

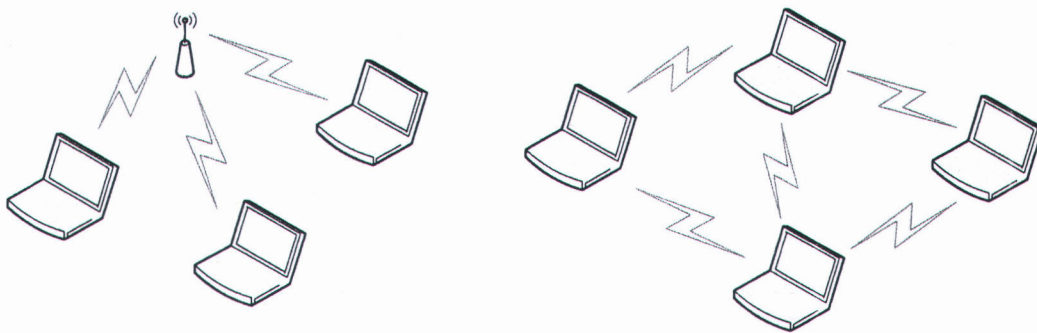
บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 การสื่อสารบนเครือข่ายไร้สายแบบแอดฮอก

เครือข่ายไร้สายแบบแอดฮอกเป็นการสื่อสารไร้สายโดยมีการทำงานแบบ multi-hop ซึ่งต่างจากเครือข่ายไร้สายแบบปกติที่มีระยะการสื่อสารแค่ 1 hop และมีโครงสร้างพื้นฐานเป็นศูนย์กลางในการทำงาน ได้แก่ Access Point ใน Wireless LAN หรือเสาส่งสัญญาณของโทรศัพท์เคลื่อนที่



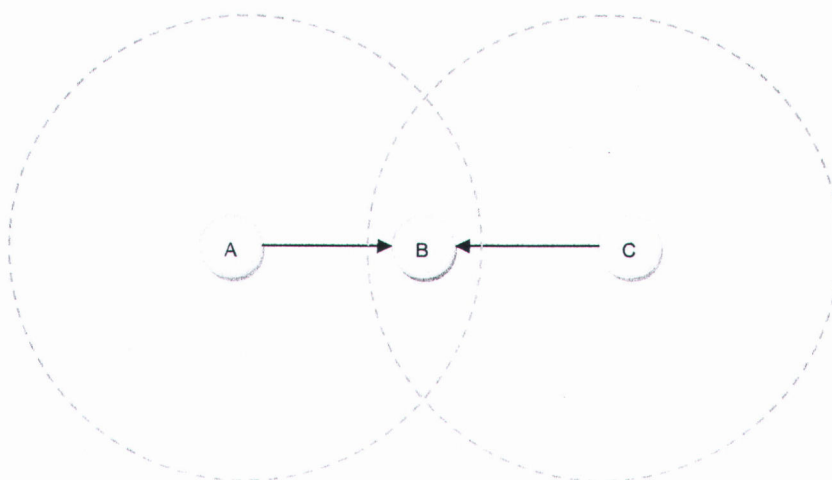
(ก) การทำงานแบบ 1 hop

(ข) การทำงานแบบ multi-hop

รูปที่ 2.1 ความแตกต่างของเครือข่ายไร้สายแบบแอดฮอก

ประโยชน์ของการทำงานบนเครือข่ายไร้สายแบบแอดฮอกคือการทำงานที่ไม่ต้องการโครงสร้างพื้นฐาน ซึ่งการติดต่อสื่อสารสามารถอยู่บนอุปกรณ์ใดๆ อีกทั้งยังสามารถทำงานในพื้นที่ที่ติดตั้งโครงสร้างพื้นฐานไม่ได้ ได้แก่ ในพื้นที่สงคราม หรือในยามที่เกิดภัยธรรมชาติซึ่งโครงสร้างพื้นฐานถูกทำลาย[1] การทำงานโดยไม่ต้องการโครงสร้างพื้นฐานนั้นการพัฒนาสามารถทำได้บนตัวอุปกรณ์โดยตรงไม่เสียเวลา และค่าใช้จ่ายในการติดตั้งและดูแลโครงสร้างพื้นฐาน ทำให้การพัฒนาเป็นไปได้อย่างรวดเร็ว

เนื่องจากการทำงานที่เป็นแบบกระจาย อุปกรณ์ทุกชิ้นมีอิสระในการติดต่อสื่อสาร ซึ่งกระทำผ่านสัญญาณไร้สายที่สามารถเกิดคลื่นรบกวนของสัญญาณ หรือการชนกันของสัญญาณได้ ในกรณีตัวอย่างเช่น มีโหนด A, B และ C ดังต่อไปนี้ กำหนดใน B อยู่ในระยะที่สามารถติดต่อได้ทั้ง A และ C แต่ A และ C นั้นไม่สามารถติดต่อกันได้โดยตรง ปัญหาจะเกิดขึ้นเมื่อ A และ C ส่งสัญญาณไปยัง B พร้อมกัน ทำให้เกิดการชนกันของสัญญาณ เรียกปัญหานี้ว่า Hidden Terminal ทำให้ B ไม่สามารถรับข้อมูลที่ถูกต้องจากทั้ง A และ C ได้ ทำให้เกิดการสูญเสียของข้อมูล [14]



