การป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งอย่างมีประสิทธิภาพสำหรับเครือข่ายไร้สายเฉพาะกิจของยานพาหนะโดยใช้การสลับโหมดความเป็นส่วนตัว

ร้อยตำรวจเอก วงศ์ยศ เกิดศรี

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
เขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ. 2559

Efficient Location Privacy Protection for Vehicular Ad-Hoc Network using Privacy Mode Switching

Pol.Capt.Wongyos Keardsri

A Thesis Submitted in Partial Fulfillment of the Requirements for

the Degree of Master of Science in Information and Communication Technology

School of Science and Technology

Sukhothai Thammathirat Open University

2016

หัวข้อวิทยานิพนธ์ การป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งอย่างมีประสิทธิภาพสำหรับเครือข่ายไร้สายเฉพาะกิจของยานพาหนะโดยใช้การสลับโหมดความเป็นส่วนตัว

ชื่อและนามสกุล ร้อยตำรวจเอก วงศ์ยศ เกิดศรี

แขนงวิชา เทคโนโลยีสารสนเทศและการสื่อสาร

สาขาวิชา วิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช

อาจารย์ที่ปรึกษา 1. ผู้ช่วยศาสตราจารย์ ดร. ขจิตพรรณ กฤตพลวิมาน

2. อาจารย์ นาวาโท กรกช วิไลลักษณ์

วิทยานิพนธ์นี้ ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 25 สิงหาคม 2558

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ

(อาจารย์ ดร. อำนาจ ขาวเน)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร. ขจิตพรรณ กฤตพลวิมาน)

..... กรรมการ

(อาจารย์ นาวาโท กรกช วิไลลักษณ์)

..... ประธานกรรมการบัณฑิตศึกษา

(รองศาสตราจารย์รสลิน ศิริยะพันธุ์)

ชื่อวิทยานิพนธ์ การป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งอย่างมีประสิทธิภาพสำหรับเครือข่ายไร้สายเฉพาะกิจของยานพาหนะโดยใช้การสลับโหมดความเป็นส่วนตัว
ผู้วิจัย ร้อยตำรวจเอก วงศ์ยศ เกิดศรี **รหัสนักศึกษา** 2549600407
ปริญญา วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศและการสื่อสาร)
อาจารย์ที่ปรึกษา (1) ผู้ช่วยศาสตราจารย์ ดร. ขจิตพรรณ กฤตพลวิมาน
(2) นาวาโท กรกช วิไลลักษณ์ **ปีการศึกษา** 2559

บทคัดย่อ

วิทยานิพนธ์เรื่องนี้มีวัตถุประสงค์คือ 1) กำหนดแบบแผนการป้องกันและปิดบังความเป็นส่วนตัวของตำแหน่งที่ตั้งในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะอย่างมีประสิทธิภาพภายใต้ระดับความเป็นส่วนตัว 3 ระดับที่กำหนดขึ้น 2) นำเสนออัลกอริทึมการสลับโหมดความเป็นส่วนตัวหรือพริมส์ เพื่อใช้สำหรับป้องกันและปิดบังข้อมูล

กระบวนการวิจัยประกอบด้วย 4 ขั้นตอน ดังนี้ ขั้นตอนแรกเป็นการกำหนดระดับความเป็นส่วนตัว 3 ระดับ ที่ประกอบไปด้วยระดับสูง ปานกลาง และต่ำ ซึ่งแต่ละระดับจะมีการกำหนดอัลกอริทึมและรูปแบบการสื่อสารของยานพาหนะเอาไว้อย่างเหมาะสม ขั้นตอนที่สองเป็นการจำแนกและพิจารณาอัลกอริทึมจำนวน 6 อัลกอริทึมที่เคยนำเสนอก่อนหน้านี้ตามระดับความเป็นส่วนตัวที่กำหนดขึ้น ขั้นตอนถัดมาคือการจำแนกรูปแบบการสื่อสารของยานพาหนะ 8 รูปแบบตามระดับความเป็นส่วนตัวที่ได้กำหนดขึ้นเช่นกัน และขั้นตอนสุดท้ายคือการสร้างอัลกอริทึมพริมส์ที่มีการสลับโหมดความเป็นส่วนตัวแล้วทดสอบในสถานการณ์จำลองภายใต้ระดับความเป็นส่วนตัวทั้ง 3 ระดับ

ผลการทดลองพบว่า 1) อัลกอริทึมพริมส์ที่นำเสนอนี้สามารถลดค่าโอเวอร์เฮดในการประมวลผลลงได้เป็นอย่างดี เพราะมีการเลือกใช้อัลกอริทึมที่เหมาะสมกับรูปแบบการสื่อสารของยานพาหนะ ณ เวลาใดเวลาหนึ่ง และ 2) สามารถป้องกันและปิดบังความเป็นส่วนตัวของตำแหน่งที่ตั้งในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะได้อย่างมีประสิทธิภาพ

คำสำคัญ ระดับความเป็นส่วนตัว การสลับโหมดความเป็นส่วนตัว การป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้ง เครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

Thesis title: Efficient Location Privacy Protection for Vehicular Ad-Hoc Network using Privacy Mode Switching

Researcher: Pol.Capt. Wongyos Keardsri; **ID:** 2549600407;

Degree: Master of Science (Information and Communication Technology);

Thesis advisors: (1) Dr.Khajitpan Kritpolviman, Assistant Professor;

(2) Cdr.Korakoch Wilailux; **Academic year:** 2016

Abstract

The objectives of this thesis were 1) to define the effective privacy protection and anonymization scheme for Vehicular Ad-Hoc Network (VANET) based on 3 privacy levels and 2) to propose the Privacy Mode Switching (PriMS) algorithm for data protection and anonymization.

The research methodology consisted of 4 parts as follows: the first part was defining privacy levels as high, medium and low levels in which privacy algorithms and communication patterns for each level were selected appropriately. Secondly, 6 algorithms regarding designated privacy levels were classified and identified. The third part was also classifying and identifying 8 communication patterns regarding privacy levels. Finally, PriMS algorithm was built as the privacy mode switching process and was implemented in simulated scenarios corresponding to 3 privacy levels.

The results showed that 1) the proposed PriMS algorithm was significantly able to reduce the processing overhead due to the appropriate privacy algorithm selection corresponding to vehicle communication patterns at each time instant and 2) this algorithm was able to protect and anonymize the location privacy in VANET efficiently.

Keywords: Privacy levels, Privacy mode switching, Location privacy protection, Vehicular Ad-Hoc Network

กิตติกรรมประกาศ

เป็นระยะเวลา 6 ปีเต็มที่ผู้วิจัยได้เพียรพยายามศึกษาค้นคว้าอย่างมุ่งมั่นจนวิทยานิพนธ์เรื่องนี้สำเร็จลุล่วงไปได้ด้วยดี ซึ่งบุคคลท่านแรกที่ผู้วิจัยขอขอบพระคุณเป็นอย่างยิ่งคือ ผู้ช่วยศาสตราจารย์ ดร.ขจิตพรรณ กฤตพลวิมาน อาจารย์ที่ปรึกษาหลัก ที่คอยให้คำปรึกษา ให้ความช่วยเหลือ และให้คำแนะนำที่เป็นประโยชน์ต่อการทำวิทยานิพนธ์เสมอมา รวมทั้งคอยกระตุ้นและติดตามความก้าวหน้าในการทำวิทยานิพนธ์อย่างต่อเนื่อง อีกท่านหนึ่งคือ อาจารย์ นาวาโท กรกช วิไลลักษณ์ อาจารย์ที่ปรึกษาร่วม ถึงแม้ว่าผู้วิจัยจะขอคำปรึกษาจากท่านไม่บ่อยนัก แต่ท่านก็คอยเป็นกำลังใจในการทำวิทยานิพนธ์อยู่เสมอ

ลำดับต่อมาผู้วิจัยขอขอบพระคุณ อาจารย์ ดร.อำนาจ ขาวเน ที่กรุณามาเป็นประธานกรรมการสอบปกป้องวิทยานิพนธ์เรื่องนี้ และให้ข้อเสนอแนะที่เป็นประโยชน์ต่อการปรับปรุงเนื้อหาของวิทยานิพนธ์ให้ออกมาอย่างสมบูรณ์ครบถ้วนที่สุด

ลำดับต่อมาผู้วิจัยขอขอบพระคุณทุนอุดหนุนสำหรับการทำวิจัยในระดับบัณฑิตศึกษา ประจำภาคปลาย ปีการศึกษา 2556 มหาวิทยาลัยสุโขทัยธรรมาธิราช ที่สนับสนุนเงินทุนในการสร้างสรรค์วิทยานิพนธ์เรื่องนี้ให้ออกมาอย่างสมบูรณ์แบบยิ่งขึ้น

ลำดับต่อมาผู้วิจัยขอขอบพระคุณคณาจารย์หลักสูตรวิทยาศาสตรมหาบัณฑิต แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัย-สุโขทัยธรรมาธิราช ที่ประสิทธิ์ประสาทความรู้อันมีค่ายิ่ง

ลำดับต่อมาผู้วิจัยขอขอบพระคุณผู้บังคับบัญชาทุกท่านจากกองบังคับการสนับสนุนทางเทคโนโลยี (บก.สสท.) และศูนย์ปฏิบัติการสำนักงานตำรวจแห่งชาติ (ศปก.ตร.) ที่กรุณาอนุญาตให้ผู้วิจัยได้ใช้เวลาว่างจากการทำงานในการทำวิทยานิพนธ์จนสำเร็จลุล่วงไปได้ด้วยดี

นอกจากนี้ผู้วิจัยขอขอบคุณเพื่อนสมาชิกไอซีทีรุ่นที่ 1 (ICT-1) ที่สร้างความสนุกสนานในการเรียน และคอยห่วงใยซึ่งกันและกันเสมอมา

สุดท้ายนี้ผู้วิจัยขอขอบพระคุณสมาชิกในครอบครัวทุกคน อันได้แก่ คุณพ่อ คุณแม่ น้องชายทั้งสองคน และหลานชาย ที่คอยให้กำลังใจอยู่เสมอ และท้ายที่สุดนี้ผู้วิจัยขออุทิศผลงานวิทยานิพนธ์เรื่องนี้แด่คุณป้ากระแสร์ เกิดศรี ผู้ล่วงลับและเป็นที่รักยิ่งของผู้วิจัย

