDependson เมื่อเชื่อมโยงการใช้งานเทคโนโลยีบางอย่างแบบดั้งเดิมเช่นISDN และX.25 คำอธิบายOSPF นี้จะควบคุมTraffice ของเครือข่าย

Hello exchange และการฟื้นฟูของLsaอาจบอกได้ว่าเป็น การสิ้นเปลืองทรัพยากรของวงจรดังกล่าวดังนั้นความต้องการของ OSPF ที่ช่วยให้ข้อความ Hellos และLsaของการฟื้นฟูถูกยับยั้งใน วงจรถ้าหากความต้องการLSA ของการฟื้นฟูจะหลีกเลี่ยงโดยการตั้ง ค่าบิตDoNotAgeในการLSAs จึงเป็นการบ่งชี้ของRouter ว่า DoNotAge LSAs ไม่ได้มีอายุเวลาเยอะมากๆจึงไม่จำเป็นที่จะต้อง ฟื้นฟูภายหลังจากนั้น

ช่วงเวลาLSRefreshTime ที่ใช้ระบุเป็นประจำของLsaที่จะฟื้นฟู เส้นทางสามารถส่งผลการประมวลผลที่สำคัญและจำนวนทรัพยากร ระบบที่จำเป็นสำหรับ Router ในเครือข่ายขนาดใหญ่ดังนั้นOSPF ณ เวลานี้จะอนุญาตให้ใช้LSAs DoNotAgeเพื่อหลีกเลี่ยงการใช้ ทรัพยากรระบบสำหรับเครือข่ายขนาดใหญ่เพื่อให้ระบบมีความ เสถียรภาพ [48] Router Aอาจตั้งค่าบิตDoNotAgeใน LSAs Self-Originatedก่อนจะทำการ Flooding ที่ไม่จำเป็นเพื่อทำการฟื้นฟู ดังกล่าวหลังจากช่วงทุกๆ LSRefreshTime จะทำให้ Instance ใหม่ ของLsaจำเป็นต้องมีการสร้างขึ้นเฉพาะในข้อมูล Lsaของการการ เปลี่ยนแปลง

C. การแบ่ง Subnet

เครือข่ายย่อยAggregationทั่วไปแต่ละพื้นที่เครือข่าย OSPF ใน Domain ที่จะต้องสร้าง Uplink ที่เชื่อมต่อในแต่ละ Router และ เครือข่ายย่อยมาตรฐานที่ OSPF สนับสนุนเครือข่ายย่อยแบบที่แบ่ง ออกเป็นกลุ่ม ซึ่งช่วยให้ Area Border Router (ABR) ทำการรวม เครือข่ายย่อยจากในหลายพื้นที่ และอธิบายถึงข้อสรุปของ Lsa ได้ 3 ประเด็น ในพื้นที่ที่แตกต่างกันจะสรุปความกระบวนการสร้างที่ทำ ให้ขนาดของฐานข้อมูลที่สำคัญมีขนาดเล็กมากและสถานะการ เชื่อมโยงที่ลดลงดังนั้นการใช้ทรัพยากรในกระบวนการ Flooding และการทำให้มีฐานข้อมูลตรงกันอย่างไรก็ตามข้อดีเหล่านี้ Optimality ในสายงานด้วยขึ้นอยู่กับวิธีการABRs ในกระบวนการ สร้างทำให้ข้อมูลบางส่วนอาจจะสูญหายซึ่งอาจทำให้Router สามารถเลือกการ Sub-Optimal (นานเกินความจำเป็น) เส้นทางไปยัง เครือข่ายย่อยในการหาพื้นที่เครือข่ายที่อยู่ห่างไกลพิจารณาตัวอย่างที่ แสดงในรูปที่ 4 ในที่นี้รูปที่Router A และB มีABRs ด้วย Interface ในเครือข่ายทั้งสองจะมีพื้นที่ 0 และพื้นที่ 1 โดยพื้นที่ 1 ประกอบด้วย เครือข่ายย่อยที่ 6 ตามที่แสดงในรูปที่ 4 ในการสูญหายใดๆเครือข่าย ย่อยแบบที่แบ่งออกเป็นกลุ่มของ Router Aและ Router B จะส่ง ข้อมูลสรุปแต่ละชนิดของ Lsa 3 อย่างในพื้นที่0 สำหรับแต่ละ เครือข่ายย่อยในพื้นที่ 1 ดังนั้นRouter C ในพื้นที่ 0 จะเลือก Router B เป็น Hop ถัดไปบนเส้นทางที่สั้นที่สุดได้อย่างถูกต้อง



รูปที่ 4 Topology ตัวอย่างเพื่อแสดงเส้นทางSuboptimal ที่เกิดจากการรวมSubnet

อย่างไรก็ตามการแบ่งย่อยเครือข่ายเป็น Subnet x.y.7.1/24ถ้า Router A และ Router Bเลือกที่จะรวมเครือข่ายย่อยที่ 6 ทั้งหมดเป็น x.y.0.0/21ด้วยทรัพยากรที่Advertised ที่สูงสุดของเครือข่ายย่อย ทั้งหมดที่ Router C จะถูกเลือกโดย Router A ให้เป็นHop ถัดไปบน เส้นทางที่สั้นที่สุดเพื่อไปยังเครือข่ายย่อยx.y.7.1/24 เนื่องจาก Router A จะกระจายจำนวน IP ให้สูงที่สุด(10, 110, 120) = 120 สำหรับการ ตั้งค่าคำนำหน้า(Prefix) x.y.0.0/21 จะดีกว่าเนื่องจากทำให้จำนวน IP

สูงที่สุด (20, 30, 130) =130 การ Advertised โดย Router B สำหรับการใช้คำนำหน้า (Prefix) เดียวกัน

การเกิด Errors เมื่อทำการเลือกเส้นทาง เช่น ไม่สามารถย่อเส้นทางข้อมูลให้เล็กที่สุดโดยระมัดระวังที่จะเลือกAggregates และ AdvertisedของRouter เหล่านั้นจะทำให้ทรัพยากรระบบถูกใช้อย่างมากเกินจำเป็น Rastogi และคณะ [49] นำเสนอการเขียนโปรแกรม Algorithm แบบ Dynamic เพื่อใช้กำหนดจำนวนผลลัพธ์สำหรับพื้นที่เครือข่ายทั้งหมดของOSPF ซึ่งเป็นการสะสมความผิดพลาดในการเลือกคู่เส้นทางจากต้นทางไปยังปลายทางทั้งหมดถูกย่อให้เล็กมากที่สุด ทั้งยังนำเสนอการค้นหาเชิงรุกเพื่อกำหนดระดับทรัพยากรเครือข่ายโดยจะกำหนดผลลัพธ์สำหรับพื้นที่เครือข่ายทั้งหมดของ OSPFShaikh และคณะ [50] ทำการตรวจสอบผลลัพธ์สำหรับพื้นที่เครือข่ายหนึ่งๆ สามารถถูกกำหนดแต่เพียงผู้เดียวตามข้อมูลเกี่ยวกับพื้นที่นั้นดังนั้นผลลัพธ์สำหรับพื้นที่หนึ่งๆสามารถกำหนด Aggregates ที่เป็นอิสระสำหรับพื้นอื่นๆที่พวกเขานำเสนอเป็น Algorithm เพื่อตรวจสอบการตั้งค่าที่น้อยที่สุดของผลลัพธ์ สำหรับพื้นที่ที่กำหนดข้อผิดพลาดที่พบสูงที่สุดในการเลือกเส้นทางที่ยอมรับได้

D. การเพิ่มประสิทธิภาพของกระบวนการFlooding

การปรับให้เหมาะสมตามที่อธิบายไว้ก่อนหน้านี้Instance ใหม่ของLSAs จะกระจาย ตลอดทั้งพื้นที่ของเครือข่ายเพื่อให้มั่นใจว่า Router ที่มีเหมือนกันของแต่ละเครือข่ายที่จะทำการเผยแพร่ของLsa นั้นใช้กับเครือข่ายที่ผ่านการรับรองความน่าเชื่อถือ การ Flooding โดย Algorithm การ Flood ของ Router ที่ทำการ FloodsของLsaการได้รับข้อความบน Interface หนึ่งจากinterfaces อื่นทั้งหมดทำให้เกิดความน่าเชื่อถือตามหลักRetransmitting Lsaของพื้นที่เครือข่ายที่เดียวกันการส่งออกของInterface ที่รับข้อมูลมาถ้าไม่มีการรับรองสำหรับการส่งข้อมูลก่อนหน้าภายในRxmtInterval จะเกิดข้อเสียหลักของAlgorithm นี้คือRouter อาจได้รับหลายสำเนาของ Lsaใหม่ที่ส่งออกในระหว่างกระบวนการFlooding จาก Router ใด Router หนึ่งโดย Router รับการปรับปรุงมุมมองของเครือข่าย (เช่นLSDB) สำเนาอื่นของ Lsaที่กำลังส่งต่อข้อมูล Router และกำลังรับข้อมูล (การส่งข้อมูล Ask-Answer เมื่อมีการส่งกลับ) จะซ้ำซ้อนกันเป็นกลายเป็นเครือข่ายขนาดใหญ่ขนาดจำนวนของ Packet มีความซ้ำซ้อนที่กำลังสร้างในระหว่างกระบวนการFlooding จะเพิ่มขึ้นทรัพยากรในการประมวลผลPacket เหล่านี้สามารถมีผลกระทบที่มีความสำคัญต่อความเสถียรภาพของเครือข่ายอย่างแท้จริงโดยเฉพาะอย่างยิ่งเมื่อOSPF LSAs ถูกใช้ในการแพร่กระจายข้อมูลTopology ไม่เพียงแต่การข้อมูลเกี่ยวกับParameter และการQoSระดับเชื่อมโยงเช่นแบนด์วิดธ์การหน่วงที่พร้อมใช้งานและ Jitter [56] การเปลี่ยนแปลง Parameter เช่นQoSบ่อยมากกว่า Topology ของเครือข่ายเพราะLSAsดำเนินการกับข้อมูลนี้เพื่อให้ได้ข้อมูลมาและการ Flooding บ่อยมากและมากกว่า Topology Carrryingข้อมูล LSAs ปกติ [57]แม้ว่ายังไม่ได้ดัดแปลงOSPF ตามมาตรฐาน (ยกเว้นในบริบทของMANETs ตามที่กล่าวไว้ในส่วนV-E), เพื่อทำการปรับให้เหมาะสมกับกระบวนการFlooding ใน Protocol กระบวนงานการสร้างเส้นทางเชื่อมโยงจากการศึกษาเพิ่มเติมทำให้ได้รับหัวข้อของการวิจัยที่ทำการค้นคว้าเป็นเวลานานในปี 1978, Dalalและ Metcalfe[51] เสนอเส้นทางการย้อนส่งต่อข้อมูลที่ส่งต่อของ NodesPacket อื่นๆจะส่งออกเฉพาะเมื่อได้รับPacket จาก Node ที่ถัดจาก Hop ที่อยู่ใกล้เคียงบนเส้นทาง "ที่ดีที่สุด" จากแหล่งที่มาของ Packet Transmissionscanที่มีความซ้ำซ้อนอาจทำการหลีกเลี่ยงได้ถ้า Node นั้นๆส่งต่อPacket ไปยัง Node ใกล้เคียงโดยเฉพาะถ้าHop ถัดไปในกระบวนการสร้างเส้นทางที่ดีที่สุดจากNode เพื่อนบ้านไปยังแหล่งที่มาของ Packet วิธีการนี้เรียกว่าเป็นเส้นทางการย้อนกลับสำหรับขยายขยายเส้นทางส่งต่อ (ERPF)[51], เพื่อให้แน่ใจว่าเป็นการส่งต่อ Packet โดยการ Broadcast ไปตาม Rootedของ Node Tree จากแหล่งที่มาของ Packet BellurและOgier [52] การ Broadcast ของ Topology ที่นำเสนอบนเส้นทางขากลับการส่งต่อ (TBRPF), วิธีใช้ ERPFซึ่งการใช้เวลาของการเผยแพร่ข้อมูลTopology จะวางรูปแบบตามแนวTree ที่ Hop Rooted ต่ำสุดแหล่งมาที่ของการส่งข้อมูลในวิธีการนี้ได้มาจากการคำนวณของParent Node pi(j) ในกระบวนการสร้างเส้นทางขั้นต่ำจาก Hop ไปหาตำแหน่งj แต่ละNode ในเครือข่ายและการยอมให้ Parent Node ทราบเกี่ยวกับเส้นทางของ Node นั้นๆ เมื่อได้รับการส่งข้อมูลParent Topology สร้างโดยNode j การส่งต่อในที่นี้จะได้ข้อมูลเฉพาะNode ที่ได้เลือกไว้เป็นหลักบนเส้นทางของ Node ตนเอง จาก Hop ต่ำสุดไปยัง Node j นั้น Topology ข้อมูลที่ส่งไปตาม Tree จาก Hop ต่ำสุดและยังใช้ในการปรับเปลี่ยนแผนภูมิ Tree ของตัวเองHumbleและSoloway [53] เสนอวิธีการทดแทนสำหรับ Topology Broadcast ซึ่งNode ยึด Topology คำนวณข้อมูลได้ของ Child มากกว่าของ Parent บน Spanning Tree ซึ่งข้อมูล Topology จะแพร่กระจายอีกครั้งจากแต่ละแหล่งข้อมูลTopology จะ