รูปที่ 2.2 ปัญหา Hidden Terminal

ตามมาตรฐานของ IEEE 802.11 [15] ในระดับ MAC นั้น มีการแก้ไขปัญหาของการชนกันของข้อมูลโดยใช้การส่งสัญญาณก่อนการส่งข้อมูลประกอบด้วย Request To Send (RTS) และ Clear To Send (CTS) โหนดที่ต้องการส่งข้อมูลจะต้องส่ง RTS ออกไป จากนั้นโหนดที่จะรับข้อมูลจะตอบกลับด้วย CTS จึงจะสามารถส่งข้อมูลได้ โดยโหนดในบริเวณนั้นที่ได้รับ CTS จะไม่สามารถส่งข้อมูลได้ หากมีโหนดที่ต้องการส่งข้อมูลจะมีการตั้งเวลาเพื่อรอให้ช่องสัญญาณว่าง โดยช่วงเวลาได้จากการสุ่ม และเวลาจะนับถอยลงเมื่อช่องสัญญาณในบริเวณนั้นว่างเท่านั้นเพื่อไม่ให้เกิดการชนของสัญญาณ เมื่อมีการส่ง RTS ใหม่อีกครั้ง จากโหนดที่คอยอยู่เหมือนกัน นอกจากการหลีกเลี่ยงการชนของสัญญาณแล้ว การส่งข้อมูลบนเครือข่ายไร้สายยังสามารถสูญเสียสัญญาณในระยะทางที่เดินทางไป การส่งข้อมูลในระดับ MAC จึงมีการส่งข้อความตอบรับ (Acknowledgement) กลับมา เมื่อการส่งข้อมูลครั้งนั้นสำเร็จ

แม้ในระดับ MAC จะมีการทำให้การส่งข้อมูลมีความเชื่อถือได้ แต่เป็นการทำงานในระดับ 1 hop เท่านั้น การแพร่ข้อมูลที่มีความเชื่อได้เป็นบริเวณกว้างจึงต้องการความช่วยเหลือจากการทำงานในระดับที่สูงกว่า โดยเฉพาะอย่างยิ่งการทำงานบนเครือข่ายรถยนต์ที่มีการเชื่อมต่อเป็นช่วงๆซึ่งต้องการวิธีการทำงานเพิ่มเติมเพื่อให้เกิดความเชื่อถือได้สูงที่สุด

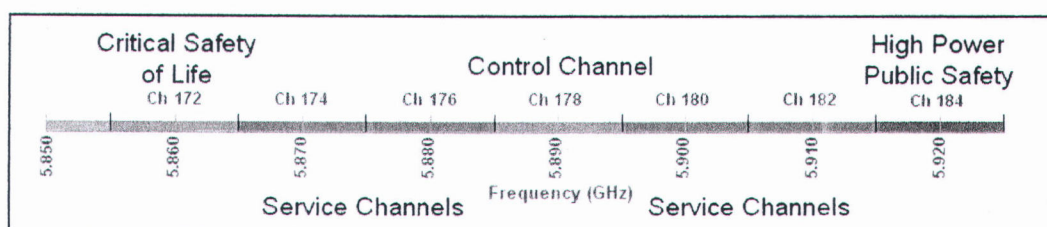
2.1.2 มาตรฐาน IEEE802.11P

เนื่องจากเครือข่ายไร้สายแบบใหม่ที่เกิดขึ้นบนพาหนะเช่นรถยนต์ เพื่อตอบสนองบริการทั้งทางด้านความปลอดภัย รวมทั้งความบันเทิง ซึ่งรถยนต์มีการเคลื่อนที่อย่างรวดเร็วและมีรูปแบบที่ซับซ้อนในการเคลื่อนที่ ดังนั้นการติดต่อสื่อสารจึงมีเวลาสำหรับการเชื่อมต่อและส่งผ่านข้อมูลเพียงสั้นๆ การทำงานตามมาตรฐาน IEEE 802.11 แบบเดิมใช้เวลานานในการเริ่ม

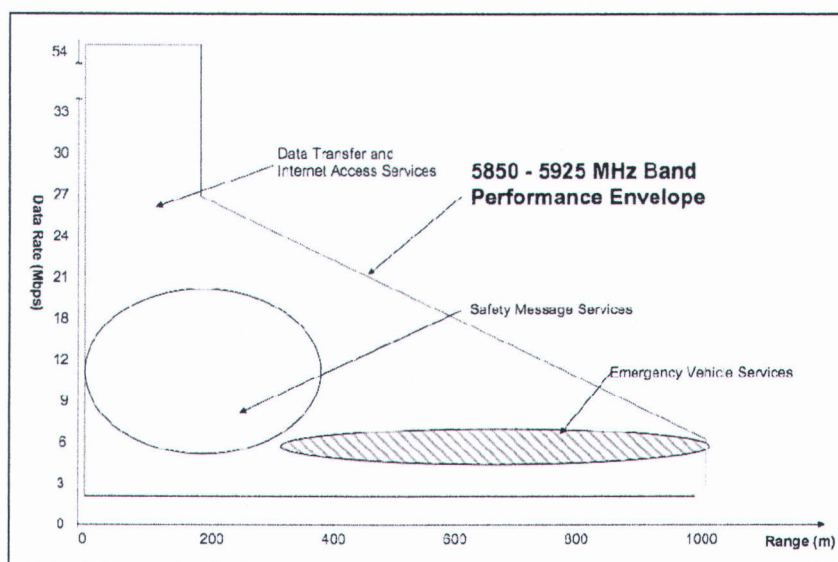
การเชื่อมต่อมากขึ้นไปอีก ทั้งความสามารถในการทำงานในระดับกายภาพที่ต้องทำงานบน โหนดที่มีความเร็วสูง ดังนั้นจึงมีการร่างมาตรฐานใหม่สำหรับการทำงานของระบบการสื่อสารไร้สายจาก IEEE 802.11 [16] โดยใช้ความถี่ที่ 5.9 GHz สามารถสื่อสารระหว่างรถยนต์ หรือรถยนต์กับอุปกรณ์ที่ติดตั้งบนถนนได้ ในระดับความเร็วอย่างน้อย 200 กิโลเมตร/ชั่วโมง และมีระยะทำการของสัญญาณประมาณ 1000 เมตร