วงศ์ยศ เกิดศรี

สิงหาคม 2560

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

สารบัญตาราง (ต่อ)

หน้า

สารบัญภาพ

หน้า

สารบัญภาพ (ต่อ)

หน้า

ภาคผนวก

ผลงานวิชาการที่ได้รับการตีพิมพ์

การกำหนดระดับความเป็นส่วนตัวสำหรับการป้องกันและปิดบังตำแหน่งที่ตั้งในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

Defining Privacy Levels for Location Protection and Anonymization in Vehicular Ad-Hoc Network

วงศ์ยศ เกิดศรี[1] ขจิตพรรณ กฤตพลวิมาน[1] และ กรกช วีไลลักษณ์[2]
[1] สาขาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
[2] กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ กองทัพเรือ
wongyos@gmail.com Khajitpan.Mak@stou.ac.th และ korakoch.w@navy.mi.th

บทคัดย่อ

ปัจจุบันการป้องกันและปิดบังความเป็นส่วนตัวของตำแหน่งที่ตั้งในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะเป็นประเด็นหนึ่งที่สำคัญเพื่อรักษาไว้ซึ่งความเป็นส่วนตัวของตำแหน่งที่ตั้งเมื่อยานพาหนะมีการเคลื่อนที่ไป ณ ตำแหน่งต่างๆ ในแผนที่ โดยเริ่มแรกนั้นได้ใช้การปิดบังข้อมูลให้กลายเป็นชื่อเทียมหรือชื่อปลอมแต่ก็ยังสามารถคาดเดาถึงข้อมูลจริงได้ และการสื่อสารยังใช้การบรอดแคสท์ที่มีการปล่อยสัญญาณอย่างต่อเนื่องทำให้สามารถติดตามเส้นทางจากสัญญาณได้ ต่อมาจึงใช้หลักการปล่อยสัญญาณแบบสุ่มและเป็นช่วงที่ไม่ต่อเนื่องทำให้การติดตามเส้นทางเกิดการขาดตอนและติดตามยากยิ่งขึ้นแต่ก็ทำให้มีโอเวอร์เฮดที่สูงขึ้นด้วยเช่นกัน จากหลักการที่กล่าวมานั้นมีความพยายามที่จะป้องกันความเป็นส่วนตัวให้ได้มากที่สุดเพียงอย่างเดียว ซึ่งในความเป็นจริงการสื่อสารมีสถานการณ์ที่มีความต้องการความเป็นส่วนตัวที่แตกต่างกัน งานวิจัยเรื่องนี้จึงได้นำเสนอและกำหนดระดับความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะที่แตกต่างกัน 3 ระดับ ได้แก่ ระดับสูง ระดับปานกลาง และระดับต่ำ ซึ่งแต่ละระดับจะมีความเหมาะสมกับสถานการณ์การสื่อสารของยานพาหนะที่แตกต่างกันออกไป ทั้งนี้เพื่อลดโอเวอร์เฮดในการประมวลผล และเพิ่มประสิทธิภาพในการทำงานให้สูงขึ้น ทั้งยังสามารถป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งได้อย่างเหมาะสมที่สุด

คำสำคัญ: การปิดบังชื่อ ความเป็นส่วนตัว ระดับความเป็นส่วนตัว ความเป็นส่วนตัวของตำแหน่งที่ตั้ง เครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

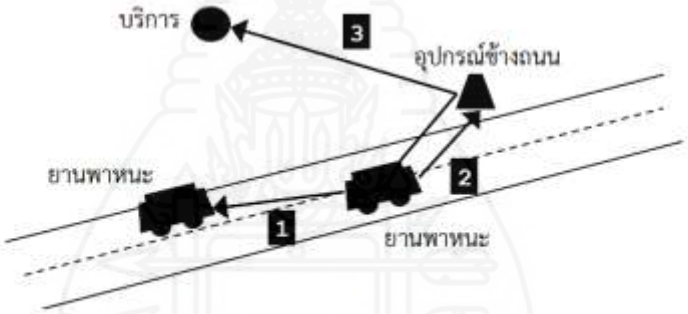
Abstract

Currently, location privacy protection and anonymization in vehicular ad-hoc networks (VANETs) is one of the important issues to preserve location privacy when the vehicle has been moving at different positions on the map. The first research proposes pseudonyms and anonyms to protect data privacy but they can also link to the real data. Moreover, VANET communication is used to broadcast mechanism continuously, so it can follow the path by signal. Next of researches propose the random signal and non-continuous signal that will be more difficult track to the path; however, they have a higher overhead as well. The previous principles were attempted to only protect privacy as possible. In fact, VANET communications have different situations and need for different demand of privacy. Therefore, this research will present the privacy levels and defines into 3 levels: high, medium and low. Each of privacy level is appropriated for the different vehicular communications, in order to reduce the processing overhead and to improve to higher performance, as well as to protect location privacy appropriately.

Key Words: Anonymization, Privacy, Privacy Levels, Location Privacy, Vehicular Ad-Hoc Network

1. บทนำ

การติดตามตำแหน่งที่ตั้ง (Location Tracking) ในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะเป็นกระบวนการหนึ่งที่ตรวจสอบว่ายานพาหนะแต่ละคันนั้นอยู่ ณ ตำแหน่งใดในแผนที่ ซึ่งกระบวนการนี้มีทั้งข้อดีและข้อเสีย โดยถ้านำไปใช้ในการตรวจหาตำแหน่งของยานพาหนะเพื่อทำให้ทราบว่ายานพาหนะคันที่สนใจนั้นอยู่ ณ บริเวณใด หรือใช้ในการติดตามโจรผู้ร้ายก็จะเป็นข้อดีของกระบวนการดังกล่าว แต่ในทางกลับกันถ้านำไปใช้เพื่อพยายามแอบดูข้อมูลยานพาหนะคันอื่นๆ ว่ากำลังเคลื่อนที่ไป ณ ที่ใด การกระทำแบบนี้เป็นการละเมิดความเป็นส่วนตัวของยานพาหนะ และของผู้ขับขี่ยานพาหนะคันนั้น ในขณะเดียวกันการสื่อสารระหว่างยานพาหนะ (Vehicle Communications) บนท้องถนนในแต่ละช่วงเวลานั้นอาจมีรูปแบบการสื่อสารที่แตกต่างกันไปตามการขับขี่และสถานการณ์ต่างๆ ของยานพาหนะได้ดังรูปแบบการสื่อสารในรูปที่ 1 ซึ่งสถานการณ์เหล่านั้นก็ต้องการความเป็นส่วนตัวของตำแหน่งที่ตั้งที่แตกต่างกันออกไป เช่น รถตำรวจ รถดับเพลิง และรถฉุกเฉินที่ไม่ต้องการความเป็นส่วนตัวเลยหรือต้องการความเป็นส่วนตัวน้อยมาก รถของผู้ใช้ตามท้องถนนทั่วไปที่ต้องการความเป็นส่วนตัวในระดับปานกลาง และรถของหน่วยสืบราชการลับที่ต้องการความเป็นส่วนตัวสูง เป็นต้น จะเห็นว่าสถานการณ์ต่างๆ ที่ได้กล่าวมามีระดับความเป็นส่วนตัว (Privacy Level) ที่แตกต่างกันไป ดังนั้นจึงต้องมีการจัดรูปแบบการป้องกันความเป็นส่วนตัวให้สอดคล้องกับสถานการณ์และระดับความเป็นส่วนตัวเหล่านั้นด้วยเช่นกัน งานวิจัยเรื่องนี้จึงได้กำหนดระดับความเป็นส่วนตัวขึ้นมา 3 ระดับ ได้แก่ ระดับสูง ระดับปานกลาง และระดับต่ำ ซึ่งแต่ละระดับจะมีความเหมาะสมกับสถานการณ์การสื่อสารของยานพาหนะที่แตกต่างกันออกไป ทั้งนี้เพื่อลดโอเวอร์เฮด (Overhead) ในการประมวลผลในอัลกอริทึมการปิดบังตำแหน่งที่ตั้งของยานพาหนะ และสามารถเพิ่มประสิทธิภาพในการประมวลผลให้สูงขึ้น ทั้งยังสามารถป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งได้อย่างเหมาะสมที่สุด



1. การสื่อสารระหว่างยานพาหนะกับยานพาหนะ (Vehicle to Vehicle: V2V)
2. การสื่อสารระหว่างยานพาหนะกับอุปกรณ์ (Vehicle to Infrastructure: V2I)
3. การสื่อสารระหว่างยานพาหนะกับบริการ (Vehicle to Service: V2S)

รูปที่ 1 รูปแบบการสื่อสารของยานพาหนะ

2. งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยในประเด็นของการป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งในยานพาหนะพบว่าช่วงเริ่มต้นนั้นได้ใช้การปิดบังชื่อหรือปิดบังข้อมูลของยานพาหนะให้กลายเป็นชื่อเทียมและชื่อปลอม (Pseudonym and Anonym) [1-2] ทำให้การติดตามตำแหน่งที่ตั้งและการติดตามเส้นทางของยานพาหนะทำได้ยากขึ้น ทั้งยังไม่สามารถทราบถึงชื่อหรือข้อมูลจริงของยานพาหนะนั้นได้ แต่การใช้ชื่อเทียมและชื่อปลอมได้ถูกกำหนดแบบตายตัวให้กับยานพาหนะแต่ละคันอย่างถาวรทำให้สุดท้ายแล้วก็สามารถคาดเดาข้อมูลจริงของยานพาหนะนั้นได้ในที่สุด งานวิจัยต่อมาจึงนำเสนอหลักการที่เรียกว่า Mix-Zone [3] ที่กำหนดให้ยานพาหนะมีการเปลี่ยนชื่อเทียมหรือชื่อปลอมอยู่เรื่อยๆ เมื่อเคลื่อนที่ไปยังเขตพื้นที่ (Zone/Area) ที่แตกต่างกันตามขอบเขตที่ได้กำหนดไว้ ทำให้ชื่อของยานพาหนะมีการเปลี่ยนแปลงแบบพลวัตร (Dynamic Name) อยู่ตลอดเวลา แต่อย่างไรก็ตามการสื่อสารของยานพาหนะยังต้องใช้