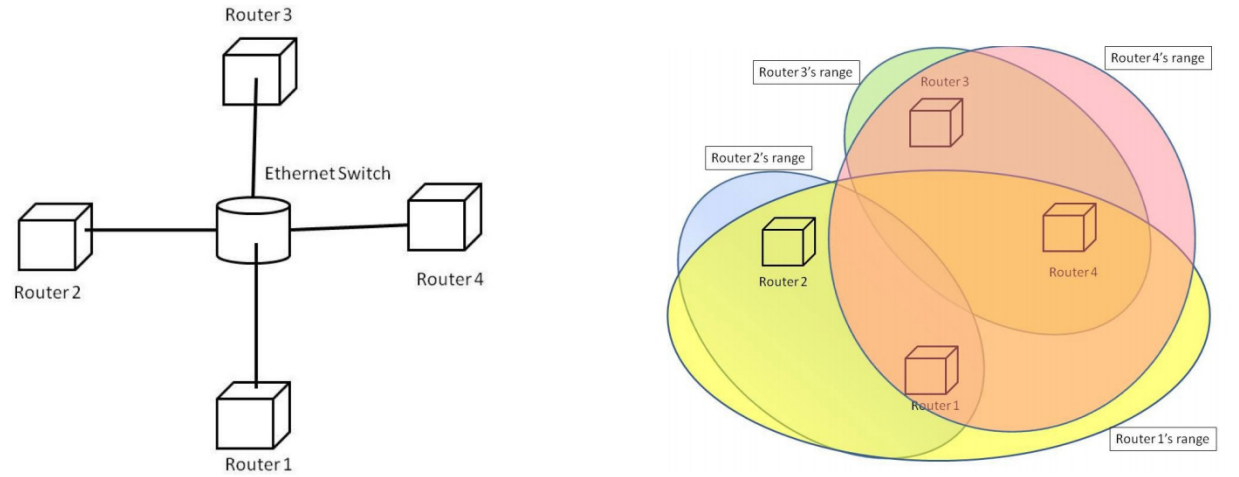
มีTree ในการแพร่กระจายข้อมูลเองโดยมีต้นกำเนิดมาจากอีกวิธีหนึ่ง คือNode ในเครือข่ายสามารถคำนวณ Subgraphตามที่เผยแพร่ Topology ทั่วไป ข้อมูลที่ใช้การส่งจากสถานที่ที่เป็นแหล่งเดียวกัน เพียงแค่มีSubgraphต่ำสุดของ Tree หรือโครงสร้างอื่นๆที่จะเชื่อมต่อ แม้จะเกิด In Face of บางจุดที่ทำให้เกิดความล้มเหลว [58]

E. การลดกระบวนการ Floodingที่เกิด Overhead ใน MANETs

บนเครือข่ายแบบใช้สาย เร้าเตอร์ไม่จำเป็นต้องส่งสัญญาณ LSA ออกจาก อินเตอร์เฟสที่มันได้รับ อย่างไรก็ตาม บนเครือข่ายสัญญาณไร้สายหลายจุด (multi-hop wireless networks) ถ้าเร้าเตอร์รับสัญญาณ LSA บนอินเตอร์เฟสของ MANET อาจจำเป็นที่จะต้องส่งสัญญาณ LSA ออกจากอินเตอร์เฟสเดิมเพื่อทำให้มั่นใจว่าเร้าเตอร์ทุกตัวบนเครือข่ายได้รับสัญญาณ LSA รูปที่ 5 ได้แสดงให้เห็นถึงตัวอย่างของกรณีเช่นนี้ ถ้าเร้าเตอร์ที่ 1 ถึง 4 เชื่อมต่อผ่านอีเทอร์เน็ต (Ethernet) ดังเช่นในรูปที่ 5 เร้าเตอร์ตัวที่ 1 สามารถคาดหวังว่าเร้าเตอร์ตัวอื่นๆ ได้รับสัญญาณ LSA ที่มันส่งบนเครือข่ายอีเทอร์เน็ต และเร้าเตอร์เหล่านั้นไม่จำเป็นต้องส่งสัญญาณนี้จากอินเตอร์เฟสของมันบนเครือข่ายอีเทอร์เน็ต อย่างไรก็ตาม ถ้าเร้าเตอร์เหล่านี้เป็นเครือข่ายสัญญาณไร้สายหลายจุดที่มีช่วงวิทยุดังที่แสดงในรูปที่ 5(b) ถ้าสัญญาณ LSA ส่งโดยเร้าเตอร์ตัวที่ 1 จาก MANET อินเตอร์เฟสของมันเองจะทำให้รับสัญญาณได้เฉพาะเร้าเตอร์ตัวที่ 2 และ 4 ดังนั้น เร้าเตอร์ตัวที่ 4 จำเป็นต้องส่งต่อสัญญาณ LSA ออกจาก MANET อินเตอร์เฟสของมันเองเพื่อให้แน่ใจว่าเร้าเตอร์ตัวที่ 3 ได้รับสัญญาณ

ถึงแม้ว่าเร้าเตอร์ควรถ่ายทอดการรับสัญญาณบน MANET อินเตอร์เฟสจากอินเตอร์เฟสเดียวกันหรือไม่ต้องการการพิจารณาอย่างรอบคอบ การถ่ายทอดสัญญาณ LSA ทั้งหมดแบบสุ่มสี่สุ่มห้าบนบน MANET อินเตอร์เฟสจากอินเตอร์เฟสเดียวกันไม่แนะนำให้ทำเนื่องจาก

- ความถี่ของแบบโครงสร้างของข่ายงานบริเวณเฉพาะที่ (topology) เกิดการเปลี่ยนแปลง และด้วยเหตุนี้รุ่นของสัญญาณ LSA จึงถูกคาดหวังที่ว่าจะเหนือกว่าใน MANETs มากกว่าในเครือข่ายแบบใช้สายเพราะว่าการเคลื่อนไหวโหนด (Node movement) และธรรมชาติการเปิด/ปิด (on/off nature) ของการเชื่อมต่อแบบไร้สายท่ามกลาง MANETs Node
- โปรโตคอลการสื่อสารแบบไร้สายส่วนใหญ่ที่ใช้งานผ่าน MANETs Node มีพื้นฐานมากจากการทำงานเข้าใช้ระบบเครือข่ายโดยวิธีช่วงชิง (CSMA) ที่ซึ่ง Node อื่นๆ แข่งขันกับอีกตัวในช่วงวิทยุเพื่อเข้าถึงช่องทางการส่งผ่าน มีเพียงตัวเดียวเท่านั้น ทามกลาง Node ตัวอื่นที่แข่งขันกันที่ได้ส่งในเวลาที่ให้ไว้ ประสิทธิภาพการทำงานของโปรโตคอล CSMA มีแนวโน้มที่จะล้มเหลว นั่นคือตัวเลขของแพ็คเก็ตที่ส่งสำเร็จลดลงในขณะที่การแข่งขันเพื่อช่องทางการส่งผ่านเพิ่มขึ้น



(a) An LSA sent on a wired broadcast LAN is received by all the routers on the LAN

(b) An LSA sent on a MANET interface may not reach all the routers in the MANET

รูปที่ 5 LSA receivedona MANET interface อาจจะต้องมีการส่งออกจากอินเตอร์เฟซเดียวกัน

ด้วยเหตุนี้ การถ่ายทอดที่ควบคุมไม่ได้จากการรับสัญญาณ LSA จาก MANET อินเตอร์เฟสอาจกลายเป็นปัญหา เป็นสิ่งที่เกิดขึ้นจริง โดยเฉพาะใน MANET Topologies ประกอบด้วยโหนดที่ใช้งานหนาแน่นขนาดใหญ่ ด้วยเหตุนี้ การเติบโตของ OSPF สำหรับ MANETs ถูกแนะนำในส่วน IV-C โดยเฉพาะกลไกที่ใช้ลด flooding overhead กลไกนี้แบบเป็นสองหมวด การเพิ่มประสิทธิภาพ flooding (Flooding optimization) และการลดโครงสร้าง (topology reduction) หมยเหตุว่ากลไกนี้สามารถนำไปใช้ได้เพื่อเพิ่มประสิทธิผลให้กับกับเครือข่ายแบบใช้สาย

1) การเพิ่มประสิทธิภาพของ Flooding ใน MANETs: การเพิ่มประสิทธิภาพของ Flooding ในการขยาย OSPF ดวดมาเนท์โดยทั่วไปเป็นการลดจำนวนของเราเตอร์ที่เข้าร่วมในกระบวนการ flooding ในขณะที่มั่นใจว่าเราเตอร์ทั้งหมดยังได้รับ LSA

ตามที่ได้พูดถึงไปแล้วก่อนหน้านี้ ในOSPF-MPR [36] เราเตอร์แต่ละตัวรักษาชุดของเราเตอร์ในการถ่ายทอดหลายจุด (MPR) เลือกจากสองทิศทางใกล้เคียง เช่น เส้นทางที่ 2 ทั้งหมดของเราเตอร์ใกล้เคียงสามารถเข้าถึงผ่านทางเส้นทางใดทางหนึ่งของ MPRs (รูป 3) แต่ละเราเตอร์ยังเก็บรักษาชุดของตัวเลือก MPR นั่นคือเราเตอร์ที่เลือกเราเตอร์นี้เป็น MPR

ใน OSPF MPR LSA ท่วมเฉพาะตามรากของ MPR ที่โหนดที่เกิดเท่านั้น ในอีกคำหนึ่ง เราเตอร์ flooded LSA มากขึ้นเมื่อได้รับจาก MPR ที่เลือกไว้

OSPF-OR [37] ได้ใช้เทคนิค MPR เช่นกัน ถึงแม้ว่า MPRs ตอนนี้จะเรียกว่าการถ่ายทอดข้อมูลแบบทับซ้อนกัน (OR) เราเตอร์แต่ละตัวเลือก ORs ที่ใช้งานอยู่จากชุดของ OR ที่ติดกันหรือ ซึ่งตัวใกล้เคียงถูกพิจารณาเป็น OR ถ้ามันสามารถเข้าถึงเราเตอร์ที่เราเตอร์ไม่สามารถเข้าถึงได้โดยตรง นั่นคือ 2-hop (hop คือ การเดินทางของแพคเกตข้อมูลที่เกิดขึ้นจาก router) จากพื้นที่ใกล้เคียงของเราเตอร์ที่ถือหรือถ้ามันสามารถเข้าถึงเราเตอร์

ขณะที่ใน OSPF-MPR, ORs ที่ใช้งานโดยกำหนด 2-hop ที่ใกล้เคียงให้สามารถเชื่อมถึงกันผ่าน ORs ที่ใช้งานอยู่

ในทำนองเดียวกันกับ OSPF-MPR ถ้าเราเตอร์ได้รับ LSA จากเพื่อนบ้านซึ่งก็คือ ORsที่เปิดใช้งานอยู่ เราเตอร์จะถ่ายทอด LSA ออกจากอินเตอร์เฟส MANET เดียวกันกับที่รับ LSA ทันที

อย่างไรก็ตาม ไม่เหมือนกับ OSPF MPR หากเราเตอร์ยังมีบทบาทในการ flooding ของ LSA ถ้าเป็น OR ถึงแม้ว่าจะไม่ได้ใช้งานก็ตาม สำหรับเพื่อนบ้านที่ส่ง LSA

ORs ที่ไม่เปิดใช้งานนั้นไม่ได้ถ่ายทอด LSA ที่ได้รับมาทันทีแต่มันจะเริ่มทำงานตัวจับเวลาและฟังสำหรับการถ่ายทอดของ LSA นี้ หรือ ACK ของมันโดยเพื่อนบ้าน ถ้าเพื่อนบ้านทั้งหมดมีถ่ายทอด LSA หรือ ACK ของมันก่อนตัวจับเวลาเริ่ม เราเตอร์ไม่จำเป็นต้องถ่ายทอด LSA ถึงแม้ว่า เราเตอร์อาจเลือกที่จะไม่ถ่ายทอด LSA นี้ถ้าเราเตอร์ได้ยินการถ่ายทอดที่จะไปถึงเพื่อนบ้านทั้งหมดซึ่งเป็น เพื่อนบ้าน 2-hop ของเราเตอร์จากที่ได้รับ LSA หรืออีกทางหนึ่งคือเราเตอร์ถ่ายทอด LSA เมื่อตัวจับเวลาเริ่ม ระยะเวลาถูกกำหนดแตกต่างกันไปตามช่วงที่ให้เพื่อที่ตัวจับเวลาเริ่มต่างกันไปตาม ORsที่ยังไม่ใช้งานในการรับ LSA