จุดเริ่มต้นของ IEEE 802.11p มาจาก DSRC (Dedicated Short Range Communication) และ WAVE (Wireless Access in Vehicular Environment)[17]

Dedicated Short Range Communications (DSRC) เป็นคลื่นความถี่ที่อนุมัติโดย คณะกรรมการการสื่อสารสหรัฐอเมริกา (Federal Communication Commission: FCC) ในปี 1999 มีความถี่ที่ 5.9 GHz จำนวน 75 MHz เพื่อใช้ในการสื่อสารระหว่างรถยนต์-รถยนต์ และ โครงสร้างพื้นฐาน-รถยนต์ โดยมีจุดประสงค์เพื่อพัฒนาระบบที่เพิ่มความปลอดภัยในการขับขี่ และปรับปรุงการทำงานของระบบจราจร แต่ละช่องสัญญาณจะถูกนำมาใช้งานตามรูปที่ 4 ส่วน ในยุโรปใช้คลื่นความถี่ที่ 5 GHz จำนวน 30 MHz ในการทำงาน



รูปที่ 2.3 การจัดสรรช่องสัญญาณ DSRC ของสหรัฐอเมริกา [17]



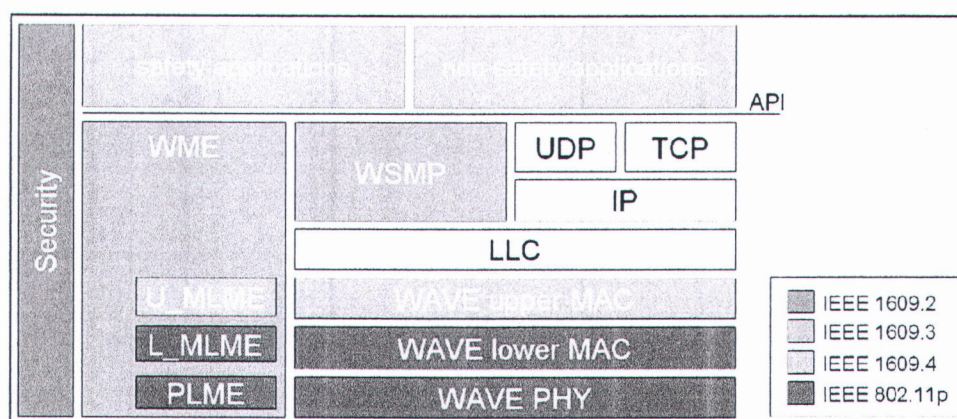
รูปที่ 2.4 ความสามารถในการทำงานของ DSRC ที่ระยะต่างๆ [18]

ในปี 2004 DSRC ถูกย้ายมาพัฒนาต่อในกลุ่มมาตรฐาน IEEE 802.11 โดยใช้ชื่อว่า IEEE 802.11p WAVE (Wireless Access in Vehicular Environment) ซึ่งหากพิจารณาถึง IEEE 802.11p เพียงอย่างเดียวเท่านั้นจะหมายถึงมาตรฐาน ดังต่อไปนี้

- ความสามารถในการทำงานพื้นฐานที่ WAVE ต้องการในสภาพแวดล้อมที่มีการเปลี่ยนแปลงอย่างรวดเร็ว และการแลกเปลี่ยนข้อมูลโดยไม่มีการใช้งาน Basic Service Set (BSS) เหมือนในมาตรฐาน IEEE 802.11 ตัวอื่นๆ
- เทคนิคการใช้สัญญาณ และส่วนต่อประสานของ WAVE ซึ่งถูกควบคุมโดย IEEE 802.11 MAC

ดังนั้น IEEE 802.11p เป็นเพียงส่วนหนึ่งของ WAVE ที่ควบคุมระดับ MAC และ PHY นอกจากนี้จึงมีมาตรฐานในการทำงานอื่นๆที่ถูกกำหนดใน IEEE 1609 ดังนี้

- IEEE 1609.2 : มาตรฐานด้านความปลอดภัย
- IEEE 1609.3 : มาตรฐานด้านการเชื่อมต่อและการจัดการ
- IEEE 1609.4 : มาตรฐานด้านบน IEEE 802.11p เพื่อสามารถทำงานได้บนหลายช่องสัญญาณโดยไม่จำเป็นต้องมีข้อมูลจาก PHY