กระบวนแบบบรอดแคสท์ (Broadcast) ซึ่งมีการปล่อยสัญญาณอย่างต่อเนื่อง ทำให้ยังสามารถติดตามเส้นทางของยานพาหนะนั้นจากสัญญาณได้ดังเดิมถึงแม้ว่าจะมีการเปลี่ยนแปลงชื่อก็ตาม เพียงแต่ทำการเดาชื่อหรือข้อมูลจริงของยานพาหนะนั้นทำได้ยากขึ้นเท่านั้น งานวิจัยต่อมาจึงได้นำเสนอหลักการที่เรียกว่า AMOEBA [4] ซึ่งมีการปล่อยสัญญาณบรอดแคสท์แบบเป็นช่วงไม่ต่อเนื่องโดยกำหนดให้มีช่วงของการเงียบ (Silent Period) และช่วงของการปล่อยสัญญาณ (Broadcast Period) ทำให้การติดตามเส้นทางของยานพาหนะเกิดการขาดตอนและยากยิ่งขึ้นต่อการติดตามเส้นทาง แต่ข้อเสียของงานวิจัยนี้คือมีโอเวอร์เฮด (Overhead) ที่สูงในการประมวลผล งานวิจัยต่อมาได้นำแนวคิดของ AMOEBA ไปประยุกต์ใช้โดยการเพิ่มหลักการเข้ารหัสชื่อแบบสุ่ม (Random Encryption Period: REP) [5] ทำให้ชื่อเทียมหรือชื่อปลอมของยานพาหนะมีการเปลี่ยนแปลงไปแบบสุ่มที่ไม่สามารถคาดเดาได้ และการปล่อยสัญญาณของการบรอดแคสท์ก็ยังเป็นช่วงเวลาที่ไม่ต่อเนื่อง ทำให้การติดตามเส้นทางทำได้ยากยิ่งขึ้นไปอีก แต่อย่างไรก็ตามงานวิจัยนี้ก็เพิ่มโอเวอร์เฮดในการประมวลผลให้สูงยิ่งขึ้นตามไปด้วย งานวิจัยต่อมาซึ่งเกิดขึ้นในช่วงเวลาเดียวกับงานวิจัย [5] ได้นำหลักการของ AMOEBA ไปประยุกต์ใช้เช่นกันแต่จะมีการพิจารณาถึงความหนาแน่น (Density) ของเขตบริเวณที่ยานพาหนะเคลื่อนที่ว่ามีปริมาณยานพาหนะมากน้อยเพียงใด (Density-based Location Privacy: DLP) [6] ซึ่งถ้ามีปริมาณยานพาหนะที่มากเกินกว่าค่าที่กำหนดไว้ (Threshold) ก็จะทำการเปลี่ยนชื่อเทียมและชื่อปลอมของยานพาหนะทันที เพราะเมื่อยานพาหนะที่อยู่ใกล้เคียงเพิ่มขึ้นก็จะทำให้ความเป็นส่วนตัวลดน้อยลงไปจึงต้องมีการเปลี่ยนชื่อหรือข้อมูลของยานพาหนะใหม่เสมอ โดยงานวิจัยนี้สามารถปกป้องความเป็นส่วนตัวในตำแหน่งที่ตั้งได้ดี แต่การประมวลผลก็ยังมีโอเวอร์เฮดที่สูงมากเช่นเดิมทำให้ไม่มีประสิทธิภาพในการทำงาน

3. แนวคิดของงานวิจัย

จากงานวิจัยที่ได้กล่าวไปทั้งหมดในหัวข้อก่อนหน้านี้ยังมีการคำนึงถึงปัจจัยทางด้านความเป็นส่วนตัวเพียงอย่างเดียวเท่านั้น ซึ่งต้องการจะหาวิธีการทุกวิถีทางเพื่อที่จะป้องกันความเป็นส่วนตัวให้ได้มากที่สุดเท่าที่จะทำได้ ทำให้เกิดโอเวอร์เฮดที่สูงมากในการประมวลผล ซึ่งในสภาพความเป็นจริงนั้นการสื่อสารมีหลากหลายสถานการณ์ เช่น รถฉุกเฉินพาคนเจ็บส่งโรงพยาบาลที่ไม่ต้องการความเป็นส่วนตัวเลย หรือรถที่ขับธรรมดาที่ต้องการความเป็นส่วนตัวมาก เป็นต้น โดยในแต่ละสถานการณ์นั้นก็มีความต้องการความเป็นส่วนตัวที่แตกต่างกันไป บางสถานการณ์ต้องการความเป็นส่วนตัวสูง บางสถานการณ์ต้องการความเป็นส่วนตัวต่ำ บางสถานการณ์ไม่ต้องการความเป็นส่วนตัวเลย นั่นคือการป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งอาจจะไม่จำเป็นในบางสถานการณ์ก็ได้ ดังนั้นงานวิจัยเรื่องจึงได้กำหนดให้มีระดับความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะเป็น 3 ระดับ ได้แก่ ระดับสูง ระดับปานกลาง และระดับต่ำ ซึ่งในแต่ละระดับก็จะมีความเหมาะสมกับสถานการณ์การสื่อสารของยานพาหนะที่แตกต่างกันออกไป และได้กำหนดอัลกอริทึม (Algorithm) และวิธีการป้องกันความเป็นส่วนตัวตามระดับความเป็นส่วนตัวทั้ง 3 ระดับนั้นโดยเลือกใช้อัลกอริทึมที่เหมาะสมที่สุดที่ได้จากงานวิจัยก่อนหน้านี้มาประยุกต์ใช้กับระดับความเป็นส่วนตัวทั้ง 3 ระดับ เพื่อทำให้กระบวนการทำงานมีประสิทธิภาพสูงที่สุด

4. ระดับความเป็นส่วนตัว

งานวิจัยเรื่องนี้ได้กำหนดระดับความเป็นส่วนตัวในการป้องกันและปิดบังตำแหน่งที่ตั้งของยานพาหนะออกเป็น 3 ระดับตามที่กล่าวไว้ในหัวข้อก่อนหน้านี้ โดยข้อมูลที่เกี่ยวข้องกับตำแหน่งที่ตั้งได้แก่ พิกัด ชื่อเรียก หมายเลขทะเบียน ยี่ห้อ รุ่น สี ข้อมูลคนขับ และข้อมูลพื้นฐานต่างๆ ที่จำเป็นของยานพาหนะ เป็นต้น โดยรายละเอียดของระดับความเป็นส่วนตัวมีดังต่อไปนี้

4.1 ระดับสูง (High Level)

เป็นระดับความเป็นส่วนตัวที่มีความต้องการความเป็นส่วนตัวสูง โดยข้อมูลตำแหน่งที่ตั้งของยานพาหนะจะต้องถูกป้องกันและปิดบังในระดับสูง และมีอัลกอริทึมที่ซับซ้อนในการประมวลผล โดยผู้ที่ไม่ได้รับอนุญาตให้เข้าถึงข้อมูลดังกล่าวจะไม่สามารถเปิดเผย ติดตาม และ ย้อนรอยข้อมูลได้เลย

4.2 ระดับปานกลาง (Medium Level)

เป็นระดับความเป็นส่วนตัวที่มีความต้องการความเป็นส่วนตัวปานกลาง โดยข้อมูลตำแหน่งที่ตั้งของยานพาหนะจะถูกป้องกันและปิดบังในบางส่วนที่จำเป็น และมีอัลกอริทึมที่ไม่ซับซ้อนมากในการประมวลผล โดยผู้ที่ไม่ได้รับอนุญาตให้เข้าถึงข้อมูลดังกล่าวจะไม่สามารถเปิดเผย ติดตาม และย้อนรอยข้อมูลที่สำคัญได้ แต่อาจจะสามารถทราบถึงข้อมูลบางอย่างที่เป็นข้อมูลพื้นฐานได้

4.3 ระดับต่ำ (Low Level)

เป็นระดับความเป็นส่วนตัวที่มีความต้องการความเป็นส่วนตัวต่ำ โดยข้อมูลตำแหน่งที่ตั้งของยานพาหนะจะไม่ถูกป้องกันและปิดบัง หรือถ้ามีความจำเป็นในการปิดบังก็จะใช้เพียงอัลกอริทึมอย่างง่ายในการประมวลผล โดยบุคคลที่เกี่ยวข้องสามารถเข้าถึงข้อมูลดังกล่าวได้อย่างเปิดเผย ทั้งยังสามารถติดตามและย้อนรอยข้อมูลได้

จากระดับความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะทั้ง 3 ระดับจะนำมากำหนดช่วงคะแนน เพื่อใช้ในการจัดกลุ่มอัลกอริทึมและจัดกลุ่มรูปแบบของการสื่อสารของยานพาหนะเพื่อให้สอดคล้องและเหมาะสมกับระดับความเป็นส่วนตัวที่กำหนดขึ้นให้มากที่สุด โดยจะได้กล่าวไว้ในหัวข้อถัดไป

5. ปัจจัยสำหรับกำหนดระดับความเป็นส่วนตัว

การจัดกลุ่มอัลกอริทึมและจัดกลุ่มรูปแบบการสื่อสารของยานพาหนะว่าอยู่ในระดับความเป็นส่วนตัวใดนั้นจำเป็นจะต้องกำหนดปัจจัยที่จำเป็นเพื่อใช้เป็นปัจจัยในการพิจารณาความต้องการความเป็นส่วนตัวของอัลกอริทึม และรูปแบบการสื่อสาร โดยแบ่งออกเป็น 5 ปัจจัยดังรายละเอียดต่อไปนี้