2) การลดโครงสร้างใน MANETs: การลดโครงสร้างกลไกที่ใช้โดยส่วนขยายของ OSPF สำหรับMANETs จุดประสงค์คือเพื่อรายงานเฉพาะข้อมูลของโครงสร้างเป็นบางส่วนใน LSAs ในขณะที่ทำให้มั่นใจว่า LSDBs ประกอบด้วยข้อมูลที่เพียงพอต่อการเชื่อมต่อเครือข่าย ดังนั้นการลดขนาด LSA ทั้งสองขนาดและจำนวนของ LSAs ที่จำเป็นต้องทิ้ง

OSPF MPR [36] รายงานเฉพาะถ้อยคำ (adjacencies) ระหว่าง MPRs และ MPR ที่ถูกเลือกใน LSAs ของพวกเขา สิ่งนี้ช่วยลดจำนวนของการเชื่อมโยงที่จำเป็นต้องจะรายงานในขณะที่ทำให้มั่นใจว่าเส้นทางที่สั้นที่สุดยังคงเป็นเครือข่ายที่มี การคำนวณไว้แล้วและเส้นทางที่ใช้ใช้เพียง adjacencies เท่านั้น

OSPF MDR [38] เสนอตัวเลือกต่างๆ เกี่ยวกับการเชื่อมโยงที่มีรายชื่อใน LSAs ขึ้นอยู่กับค่าพารามิเตอร์ของ LSAFullness ด้วยค่าที่ต่ำสุดของ LSAFullness LSAs จะรายงานเฉพาะจำนวนน้อยที่สุดของการเชื่อมโยงเพื่อให้เครือข่ายยังเชื่อมโยงกันได้ แต่การคำนวณเส้นทางอาจใช้ระยะเวลานานกว่าที่จำเป็น แต่ด้วยค่า LSAFullness ที่สูง LSAs จะรายงานการเชื่อมต่อที่มากขึ้น เพื่อให้มั่นใจว่าการคำนวณเส้นทางจะสั้นที่สุดขณะที่ค่าใช้จ่ายก็สูงขึ้น และด้วยค่า LSAFullness สูงที่สุด LSAs รายงานการเชื่อมต่อทั้งหมด อย่างไรก็ตาม ข้อเสียข้อหนึ่งของ OSPF MDR คือการคำนวณเส้นทางอาจใช้การเชื่อมต่อที่ไม่ใช่ adjacencies

OSPF- OR [37] เลือกนำเสนอว่า LSAs รายงานเฉพาะ adjacencies โดยผ่าน Smart peering (ดูส่วน IV-C) ด้วยเหตุนั้นเรา

เตอร์จึงอยู่ติดกันเฉพาะกับเพื่อนบ้านใหม่ซึ่งยังไม่สามารถไปถึงต้นไม้ที่มีเส้นทางที่สั้นที่สุดได้ (SPT) สิ่งนี้ช่วยลดจำนวนของการเชื่อมโยงที่จำเป็นต้อง advertized ใน LSAs แต่โดยทั่วไปอัตราเส้นทางยาว

ส่วนขยายของ OSPF สำหรับดวดมาเนท์ยังใช้กลไก Hello redundancy Reduction Incremental hellos [37] และdifferential hellos [38] อนุญาตให้เราเตอร์รายงานเฉพาะการเปลี่ยนแปลงที่สังเกตเห็นในละแวกผ่าน HelloIntervalล่าสุดแทนละแวกข้อมูลที่เสร็จสมบูรณ์ ดังนั้นถ้าโครงสร้างคงที่ แพ็คเกต Hello ส่วนใหญ่ขนาดจะเล็กลงอย่างมากอย่างไรก็ตาม ในการทำเช่นนี้ การส่งผ่านที่ล้มเหลวอาจส่งผลต่อ Hello synchronism และอาจทำให้ความสามารถของ Nodeในการติดตามการเปลี่ยนแปลงของเพื่อนบ้านไม่เป็นไปตามที่ควรในการที่จะป้องกันกรณีเช่นนี้ ควรเพิ่มกลไกการตรวจสอบช่องว่างหมายเลขลำดับในการรับแพ็คเกจ Hello Differential Hello ใช้ synchronism เชิงรุก Recovery กลไก ในขณะที่ Incremental Hello ให้ผู้รับดูแลในส่วนการจัดการ synchronism กลไกเหล่านี้จะยังสามารถติดตามโครงสร้างที่มีเสถียรภาพน้อยกว่าแต่ไม่ได้เสนอการประหยัดค่าโสหุ้ยที่สำคัญในบริบทดังกล่าว [40]

VI. สายงานตารางคำนวณ

เมื่อรับเราเตอร์ใหม่หรือเครือข่าย LSAเราเตอร์จำเป็นต้องสร้างตารางสายงานขึ้นใหม่จาก scratch [1], [2]กระบวนการนี้เกี่ยวข้องกับการคำนวณ

1) เส้นทางภายในพื้นที่สำหรับบริเวณ OSPF ทั้งหมดซึ่งเป็นของเราเตอร์(โดยปกติจะใช้เส้นทางที่สั้นที่สุดของ Dijkstra (SPT) อัลกอริธึม [62], [63] บนเนื้อหาของเราเตอร์และเครือข่าย LSAs) และ

2) เส้นทางภายในพื้นที่โดยการตรวจสอบเนื้อหาทั้งหมดที่สรุปของ LSAs

3) เส้นทางภายนอกAS โดยการตรวจสอบเนื้อหาทั้งหมดของ ASE LSAs

ปกติเราเตอร์แกนหลักอาจมีมากถึงหลายร้อยเราเตอร์/เครือข่าย LASs และมากถึงหลายพันโดยรวม/ASE LSAs ในการเชื่อมโยงในฐานข้อมูลสถานะการคำนวณเส้นทางภายในพื้นที่โดยใช้อัลกอริทึมของDijkstra(กับความซับซ้อนของการเวลาO (n × log(n))) ใช้เวลาไม่กี่มิลลิวินาทีบนเราเตอร์ที่ทันสมัย [64], [65] เวลานี้สามารถลดลงได้อีกโดยใช้ ไดนามิก SPT อัลกอริทึม (ส่วน VI-B)แทนการใช้อัลกอริทึมของDijkstra การตรวจสอบ/ทดลองโดยรวมของ ASE/LSAsอาจใช้เวลาอย่างมากตามจำนวนของ LSAs ถ้าผลการคำนวณตารางสายงานมีการเปลี่ยนแปลงใน hops ถัดไปเพื่อจุดหมายอื่น ข้อมูลเหล่านี้จำเป็นต้องถ่ายทอดไปยัง line card เราเตอร์ที่ทันสมัยทำให้การคำนวณตารางและการกระจายตัวของ hops ถัดไปไปสู่ line card พร้อมต่อการใช้งาน ลำดับการติดตั้งของ hops ถัดไปสามารถที่จะเรียงความสำคัญเพื่อ hops ที่มีความสำคัญมากกว่า (เช่นไปยัง VoIP gateway destination) ถูกติดตั้งเป็นสิ่งแรกและทำที่ว่างให้เพื่อการส่งต่อเร็วขึ้นกว่าตัวที่มีความสำคัญน้อยกว่า [64], [66] Francois และคณะ [64] รายงานการหน่วงเวลาระหว่างการคำนวณของการฮอปถัดไปและการปลอมแปลงข้อมูลนี้ไปสู่ line card เพื่อเป็นลำดับของ 50ms บนเราเตอร์ที่ทันสมัย ดังนั้น การคำนวณตารางสายงานอาจทำให้เราเตอร์ CPU ยุ่งเป็นเวลานาน (～100ms)ที่เหลือของส่วนนี้เราอธิบายกลไกเป็นสิ่งแรกเพื่อใช้ในการหลีกเลี่ยงการคำนวณตารางสายงานที่มีเป็นประจำในกรณีการเปลี่ยนแปลงโครงสร้าง ภายหลังเราอธิบายอัลกอริทึมของ Dijkstra เช่นเดียวกับที่ไดนามิคอัลกอริทึมใช้เพื่อสร้างเส้นทางต้นไม้ที่สั้นที่สุดระหว่างการคำนวณตารางสายงาน กลไกอธิบายในส่วนที่เหลือของเซคชั่นและสรุปในตาราง VI

A. ความล่าช้าในการวางแผนการคำนวณตารางสายงาน

การเปลี่ยนแปลงโครงสร้างทั่วไป เช่น ความล้มเหลวของเราเตอร์อาจทำให้เกิด LSAs ใหม่ๆ ขึ้นมา (หนึ่ง LSAs สำหรับแต่ละเราเตอร์ซึ่งเราเตอร์ที่ล้มเหลวได้ adjacency) ลักษณะการเปลี่ยนแปลงของโทโพโลยีที่ (เช่น ไม่ว่าการเชื่อมโยงหรือเราเตอร์ลงหรือขึ้น) วิธีการตรวจสอบความล้มเหลวในการใช้ (เช่นใช้ฐาน Hello หรือฐานฮาร์ดแวร์) และค่าของพารามิเตอร์ OSPF เช่น HelloInterval และ minLSInterval กำหนดช่วงเวลาที่จะส่งผลกระทบต่อเราเตอร์จะก่อให้เกิด LSAs ใหม่ สมมุติว่ามาตรฐาน OSPF flooding LSAs เหล่านี้จะเดินทางผ่านเส้นทางที่สั้นที่สุดจากเราเตอร์เดิมของมันไปที่เราเตอร์เฉพาะ เวลาที่ LSAs เดินทางมาถึงเราเตอร์เฉพาะขึ้นอยู่กับช่วงเวลาที่ LSAs เหล่านี้ถูกสร้างขึ้น เส้นทางที่แน่นอนตามด้วย LSAs ไปที่เราเตอร์เป้าหมาย การใช้ pacing/flood ทำให้ช้าโดยเราเตอร์และจราจรบนการเชื่อมโยงที่สำรวจโดย LSAs เหล่านี้ (ซึ่งกำหนดการเข้าคิวช้าและความน่าจะเป็นของการสูญหายสำหรับ LSAs เหล่านี้) ดังนั้น จึงมีโอกาสเป็นไปได้สูงที่ผล LSAs จากการเปลี่ยนแปลงของโทโพโลยีถึงเราเตอร์เป้าหมายในช่วงเวลามีมาก

กลไกการทำงาน	คำอธิบาย	ข้อดี / ข้อเสีย
Fixed hold time	กำหนดค่า delay ตัว (ช่วง Hold Time) บังคับระหว่างเส้นทางตามลำดับ	หลีกเลี่ยงเส้นทางที่มากเกินไปแล้วคำนวณตารางที่Topology มีการเปลี่ยนแปลง ทำให้ระบบเสถียร แต่จะเกิดการหน่วงของกระบวนการ Convergence
SPF throttling[67]	ช่วง Hold Time สั้น ได้รับ Packet LSA อย่างน้อยหนึ่ง Packet ในช่วง Hold Time ถ้าไม่ได้รับ LSA ในช่วง Hold Timeจะปรับใหม่ให้มีค่าน้อยที่สุด	การ Convergence รวดเร็วหลีกเลี่ยง การค้นหาเส้นทางที่ไม่จำเป็นเมื่อ Topology มีการเปลี่ยนแปลงค่า LSAs Reset hold time ถ้าไม่ได้รับ LSA
SPF throttlingwith quietperiod [68]	เหมือนกันกับ SPF throttling โดยที่Hold time จะReset ให้มีค่าน้อยเฉพาะเมื่อLSA ที่เข้ามามีขนาดใหญ่	ข้อดีของการอุด SPF ให้ไม่มีการตั้งค่าก่อนถึง Hold Time ที่เหมาะสม
Juniper scheme [69]	ก่อนเวลาการคำนวณตารางเส้นทางเล็กน้อยทำจะมีการคำนวณที่โดยใช้ Hold Time นานๆ ถ้าไม่ได้รับLSA ในช่วง Hold Time นานๆก็จะรีเซ็ตค่าให้มีขนาดเล็ก	การ Convergence เร็วที่สุดเมื่อ Topology มีการเปลี่ยนแปลงโดยการคำนวณ Routing Table ปริมาณน้อย และจำกัดความถี่ในการคำนวณ Topology ที่มีขนาดใหญ่
LSA correlation [68]	ความสัมพันธ์ของLSAs ในการระบุการเปลี่ยนแปลงTopology พื้นฐาน การคำนวณตารางเส้นทางเกี่ยวกับการระบุการเปลี่ยนแปลงTopology	ช่วยให้Convergence รวดเร็วต่อการเปลี่ยนแปลงTopologyที่มีจำนวนน้อยที่สุดของการกำหนดเส้นทางการคำนวณตาราง
Dynamic SPTalgorithms [5][71]–[74]	จากการแก้ไขที่มีSPT มากกว่าการสร้าง SPT ใหม่ตั้งแต่เริ่มต้นมักจะใช้ได้ใน Router เชิงพาณิชย์[70]	การปรับปรุงในการกำหนดเส้นทางการคำนวณตารางครั้งตั้งแต่การคำนวณ SPT ไม่ได้เป็นขั้นตอนที่ใช้เวลานานที่สุดในการคำนวณตารางเส้นทาง