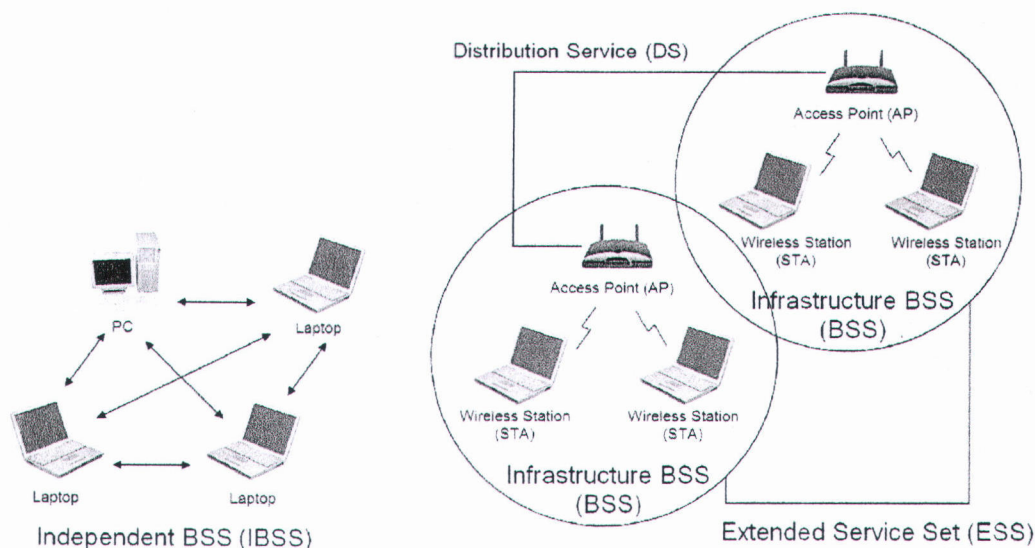
รูปที่ 2.5 มาตรฐานต่างๆของ IEEE ใน DSRC [17]

ความแตกต่างของ IEEE 802.11P และมาตรฐาน IEEE 802.11 อื่น ๆ

ระดับ MAC Layer

โดยปกติในการเชื่อมต่อเครือข่ายไร้สายในมาตรฐาน IEEE 802.11 ตัวอื่นๆจะประกอบด้วยขั้นตอนสำคัญ คือ กระบวนการของ Basic Service Set (BSS) ซึ่ง Access Point (AP) จะใช้ในการกำจัดสัญญาณรบกวนจากคลื่นวิทยุที่ไม่เกี่ยวข้องได้ และโดยมี Extended Service Set ที่รวม BSS ใดๆเป็นแบบ Logical Link Control (LLC) หรือ IBSS (Independent

BSS) ซึ่งใช้ในการทำงานบนเครือข่ายไร้สายแบบแอดฮอค แต่ขั้นตอนในการทำงานที่ใช้เวลานานเกินไป ตั้งแต่การ Beacon Message ของ AP จนถึงขั้นตอนการยืนยันตัวตนและเชื่อมต่อ จึงไม่เหมาะสมสำหรับใช้ในรถยนต์ที่มีเวลาในการเชื่อมต่อสั้นมากๆ และเหตุการณ์ฉุกเฉินที่เวลา มีความสำคัญต่อความปลอดภัย



รูปที่ 2.6 Independent Basic Service Set และ Extended Service Set [17]

ดังนั้นในการทำงานของ IEEE 802.11p จึงมีการทำงาน เรียกว่า “WAVE mode” ซึ่งอนุญาตให้มีการแลกเปลี่ยนข้อมูลโดยค่าของ BSSID เป็น “*” โดยที่ไม่จำเป็นต้องอยู่ใน BSS ใดๆ นั้นหมายความว่ารถยนต์สามารถแลกเปลี่ยนข้อมูลกันได้โดยตรงทันที เมื่ออยู่ในช่องสัญญาณเดียวกัน

การทำงานอีกรูปแบบหนึ่งเรียกว่า “WAVE BSS” (WBSS) โดยขั้นตอนการแพร่ Beacon Message ของ WAVE AP จะทำงานใน WAVE mode โดยมีข้อมูลที่จำเป็นทั้งหมดสำหรับผู้รับในการเป็นสมาชิก WBSS นั้น ดังนั้นขั้นตอนในการเข้าร่วม WBSS จะสามารถทำได้โดยการโต้ตอบแค่ครั้งเดียวเท่านั้น

โหมดที่ทำงานใน WAVE mode จะสามารถแลกเปลี่ยนข้อมูลโดยไม่จำเป็นต้องเป็นสมาชิกของ WBSS แต่จะไม่สามารถเข้าร่วมเป็นสมาชิก BSS หรือ IBSS ได้ และไม่สามารถกระทำการขั้นตอนการยืนยันตัวตนและเริ่มการเชื่อมต่อของ MAC ได้

ระดับ Physical Layer

เนื่องจากการเปลี่ยนแปลงในระดับ MAC ที่สามารถเปลี่ยนแปลงผ่านการปรับปรุงซอฟต์แวร์ได้ ดังนั้นในระดับ PHY จึงมีการจำกัดให้สามารถเปลี่ยนแปลงได้ โดยหลีกเลี่ยงการ