1. **การป้องกันและปิดบังพิกัดของยานพาหนะ** (Vehicle Position) โดยเป็นความสามารถในการป้องกันและปิดบังข้อมูลพิกัดซึ่งได้แก่ พิกัดละติจูด พิกัดลองติจูด เป็นต้น
2. **การป้องกันและปิดบังชื่อของยานพาหนะ** (Vehicle Name) โดยเป็นความสามารถในการป้องกันและปิดบังชื่อซึ่งได้แก่ ชื่อเรียก หมายเลขป้ายทะเบียน เป็นต้น
3. **การป้องกันและปิดบังคุณสมบัติของยานพาหนะ** (Vehicle Properties) โดยเป็นความสามารถในการป้องกันและปิดบังข้อมูลซึ่งได้แก่ สี รุ่น ยี่ห้อ เป็นต้น
4. **การป้องกันและปิดบังข้อมูลผู้ขับยานพาหนะ** (Vehicle Driver) โดยเป็นความสามารถในการป้องกันและปิดบังข้อมูลผู้ขับซึ่งได้แก่ ชื่อ เพศ อายุ เป็นต้น
5. **การป้องกันและปิดบังสถานะของยานพาหนะ** (Vehicle Status) โดยเป็นความสามารถในการป้องกันและปิดบังสถานะบางอย่างซึ่งได้แก่ เลี้ยวซ้าย เลี้ยวขวา เดินหน้า ถอยหลัง อยู่บนทางด่วน อยู่กลางสี่แยก เป็นต้น

จากปัจจัยปัจจัย 5 ปัจจัยในการพิจารณาความต้องการความเป็นส่วนตัว สามารถนำมากำหนดค่าระดับคะแนนที่เป็นระดับความสามารถในการป้องกันและปิดบังความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะได้ 5 ระดับโดยมีค่าคะแนนตั้งแต่ 0-4 ดังรายละเอียดในตารางที่ 1

ตารางที่ 1 ตารางค่าคะแนนของระดับความสามารถในการป้องกันและปิดบังความเป็นส่วนตัว

ระดับความสามารถ	คะแนน
ระดับมากที่สุด	4
ระดับมาก	3
ระดับปานกลาง	2
ระดับน้อย	1
ระดับน้อยที่สุด	0

การให้คะแนนระดับความสามารถในการป้องกันและปิดบังความเป็นส่วนตัวของแต่ละอัลกอริทึมและรูปแบบการสื่อสารตามปัจจัยที่กำหนดไว้นั้นจะใช้เกณฑ์การให้คะแนนที่มาจากการศึกษาคุณสมบัติของอัลกอริทึมและรูปแบบการสื่อสารต่างๆ จากรายละเอียดที่ระบุไว้ในเอกสารงานวิจัยและเอกสารทางวิชาการที่เกี่ยวข้องพร้อมทั้งการปรึกษาผู้เชี่ยวชาญ โดยเมื่อกำหนดค่าคะแนนระดับความสามารถในการป้องกันและปิดบังความเป็นส่วนตัวให้กับแต่ละอัลกอริทึมและรูปแบบการสื่อสารตามปัจจัยที่กำหนดไว้เรียบร้อยแล้วก็จะนำค่าคะแนนที่ได้ทุกปัจจัยมารวมกันเป็นค่าคะแนนรวมแล้วแบ่งเป็นช่วงคะแนนเพื่อใช้ในการจัดกลุ่มอัลกอริทึมและรูปแบบการสื่อสารตามระดับความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะที่เหมาะ โดยช่วงคะแนนดังกล่าวแสดงไว้ในตารางที่ 2

ตารางที่ 2 ตารางช่วงคะแนนของระดับความเป็นส่วนตัว

ระดับความเป็นส่วนตัว	ช่วงคะแนน
ระดับสูง	14 - 20
ระดับปานกลาง	7 - 13
ระดับต่ำ	0 - 6

จากช่วงคะแนนที่กำหนดขึ้นตามตารางที่ 2 จะนำมาใช้ในการจัดกลุ่มอัลกอริทึมและรูปแบบการสื่อสารพร้อมทั้งแจกแจงค่าคะแนนตามรายละเอียดในตารางที่ 3 และตารางที่ 4 ของหัวข้อถัดไป

6. อัลกอริทึมการป้องกันความเป็นส่วนตัว

จากการศึกษาอัลกอริทึมการป้องกันและปิดบังความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะในหัวข้องานวิจัยที่

เกี่ยวข้องมาแล้วนั้น ผู้วิจัยได้เลือกอัลกอริทึมที่สำคัญสำหรับนำมาใช้ในงานวิจัยเรื่องนี้ทั้งหมด 5 อัลกอริทึมดังรายละเอียดต่อไปนี้

6.1 อัลกอริทึมชื่อเทียมและชื่อปลอม (Pseudonym and Anonym Algorithm) [1,2]

เป็นอัลกอริทึมการป้องกันและปิดบังข้อมูลอย่างง่ายที่นำมาใช้ในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะในช่วง 10 ปีที่ผ่านมา ซึ่งใช้เทคนิคการเข้ารหัส (Encryption) และเทคนิคการแฮช (Hashing) ในการปิดบังข้อมูล

6.2 อัลกอริทึมมิกซ์โซน (Mix-Zone Algorithm) [3]

เป็นอัลกอริทึมการเปลี่ยนตำแหน่งที่ตั้งโดยการแลกเปลี่ยนกุญแจที่ใช้ในการเข้ารหัสข้อมูลของตำแหน่งที่ตั้ง ซึ่งจะแบ่งพื้นที่ต่างๆ ในแผนที่ออกเป็นมิกซ์โซนหลายมิกซ์โซน โดยแต่ละมิกซ์โซนจะมีกุญแจการเข้ารหัสเพื่อใช้ในการปิดบังข้อมูลของตำแหน่งที่ตั้งที่แตกต่างกันออกไป ยานพาหนะจะต้องใช้กุญแจในการปิดบังข้อมูลที่แตกต่างกันไปตามมิกซ์โซนปัจจุบันที่กำลังเคลื่อนที่ไปถึง

6.3 อัลกอริทึมอะมีบา (AMOEBA Algorithm) [4]

เป็นอัลกอริทึมที่กำหนดให้ยานพาหนะแต่ละคันมีช่วงเวลาของการปล่อยสัญญาณที่แตกต่างกันตามช่วงเวลาที่กำหนดไว้ และมีช่วงเวลาเงียบ (Silent Period) ที่จะไม่มีการปล่อยสัญญาณใดๆ จึงทำให้การติดตามตำแหน่งของยานพาหนะทำได้ยากยิ่งขึ้น นอกจากนี้ยังใช้กระบวนการสื่อสารผ่านทางตัวแทนหรือหัวหน้ากลุ่มของเขตพื้นที่ที่ยานพาหนะกำลังเคลื่อนที่อยู่ ณ ปัจจุบันเพื่อปิดบังข้อมูลจริงของยานพาหนะแต่ละคัน

6.4 อัลกอริทึมเรป (REP Algorithm) [5]

เป็นอัลกอริทึมที่มีการทำงานคล้ายกับอัลกอริทึมอะมีบา แต่มีการปรับปรุงระยะเวลาในการเงียบและระยะเวลาในการส่งข้อมูลโดยใช้หลักของการสุ่มคาบเวลาในการเข้ารหัสข้อมูล (Random Encryption Period) โดยกำหนดกุญแจที่เป็นตัวเลขสุ่มที่ใช้สำหรับการเข้ารหัสและใช้ในการปล่อยสัญญาณตามคาบที่ถูกระบุด้วยตัวเลขสุ่มนั้น

6.5 อัลกอริทึมดีแอลพี (DLP Algorithm) [6]

เป็นอัลกอริทึมที่มีการปิดบังข้อมูลของตำแหน่งที่ตั้งของยานพาหนะโดยพิจารณาความหนาแน่นของยานพาหนะเพื่อนบ้านที่อยู่ใกล้เคียงกัน เพื่อให้มีขอบเขตการรับส่งข้อมูลระหว่างยานพาหนะที่จำกัด โดยถ้ามีความหนาแน่นของยานพาหนะเพื่อนบ้านมากเกินขอบเขตที่กำหนดไว้ก็จะต้องทำการเข้ารหัสข้อมูลใหม่อีกครั้ง

นอกจากอัลกอริทึมทั้ง 5 อัลกอริทึม พบว่าในบางช่วงเวลาของการสื่อสารของยานพาหนะนั้นอาจไม่จำเป็นที่จะต้องใช้อัลกอริทึมใดเลยในการป้องกันและปิดบังตำแหน่งที่ตั้ง เพราะในกระบวนการสื่อสารดังกล่าวต้องการความเป็นสาธารณะแทนความเป็นส่วนตัว

จากปัจจัยในการพิจารณาความต้องการความเป็นส่วนตัวที่กล่าวไว้ในหัวข้อก่อนหน้านี้ สามารถนำมาใช้ในการจัดกลุ่มอัลกอริทึมได้ตามรายละเอียดในตารางที่ 3

ตารางที่ 3 ตารางคะแนนของระดับความสามารถในการป้องกันและปิดบังความเป็นส่วนตัวของของอัลกอริทึม

อัลกอริทึม	พิกัด	ชื่อ	คุณ-สมบัติ	ข้อมูลผู้ขับ	สถานะ	คะแนนรวม	ระดับความเป็นส่วนตัว
อัลกอริทึมชื่อเทียมและชื่อปลอม	1	3	2	2	1	9	ระดับปานกลาง
อัลกอริทึมมิกซ์โซน	1	3	2	2	2	10	ระดับปานกลาง
อัลกอริทึมอะมีบา	3	4	3	4	3	17	ระดับสูง
อัลกอริทึมเรป	4	4	3	3	4	18	ระดับสูง
อัลกอริทึมดีแอลพี	3	4	3	3	3	16	ระดับสูง
ไม่ใช้อัลกอริทึม	0	0	0	0	0	0	ระดับต่ำ

7. รูปแบบการสื่อสารของยานพาหนะ

รูปแบบการสื่อสารของยานพาหนะสามารถจำแนกออกได้เป็น 3 รูปแบบหลักได้แก่ การสื่อสารระหว่างยานพาหนะกับยานพาหนะหรือวีทูวี (V2V) การสื่อสารระหว่างยานพาหนะกับอุปกรณ์หรือวีทูไอ (V2I) และการสื่อสารระหว่างยานพาหนะกับบริการหรือวีทูเอส (V2S) โดยในแต่ละรูปแบบหลักก็จะแบ่งเป็นรูปแบบการสื่อสารย่อยได้อีกหลายรูปแบบ ซึ่งมีรายละเอียดดังต่อไปนี้