ตารางที่ 6 การปรับปรุงการคำนวณเส้นทางของ ROUTING TABLE

ถ้าเราเตอร์มีขึ้นเพื่อแสดงการคำนวณตารางสายงานทันทีเมื่อมีการรับการ LSA ใหม่ อาจจบลงที่ทำการคำนวณดังกล่าวหลายครั้งอย่างรวดเร็วซึ่งอาจทำให้เราเตอร์ CPU ยุ่งอยู่ประมาณหลายร้อยมิลลิวินาทีและขัดขวางไม่ให้ทำงานสิ่งอื่นที่มีความสำคัญกว่า เช่น timely generation และการประมวลผลข้อความสวัสดี สถานการณ์ดังกล่าวไม่พึงประสงค์เพราะอาจนำไปสู่การที่เครือข่ายเส้นทางไม่แน่นอน (network-wide routing instability) [22] ดังนั้นเราเตอร์เชิงพาณิชย์โดยทั่วไปไม่ควรทำการคำนวณตารางสายงานทันทีเมื่อได้รับ LSA ใหม่ Ciscoเราเตอร์ที่ใช้ IOS รุ่นเก่า ใช้ค่าพารามิเตอร์ spfHoldTime แบบคงที่ ต่อจากนี้เรียกว่าเวลาค้าง การจำกัดความถี่ของการปรับปรุงตารางเส้นทางการหนึ่งครั้งต่อ 10วินาที นอกจากนี้ยังมี spfDelay (5 วินาที) ในการคำนวณตารางสายงานการผลิตหลังจากได้รับ LSA ใหม่อันแรกตั้งแต่การคำนวณตารางสายงานการผลิตก่อนหน้านี้

ในขณะที่ spfDelay คงที่และจำกัดพารามิเตอร์sptHoldTime จำนวนของการคำนวณตารางสายงานการผลิตและจึงช่วยหลีกเลี่ยงความไม่เสถียรของสายงานการผลิต พวกเขาทำให้การรวมกันของเราเตอร์ช้าลงไปจนถึงการเปลี่ยนแปลงโทโพโลยีใหม่ ด้วยค่าเริ่มต้น (5 วินาทีสำหรับ spfDelay และ 10 วินาทีสำหรับ spfHoldTime) เราเตอร์อาจใช้เวลาใดก็ได้ระหว่าง 5 ถึง 15 วินาทีเพื่อเข้าใกล้การเปลี่ยนโทโพโลยีหลังจากได้รับการ LSA ใหม่ เพื่อให้เกิดความสมดุลย์ในความจำเป็นสำหรับการบรรจบกันอย่างรวดเร็วและความเสถียรของสายงาน เราเตอร์Cisco ลง 12.2 (14) กับ IOS ใช้โครงร่างการ backoff ที่เรียบง่ายเพื่อปรับและค้างเวลาระหว่างการคำนวณตารางสายงานอย่างต่อเนื่อง [67] ในโครงร่างนี้กล่าวถึง SPF throttling ใน Cisco literature เวลาค้างระหว่างการคำนวณตารางสายงานถูกกำหนดที่ค่าขนาดเล็ก อย่างไรก็ตาม ใบเสร็จของหนึ่งหรือมากกว่า LSAs ในระหว่างการกดค้างทำให้ค่าสูงจากสองเท่าถึงสูงสุด

ดังนั้นการบรรจบอย่างรวดเร็วสามารถนำไปสู่การเปลี่ยนแปลงโทโพโลยี ที่นำไปสู่การสร้างเท่าจำนวนขนาดเล็กของ LSAs (เช่น ล้มเหลวในการเชื่อมโยงแบบปัจเจก) สำหรับการเปลี่ยนแปลงของโทโพโลยีนำไปสู่การสร้างของ LSAs จำนวนมากของ LASs ที่มาถึงเราเตอร์ผ่านช่วงเวลาขยายเพิ่มเติม เวลาค้างคาดว่าถึงจะถึงค่าสูงสุดอย่างรวดเร็วและดังนั้นจึงจำกัดจำนวนของการคำนวณตารางสายงานที่ค่าใช้จ่ายของความล่าช้าที่เกิดขึ้น อย่างไรก็ตามโครงร่างนี้จะเสี่ยงต่อการตั้งค่าใหม่ที่ไม่พึงประสงค์ในเวลาค้างไปถึงค่าเริ่มต้นขนาดเล็กถ้า LSA ไม่มีมาถึงสำหรับช่วงเวลาเท่ากับค่าเวลาคงค้างของปัจจุบัน การตั้งค่าเวลาค้างใหม่ที่ไม่พึงประสงค์ดังกล่าวสามารถหลีกเลี่ยงด้วยการร้องขอระยะเวลาที่ค่อนข้างเงียบนานในระหว่างที่ไม่มี LSA ใหม่มาถึงในเวลาที่ควร ก่อนที่จะเวลาค้างจะสามารถกลับไปที่ค่าเริ่มต้นเล็ก [68] แทนที่จะแสร้งค่าเวลาคงค้างสำหรับการมาอย่างต่อเนื่องของ LSA เราเตอร์Juniper ถูกใช้สองค่าคงที่สำหรับรอเวลา [69] จำนวนที่แน่ชัด (โดยค่าเริ่มต้น 3) ของการคำนวณตารางสายงานถูกแสดงด้วยค่าของเวลาค้างขนาดเล็ก (โดยค่าเริ่มต้นที่

200ms) ถ้า LSAs ใหม่มาถึงอย่างต่อเนื่อง การคำนวณตารางสายงานที่ตามมาจะเกิดมีค่าของเวลาค้างมาก (โดยค่าเริ่มต้น 5 วินาที) เวลารอมีการตั้งค่าที่ค่าขนาดเล็ก ถ้าเราเตอร์ไม่ได้รับ LSA ใหม่ระหว่างเวลาที่รอนานหลังจากการการคำนวณตารางสายงาน สมมุติฐานพื้นฐานหลังโครงสร้างนี้คือ ส่วนใหญ่โทโพโลยี LSAs ใหม่จะมาที่เราเตอร์ภายในไม่กี่ร้อยมิลลิวินาที บรรจบกันอย่างรวดเร็วกับการปลี่ยนแปลงโทโพโลยีดังกล่าวสามารถรับโดยใช้ค่าเวลารอไม่นาน มาตราส่วนขนาดใหญ่ของการเปลี่ยนแปลงโทโพโลยีที่ส่งผลต่อเนื่องมาถึงการรับ LSAs ใหม่ผ่านช่วงเวลาขนาดใหญ่ จะทำให้ค่าเวลาคงค้างขนาดใหญ่มีผลมาและจำกัดความถี่ของการคำนวณตารางสายงาน

สำหรับเครือข่ายส่วนใหญ่ การกำหนดชุดรูปแบบเวลาค้างเพื่อการค้าปิดที่ดีระหว่างการหน่วงเวลาบรรจบกันและจำนวนของการคำนวณตารางสายงานไม่เป็นง่าย โดยเฉพาะการกำหนดค่าเวลาอาจส่งผลทั้งการบรรจบกันหน่วงเวลามากเกินไปหรือมีการคำนวณตารางสายงานมากเกินไปสำหรับการเปลี่ยนแปลงโทโพโลยี ข้อควรพิจารณาเหล่านี้กระตุ้นวิธีการอื่นเพื่อจัดตารางเวลาการคำนวณตารางสายงาน ในวิธีการนี้ที่เรียกว่าสหสัมพันธ์ของ LSA [68] โดยตัว LSA ไม่ได้กระตุ้นการคำนวณตารางสายงาน แต่โดยตัว LSAs จะเทียบเคียงเพื่อตรวจสอบการเปลี่ยนแปลงโทโพโลยีที่เกิดจากการสร้างของพวกเขา การคำนวณตารางสายงานสามารถดำเนินการโดยได้ทันทีที่ LSAs ทั้งหมด สร้างขึ้นตามการเปลี่ยนแปลงของโทโพโลยี ได้มาถึงที่เราเตอร์และมีการระบุการเปลี่ยนแปลงของโทโพโลยี ดังนั้นการเทียบเคียงสหสัมพันธ์ของ LSA ไม่เพียงแต่หลีกเลี่ยงการรอเวลาที่เกี่ยวข้องกับความล่าช้าในการบรรจบกันเท่านั้น แต่คำนวณตารางสายงานที่จำเป็นโดยใช้ LSAs เฉพาะบางชุดเท่านั้น มาตราส่วนขนาดใหญ่ของการเปลี่ยนแปลงโทโพโลยีเช่นการรีบูตพร้อมๆกันของเราเตอร์จำนวนมาก สามารถจัดการโดยเพิ่มการบังคับใช้ไดนามิครอเวลาระหว่างการคำนวณตารางสายงานการผลิตต่อเนื่อง

B. ไดนามิกแบบ SPT อัลกอริทึม

SPT ของ Dijkstra อาจจัดประเภทเป็นอัลกอริทึมแบบคงที่เนื่องจากการสร้างแผนภูมิเส้นทางที่สั้นที่สุด (SPT) จาก แบบร่างเมื่อใดก็ตามที่ดำเนินการ เริ่มแรก SPT มีส่วนประกอบแค่โหนดราก เช่น โหนดดำเนินงานอัลกอริทึม โหนดเชื่อมต่อโดยตรงไปที่รากที่มีกำหนดระยะทาง(Root) เช่นเดียวกับต้นทุนของการเชื่อมโยงไปยังรากในขณะที่โหนดอื่นๆ มีกำหนดระยะทางอนันต์ ในแต่ละการทวนโหนดที่มีระยะทางไกลสุดจากรากถูกเพิ่มไปที่ SPT และระยะทางที่เกี่ยวข้องกับ ออกจากต้นไม้เพื่อนบ้านจะปรับปรุงให้เล็กลงจากระยะห่างของต้นฉบับและระยะทางของพวกเขาจากรากผ่านโหนดที่ถูกเพิ่มไปยังแผนภูมิ การทวนซ้ำมีจนกระทั้งโหนดทั้งหมดถูกรวมไว้ใน SPT

โดยทั่วไปเส้นทางต้นไม้ที่สั้นที่สุด ก่อนและหลังการโครงสร้างเปลี่ยนอย่างมีนัยสำคัญมีคาบเกี่ยวกัน ตัวอย่างเช่นเมื่อการเชื่อมโยง x: y ลงไปหรือเพิ่มขึ้นในค่าใช้จ่ายเพียงโหนดในทรีเชื่อมต่อกับที่มีอยู่ผ่านทาง SPT link X: Y จะต้องมีการรีการเชื่อมต่อกับ SPT ตำแหน่งของโหนดอื่น ๆ ใน SPT ไม่ได้รับผลกระทบจากเรื่องนี้ เหตุการณ์การเปลี่ยนแปลงโครงสร้าง แม้จะอยู่ใน เชื่อมต่อไปยังกิ่งย่อยที่มีอยู่ SPT ผ่าน link X: Y, มันอาจจะเป็นเป็นไปได้ที่จะแนบไปหลายสาขา SPT ใหม่โดยไม่ต้องใด ๆ การเปลี่ยนแปลงรูปที่ 6 แสดงตัวอย่างหนึ่งดังกล่าวที่ กิ่งย้อยที่เชื่อมโยงล้มเหลวต้องปรับเปลี่ยนน้อยมากสำหรับการเชื่อมต่อส่วนที่เหลือของ SPT เมื่อ link X: Y ลดลงในค่าใช้จ่ายในทรีย่อยที่เชื่อมต่อกับ SPT ที่มีอยู่ผ่านทางลิงค์นี้จะไม่ได้รับผลกระทบ

มากกว่าการคำนวณ SPT ใหม่ตั้งแต่เริ่มต้นต่อไปนี้การเปลี่ยนแปลงโครงสร้างแบบไดนามิก SPTอัลกอริทึมแก้ไข SPT ที่มีอยู่ อัลกอริทึมดังกล่าวจำนวนมากเป็นภาพรวมของ อัลกอริทึมของ Dijkstra [5], [71] - [73] ในแง่ที่ว่าต่อไปโหนดเพิ่ม SPT เป็นหนึ่งกับระยะทางที่สั้นที่สุดเพื่อดึงกลยุทธ์หนึ่งที่แสดงถึงผลในการคำนวณน้อยลง[74] คือการเลือกโหนดกับการลดลงมากที่สุด (หรืออย่างน้อยเพิ่มขึ้น)

ในระยะห่างที่เกี่ยวกับการเปลี่ยนแปลงโครงสร้างหลายการใช้งาน OSPF เชิงพาณิชย์ (เช่น, [70]) ในขณะนี้ให้ใช้ขั้นตอนวิธีแบบไดนามิกสำหรับการคำนวณเป็น SPTตัวเลือกการกำหนดค่า