เปลี่ยนการทำงานทั้งหมดของระบบเครือข่ายไร้สาย จึงเลือกใช้มาตรฐาน IEEE 802.11a เป็นมาตรฐานในการพัฒนา ซึ่งมีความกว้างช่องสัญญาณ 20 MHz เป็น 10 MHz และใช้ความถี่ที่ 5.9 GHz แต่ความสามารถในการรับส่งและสัญญาณมีสัญญาณรบกวนได้น้อยตามที่มาตรฐาน IEEE 802.11p กำหนดนั้น [17] มองว่าเป็นเรื่องท้าทายของผู้ผลิตอุปกรณ์ว่าจะสามารถทำได้ตามมาตรฐานหรือไม่

ตารางที่ 2.1 ตารางเปรียบเทียบมาตรฐาน IEEE 802.11 ต่างๆ

IEEE	Release[23]	Frequency (GHz)	Bandwidth (MHz)	Data Rate (Mbps)	Modulation	Outdoor Distance (m.)
802.11a	Sep. 1999	5	20	54	OFDM	120
802.11b	Sep. 1999	2.4	20	11	DSSS	140
802.11g	Sep. 2003	2.4	20	54	OFDM,DSSS	140
802.11n	Oct. 2009	2.4/5	20/40	72.2/150	OFDM	250
802.11p	In progress, IEEE-SA Sponsors Ballots (Last Schedule, Nov. 2010)	5.9	10	6-27	OFDM (doubling 802.11a parameter)	Up to 1000

2.2 งานวิจัยที่เกี่ยวข้อง

งานวิจัยที่พัฒนาการแพร่ข้อมูลแบบเชื่อถือได้บนเครือข่ายไร้สายแบบแอดฮอค สำหรับรถยนต์มักจะถูกพัฒนาอยู่บนพื้นฐานของการทำงานแบบ Store-and-Forward คือ โหนดที่ได้รับข้อความจะเก็บข้อความไว้จนกระทั่งข้อความนั้นหมดอายุ โดยโหนดอาจจะส่งต่อข้อความทันที หรือเก็บข้อความนั้นไว้ เพื่อแพร่ข้อความให้แก่โหนดเพื่อนบ้านที่ยังไม่ได้รับข้อความในเวลาต่อมา มีงานวิจัยที่ออกแบบวิธีการแพร่ข้อมูลบนเครือข่ายไร้สายแบบแอดฮอค สำหรับรถยนต์ที่น่าสนใจดังต่อไปนี้

PGB : Prefer Group Broadcast [6] เป็นขั้นตอนวิธีในการแพร่ข้อมูลสำหรับ ยานพาหนะเพื่อลดการเกิดปัญหาการชนกันของสัญญาณในบริเวณที่มีความหนาแน่นสูง เช่น บริเวณสี่แยกที่มีไฟสัญญาณจราจร เป็นต้น PGB ถูกออกแบบมาเพื่อใช้ในการแก้ปัญหาของการแพร่ข้อความ RREQ ของ AODV ที่เกิดการชนสูง เนื่องจากการแพร่แบบ Simple

สำนักงานคณะกรรมการวิจัยแห่งชาติ
ห้องสมุดงานวิจัย
วันที่.....1.8.ก.ค. 2555.....
เลขทะเบียน.....247861.....
เลขเรียกหนังสือ.....

Flooding ที่ทุกโหนดจะส่งข้อความต่อทันที โดยไม่ใช้ข้อมูลใดๆในการตัดสินใจสำหรับการส่งต่อข้อความ และส่งผลให้ AODV มีประสิทธิภาพลดลงมาก การทำงานของ PGB โหนดจะใช้ระดับสัญญาณของโหนดเพื่อนบ้านในการคำนวณค่าเวลารอ โดยโหนดที่อยู่ห่างจากโหนดต้นทาง (Source) มากกว่าจะมีเวลารอสั้นกว่า ดังนั้นโหนดที่จะแพร่ต่อมาจึงมักจะเป็นโหนดที่บริเวณขอบของวงการแพร่ PGB จึงสามารถลดจำนวนข้อความ RREQ ได้เป็นจำนวนมาก แต่การทำงานของ PGB ยังไม่มีประสิทธิภาพในบริเวณที่มีความหนาแน่นน้อย และ PGB ถูกออกแบบมาเพื่อใช้ในการแพร่ RREQ ซึ่งไม่สนับสนุนการทำงานที่ต้องการการแพร่ข้อมูลความเชื่อถือได้