7.1 การสื่อสารระหว่างยานพาหนะกับยานพาหนะ

เป็นการสื่อสารระหว่างยานพาหนะตั้งแต่สองคันขึ้นไปที่มาแลกเปลี่ยนข้อมูลและสถานะระหว่างกัน เช่น การเลี้ยวซ้ายเลี้ยวขวา การเดิน หน้าถอยหลัง การเพิ่มลดความเร็ว การบอกตำแหน่งที่ตั้ง การบอกสถานะของคนขับ เป็นต้น

7.2 การสื่อสารระหว่างยานพาหนะกับอุปกรณ์

เป็นการสื่อสารระหว่างยานพาหนะกับเครื่องมือสื่อสารและอุปกรณ์ควบคุมต่างๆ ที่ติดตั้งบริเวณรอบถนน อาจจะเป็นเสาข้างถนนหรือเครื่องมือที่ติดอยู่บนถนน เช่น การแจ้งเตือนเขตชุมชน การแจ้งเตือนเขตโรงเรียน การแจ้งเตือนก่อนถึงสี่แยก เป็นต้น

7.3 การสื่อสารระหว่างยานพาหนะกับบริการ

เป็นการสื่อสารระหว่างยานพาหนะกับผู้ให้บริการต่างๆ ที่อยู่ห่างจากบริเวณพื้นที่ถนน เช่น การรับส่งข้อมูลจากบริการของผู้ให้บริการในรูปแบบของข้อความ รูปภาพ เพลง เสียง วีดีโอ ภาพเคลื่อนไหว เป็นต้น

จากรูปแบบการสื่อสารของยานพาหนะทั้ง 3 รูปแบบ สามารถนำมาจัดกลุ่มโดยกำหนดค่าคะแนนให้กับรูปแบบการสื่อสารต่างๆ ตามปัจจัยของความต้องการความเป็นส่วนตัว 5 ปัจจัย ได้แก่ การป้องกันและปิดบังพิกัด ชื่อ คุณสมบัติ ข้อมูลผู้ขับ และสถานะของยานพาหนะ ซึ่งมีรายละเอียดตามตารางที่ 4

ตารางที่ 4 ตารางคะแนนของระดับความสามารถในการป้องกันและปิดบังความเป็นส่วนตัวของของรูปแบบการสื่อสาร

รูปแบบการสื่อสาร	พิกัด	ชื่อ	คุณ-สมบัติ	ข้อมูลผู้ขับ	สถานะ	คะแนนรวม	ระดับความเป็นส่วนตัว
การสื่อสารระหว่างยานพาหนะกับยานพาหนะ							
การบอกสถานะของยานพาหนะ	1	2	0	1	4	8	ระดับปานกลาง
การบอกตำแหน่งที่ตั้ง	4	3	2	2	1	12	ระดับปานกลาง
การบอกสถานะของคนขับ	1	3	2	4	1	11	ระดับปานกลาง
การสื่อสารส่วนบุคคล	4	4	4	4	4	20	ระดับสูง
การสื่อสารระหว่างยานพาหนะกับอุปกรณ์							
การแจ้งเตือนแบบสาธารณะ	0	0	0	2	1	3	ระดับต่ำ
การแจ้งเตือนแบบส่วนบุคคล	2	4	3	4	2	15	ระดับสูง
การสื่อสารระหว่างยานพาหนะกับบริการ							
การลงทะเบียนจากบริการ	1	4	3	3	1	12	ระดับปานกลาง
การรับส่งข้อมูลจากบริการ	3	4	1	2	3	13	ระดับปานกลาง

8. การป้องกันความเป็นส่วนตัวภายใต้ระดับความเป็นส่วนตัว

จากการจัดกลุ่มอัลกอริทึมและรูปแบบการสื่อสารของยานพาหนะตามระดับความเป็นส่วนตัวในหัวข้อก่อนหน้านี้ สามารถนำมาใช้ในกระบวนการป้องกันและปิดบังตำแหน่งที่ตั้งของยานพาหนะแบบใหม่ที่อยู่บนพื้นฐานของระดับความเป็นส่วนตัวนั้น โดยอัลกอริทึมที่ใช้ในการปิดบังจะปรับเปลี่ยนไปตามสถานการณ์และรูปแบบการสื่อสาร ณ ขณะใดขณะหนึ่งโดยมีรายละเอียดดังตารางที่ 5

จากข้อมูลการป้องกันและปิดบังตำแหน่งที่ตั้งบนพื้นฐานของระดับความเป็นส่วนตัวในตารางที่ 5 สามารถนำมาเขียนเป็นรหัสเทียม (Pseudocode) ได้ดังนี้

```
1  Function protectLocation(event)
2     score ← checkEventScore(event)
3     If score between 0 to 6
4        algor ← callLowLevel()
5     Else If score between 7 to 13
6        algor ← callMediumLevel()
7     Else If score between 14 to 20
8        algor ← callHighLevel()
9     Else
10       algor ← null
11    End If
12    anonymizeData(algor)
13 End Function
```

จากรหัสเทียมแสดงให้เห็นว่าเมื่อมีสถานการณ์เข้ามาก็จะพิจารณาค่าคะแนนและตรวจสอบช่วงคะแนนเพื่อกำหนดอัลกอริทึมที่เหมาะสมในการป้องกันและปิดบังข้อมูล

ตารางที่ 5 ตารางการกำหนดรูปแบบการสื่อสารกับอัลกอริทึมการปิดบังที่เหมาะสมภายใต้ระดับความเป็นส่วนตัว

รูปแบบการสื่อสาร	คะแนนรวม	ระดับความเป็นส่วนตัว	อัลกอริทึม
การสื่อสารระหว่างยานพาหนะกับยานพาหนะ			
การบอกสถานะของยานพาหนะ	8	ระดับปานกลาง	อัลกอริทึมซื่อเทียมและซื่อปลอม (9) อัลกอริทึมมิกซ์โซน (10)
การบอกตำแหน่งที่ตั้ง	12	ระดับปานกลาง	อัลกอริทึมซื่อเทียมและซื่อปลอม (9) อัลกอริทึมมิกซ์โซน (10)
การบอกสถานะของคนขับ	11	ระดับปานกลาง	อัลกอริทึมซื่อเทียมและซื่อปลอม (9) อัลกอริทึมมิกซ์โซน (10)
การสื่อสารส่วนบุคคล	20	ระดับสูง	อัลกอริทึมอะมีบา (17) อัลกอริทึมเรป (18) อัลกอริทึมดีแอลพี (16)
การสื่อสารระหว่างยานพาหนะกับอุปกรณ์			
การแจ้งเตือนแบบสาธารณะ	3	ระดับต่ำ	ไม่ใช้อัลกอริทึม (0)
การแจ้งเตือนแบบส่วนบุคคล	15	ระดับสูง	อัลกอริทึมอะมีบา (17) อัลกอริทึมเรป (18) อัลกอริทึมดีแอลพี (16)
การสื่อสารระหว่างยานพาหนะกับบริการ			
การลงทะเบียนจากบริการ	12	ระดับปานกลาง	อัลกอริทึมซื่อเทียมและซื่อปลอม (9) อัลกอริทึมมิกซ์โซน (10)
การรับส่งข้อมูลจากบริการ	13	ระดับปานกลาง	อัลกอริทึมซื่อเทียมและซื่อปลอม (9) อัลกอริทึมมิกซ์โซน (10)

9. การวัดประสิทธิภาพการทำงานเบื้องต้น

การวัดประสิทธิภาพการทำงานของวิธีการป้องกันและปิดบังตำแหน่งที่ตั้งของยานพาหนะบนพื้นฐานของระดับความเป็นส่วนตัวนี้จะใช้วิธีการคำนวณตามทฤษฎีเบื้องต้น โดยกำหนดให้ใช้อัลกอริทึมเรปกับความเป็นส่วนตัวระดับสูง อัลกอริทึมมิกซ์โซนกับความเป็นส่วนตัวระดับปานกลาง และไม่ใช้อัลกอริทึมกับความเป็นส่วนตัวระดับต่ำ และกำหนดให้ค่าโอเวอร์เฮดที่ใช้ในการวัดประสิทธิภาพการทำงานเป็นตัวเลขจำนวนเต็มที่มีค่าตั้งแต่ 0-5 ตามลำดับคะแนนของอัลกอริทึมที่คำนวณได้ในหัวข้อก่อนหน้านี้ ซึ่งจะได้ค่าโอเวอร์เฮดเป็นดังนี้

$$\text{overhead} = \frac{2+2+2+5+0+5+2+2}{8} = 2.50$$

ค่าโอเวอร์เฮดที่คำนวณได้จะมีค่าต่ำกว่าค่าโอเวอร์เฮดจากการใช้อัลกอริทึมอะมีบา อัลกอริทึมเรป และอัลกอริทึมดีแอลพี ดังที่แสดงไว้ในตารางที่ 6

ตารางที่ 6 ตารางค่าโอเวอร์เฮดของอัลกอริทึม

อัลกอริทึม	ค่าโอเวอร์เฮด
อัลกอริทึมซื่อเทียมและซื่อปลอม	1.00
อัลกอริทึมมิกซ์โซน	2.00
อัลกอริทึมอะมีบา	4.00
อัลกอริทึมเรป	5.00
อัลกอริทึมดีแอลพี	3.00
ไม่ใช้อัลกอริทึม	0.00
การใช้ระดับความเป็นส่วนตัว	2.50

10. บทสรุปและแนวทางการวิจัยในอนาคต

งานวิจัยเรื่องนี้ได้นำเสนอระดับความเป็นส่วนตัว 3 ระดับ ได้แก่ ระดับสูง ระดับปานกลาง และระดับต่ำ เพื่อใช้ในการป้องกันและปิดบังตำแหน่งที่ตั้งของยานพาหนะในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ โดยระดับความเป็นส่วนตัวแต่ละระดับนั้นจะมีอัลกอริทึมการป้องกันและ

ปิดบังที่แตกต่างกันออกไปอย่างเหมาะสมตามสถานการณ์และกระบวนการสื่อสารของยานพาหนะ ณ ขณะใดขณะหนึ่ง และสามารถปรับเปลี่ยนไปตามรูปแบบจริงของการสื่อสาร โดยจากการคำนวณค่าโอเวอร์เฮดตามทฤษฎีเบื้องต้นพบว่ากระบวนการป้องกันและปิดบังตำแหน่งที่ตั้งของยานพาหนะที่ทำงานภายใต้ระดับความเป็นส่วนตัวทั้ง 3 ระดับนี้มีประสิทธิภาพการทำงานที่ดีกว่ากระบวนการป้องกันและปิดบังแบบเดิม แต่อย่างไรก็ตามงานวิจัยเรื่องนี้ยังมีการวิจัยต่อเนื่องในอนาคตโดยการทดลองกับระบบจำลองที่กำหนดสภาพแวดล้อมและการบวนการทำงานเสมือนจริง เพื่อวัดประสิทธิภาพจากการคำนวณตามแบบจำลองอีกครั้งหนึ่ง ทั้งยังจะต้องกำหนดวิธีการคำนวณการเลือกใช้อัลกอริทึมที่มีความน่าเชื่อถือมากยิ่งขึ้นในอนาคต

11. เอกสารอ้างอิง

[1] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy, "Efficient and Robust Pseudonymous Authentication in VANET". In Proceedings of 4th ACM International Workshop on Vehicular Ad-Hoc Networks (VANET 2007), Montreal, Canada, 10 September 2007.