VII. GRACEFULRESTART

เราเตอร์ที่ทันสมัยมีสถาปัตยกรรมกระจายกับ CPU ทำงานกลางโปรโตคอลค้นหาเส้นทางเช่น OSPF ในขณะที่บัตรสายจัดการงานของส่ง packet (เช่นย้ายแพ็คเก็ตจากอินเทอร์เฟซหนึ่งไปยังอีกที่หนึ่ง) นี้แยกชัดเจนของการควบคุมและส่งต่อที่อยู่ให้เราเตอร์เพื่อดำเนินการต่อการทำงานของการส่งต่อแพ็คเก็ต แม้ระดับชั้นเส้นทางจะถูกเริ่มต้นใหม่เพราะกิจกรรมตามแผน(เช่นการอัพเกรดซอฟต์แวร์)

โดยปกติ ระดับชั้นการควบคุมเริ่มต้นใหม่ จะทำให้เราเตอร์เพื่อนบ้านแบ่งความต่อเนื่องกันด้วยเราเตอร์นี้ เราเตอร์เพื่อนบ้านที่จะสร้างLSAs ใหม่ ที่ครอบคลุมตลอดทั้งพื้นที่ และเราเตอร์ทั้งหมดในพื้นที่จะต้องดำเนินการ (หลาย) ตารางเส้นทางคำนวณรับ LSAs เหล่านี้ ไม่กี่นาทีภายหลัง เมื่อระดับควบคุมเริ่มใหม่เสร็จ เราเตอร์เพื่อนบ้านจะสร้างความต่อเนื่องกันกับเราเตอร์นี้และ lsa จำนวนมากของ ลำดับการคำนวณตารางสายงานการผลิตจะ ต้องทำซ้ำ ตั้งแต่ที่ส่งต่อระดับฟังก์ชันปกติ แม้ว่าระดับชั้นควบคุมเริ่มต้นใหม่ ไม่จำเป็นสำหรับเครือข่ายที่จะได้รับความสับสนวุ่นวายนี้

ด้วยการเริ่มต้นใหม่ที่ดี [75] เราเตอร์ซึ่งเป็นระดับชั้นควบคุมเกี่ยวกับการเริ่มการทำงาน และระดับชั้นส่งต่อเป็นการทำงานปกติจะส่ง LSA ของเพื่อนบ้านที่อยู่ใกล้เคียง ประกาศความตั้งใจที่จะดำเนินการเริ่มต้นที่ดีภายในระยะเวลาผ่อนผันที่ระบุ เราเตอร์ดังกล่าวเรียกว่า initiating Router การทำงานที่ดีของ LSAs จะเชื่อมโยง

ท้องถิ่น (link-local) ในขอบเขต คือเพื่อนบ้านที่อยู่ติดกันครอบคลุม LSAs เหล่านี้ เพื่อนบ้านติดกัน เรียกว่า helpers ยังคงรายการเราเตอร์เริ่มต้นอย่างอย่างสมบูรณ์ที่อยู่ติดกันใน LSAs ทั้งหมดในช่วงระยะเวลาผ่อนผัน ดังนั้น จะช่วยเหลือซ่อนระดับชั้นควบคุมการเริ่มต้นใหม่ ของเราเตอร์เริ่มต้น จากส่วนที่เหลือของเครือข่ายในระหว่างช่วงเวลาผ่อนผัน เมื่อรีสตาร์ทระดับชั้นควบคุมเราเตอร์เริ่มต้น ต้องผ่านขั้นตอนก่อตั้งความต่อเนื่องกันปกติด้วย helpers ทั้งหมด ในตอนท้ายของการที่เราเตอร์เริ่มต้นและผู้ช่วยสร้าง router/network LSAs กลไกในการเริ่มการทำงานที่ดีงามจะมีอยู่ในเราเตอร์เชิงพาณิชย์ [76],[77]

VIII. PROACTIVE APPROACHES TO FAILURE RECOVERY

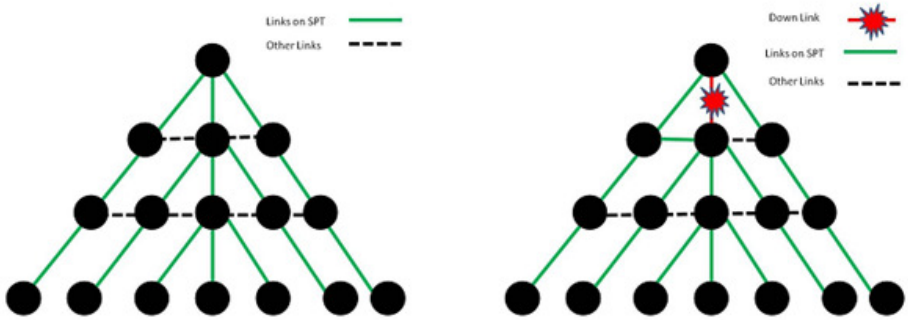
การกู้คืนความล้มเหลวของ OSPF นั้นเป็นเรื่องปกติทั่วไป ตัวอย่างเช่น เส้นทางใหม่ที่จะใช้ในกรณีของเหตุการณ์ที่มีความล้มเหลวจะถูกกำหนดหลังจากที่มีความล้มเหลวเกิดขึ้น วิธี Reactive นั้นเป็นพื้นฐานที่ช้ากว่าวิธี Proactive ที่เส้นทางใหม่จะคำนวณล่วงหน้าก่อนที่จะมีความล้มเหลวเกิดขึ้น ดังนั้นจึงจำเป็นที่จะต้องมีการกู้คืนความล้มเหลวอย่างรวดเร็วซึ่งได้มีการกระตุ้นให้เกิดการพัฒนา Proactive Failure Recovery Mechanisms ขึ้นบน Internet วิธี Proactive มีเป้าหมายคือการกู้คืนความล้มเหลวอย่างรวดเร็ว (ประมาณ50ms) ในส่วนนี้จะอธิบายถึงกลไกทั้งสองกลไกคือ Multi-Protocol Label Switching Fast Reroute (MPLS FRR) และ IP/label distri-bution protocol fast reroute (IP/LDP FRR หรือ simply IP FRR) ข้อมูลของทั้งสองประเภทได้สรุปไว้ในตารางที่ 7
วิธีการเหล่านี้เป็นส่วนหนึ่งของวิธีการด้านจราจรต่างๆของวิศวกรรม [81]-[83] ที่มีจุดมุ่งหมายสำหรับ Traffic Load Distribution ในความต้องการของเครือข่าย

A. Multi-protocol Label Switching Fast Reroute (MPLS FRR)

MPLS [27], [28] คือกลไกการเชื่อมต่อเชิงการส่งต่ออย่างรวดเร็วบน Labels แทนการจับคู่ความยาวของ Prefix MPLS อยู่ระหว่างชั้นที่2และ3ของ Protocol ไม่ได้แทนที่การกำหนดเส้นทาง IP แต่เพื่อเพิ่มการบริการ เช่น Traffic Engineering (TE) ซึ่งรวมถึงความสมดุลของ Traffic Loads การเชื่อมโยงในเครือข่ายและ Fast Reroute (FRR) ข้อมูลนี้จะถูกนำมาใช้โดยMPLSเพื่อสร้างช่องทางที่เรียกว่า Label Switched Paths (LSPs)

MPLS FRR จะขึ้นอยู่กับการใช้งานของ LSPs สำรองเพื่อป้องกัน LSPs หลักในกรณีเกิดความล้มเหลว มันเป็นกลไกการป้องกันที่จุดของการซ่อมแซมภายในที่อยู่ติดกับความล้มเหลว สวิตซ์การเข้าชมของLSPs หลักได้รับผลกระทบจากความล้มเหลว ในการสำรองข้อมูล LSPs [85] ข้อมูลสำรองของ LSP ช่วยให้หลีกเลี่ยงความล้มเหลวและรวมตัวกับ LSPหลัก แผนป้องกันหลายๆแผน เช่น 1+1, 1:1, 1:n และ m:n ที่เป็นไปได้ ในการกำหนดค่าทั้ง 1 +1 และ 1:1 จะแยกการสำรอง LSP เพื่อปกป้องแต่ละ LSPหลัก ความแตกต่างระหว่าง 1 +1 และ 1:1 คือการกำหนดค่าในกรณีที่ไม่มีความเหลวทั้งคู่ และการสำรอง LSP การดำเนินการกำหนดค่าจะเหมือนกับ 1+1 ในการกำหนดค่า 1:n จะสำรองเฉพาะ LSP ที่แชร์โดยn จากLSPหลักในm:n คือการกำหนดค่ากรณีทั่วไปที่m เฉพาะLSPs สำรองที่ใช้ร่วมกันโดยLSPsหลัก (m<=n)

รายละเอียดเกี่ยวกับวิธีการLSP ก่อนการจัดตั้งและกลไกที่ใช้ในการเปลี่ยนเส้นทางการจราจรเพื่อสำรองLSP เมื่อมีการตรวจพบความล้มเหลวMPLS FRR หลีกเลี่ยงการส่งต่อความล้มเหลวและแจ้งเตือนไปยัง Router ต้นทางของLSP หลักดังนั้นความล่าช้าในการกู้คืนความล้มเหลวนั้นคือเวลาที่ตรวจสอบความล้มเหลวและดังนั้นจึงเป็นไปได้ที่จะเกิดการกู้คืนความล้มเหลวอย่างรวดเร็ว(น้อยกว่า 50ms)



(a) The shortest path tree before the link failure (b) The shortest path tree after the link failure

รูปที่ 6 เมื่อการเชื่อมโยงล้มเหลวเฉพาะ Node ใน Sub Tree ของ Root ในเส้นทางเดิมของ Tree ที่สั้นที่สุดต้องทำการReattachment ใน topology ตัวอย่างนี้ การเชื่อมโยงทั้งหมดมีน้ำหนัก

Mechanism	Description	Pros/Cons
MPLS FRR [85]	อ้างอิงจากการใช้งานของ LSPs สำรองเพื่อป้องกัน LSPs หลักในกรณีเกิดล้มเหลว	ต้องการโครงสร้างพื้นฐาน MPLS
MPLS FRR Mechanisms		
IP FRR [86]	อ้างอิงจาก Router Directing Traffic ไปยังเส้นทางสำรองก่อนการคำนวณในกรณีที่เกิดความล้มเหลวภายใน	กู้คืนความล้มเหลวอย่างรวดเร็วใน MPLS FRR
IP FRR Mechanisms		
Equal Cost Multi Path	Router ส่ง Packet ไปตามเส้นสำรองที่มีค่าเดียวกับเส้นทางที่ล้มเหลว	ส่วนหนึ่งของมาตรฐาน OSPF
Loop Free Alternate [87]	Router ส่ง Packet ไปยังการเชื่อมต่อที่ใกล้เคียงทันทีที่มีเส้นทางที่ปลอดภัยไปยังปลายทางของ Packet	
Multihop Repair Paths [86]	Router ส่ง Packet ให้กับการเชื่อมต่อที่ใกล้เคียงกัน ฮ็อปหรือมากกว่านั้น ที่มีเส้นทางที่ 2 ปลอดภัยไปยังปลายทางของ Packet ใช้เมื่อ ECMP / LFA ไม่สามารถใช้ได้	ยากที่จะกำหนดและเรียกใช้
Multihop Repair Path Mechanisms		
Not-via Address [88]	Special address ถูกกำหนดห้ามไม่ให้ Router ผ่านไปถึงการเชื่อมต่อที่ใกล้เคียงกัน เมื่อ Router ตรวจพบความล้มเหลวในการเข้าถึงของ Next Hop สำหรับ Packet Router B จะส่งต่อ Packet ”not-via B” ไปยัง Router C Next Hop จาก Router B	
U Turn Alternates [89]	การเชื่อมต่อใกล้เคียงกันจะพิจารณา Router เป็น Next Hop สำหรับสำหรับปลายทางของ Packet และมี LFA สำหรับปลายทางที่ไม่ได้นำ Packet กลับไปที่ Router การตรวจสอบความล้มเหลวในการเข้าถึง Next Hop Router จะส่ง Packet ไป U Turn Alternate	
Tunnels [90]	Router Tunnels แพ็คเก็ตต่อ Router ที่มันสามารถเข้าถึงปลายทางผ่านการส่งต่อ IP แบบปกติ	