EAEP : Edge-Aware Epidemic Protocol [10] เป็นโพรโทคอลการแพร่ข้อมูลที่มีความเชื่อถือได้สำหรับเครือข่ายไร้สายแบบแอ็ดฮอคบนยานพาหนะ มีลักษณะการทำงานแบบ Store-and-Forward หลักการทำงาน คือ เมื่อโหนดได้รับข้อความใหม่ โหนดจะคำนวณเวลารอโดยใช้ระยะทางจากตัวมันถึงผู้ส่ง ซึ่งต้องอาศัยข้อมูลตำแหน่งของโหนดจากจีพีเอส โหนดที่มีเวลารอสั้นที่สุดคือโหนดบริเวณขอบของความกว้างสัญญาณของตัวส่ง ในขณะที่อยู่ในช่วงเวลาที่คอยโหนดจะทำการนับจำนวนครั้งที่มีการส่งต่อข้อความจากเพื่อนบ้าน เมื่อหมดเวลารอโหนดจะนับจำนวนครั้งที่เพื่อนบ้านส่งข้อความมาคำนวณหาความน่าจะเป็นที่จะส่งข้อความนั้นต่อ จากหลักการทำงาน EAEP ไม่สามารถทำงานได้บนสภาพแวดล้อมที่มีปัญหาการเชื่อมต่อเป็นช่วงๆ (Intermittent Connectivity) ได้ดี กรณีที่มีโหนดเพื่อนบ้านใหม่เข้ามาบริเวณที่มีการส่งข้อความเสร็จสิ้นแล้ว จะทำให้โหนดเพื่อนบ้านใหม่นั้นไม่ได้รับการส่งข้อความใหม่

การใช้ความน่าจะเป็นมาคำนวณว่าควรมีการส่งต่อข้อความนั้นหรือไม่ย่อมจะทำให้เกิดการส่งข้อความซ้ำมากกว่าหนึ่งครั้งในบริเวณเดียวกันได้ จึงส่งผลให้ประสิทธิภาพในการทำงานลดลง นอกจากนี้จาก [10] พบว่า EAEP สามารถกำหนดทิศทางการแพร่ข้อมูล อีกทั้งยังรองรับการแพร่ข้อมูลอิสระจากความสามารถในการส่งสัญญาณของอุปกรณ์ แต่เป็นการทดลองเพียงในสภาพแวดล้อมที่เป็นถนนทางหลวงเท่านั้น จึงอาจจะสรุปได้ว่า EAEP ถูกออกแบบเพื่อทำงานบนถนนทางหลวง หรืออาจจะทำงานได้ไม่ดีบนถนนในเมือง เมื่อพิจารณาถึงผลการทดลอง [10] EAEP สามารถทำงานได้ดีกว่า Simple Flooding มากทั้งทางด้านความเชื่อถือได้ และประสิทธิภาพ แต่ใช้เวลาในการแพร่ข้อมูลให้กับรถยนต์ส่วนใหญ่บนถนนทางหลวงถึง 30 วินาที ซึ่งไม่สามารถนำไปใช้งานกับบริการที่ต้องการความเร็ว และแม่นยำของข้อมูลสูง

DV-Cast : Distributed Vehicular Broadcast Protocol for Vehicular Ad-Hoc Networks [13] เป็นวิธีการแพร่ที่ออกแบบเพื่อให้แพร่ข้อมูลให้กับรถในบริเวณหนึ่งๆให้ได้รับมากที่สุด ตัวอย่างเช่นเมื่อเกิดอุบัติเหตุขึ้น โหนดต้องการส่งข้อความเตือนไปยังโหนดทั้งหมดที่ตามหลังเป็นระยะทาง 2 กิโลเมตร การทำงานจะอาศัยข้อมูลจีพีเอส และ Beacon Message เพื่อให้โหนดทราบถึงข้อมูลของตำแหน่งและทิศทางของโหนดเพื่อนบ้าน การทำงานจะแบ่งออกเป็นสามกรณี คือ 1) กรณีที่มีโหนดตามหลังที่อยู่ในระยะเชื่อมต่อ จะใช้การแพร่โดยตั้งเวลา

รอ โหนดที่อยู่บริเวณขอบของการแพร่จะมีเวลารอที่สั้นกว่า 2) กรณีที่ไม่พบโหนดตามหลังแต่มีโหนดที่วิ่งในทิศทางตรงข้าม โหนดจะแพร่ข้อความให้กับโหนดในทิศตรงข้ามทันที เพื่อให้โหนดนั้นเก็บข้อความและส่งต่อไปให้โหนดที่ตามหลังโหนดต้น (Source) ที่มีระยะห่างมากกว่าระยะสัญญาณ 3) กรณีที่ไม่พบโหนดใด โหนดจะเก็บข้อความนั้นไว้จนกว่าจะพบโหนดเพื่อนบ้านใหม่ การส่งข้อมูลจะขึ้นอยู่กับความน่าจะเป็นที่โหนดนั้นคำนวณได้จากระยะห่างระหว่างโหนดกับโหนดแพร่ก่อนหน้า (Source/Precursor Node) และค่าความน่าจะเป็นจะลดลงเมื่อได้ยืนยันการแพร่จากโหนดเพื่อนบ้าน

จากหลักการทำงานจะพบว่า DV-Cast มีการทำงานแบบ store-and-forward และมีการทำงานที่คล้ายคลึงกับการทำงานของ EAEP ซึ่งใช้ความน่าจะเป็นในการตัดสินใจการแพร่ข้อมูลของโหนด แต่มีการใช้ Beacon Message เพื่อทราบตำแหน่งและทิศทางของโหนดเพื่อนบ้าน ซึ่งทำให้การแพร่มีโอกาสประสบความสำเร็จมากขึ้น แต่เนื่องจากการออกแบบที่เน้นให้มีการส่งข้อความแบบทิศเดียวมากกว่าทั้งสองทิศพร้อมกัน และโหนดไม่ทราบข้อมูลของข้อความที่เพื่อนบ้านมีจึงทำให้เกิดปัญหาในกรณีที่มีการขาดการเชื่อมต่อเป็นเวลานานได้เช่นเดียวกับ EAEP