[2] Matthias Gerlach and Felix Guttler, "Privacy in VANETs using Changing Pseudonyms-Ideal and Real". In Proceedings of IEEE 65th Vehicular Technology Conference (VTC 2007), Dublin, Ireland, 22-25 April 2007.

[3] Julien Freudiger, Maxim Raya, Márk Félegyházi, "Mix Zones for Location Privacy in Vehicular Networks". In Proceedings of WiN-ITS 2007, Vancouver, British Columbia, August 14, 2007.

[4] Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET". IEEE Journal on Selected Areas in Communications, Volume 25, Issue 8, October 2007.

[5] Albert Wasef and Xuemin (Sherman) Shen, "REP: Location Privacy for VANETs Using Random Encryption Periods". Journal on Mobile Networks and Applications Archive, Volume 15, Issue 1, February 2010.

[6] Joo-Han Song, Vincent W.S. Wong, and Victor C. Leung, "Wireless Location Privacy Protection in Vehicular Ad-Hoc Networks". Journal of Mobile Networks and Applications Archive, Volume 15, Issue 1, February 2010.

การรักษาความเป็นส่วนตัวแบบหลายระดับของระบบตรวจสอบตำแหน่งที่ตั้งในวาเน็ต
Multi-Level Privacy-Preserving for Location Monitoring System in VANET

วงศ์ยศ เกิดศรี[1,*], ขจิตพรรณ กฤตพลวิมาน[1] และ กรกช วิไลลักษณ์[2]

[1] สาขาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
[2] กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ กองทัพเรือ
*ผู้ติดต่อ: wongyos@gmail.com, +66(0)89-599-3490

บทคัดย่อ

การรักษาความเป็นส่วนตัวในระบบตรวจสอบตำแหน่งที่ตั้งเป็นประเด็นหนึ่งที่ท้าทายในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะหรือวาเน็ต งานวิจัยก่อนหน้านี้ได้ใช้ชื่อเทียม ชื่อปลอม การปล่อยสัญญาณแบบสุ่ม และการปล่อยสัญญาณแบบช่วงที่ไม่ต่อเนื่องในการปิดบังข้อมูล แต่งานเหล่านั้นทำให้เกิดค่าโอเวอร์เฮดที่สูงมาก ในความเป็นจริงพบว่าการสื่อสารบนวาเน็ตมีการทำงานในหลากหลายสถานการณ์และยังมีความต้องการต่อข้อตกลงในด้านความเป็นส่วนตัวที่แตกต่างกันอีกด้วย บทความนี้จึงได้นำเสนอการรักษาความเป็นส่วนตัวแบบหลายระดับขึ้น โดยกำหนดไว้ 3 ระดับได้แก่ สูง ปานกลาง และต่ำ ซึ่งระดับความเป็นส่วนตัวเหล่านี้สามารถเปลี่ยนไปตามการปรับเปลี่ยนสถานการณ์และการใช้งาน โดยจะเลือกใช้อัลกอริทึมที่เหมาะสมเพื่อปิดบังข้อมูล จากการวัดค่าประสิทธิภาพพบว่าวิธีการที่ได้นำเสนอนี้สามารถลดค่าโอเวอร์เฮดลงได้ในระดับหนึ่ง และสามารถป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งได้อย่างมีประสิทธิภาพ

คำหลัก: ความเป็นส่วนตัวแบบหลายระดับ, การปิดบังข้อมูล, ระบบตรวจสอบตำแหน่งที่ตั้ง, เครือข่ายไร้สายเฉพาะกิจของยานพาหนะ, วาเน็ต

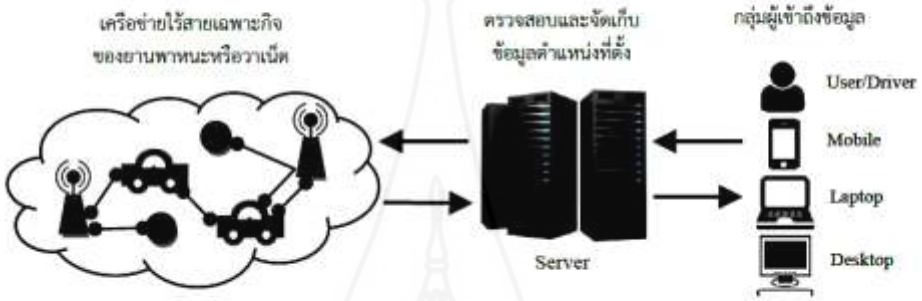
Abstract

Privacy-preserving in location monitoring system is one of the main challenges in Vehicular Ad-Hoc Network or VANET. The previous works proposed the pseudonyms, anonyms, random signal and non-continuous signal for data anonymization; however, very high processing overheads were generated. In fact, VANET communications are implemented on varieties of situation and also required for different privacy protocols. As a consequence, multi-level privacy-preserving with three levels: high, medium and low are proposed. These privacy levels are able to be changed by updating situations and functions with selecting suitable algorithms for data anonymization. The results showed that the proposed scheme was able to reduce the processing overhead as well as to protect location privacy with high efficiency.

Keywords: Multi-level Privacy, Data Anonymization, Location Monitoring System, Vehicular Ad-Hoc Network, VANET

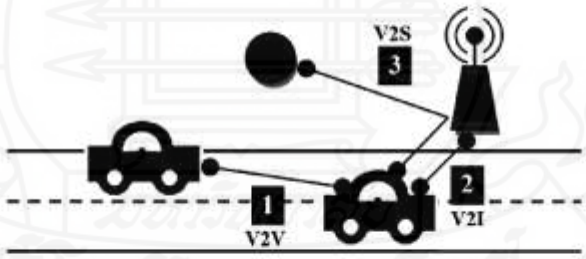
1. บทนำ

การรักษาความเป็นส่วนตัวของข้อมูลในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะหรือวาเน็ต (Vehicular Ad-hoc Network: VANET) เป็นประเด็นหนึ่งที่มีความท้าทายในปัจจุบันโดยเฉพาะข้อมูลที่เกี่ยวข้องกับตำแหน่งที่ตั้ง (Location) เพราะเนื่องจากการสื่อสารของยานพาหนะในอนาคตนั้นจะมีการสื่อสารผ่านทางเซ็นเซอร์ (Sensor) ที่ติดตั้งโดยการปล่อยสัญญาณบรอดแคสท์ (Broadcast) ไปยังอุปกรณ์ต่างๆ ซึ่งสามารถเชื่อมต่อถึงกันได้แบบทั่วทุกหนทุกแห่ง โดยกระบวนการดังกล่าวจะทำให้ผู้ใช้งานไม่ว่าจะเป็นผู้ขับขี่ อุปกรณ์ในตัวยานพาหนะ อุปกรณ์สื่อสารต่างๆ และบุคคลที่สามสามารถติดตามตำแหน่งที่ตั้งจากระบบตรวจสอบตำแหน่งที่ตั้ง (Location Monitoring System) [1] ของยานพาหนะนั้นได้ทุกเวลาดังแสดงไว้ในรูปที่ 1



รูปที่ 1 ระบบตรวจสอบตำแหน่งที่ตั้งของยานพาหนะในเครือข่ายวาเน็ต

จากกระบวนการตรวจสอบตำแหน่งที่ตั้งของยานพาหนะในรูปที่ 1 ทำให้กลุ่มผู้เข้าถึงข้อมูลทราบถึงตำแหน่งพิกัดปัจจุบันของยานพาหนะแต่ละคันในแผนที่ทางภูมิศาสตร์ได้ จึงจำเป็นต้องมีระบบการป้องกันความเป็นส่วนตัวในการตรวจสอบตำแหน่งที่ตั้งขึ้น โดยทั่วไปการสื่อสารของยานพาหนะ (Vehicle Communications) บนท้องถนนในแต่ละช่วงเวลานั้นจะมีรูปแบบการสื่อสารที่แตกต่างกันออกไปตามสถานการณ์และการทำงานจริงดังแสดงไว้ในรูปที่ 2



รูปที่ 2 รูปแบบการสื่อสารของยานพาหนะในเครือข่ายวาเน็ต

รูปแบบการสื่อสารของยานพาหนะที่ปรากฏในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะตามที่ปรากฏในรูปที่ 2 นั้นประกอบไปด้วย 3 รูปแบบหลัก [2] ได้แก่

1) การสื่อสารระหว่างยานพาหนะกับยานพาหนะหรือวีทูวี (Vehicle to Vehicle: V2V) เป็นรูปแบบการสื่อสารระหว่างยานพาหนะตั้งแต่สองคันขึ้นไปที่แลกเปลี่ยนข้อมูลต่างๆ ระหว่างกัน โดยตัวอย่างของการสื่อสารประเภทนี้ได้แก่ การเลี้ยวซ้ายเลี้ยวขวา การเดินหน้าถอยหลัง การเพิ่มลดความเร็ว การบอกตำแหน่งที่ตั้ง การบอกสถานะของคนขับ เป็นต้น