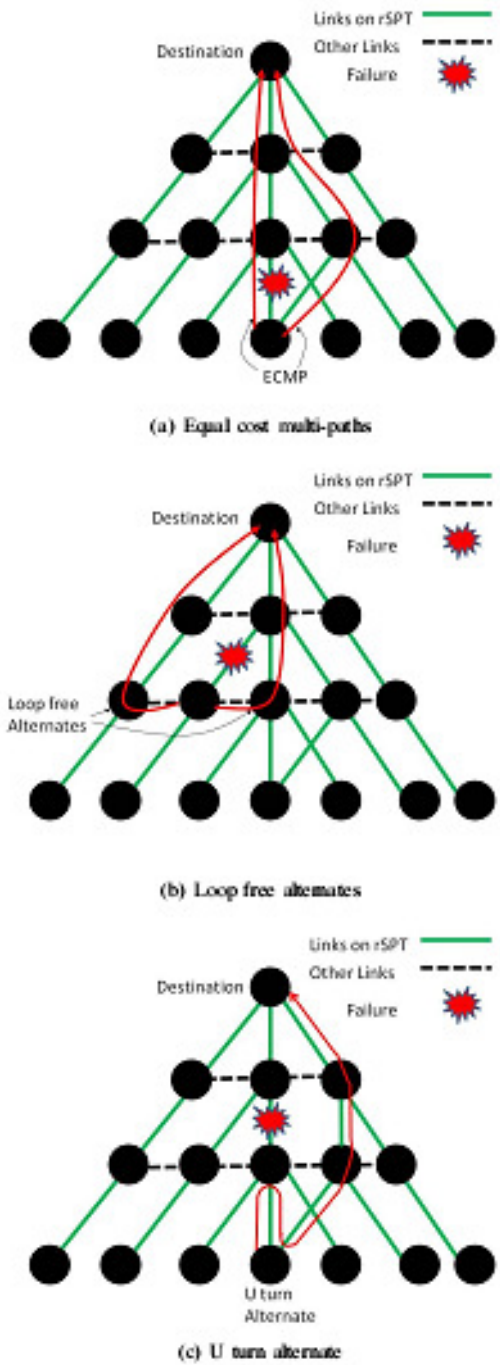
ตารางที่ 7 กลไกในการปรับปรุงเส้นทางด้วย 7MPLS / IP

B. IP Fast Reroute (IP FRR)

MPLS-FRR ต้องใช้เครือข่าย IP ให้มีโครงสร้างพื้นฐาน MPLS ในกรณีที่เลวร้ายที่สุดจะใช้ O(nk) และ $O(nk^2)$LSPs เพื่อจัดการความล้มเหลวของการเชื่อมโยงและโหนดตามลำดับที่ n คือจำนวนของโหนดและ k คือจำนวนของการเชื่อมโยงในเครือข่าย ปัญหาเหล่านี้นำไปสู่ความสนใจในวิธี[92]Proactive เพื่อบรรเทาผลกระทบจากการกู้คืนความล้มเหลวของ IGP ขนาดใหญ่ในเครือข่าย IP แผนการดังกล่าวจำแนกเป็น IP Fast Reroute (IP FRR) [[86, [[93เพื่อพยายามที่จะหลีกเลี่ยงการสูญเสียของข้อมูลที่เกิดจากความไม่สอดคล้องกันเราเตอร์FIBS ระหว่างเวลา IGP Convergence ที่เกิดขึ้น

IP FRR คล้ายกับ MPLS FRR ในแง่ที่ว่าทั้งสองชุดของแผนการนั้นขึ้นอยู่กับการคำนวณเส้นทางสำรองที่ทำให้การกู้คืนความล้มเหลวภายในของ Router ตรวจสอบความล้มเหลวโดยไม่จำเป็นต้องรีบแจ้งเราเตอร์อื่น ๆ เกี่ยวกับความล้มเหลวนั้น IP FRR แตกต่างจาก MPLS FRR เพราะมันไม่ได้ใช้ LSPs MPLS เป็นเส้นทางสำรอง ใน IP FRR Router ก่อนคำนวณจะปรับปรุงเส้นทางที่จะใช้สำหรับความล้มเหลวของแต่ละพื้นที่ที่เป็นไปได้ ถ้า Router รู้เกี่ยวกับ Equal Cost Multi- Paths(ECMP) สำหรับปลายทางและบางส่วนของเส้นทางเหล่านี้ไม่ได้ตัดผ่านความล้มเหลว เส้นทางดังกล่าวสามารถจะใช้เป็นเส้นทางในการซ่อมแซมได้ ในกรณีที่ไม่มีเส้นทางดังกล่าว Router จะมองหาการเชื่อมต่อที่ใกล้เคียงที่เชื่อมต่อโดยตรงที่มีเส้นทางที่ปลอดภัยคือเส้นทางที่ไม่ได้เดินทางผ่านความล้มเหลวไปยังปลายทาง รูปที่ 7แสดงถึงปริมาณเส้นทางอันหลากหลายที่ใช้ใน IP FRR เกิดจาก Loop Free Alternate และ Uturn Alternate ในภาพทุก Link มีน้ำหนักการเชื่อมโยงหากเส้นทางของ ECMP/LFA ไม่พร้อมใช้งาน Router จะมองหาการเชื่อมต่อที่อยู่ใกล้เคียง สองฮ็อปหรือมากกว่านั้นที่มีเส้นทางที่ปลอดภัยไปยังปลายทาง การซ่อมแซมเส้นทางผ่านทางการเชื่อมต่อที่ใกล้เคียงกันเช่นนี้เรียกว่า Multi-Hop Repair Paths [86] หลายๆ กลไก IP FRR ใช้ Multi-Hop Repair Paths

Multi-Hop Repair Paths เป็นพื้นฐานที่ยากเพื่อที่จะกำหนด รวมถึงการเรียกใช้ อย่างไรก็ตามเป็นที่คาดว่าในเครือข่าย IP ทั่วๆไปเป็นเพียงส่วนเล็กๆของปลายทางที่จะต้องซ่อมแซมเส้นทางดังกล่าว สังเกตว่าการซ่อมแซมเส้นทางนั้นจะใช้เพียงชั่วคราวใน IGP (OSPF) เมื่อ IGP Convergence สิ้นสุดลงแพ็คเก็ตจะถูกส่งต่อโดยใช้เส้นทางใหม่ที่สร้างโดย IGP



รูปที่ 7ปริมาณเส้นทางอันหลากหลายที่ใช้ใน IP FRR เกิดจาก Loop Free Alternate และ Uturn Alternate ในภาพทุก Link มีน้ำหนักการเชื่อมโยง

การเปลี่ยนเส้นทางของการเข้าชมได้รับผลกระทบตามเส้นทางสำรองหลังจากการเชื่อมโยงเกิดความล้มเหลวอาจจะสร้างเส้นทางเกินในบางส่วนของเครือข่าย ดังนั้น Nucciและคณะ [100] ชี้ให้เห็นว่าชุดของLink weights สำหรับเครือข่ายควรจะถูกกำหนดในลักษณะที่มีการเชื่อมโยงมากเกินไปซึ่งสามารถหลีกเลี่ยงได้ทั้งใน

ระหว่างการทำงานตามปกติและในช่วงการเชื่อมโยงเกิดความล้มเหลวชั่วคราว สำหรับเครือข่ายขนาดใหญ่มากการคำนวณก็จะมีความซับซ้อนซึ่งงานนี้สามารถลดลงได้โดยการประเมินของการเชื่อมโยงที่สำคัญเท่านั้น Sridharanและ Guerin [[103แนะนำเทคนิคในการระบุการเชื่อมโยงที่สำคัญในเครือข่ายและแจ้งลดความสำคัญในเวลาที่จำเป็นในการกำหนด Link Weights โดยเฉพาะอย่างยิ่งสำหรับเครือข่ายขนาดใหญ่

นอกจากนี้ยังมีข้อเสนออื่นๆหลายๆข้อเสนอเพื่อป้องกันไม่ให้เส้นทางชั่วคราววนลูป Francois และคณะ แนะนำให้ [104] เพิ่มค่าของการกำหนดเส้นทางของความล้มเหลวของการเชื่อมโยงในแต่ละขั้นตอนเพื่อป้องกันไม่ให้เส้นทางชั่วคราววนลูป ค่าพื้นฐานที่เพิ่มขึ้นของ x สำหรับการเชื่อมโยงล้มเหลวสามารถสร้างเส้นทางวนลูปชั่วคราวเฉพาะในพื้นที่ที่ของเครือข่ายที่มีค่าน้อยกว่าหรือเท่ากับ เนื่องจากเส้นทางเกิดวนลูปขึ้นชั่วคราวเกิดจากการที่ Router ที่ใกล้ชิดกับการเชื่อมโยงการล้มเหลวหรือ Router ปรับปรุง FIBs ก่อน Router ตัวที่ห่างไกลออกไป ลูปดังกล่าวยังสามารถป้องกันได้โดยการที่ต้องให้ Router ปรับปรุง FIBs เท่านั้น หลังจาก Router ลูกในเส้นทางที่สั้นที่สุดของแบบรูปรากต้นไม้นั้นล้ไหลวที่อุปกรณ์ อีกวิธีที่คล้ายกันที่สามรถใช้งานได้ในสถานการณ์ที่เวลาปรับปรุง FIB นั้นมีความสำคัญ ที่จะต้องให้ Router ทุกๆตัวสลับไป FIB ใหม่ที่สอดคล้องกันเพื่อให้ Topology ใหม่ใช้เวลาเดียวกันในทันทีและ Router ทั้งหมดจะคำนวณ FIB ใหม่ วิธีการดังกล่าวต้องทำข้อมูลให้ตรงกันและมีความแม่นยำในด้านเวลาใน Router ทุกๆตัวในเครือข่าย

IX. CONCLUSION

OSPF เป็นหนึ่งใน Protocol ที่นิยมใช้มากที่สุดบน Internet Protocol นี้ได้พิสูจน์แล้วว่ามีความยืดหยุ่นสูงในความต้องการการเปลี่ยนแปลงโครงสร้างพื้นฐานของการกำหนดเส้นทาง แต่ก่อนการออกแบบ Protocol จะมุ่งความสนใจไปที่ความสเถียรภาพและความทนทานต่อความล้มเหลว ซึ่งวัตถุประงสงค์เหล่านี้ก็ประสบความสำเร็จโดยวิธีการหาร Domain เส้นทางเข้าไปในหลายๆพื้นที่และการจำกัด Overhead ในการประมวลผลของ Protocol คุณลักษณะเหล่านี้อยู่ในเครือข่าย OSPF ขนาดใหญ่เพื่อจะทำงานกับ Router ที่ไม่มีประสิทธิภาพได้และเพื่อหลีกเลี่ยง Routing Meltdowns แม้จะพบบ่อยๆในการเปลี่ยนแปลงโครงสร้าง

ถึงแม้ว่าจะมีการกู้คืนหลังจากเกิดความผิดพลาดภายในไม่กี่สิบวินาทีก็ถือว่าเพียงพอแล้วสำหรับการเริ่มต้นใหม่อย่างรวดเร็ว สถานการณ์มีการเปลี่ยนแปลงเพราะมีการใช้งาน Internet เพิ่มขึ้นในด้านของการพาณิชย์ การเสื่อมสภาพของการให้บริการต่างๆที่มากกว่าสองวินาทีนั้นไม่สามารถยอมรับได้ ทั้งในความเป็นจริงและแอพพลิเคชั่นแบบเรียลไทม์ อย่างไรก็ตามความต้องการความรวดเร็วของ Convergence Times จะต้องมีการพบกันโดยไม่มีการเพิ่มค่า Overhead ในการประมวลผลของ Protocol ซึ่งจะมีผลกระทบต่อความเสถียรภาพของเส้นทาง ถึงแม้ว่า Router จำนวนมากจะมีประสิทธิภาพและเชื่อถือได้มากกว่าเมื่อก่อนซึ่งมีการเพิ่มขึ้นอย่างมากในระดับของเครือข่ายซึ่งก็หมายความว่าจำเป็นที่จะต้องจำกัด Overhead ในการประมวลผลของ Protocol ซึ่งยังคงมีความสำคัญแม้กระทั่งทุกวันนี้ ในความเป็นจริงแล้วมีความต้องการที่ชัดเจนเพื่อที่จะลด Overhead ของ Protocol ที่จะทำให้ทำงานในสภาพแวดล้อมใหม่ๆได้ เช่น MANET

ในขณะที่มีการเพิ่มประสิทธิภาพของ OSPF ทั้งในด้านของความรวดเร็วของการ Convergence หรือการประมวลผลของ Overhead การปรับเปลี่ยนแก้ไขของการดำเนินงานต่างๆบน OSPF ต้องไม่ยอมรับความถูกต้องของ Protocol ในทุกๆสถานการณ์โดยเฉพาะการให้ความสำคัญกับเงื่อนไขทั้งหมดที่เป็นไปได้และอาจเกิดขึ้นในการดำเนินการแบบกระจายของ Protocol