AckPBSM : Acknowledge Parameterless Broadcast in Static to Highly Mobile Ad-Hoc Networks [11] เป็นอีกหนึ่งโพรโทคอลการแพร่ข้อมูลที่มีความเชื่อถือได้สำหรับเครือข่ายไร้สายแบบแอ็ดฮอคบนยานพาหนะที่ทำงานโดยใช้หลักการ Store-and-Forward ลักษณะการทำงานของ AckPBSM ในทุกๆ ช่วงเวลาหนึ่งโหนดจะมีการส่ง Beacon Message ให้กับโหนดเพื่อนบ้าน ซึ่งภายในจะประกอบด้วยตำแหน่งของโหนด และการตอบรับ (Acknowledgement) ของข้อความที่โหนดเพื่อนบ้านนั้นได้รับทั้งหมด ตำแหน่งของโหนดเพื่อนบ้านจะถูกนำมาใช้เพื่อสร้าง Connected Dominating Sets (CDS) ซึ่งสามารถคำนวณโดยใช้ระยะห่างระหว่างแต่ละโหนด และความสามารถในการรับส่งสัญญาณ [12] ทำให้โหนดทราบได้ว่าตนเองอยู่ภายในกลุ่มของ CDS หรือไม่ ซึ่ง CDS จะเป็นกลุ่มของโหนดที่ต้องการให้มีการส่งต่อข้อมูลมากกว่า เมื่อมีการแพร่ข้อมูล ทุกโหนดจะมีการตั้งเวลารอโดยที่คำนวณจากจำนวนของเพื่อนบ้านที่อยู่รอบโหนดนั้น ซึ่งโหนดที่อยู่ใน CDS จะมีสมการในการคำนวณเวลาให้ได้ค่าที่น้อยกว่าเสมอ ในกรณีที่เมื่อหมดเวลารอ โหนดจะตรวจจะตรวจสอบว่ายังมีเพื่อนบ้านที่ไม่ได้รับข้อความหรือไม่ ในกรณีที่โหนดได้รับการตอบรับ (ACK) จากโหนดเพื่อนบ้านทุกโหนด โหนดนั้นจะไม่ทำการส่งข้อมูลต่อ ซึ่งจะสามารถลดจำนวนการส่งข้อความในแต่ละครั้งที่มีการแพร่ได้ แต่ในกรณีที่มิเพื่อนบ้านที่ยังไม่ได้รับข้อความก็จะมีส่งต่อให้ตามปกติ จากงานวิจัย AckPBSM สามารถทำงานในสภาพแวดล้อมที่เป็นการจราจรทั้งบนทางหลวงและถนนในเมืองได้ดีกว่า PBSM และ DV-CAST [13] ที่ถูกนำมาเปรียบเทียบ

แต่เนื่องจากการทำงานของ AckPBSM ใช้การคำนวณเวลาจากจำนวนโหนดเพื่อนบ้านเพื่อส่งข้อมูลต่อ ดังนั้นกรณีโหนดที่โหนดใน CDS เหมือนกัน หรือแม้แต่ไม่เป็นโหนดใน

CDS เหมือนกันแต่อยู่ในบริเวณเดียวกัน ย่อมมีโอกาสที่จะมีจำนวนโหนดเพื่อนบ้านเท่ากัน และทำให้เวลาที่คำนวณได้มีค่าเท่ากัน ส่งผลให้มีการแพร่ข้อความนั้นพร้อมๆกัน เกิดการแพร่ซ้ำซ้อนที่บริเวณเดียวกันจำนวนมาก ส่งผลให้ประสิทธิภาพในการทำงานของ AckPBSM จึงลดลงมาก

เมื่อพิจารณาถึงงานวิจัยที่กล่าวมา สามารถสรุปการหลักทำงานของโปรโตคอลได้ตามตารางที่ 2.2 ซึ่งโปรโตคอลทั้งหมดการแพร่ข้อมูลแต่ละครั้งจำเป็นจะต้องมีการตั้งเวลารอเพื่อเก็บข้อมูลหรือคอยฟังโหนดเพื่อนบ้าน ดังนั้นการแพร่แต่ละครั้งจึงใช้ระยะเวลามากขึ้น เวลาที่โหนดในพื้นที่ทั้งหมดจะได้รับข้อความจะขึ้นอยู่กับเวลารอที่ใช้ในการแพร่แต่ละครั้งและจำนวน hop ดังนั้นการส่งผ่านข้อมูลโดยที่มีการกำหนดผู้ส่งไว้ล่วงหน้า สามารถทำให้การส่งต่อข้อความทำได้ทันที และลดจำนวนการแพร่ซ้ำในบริเวณการส่งเดียวกันได้