2) การสื่อสารระหว่างยานพาหนะกับอุปกรณ์หรือวีทูไอ (Vehicle to Infrastructure: V2I) เป็นรูปแบบการสื่อสารระหว่างยานพาหนะกับเครื่องมือสื่อสารและอุปกรณ์ควบคุมต่างๆ ที่ติดตั้งบริเวณรายรอบถนน โดยอาจจะเป็นเสาสัญญาณข้างถนน อุปกรณ์หรือเครื่องมือที่ติดอยู่บนเกาะกลางถนน โดยตัวอย่างของการสื่อสารประเภทนี้ได้แก่ การแจ้งเตือนเขตชุมชน การแจ้งเตือนเขตโรงเรียน การแจ้งเตือนก่อนถึงสี่แยก เป็นต้น

3) การสื่อสารระหว่างยานพาหนะกับบริการหรือวีทูเอส (Vehicle to Service: V2S) เป็นรูปแบบการสื่อสารระหว่างยานพาหนะกับผู้ให้บริการต่างๆ ที่อยู่ห่างจากบริเวณพื้นที่ถนน โดยตัวอย่างของการสื่อสารประเภทนี้ได้แก่ การรับส่งข้อมูลจากบริการของผู้ให้บริการในรูปแบบของข้อความ รูปภาพ เสียง วีดีโอ เป็นต้น

จากการศึกษารูปแบบการสื่อสารของยานพาหนะทั้งสามรูปแบบนั้นพบว่ามีความต้องการในความเป็นส่วนตัวของการสื่อสารข้อมูลที่แตกต่างกันออกไปตามสถานการณ์และสภาพการใช้งานจริง เช่น รถตำรวจ รถดับเพลิง และรถฉุกเฉินที่ไม่ต้องการความเป็นส่วนตัวเลยหรือต้องการความเป็นส่วนตัวน้อยมาก รถของผู้ใช้ตามท้องถนนทั่วไปที่ต้องการความเป็นส่วนตัวในระดับปานกลาง และรถของหน่วยสืบราชการลับที่ต้องการความเป็นส่วนตัวสูง เป็นต้น งานวิจัยเรื่องนี้จึงได้นำเสนอวิธีการการรักษาความเป็นส่วนตัวแบบหลายระดับ (Multi-Level Privacy-Preserving) โดยกำหนดไว้ 3 ระดับได้แก่ สูง ปานกลาง และต่ำ ซึ่งระดับความเป็นส่วนตัวเหล่านี้จะเปลี่ยนไปตามการปรับเปลี่ยนสถานการณ์และการใช้งานของยานพาหนะ โดยจะเลือกใช้อัลกอริทึมที่เหมาะสมเพื่อปิดบังข้อมูล ซึ่งจะได้กล่าวถึงรายละเอียดในหัวข้อถัดไป จากผลการวัดประสิทธิภาพเชิงทฤษฎีพบว่าวิธีการที่ได้นำเสนอนี้สามารถลดค่าโอเวอร์เฮด (Overhead) ลงได้ในระดับหนึ่ง และสามารถป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งได้อย่างเป็นที่น่าพอใจและมีประสิทธิภาพ

2. งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยในประเด็นของการป้องกันความเป็นส่วนตัวของข้อมูลในระบบตรวจสอบตำแหน่งที่ตั้งของเครือข่ายวาเน็ตพบว่าช่วงเริ่มต้นนั้นได้ใช้การปิดบังชื่อหรือปิดบังข้อมูลของยานพาหนะให้กลายเป็นชื่อเทียมและชื่อปลอม (Pseudonym and Anonym) [3-4] โดยเป็นอัลกอริทึมอย่างง่ายที่นำมาใช้ในช่วง 10 ปีที่ผ่านมา ซึ่งใช้เทคนิคการเข้ารหัส (Encryption) และเทคนิคการแฮช (Hashing) ในการปิดบังข้อมูลทำให้การติดตามข้อมูลของยานพาหนะทำได้ยากขึ้น ทั้งยังไม่สามารถทราบถึงชื่อหรือข้อมูลจริงของยานพาหนะนั้นได้ แต่การใช้ชื่อเทียมและชื่อปลอมได้ถูกกำหนดให้กับยานพาหนะแต่ละคันอย่างถาวรทำให้สุดท้ายสามารถคาดเดาถึงข้อมูลจริงของยานพาหนะนั้นได้ในที่สุด งานวิจัยต่อมามีการนำเสนอหลักการที่เรียกว่ามิกซ์โซน (Mix-Zone) [5] ซึ่งเป็นอัลกอริทึมที่มีการแลกเปลี่ยนกุญแจที่ใช้ในการเข้ารหัสของข้อมูล ซึ่งจะแบ่งพื้นที่ต่างๆ ในแผนที่ออกเป็นมิกซ์โซนหลายมิกซ์โซน โดยแต่ละมิกซ์โซนจะมีกุญแจการเข้ารหัสเพื่อใช้ในการปิดบังข้อมูลที่แตกต่างกันออกไป ยานพาหนะจะต้องใช้กุญแจในการปิดบังข้อมูลที่แตกต่างกันไปตามมิกซ์โซนปัจจุบันที่กำลังเคลื่อนที่ไปถึง ทำให้ชื่อของยานพาหนะมีการเปลี่ยนแปลงแบบพลวัต (Dynamic) อยู่ตลอดเวลา แต่อย่างไรก็ตามการสื่อสารของยานพาหนะยังต้องใช้กระบวนแบบบรอดแคสท์ซึ่งมีการปล่อยสัญญาณอย่างต่อเนื่อง ทำให้ยังสามารถติดตามเส้นทางของยานพาหนะนั้นจากสัญญาณที่ปล่อยออกมาได้ดังเดิมถึงแม้ว่าจะมีการเปลี่ยนแปลงชื่อก็ตาม เพียงแต่การเดาชื่อหรือข้อมูลจริงของยานพาหนะนั้นทำได้ยากขึ้นเท่านั้น งานวิจัยต่อมาจึงได้นำเสนอหลักการที่เรียกว่าอะโมอีบา (AMOEBA) [6] ซึ่งเป็นอัลกอริทึมที่กำหนดให้ยานพาหนะแต่ละคันมีการปล่อยสัญญาณบรอดแคสท์แบบเป็นช่วงที่ไม่ต่อเนื่องโดยกำหนดให้มีช่วงเงียบ (Silent Period) และช่วงปล่อยสัญญาณ (Broadcast Period) จึงทำให้การติดตามข้อมูลของยานพาหนะเกิดการขาดช่วงจังหวะและยากยิ่งขึ้นต่อการติดตามเส้นทาง นอกจากนี้ยังใช้กระบวนการสื่อสารผ่านทางหัวหน้ากลุ่ม (Group Leader) ของเขตพื้นที่ที่ยานพาหนะกำลังเคลื่อนที่อยู่ ณ ปัจจุบันเพื่อเป็นตัวแทนในการแลกเปลี่ยนข้อมูล อัลกอริทึมอะโมอีบ้านี้มีข้อเสียคือมีโอเวอร์เฮดในการประมวลผลที่สูงมาก จึงมีงานวิจัยต่อมาได้นำเอาแนวคิดของอะโมอีบ้าไปประยุกต์ใช้โดยการเพิ่มหลักการเข้ารหัสชื่อแบบสุ่ม

หรือเรป (Random Encryption Period: REP) [7] ซึ่งจะมีการปรับปรุงระยะเวลาในการเงียบและระยะเวลาในการส่งสัญญาณเป็นแบบสุ่ม โดยกำหนดกุญแจการเข้ารหัสที่เป็นตัวเลขสุ่มแล้วปล่อยสัญญาณตามคาบที่ถูกระบุด้วยตัวเลขสุ่มนั้น ทำให้ชื่อเทียมหรือชื่อปลอมของยานพาหนะมีการเปลี่ยนแปลงไปแบบที่ไม่สามารถคาดเดาได้ยากต่อการติดตามข้อมูลยิ่งขึ้น แต่อย่างไรก็ตามงานวิจัยนี้ก็เพิ่มโอเวอร์เฮดในการประมวลผลให้สูงยิ่งขึ้นตามไปด้วย งานวิจัยต่อมาคือดีแอลพี (Density-based Location Privacy: DLP) [8] ซึ่งเกิดขึ้นในช่วงเวลาเดียวกับงานวิจัย [7] ได้นำเอาหลักการของอะโมอีบ้าไปประยุกต์ใช้เช่นกันแต่จะมีการพิจารณาถึงความหนาแน่น (Density) ของเขตพื้นที่ใกล้เคียงว่ามีปริมาณของยานพาหนะมากน้อยเพียงใด ซึ่งถ้ามีปริมาณยานพาหนะที่มากเกินกว่าค่าเกณฑ์ (Threshold) ที่กำหนดไว้ก็จะทำการเปลี่ยนชื่อเทียมและชื่อปลอมของยานพาหนะนั้นทันที เพราะยิ่งมีปริมาณของยานพาหนะในเขตพื้นที่หนึ่งๆ เพิ่มขึ้นก็จะทำให้ค่าความเป็นส่วนตัวลดน้อยลง โดยงานวิจัยนี้สามารถปกป้องความเป็นส่วนตัวของข้อมูลได้เป็นอย่างดีแต่การประมวลผลยังมีค่าโอเวอร์เฮดที่สูงมากเช่นเดิมทำให้ยังคงขาดประสิทธิภาพในการทำงาน

จากงานวิจัยที่ได้กล่าวไปทั้งหมดนั้นพบว่าการใช้อัลกอริทึมเพียงอัลกอริทึมเดียวเพื่อปิดบังข้อมูลอาจไม่เพียงพอและเหมาะสม จึงจำเป็นต้องนำเอาอัลกอริทึมหลายๆ อัลกอริทึมมาประยุกต์ใช้ร่วมกัน ซึ่งพิจารณาไปตามสถานการณ์และสภาพการทำงานของยานพาหนะในช่วงเวลาหนึ่งๆ ดังแสดงในหัวข้อถัดไป