ในบทความนี้เรามีความพยายามในการปรับปรุงความเร็วการ Convergence ของ Protocol OSPF และกำจัดความซ้ำซ้อนในการดำเนินงาน ความต้องการสำหรับความรวดเร็วของ Convergence และการขยายความเร็วได้โดยไม่จำกัดความเร็วใน Link State Routing Protocols เป็นความท้าทายในการวิจัยทั้งการเติบโตขนาดใหญ่ของ Domain เส้นทางและมีความซับซ้อนมากยิ่งขึ้น ขนาดพื้นที่เล็กๆนั้นเป็นสิ่งที่ดีจาก Convergence Speed และในมุมมองของการขยายความเร็วได้โดยไม่จำกัดความเร็ว แต่อาจจะเป็นเรื่องยากที่จะประสบความสำเร็จ Domain เส้นทางขนาดใหญ่ที่ระบุข้อจำกัดในการจัดระเบียบพื้นที่ใน Hub และ Spokes Fashion เห็นได้ชัดว่ามีกรณีการตรวจสอบความเป็นไปได้ของการลบข้อจำกัดนี้และปล่อยให้มีการเชื่อมต่อในพื้นที่คล้ายคลึงกับวิธี Autonomous Systems ทิศทางอื่นๆที่เกี่ยวข้องกันงานวิจัยในอนาคตคือการตรวจสอบองค์กรแบบไดนามิกของ Router ในพื้นที่ที่ Router เป็นส่วนประกอบจะรันบน Distributed Algorithm ที่จะตัดสินใจว่า

จะผสมผสานสองพื้นที่ให้เป็นหนึ่งเดียวหรือจะแยกออกเป็นสองพื้นที่

Link State Routing Protocols เป็นองค์ประกอบสำคัญของ Internet ในปัจจุบันจะยังคงทำหน้าที่นี้ต่อไปอีกในอนาคต อย่างไรก็ตามเพื่อสังเกตวิธีการของ Link state routing protocols ซึ่งจะมีผลต่อ Internet ในอนาคตโดยเฉพาะอย่างยิ่งในมุมมองของ Internet ที่ต่อไปจะคาดว่าจะมีการขยายตัวอย่างยอดเยี่ยม ในเครือข่ายขนาดใหญ่ของเซ็นเซอร์ไร้สายวิธี Hybrid ซึ่งเป็นไปได้ที่ Link State Routing Protocols มีการใช้ Domain เส้นทางภายในขนาดเล็กซึ่งในทางกลับกันมีการเชื่อมต่อระหว่างวิธี Distance Vector เห็นได้ชัดว่าข้อความดังกล่าวจะเป็นประโยชน์ Link State Routing Protocols เป็นองค์ประกอบสำคัญของ Internet ในปัจจุบันจะยังคงทำหน้าที่นี้ต่อไปอีกในอนาคต อย่างไรก็ตามเพื่อสังเกตวิธีการของ Link State Routing Protocols ซึ่งจะมีผลต่อ Internet ในอนาคตโดยเฉพาะอย่างยิ่งในมุมมองของ Internet ที่ต่อไปจะคาดว่าจะมีการขยายตัวอย่างยอดเยี่ยม ในเครือข่ายขนาดใหญ่ของเซ็นเซอร์ไร้สายวิธี Hybrid ซึ่งเป็นไปได้ที่ Link State Routing Protocols มีการใช้ Domain เส้นทางภายในขนาดเล็กซึ่งในทางกลับกันมีการเชื่อมต่อระหว่างวิธี Distance vector จะเห็นได้ชัดว่าข้อความดังที่กล่าวมาจะเป็นประโยชน์ต่อ Link State Routing Protocols ซึ่งต้องปรับปรุงแก้ไขต่อไปในด้านการขยายขีดความสามรถและความยืดหยุ่น

REFERENCES

[1] J. Moy, "OSPF version 2," Internet Engineering Task Force, Request For Comments (Standards Track) RFC 2328, April 1998.

[2] R. Coltun, D. Ferguson, J. Moy, and A. Lindem, "OSPF for IPv6," Internet Engineering Task Force, Request For Comments (Standards Track) RFC 5340, July 2008.

[3] J. Hawkinson and T. Bates, "Guidelines for creation, selection and registration of an autonomous system (AS)," Internet Engineering Task Force, Request For Comments (Best Current Practice) RFC 1930, March 1996.

[4] J. McQuillan, "The birth of link-state routing," *IEEE Annals of the History of Computing*, vol. 31, no. 1, January/March 2009.

[5] J. McQuillan, I. Richer, and E. Rosen, "The new routing algorithm for the ARPANET," *IEEE Trans. Commun.*, vol. 28, no. 5, May 1980.

[6] "ISO 10589: Intermediate system to intermediate system routing exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service," 2002.

[7] J. Soldatos, E. Vayias, and G. Kormentzas, "On the building blocks of quality of service in heterogeneous IP networks," *IEEE Commun. Surveys & Tutorials*, vol. 7, no. 1, 2005.

[8] G. Scheets, M. Parperis, and R. Singh, "Voice over the internet: a tutorial discussing problems and solutions associated with alternative transport," *IEEE Commun. Surveys & Tutorials*, vol. 6, no. 2, 2004.

[9] L. Hanzo and R. Tafazolli, "A survey of QoS routing solutions for mobile ad hoc networks," *IEEE Commun. Surveys & Tutorials*, vol. 9, no. 2, 2007.

[10] J. Moy, *OSPF: Anatomy of an Internet Routing Protocol*. Addison-Wesley Professional, 1998.

[11] T. Thomas, *OSPF Network Design Solutions, Second Edition*. Cisco Press, 2003.

[12] C. Boutremans, G. Iannaccone, and C. Diot, "Impact of link failures on VoIP performance," in *Proc. The 12th International Workshop on Network and Operating Systems Support for Digital Audio and Video, Miami, USA*, 2002.

[13] B. Choi, S. Song, G. Koffler, and D. Medhi, "Outage analysis of a university campus network," in *Proc. 16th International Conference on Computer Communication and Networks (ICCCN)*, August 2007.

[14] C. Labovitz, A. Ahuja, and F. Jahanian, "Experimental study of internet stability and backbone failures," in *Proc. The 29th International Symposium on Fault-Tolerant Computing*, 1999.

[15] A. Markopoulo, G. Iannaccone, S. Bhattacharya, C. Chua, Y. Ganjali, and C. Diot, "Characterization of failures in an operational IP backbone network," *IEEE/ACM Trans. Netw.*, vol. 16, no. 4, August 2008.

[16] A. Medem, R. Teixeira, N. Feamster, and M. Meulle, "Determining the causes of intradomain routing changes," University Pierre and Marie Curie," Technical Report, 2009, http://www-rp.lip6.fr/ medem/ inmworkshop tech report.pdf.

[17] Y. Ganjali, S. Bhattacharyya, and C. Diot, "Limiting the impact of failures on network performance," Sprint ATL Tech. Res. Rep., Tech. Rep. RR04-ATL-020666, 2003.

[18] B. Wu, P. Ho, K. Yeung, J. Tapolcai, and H. Mouftah, "Optical layer monitoring schemes for fast link failure localization in all-optical networks," *Accepted for publication in IEEE Commun. Surveys & Tutorials*.

[19] J. Vasseur, M. Pickavet, and P. Demeester, *Network Recovery: Protection and Restoration of Optical SONET-SDH and MPLS*. Morgan Kaufmann Publishers, Inc., 2004.

[20] C. Alaettinoglu, V. Jacobson, and H. Yu, "Towards millisecond IGP convergence," in *NANOG 20*, October 2000.

[21] A. Basu and J. Riecke, "Stability issues in OSPF routing," *Computer Commununication Review*, vol. 31, no. 4, October 2001.

[22] G. Choudhury, "Prioritized treatment of specific OSPF version 2 packets and congestion avoidance," Internet Engineering Task Force, Request For Comments (Best Current Practice) RFC 4222, October 2005.

[23] G. Choudhury, G. Ash, V. Manral, A. Maunder, and V. Sapozhnikova, "Prioritized treatment of specific OSPF packets and congestion avoidance: algorithms and simulations," Technical Report, AT&T, Tech. Rep., August 2003.

[24] M. Goyal, K. Ramakrishnan, and W. Feng, "Achieving faster failure detection in OSPF networks," in *Proc. IEEE International Conference on Communications (ICC 2003)*, 2003, pp. 296–300.

[25] R. Aggarwal, "Applications of bidirectional forwarding detection (BFD)," May 2004, presented at RIPE-48.

[26] K. Kompella and G. Swallow, "Detecting multi-protocol label switched (MPLS) data plane failures," Internet Engineering Task Force, Request For Comments (Standards Track) RFC 4379, February 2006.

[27] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol label switching architecture," Internet Engineering Task Force, Request For Comments (Standards Track) RFC 3031, January 2001.

[28] B. Davie and Y. Rekhter, *MPLS: Technology and Applications*. Morgan Kaufmann, 2000.

[29] D. Katz and D. Ward, "Bidirectional forwarding detection (BFD)," Internet Engineering Task Force, Request For Comments (Standards Track) RFC 5880, June 2010.

[30] , "Generic application of bidirectional forwarding detection (BFD)," Internet Engineering Task Force, Request For Comments (Standards Track) RFC 5882, June 2010.

[31] R. Aggarwal, K. Kompella, T. Nadeau, and G. Swallow, "BFD for MPLS LSPs," INTERNET-DRAFT, draft-ietf-bfd-mpls-07.txt, June 2008, (work in progress).

[32] J. Doyle, "Reducing link failure detection time with BFD," Network World, December 2007, http://www.networkworld.com/community/node/23380.

[33] R. Ogier, "OSPF database exchange summary list optimization," Internet Engineering Task Force, Request For Comments (Informational) RFC 5243, May 2008.

[34] E. Baccelli, T. Clausen, and P. Jacquet, "OSPF database exchange and reliable synchronization in mobile ad hoc networks," in *Proc. IASTED Conference on Wireless Networks and Emerging Technologies (WNET), Banff, Canada*, 2004.

[35] M. Goyal, W. Xie, S. H. Hosseini, K. Vairavan, and D. Rohm, "Improving OSPF dynamics on a broadcast LAN," *Simulation*, vol. 82,