นอกเหนือจากการจัดการที่ระดับ Network Layer แล้วยังมีงานวิจัยที่พัฒนาการแพร่ข้อมูลที่มีขนาดเล็ก เช่นการแพร่ Beacon Message ให้กับเพื่อนบ้าน ในระดับ MAC Layer [19] งานวิจัยนี้สนใจเวลาที่ถูกใช้ไป และสนใจค่าใช้จ่าย (Overhead) ที่เกิดขึ้นขณะที่รถยนต์มีการแพร่ Beacon Message จำนวนมากเข้าสู่เครือข่าย ซึ่งเมื่อเปรียบเทียบขนาดของ Packet ในการทำ CTS และ RTS ตามมาตรฐาน IEEE 802.11 [15] และ Beacon Message จะมีความแตกต่างขนาดของข้อมูลไม่มากนัก งานวิจัยนี้จึงเสนอวิธีการนำข้อมูลใน Beacon Message แแนบเข้าไปกับ Packet ของ CTS และ RTS เพื่อลดปริมาณการส่งข้อความที่เกิดขึ้นในระบบ จึงเป็นวิธีการการส่งข้อมูลของ Beacon Message ที่น่าสนใจ และนำมาใช้ร่วมกับการทำงานของโปรโตคอลการแพร่ข้อมูลที่มีความเชื่อถือได้สำหรับเครือข่ายไร้สายแบบแอดฮอกบนยานพาหนะ ที่มักจะมีการใช้งาน Beacon Message อยู่แล้ว

ตารางที่ 2.2 ตารางเปรียบเทียบหลักการทางของโปรโตคอลการแพร่ข้อมูลที่มีความเชื่อถือได้สำหรับเครือข่ายไร้สายแบบแอดฮอกบนยานพาหนะ

	PGB [6]	EAEF[10]	DV-CAST[13]	AckPBSM[11]	DECA	POCA
ตัวแปรในการพิจารณาโหนดส่งต่อ (forwarder node)	บริเวณของขอบการแพร่ข้อมูล	บริเวณของขอบการแพร่ข้อมูล	บริเวณของขอบการแพร่ข้อมูล	บริเวณที่เป็นส่วนเชื่อมต่อของกลุ่ม (Connected Dominating Set :CDS)	บริเวณที่มีความหนาแน่นสูง	บริเวณของขอบการแพร่ข้อมูล
วิธีการเลือกโหนดส่งต่อ	ใช้การตั้งเวลารอ	ใช้การตั้งเวลารอและคำนวณค่าความน่าจะเป็น	ใช้การตั้งเวลารอและคำนวณค่าความน่าจะเป็น	ใช้การตั้งเวลารอ	โหนดต้นทาง หรือโหนดก่อนหน้าเป็นผู้เลือก	โหนดต้นทาง หรือโหนดก่อนหน้าเป็นผู้เลือก
เวลาหน่วงที่เกิดขึ้นในการแพร่ข้อมูลแต่ละครั้ง	เวลารอและเวลาการส่ง	เวลารอและเวลาการส่ง	เวลารอและเวลาการส่ง	เวลารอ และเวลาการส่ง	เวลารอและเวลาการส่ง (propagation delay)	เวลารอและเวลาการส่ง (propagation delay)
ความซับซ้อนในการคำนวณเพื่อเลือกโหนดส่งต่อ	$O(1)$	$O(1)$	$O(1)$	$O(n^3)$	$O(n)$	$O(n)$



ตารางที่ 2.2 ตารางเปรียบเทียบหลักการการทำงานของโปรโตคอลการแพร่ข้อมูลที่มีความเชื่อถือได้สำหรับเครือข่ายไร้สายแบบแอดฮอคสำหรับยานพาหนะ(ต่อ)

	PGB [6]	EAEP[10]	DV-CAST[13]	AckPBSM[11]	DECA	POCA
ค่าที่ใช้ในการคำนวณเวลา	ระดับของสัญญาณจาก RSSI	ระยะทางระหว่างโหนดและโหนดก่อนหน้า	ระยะทางระหว่างโหนดและโหนดก่อนหน้า	จำนวนของโหนดเพื่อนบ้าน	จำนวนของโหนดเพื่อนบ้าน	ระยะทางระหว่างโหนดและโหนดก่อนหน้า
การตั้งเวลาจะถูกใช้เมื่อ	ทุกครั้งเมื่อมีการส่งต่อข้อมูล	ทุกครั้งเมื่อมีการส่งต่อข้อมูล	ทุกครั้งเมื่อมีการส่งต่อข้อมูล	ทุกครั้งเมื่อมีการส่งต่อข้อมูล	เฉพาะเมื่อมีการเชื่อมต่อเป็นช่วงๆ	เฉพาะเมื่อมีการเชื่อมต่อเป็นช่วงๆ
ช่วงเวลาในการแพร่ Beacon	ปรับช่วงเวลาตามความหนาแน่นของโหนด	-	ทุก 1 วินาที	ทุก 0.5 วินาที	ปรับช่วงเวลาตามความหนาแน่นของเครือข่าย (ทุก 1.5-7 วินาที)	ปรับช่วงเวลาตามความหนาแน่นของเครือข่าย (ทุก 1.5-7 วินาที)
ข้อมูลภายใน Beacon Message	ข้อมูลจีพีเอส	-	ข้อมูลจีพีเอส	ข้อมูลจีพีเอส และข้อความตอบรับ (Acknowledge Message)	จำนวนเพื่อนบ้าน และข้อความตอบรับ (Acknowledge Message)	ข้อมูลจีพีเอส และข้อความตอบรับ (Acknowledge Message)
การรองรับเครือข่ายที่มีปัญหาขาดการเชื่อมต่อเป็นเวลานาน	ไม่ใช่	ไม่ใช่	ไม่ใช่	ใช่	ใช่	ใช่