no. 2, pp. 107–129, 2006.
[36] E. Baccelli, P. Jacquet, D. Nguyen, and T. Clausen, “OSPF multipoint relay (MPR) extension for ad hoc networks,” Internet Engineering Task Force, Request For Comments (Experimental) RFC 5449, February 2009.
[37] A. Roy and M. Chandra, “Extensions to OSPF to support mobile ad hoc networking,” Internet Engineering Task Force, Request For Comments (Experimental) RFC 5820, March 2010.
[38] R. Ogier and P. Spagnolo, “Mobile ad hoc network MANET extension of OSPF using connected dominating set CDS flooding,” Internet Engineering Task Force, Request For Comments (Experimental) RFC 5614, August 2009.
[39] S. Venkatesh, “Smart adjacency establishment in OSPF routing protocol,”
Master’s thesis, University of Wisconsin - Milwaukee, 2006.
[40] E. Baccelli, J. Cordero, and P. Jacquet, “Multi-point relaying techniques with OSPF on ad hoc networks,” in *Proc. IEEE International Conference on Systems and Networks Communications (ICSNC)*, September 2009.
462 IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 14, NO. 2, SECOND QUARTER 2012
[41] T. Clausen and P. Jacquet, “Optimized link state routing protocol (OLSR),” Internet Engineering Task Force, Request For Comments (Experimental) RFC 3626, October 2003.
[42] P. Murphy, “The OSPF not-so-stubby area (NSSA) option,” Internet Engineering Task Force, Request For Comments (Standards Track) RFC 3101, January 2003.
[43] J. Moy, “Multicast extensions to OSPF,” Internet Engineering Task Force, Request For Comments (Standards Track) RFC 1584, March 1994.
[44] D. Katz, “Why are we scared of SPF? IGP scaling and stability,” in *NANOG 25*, October 2002.
[45] G. Choudhury, “Models for IP/MPLS routing performance: Convergence,
fast reroute and QoS impact,” in *Keynote Speech at ITCOM Conference on Performance, QoS and Control of Next Generation Communication Networks, Philadelphia, USA*, October 2004.
[46] Cisco, “OSPF link-state advertisement (LSA) throttling,” http://www.cisco.com/en/US/docs/ios/12 0s/feature/guide/fsolsath.html.
[47] , “OSPF update packet-pacing configurable timers,” http://www.cisco.com/en/US/docs/ios/12 2t/12 2t4/feature/guide/ftospfct.html.
[48] P. Pillay-Esnault, “OSPF refresh and flooding reduction in stable topologies,” Internet Engineering Task Force, Request For Comments (Informational) RFC 4136, July 2005.
[49] R. Rastogi, Y. Breitbart, M. Garofalakis, and A. Kumar, “Optimal configuration of OSPF aggregates,” *IEEE/ACM Trans. Netw.*, vol. 11, no. 2, pp. 181–194, 2003.
[50] A. Shaikh, D. Wang, G. Li, J. Yates, and C. Kalmanek, “An efficient algorithm for OSPF subnet aggregation,” in *Proc. International Conference on Network Protocols (ICNP)*, November 2003.
[51] Y. K. Dalal and R. M. Metcalfe, “Reverse path forwarding of broadcast packets,” *Communications of the ACM*, vol. 21, no. 12, pp. 1040–1048, 1978.
[52] B. R. Bellur and R. G. Ogier, “A reliable, efficient topology broadcast protocol for dynamic networks,” in *Proc. IEEE INFOCOM*, 1999, pp. 178–186.
[53] P. A. Humblet and S. R. Soloway, “Topology broadcast algorithms,” *Computer Networks and ISDN Systems*, vol. 16, no. 3, pp. 179–186, 1989.
[54] J. Moy, “Extending OSPF to support demand circuits,” Internet Engineering
Task Force, Request For Comments (Standards Track) RFC 1793, April 1995.
[55] P. Baran, S. Boehm, and P. Smith, “On distributed communication,” Rand Corp., Santa Monica, California,” Technical Report, 1964.
[56] G. Apostolopoulos, D. Williams, S. Kamat, R. Guerin, A. Orda, and T. Przygienda, “QoS routing mechanisms and OSPF extensions,” Internet Engineering Task Force, Request For Comments (Experimental) RFC 2676, August 1999.
[57] G. Apostolopoulos, R. Gu´erin, S. Kamat, and S. K. Tripathi, “Quality of service based routing: a performance perspective,” *SIGCOMM Comput. Commun. Rev.*, vol. 28, no. 4, pp. 17–28, 1998.
[58] M. Takashi, K. Takashi, and A. Michihiro, “Enhancing the network scalability of link-state routing protocols by reducing their flooding overhead,” in *Proc. IEEE Workshop on High Performance Switching and Routing (HPSR)*, June 2003, pp. 263–268.
[59] E. Baccelli, T. Clausen, U. Herberg, and C. Perkins, “IP links in multihop ad hoc networks?” in *Proc. IEEE International Conference on Software Telecommunications and Computer Networks (SOFTCOM)*, September 2009.
[60] “Part 11: Wireless LAN medium access control and physical layer specifications,” *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, 12 2007.
[61] L. Kleinrock and F. Tobagi, “Packet switching in radio channels: Part 1 - carrier sense multiple-access modes and their throughput-delay characteristics,” *IEEE Trans. Commun.*, vol. 23, no. 12, pp. 1400–1416, December 1975.
[62] E. Dijkstra, “A note on two problems in connexion with graphs,” *Numerische Mathematik*, vol. 1, pp. 269–271, 1959.
[63] T. Cormen, C. Leiserson, R. Rivest, and C. Stein, *Introduction to Algorithms*. MIT Press, 2009.
[64] P. Francois, C. Filsfils, J. Evans, and O. Bonaventure, “Achieving subsecond
IGP convergence in large IP networks,” *Computer Commun. Rev.*, vol. 35, no. 3, July 2005.
[65] A. Shaikh and A. Greenberg, “Experience in black-box OSPF measurement,”
in *Proc. 1st ACM SIGCOMM Workshop on Internet Measurement*, November 2001, pp. 113–125.
[66] Juniper, “Applying policies to OSPF routes,” http://www.juniper.net/techpubs/en US/junos9.6/informationproducts/topic-collections/config-guide-routing/routing-applyingpolicies-to-ospf-routes.html.
[67] Cisco, “OSPF shortest path first throttling,” http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products feature guide09186a0080134ad8.html.
[68] M. Goyal, W. Xie, M. Soperi, H. Hosseini, and K. Vairavan, “Scheduling routing table calculations to achieve fast convergence in OSPF protocol,” in *Proc. IEEE Broadnets*, September 2007.
[69] Juniper, “Configuring SPF options for OSPF,” http://www.juniper.net/techpubs/en US/junos9.6/informationproducts/topic-collections/config-guide-routing/routing-configuringspf-options-for-ospf.html.
[70] Cisco, “OSPF incremental SPF.” [Online]. Available: http://www.cisco.com/en/US/docs/ios/12 0s/feature/guide/ospfispf.pdf
[71] P. Franciosa, D. Frigioni, and R. Giaccio, “Semi-dynamic shortest paths and breadth-first search in digraphs,” in *Proc. The 14th Annual Symposium on Theoretical Aspects of Computer Science*, 1997, pp. 33–46.
[72] D. Frigioni, A. Marchetti-Spaccamela, and U. Nanni, “Fully dynamic output bounded single source shortest path problem,” in *Proc. ACMSIAM Symposium on Discrete Algorithms*, January 1996.
[73] G. Ramalingam and T. Reps, “An incremental algorithm for a generalization
of the shortest-path problem,” *Journal of Algorithms*, vol. 21, pp. 267–305, 1996.
[74] P. Narv´aez, K.-Y. Siu, and H.-Y. Tzeng, “New dynamic SPT algorithm based on a ball-and-string model,” *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 706–718, 2001.
[75] J. Moy, P. Pillay-Esnault, and A. Lindem, “Graceful OSPF restart,” Internet Engineering Task Force, Request for Comments (Standards Track) RFC 3623, November 2003.
[76] Juniper, “Configuring graceful restart for OSPF,” http://www.juniper.net/techpubs/en US/junos9.6/informationproducts/topic-collections/config-guide-routing/routing-configuringgraceful-restart-for-ospf.html.
[77] Cisco, “NSF–OSPF (RFC 3623 OSPF graceful restart),” http://www.cisco.com/en/US/docs/ios/12 0s/feature/guide/gr ospf.html.
[78] A. Shaikh, R. Dube, and A. Varma, “Avoiding instability during graceful shutdown of OSPF,” in *Proc. IEEE INFOCOM*, June 2002.
[79] , “Avoiding instability during graceful shutdown of multiple OSPF routers,” *IEEE/ACM Trans. Netw.*, vol. 14, no. 3, June 2006.
[80] A. Raj and O. Ibe, “A survey of IP and multiprotocol label switching fast reroute schemes,” *Comput. Netw.*, vol. 51, no. 8, pp. 1882–1907, 2007.
[81] N. Wang, K. Ho, G. Pavlou, and M. Howarth, “An overview of routing optimization for internet traffic engineering,” *IEEE Commun. Surveys & Tutorials*, vol. 10, no. 1, 2008.
[82] Y. Lee and B. Mukherjee, “Traffic engineering in next-generation

optical networks," *IEEE Commun. Surveys & Tutorials*, vol. 6, no. 3, 2004.
[83] O. Younis and S. Fahmy, "Constraint-based routing in the internet: basic principles and recent research," *IEEE Commun. Surveys & Tutorials*, vol. 5, no. 1, 2003.
[84] N. Ayari, D. Barbaron, L. Lefevre, and P. Primet, "Fault tolerance for highly available internet services: concepts, approaches, and issues," *IEEE Commun. Surveys & Tutorials*, vol. 10, no. 2, 2008.
[85] P. Pan, G. Swallow, and A. Atlas, "Fast reroute extensions to RSVPTE for LSP tunnels," Internet Engineering Task Force, Request For Comments (Standards Track) RFC 4090, May 2005.
[86] M. Shand and S. Bryant, "IP fast reroute framework," Internet Engineering
Task Force, Request For Comments (Informational) RFC 5714, January 2010.
[87] A. Atlas and A. Zinin, "Basic specification for IP fast reroute: Loop-free alternates," Internet Engineering Task Force, Request For Comments (Standards Track) RFC 5286, September 2008.
[88] M. Shand, S. Bryant, and S. Previdi, "IP fast reroute using not-via addresses," INTERNET-DRAFT, draft-ietf-rtgwg-ipfrr-notvia-adresses-06.txt, October 2010, (work in progress).
[89] A. Atlas, "U-turn alternates for IP/LDP fast-reroute," INTERNETDRAFT,
draft-atlas-ip-local-protect-uturn-03.txt, March 2006, (work in progress).
[90] S. Bryant, C. Filsfils, S. Previdi, and M. Shand, "IP fast reroute using tunnels," INTERNET-DRAFT, draft-bryant-ipfrr-tunnels-03.txt, November 2007, (work in progress).
[91] K. Kompella and Y. Rekhter, "OSPF extensions in support of generalized multi-protocol label switching (GMPLS)," Internet Engineering
Task Force, Request For Comments (Standards Track) RFC 4203, October 2005.
GOYAL *et al.*: IMPROVING CONVERGENCE SPEED AND SCALABILITY IN OSPF: A SURVEY 463
[92] M. Gjoka, V. Ram, and X. Yang, "Evaluation of IP fast reroute proposals," in *Proc. COMSWARE*, January 2007.
[93] A. Atlas, G. Choudhury, and D. Ward, "IP fast reroute overview and things we are struggling to solve," North American Network Operators Group (NANOG) 33, January 2005.
[94] S. Nelakuditi, S. Lee, Y. Yu, Z.-L. Zhang, and C.-N. Chuah, "Fast local rerouting for handling transient link failures," *IEEE/ACM Trans. Netw.*, vol. 15, no. 2, pp. 359–372, 2007.
[95] T. Cicic, A. Hansen, A. Kvalbein, M. Hartmann, R. Martin, M. Menth, S. Gjessing, and O. Lysne, "Relaxed multiple routing configurations: IP fast reroute for single and correlated failures," *IEEE Trans. Netw. Service Management*, vol. 6, no. 1, pp. 1–14, March 2009.
[96] P. Psenak, S. Mirtorabi, A. Roy, L. Nguyen, and P. Pillay-Esnault, "Multi-topology (MT) routing in OSPF," Internet Engineering Task Force, Request For Comments (Standards Track) RFC 4915, June 2007.
[97] K. Xi and J. Chao, "IP fast rerouting for single-link/node failure recovery," in *Proc. IEEE Broadnets*, September 2007.
[98] W. Simpson, "IP in IP tunneling," Internet Engineering Task Force, Request For Comments (Informational) RFC 1853, October 1995.
[99] S. Hanks, T. Li, D. Farinacci, and P. Traina, "Generic routing encapsulation
(GRE)," Internet Engineering Task Force, Request For Comments (Informational) RFC 1701, October 1994.
[100] A. Nucci, B. Schroeder, S. Bhattacharyya, N. Taft, and C. Diot, "IGP link weight assignment for transient link failures," in *in Proc. International Teletraffic Congress*, 2003.
[101] B. Fortz and M. Thorup, "Internet traffic engineering by optimizing OSPF weights," in *Proc. IEEE INFOCOM*, March 2000.
[102] A. Ghazala, A. El-Sayed, and M. Mousa, "A survey for open shortest path first weight setting (OSPFWS) problem," in *Proc. The 2nd International Conference on Information Security and Assurance (ISA 2008)*, April 2008.
[103] A. Sridharan and R. Guerin, "Making IGP routing robust to link failures," in *Proc. Networking 2005*, May 2005.
[104] P. Francois, M. Shand, and O. Bonaventure, "Disruption free topology reconfiguration in OSPF networks," in *Proc. IEEE INFOCOM*, May 2007.
[105] P. Francois, "Loop-free convergence using oFIB," INTERNET-DRAFT,
draft-ietf-rtgwg-ordered-fib-02.txt, February 2008, (work in progress).
[106] M. Shand and S. Bryant, "A framework for loop-free convergence," Internet
Engineering Task Force, Request For Comments (Informational) RFC 5715, January 2010.
[107] RFC 2328: 'OSPF version 2', 1998.
[108] RFC 4062: 'OSPF benchmarking terminology and concepts', 2005
[109] http://www.gated.org/
[110] RFC 4061: 'Benchmarking basic OSPF single router control plane convergence', 2005
[111] RFC 4063: 'Considerations when using basic OSPF convergence benchmarks', 2005
[112] J. Moy, "OSPF Version 2," IETF RFC, No. 2328, April 1998.
[113] R. Coltun, D. Ferguson, J. Moy, OSPF for IPv6," Requests for Comments: 2740, December 1999. 2005. Internet-Draft (work in progress) draft-roy-ospf-smart-peering-01.
[114] B. Fortz and M. Thorup, "Internet traffic engineering by optimizing OSPF weights," in Proc. IEEE INFOCOM, Tel Aviv, Israel, pp. 519–528, March 2000.
[115] T. Ye, H. T. Kaur, S. Kalyanaraman, K. S. Vastola and S. Yadav "Dynamic optimization of OSPF weights using online simulation," proceedings of IEEE INFOCOM, 2002.
[116] Zinin, Lindem, D. Yeung, "Alternative Implementations of OSPF Area Border Routers," Request for Comments: 3509, April 2003
[117] P. Murphy, "The OSPF Not-So-Stubby Area (NSSA) Option," Request for Comments: 3101 (Obsoletes: 1587), January 2003.
[118] R. Rastogi, Y. Breitbart, M. Garofalakis, and A. Kumar "Optimal Configuration for OSPF Aggregates", IEEE/ACM Transactions on Networking, Vol. 11, No. 2, April 2003.
[119] P. Narvaez, K.-Y. Siu, and H.-Y. Tzeng. New dynamic algorithms for shortest path tree computation, IEEE Transaction on Networking, vol. 8, pp. 734-746, 2000.
[120] Rocketfuel Project [Online]. Available http://www.cs.washington.edu/research/networking/rocketfuel