3. ความเป็นส่วนตัวแบบหลายระดับ

จากงานวิจัยที่เกี่ยวข้องก่อนหน้านี้พบว่าอัลกอริทึมในการป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งในเครือข่ายวาเน็ตนั้นมีค่าโอเวอร์เฮดที่สูงในการประมวลผล และยังขาดประสิทธิภาพในการปิดบังข้อมูลตามรูปแบบการสื่อสารของยานพาหนะทั้งสามรูปแบบอย่างเหมาะสม งานวิจัยเรื่องนี้จึงได้นำเสนอแนวคิดของความเป็นส่วนตัวแบบหลายระดับ (Multi-Level Privacy) ซึ่งถูกกำหนดไว้ในรูปแบบของระดับความเป็นส่วนตัว (Privacy Levels) 3 ระดับ พร้อมทั้งนำเสนอปัจจัยสำหรับกำหนดระดับความเป็นส่วนตัว (Privacy Level Factors) และคะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัว (Privacy-Preserving and Requiring Score) ในการจัดระดับความเป็นส่วนตัวที่เหมาะสมในการใช้งาน โดยมีรายละเอียดดังต่อไปนี้

3.1 ระดับความเป็นส่วนตัว

งานวิจัยเรื่องนี้ได้กำหนดระดับความเป็นส่วนตัวในการป้องกันและปิดบังข้อมูลของยานพาหนะในเครือข่ายวาเน็ตเป็น 3 ระดับดังรายละเอียดตามตารางที่ 1

ตารางที่ 1 การจำแนกระดับความเป็นส่วนตัว

ระดับ	นิยาม	ตัวอย่างสถานการณ์
สูง (High)	เป็นระดับความเป็นส่วนตัวที่ต้องการความเป็นส่วนตัวสูง โดยข้อมูลของยานพาหนะจะต้องถูกป้องกันและปิดบังในระดับสูง และมีอัลกอริทึมที่ซับซ้อนในการประมวลผล โดยผู้ที่ไม่ได้รับอนุญาตให้เข้าถึงข้อมูลดังกล่าวจะไม่สามารถเปิดเผย ติดตาม และย้อนรอยข้อมูลได้	ยานพาหนะของหน่วยสืบราชการลับ ยานพาหนะขนเงินของธนาคาร ที่ต้องการความเป็นส่วนตัวสูง
ปานกลาง (Medium)	เป็นระดับความเป็นส่วนตัวที่ต้องการความเป็นส่วนตัวปานกลาง โดยข้อมูลของยานพาหนะจะถูกป้องกันและปิดบังในบางส่วนที่จำเป็น และมีอัลกอริทึมที่ไม่ซับซ้อนมากในการประมวลผล โดยผู้ที่ไม่ได้รับอนุญาตให้เข้าถึงข้อมูลดังกล่าวจะไม่สามารถเปิดเผย	ยานพาหนะของผู้ใช้ตามท้องถนนทั่วไปที่ต้องการความเป็นส่วนตัวในระดับปานกลาง

ระดับ	นิยาม	ตัวอย่างสถานการณ์
	ติดตาม และย้อนรอยข้อมูลที่สำคัญได้ แต่อาจสามารถทราบถึงข้อมูลบางอย่างที่เป็นข้อมูลพื้นฐานได้	
ต่ำ (Low)	เป็นระดับความเป็นส่วนตัวที่ต้องการความเป็นส่วนตัวต่ำ โดยข้อมูลของยานพาหนะจะไม่ถูกป้องกันและปิดบัง หรือถ้ามีความจำเป็นในการปิดบังก็จะใช้เพียงอัลกอริทึมอย่างง่ายในการประมวลผล โดยผู้ที่เกี่ยวข้องสามารถเข้าถึงข้อมูลดังกล่าวได้อย่างเปิดเผยทั้งยังสามารถติดตามและย้อนรอยข้อมูลได้	ยานพาหนะสาธารณะ เช่น รถตำรวจ รถดับเพลิง และรถฉุกเฉินที่ไม่ต้องการความเป็นส่วนตัวหรือต้องการความเป็นส่วนตัวต่ำ

3.2 ปัจจัยสำหรับกำหนดระดับความเป็นส่วนตัว

เมื่อกำหนดระดับความเป็นส่วนตัวในการปิดบังข้อมูลของยานพาหนะเป็น 3 ระดับแล้ว ต่อไปจะเป็นการกำหนดปัจจัยต่างๆ ของยานพาหนะที่จะนำมาพิจารณาเพื่อจำแนกและจัดกลุ่มระดับความเป็นส่วนตัวที่เหมาะสม โดยจากการศึกษางานวิจัยที่เกี่ยวข้อง [2-8] สามารถแบ่งปัจจัยต่างๆ เป็น 5 ปัจจัยดังรายละเอียดตามตารางที่ 2

ตารางที่ 2 การจำแนกปัจจัยของยานพาหนะสำหรับกำหนดระดับความเป็นส่วนตัว

ปัจจัย	คำอธิบาย
พิกัด (Position)	เป็นข้อมูลพิกัดหรือตำแหน่งของยานพาหนะ เช่น พิกัดละติจูด พิกัดลองจิจูด อยู่บนทางด่วน อยู่กลางสี่แยก เป็นต้น
ชื่อ (Name)	เป็นชื่อเรียกขานหรือชื่อที่ใช้สำหรับการอ้างอิงของยานพาหนะ เช่น ชื่อเรียก หมายเลขทะเบียน เป็นต้น
คุณสมบัติ (Properties)	เป็นข้อมูลคุณสมบัติต่างๆ ของยานพาหนะ เช่น สี รุ่น ยี่ห้อ จำนวนที่นั่ง ความแรงของเครื่องยนต์ เป็นต้น
ข้อมูลผู้ขับขี่ (Driver)	เป็นข้อมูลผู้ขับขี่ยานพาหนะ เช่น ชื่อ เพศ อายุ น้ำหนัก ส่วนสูง หมายเลขบัตรประจำตัวประชาชน หมายเลขใบขับขี่ เป็นต้น
สถานะ (Status)	เป็นสถานะของยานพาหนะ เช่น เลี้ยวซ้าย เลี้ยวขวา เดินหน้า ถอยหลัง เร่งความเร็ว ลดความเร็ว เป็นต้น

3.3 คะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัว

จากปัจจัยของยานพาหนะสำหรับกำหนดระดับความเป็นส่วนตัวที่ระบุไว้ในตารางที่ 2 จะนำมาพิจารณาเพื่อกำหนดเป็นคะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวของข้อมูลของยานพาหนะ โดยมีค่าคะแนนตั้งแต่ 0-4 คะแนนดังรายละเอียดตามตารางที่ 3

ตารางที่ 3 ค่าคะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัว

ระดับความสามารถ	คะแนน
มากที่สุด	4
มาก	3
ปานกลาง	2
น้อย	1
น้อยที่สุด	0

3.4 การกำหนดระดับความเป็นส่วนตัว

เมื่อกำหนดคะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวที่พิจารณาไปตามปัจจัยทั้ง 5 ปัจจัยของยานพาหนะแล้ว ต่อไปจะนำค่าคะแนนที่ได้ทุกปัจจัยมารวมกันเป็นคะแนนรวมสุทธิเพื่อจำแนกและจัดกลุ่มระดับความเป็นส่วนตัว โดยได้แบ่งช่วงคะแนนออกเป็น 3 ช่วงดังแสดงในตารางที่ 4

ตารางที่ 4 ช่วงคะแนนของระดับความเป็นส่วนตัว

ระดับความเป็นส่วนตัว	ช่วงคะแนน
สูง (High)	14 - 20
ปานกลาง (Medium)	7 - 13
ต่ำ (Low)	0 - 6

จากช่วงคะแนนที่กำหนดขึ้นตามตารางที่ 4 จะนำมาใช้ในการจำแนกระดับความเป็นส่วนตัวตามประสิทธิภาพเชิงทฤษฎีของอัลกอริทึม และตามความต้องการความเป็นส่วนตัวในการสื่อสารของยานพาหนะรูปแบบต่างๆ ซึ่งมีรายละเอียดอยู่ในหัวข้อถัดไป

4. การจำแนกอัลกอริทึมภายใต้ความเป็นส่วนตัวแบบหลายระดับ

งานวิจัยเรื่องนี้ได้พิจารณาอัลกอริทึมที่สำคัญสำหรับนำมาใช้ในการวัดประสิทธิภาพเชิงทฤษฎีจำนวน 5 อัลกอริทึมได้แก่ อัลกอริทึมชื่อเทียมและชื่อปลอม (Pseudonym and Anonym Algorithm) [3,4] อัลกอริทึมมิกซ์โซน (Mix-Zone Algorithm) [5] อัลกอริทึมอะโมอีบา (AMOEBA Algorithm) [6] อัลกอริทึมเรป (REP Algorithm) [7] และอัลกอริทึมดีแอลพี (DLP Algorithm) [8] นอกจากอัลกอริทึมทั้ง 5 อัลกอริทึม พบว่าในบางช่วงเวลาของการสื่อสารของยานพาหนะนั้นอาจไม่จำเป็นต้องใช้อัลกอริทึมใดเลยในการป้องกันและปิดบังตำแหน่งที่ตั้ง เพราะในกระบวนการสื่อสารดังกล่าวต้องการความเป็นสาธารณะแทนความเป็นส่วนตัว โดยจากปัจจัยของยานพาหนะทั้ง 5 ปัจจัย และคะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวที่กล่าวไว้ในหัวข้อก่อนหน้านี้ สามารถนำมาใช้ในการจำแนกและจัดกลุ่มอัลกอริทึมได้ดังรายละเอียดตามตารางที่ 5

ตารางที่ 5 การวิเคราะห์คะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวของอัลกอริทึมเพื่อจำแนกระดับความเป็นส่วนตัว

อัลกอริทึม	พิกัด	ชื่อ	คุณสมบัติ	ข้อมูลผู้ขับขี่	สถานะ	คะแนนรวม	ระดับความเป็นส่วนตัว
ไม่ใช้อัลกอริทึม	0	0	0	0	0	0	ระดับต่ำ
อัลกอริทึมชื่อเทียมและชื่อปลอม	1	3	2	2	1	9	ระดับปานกลาง
อัลกอริทึมมิกซ์โซน	1	3	2	2	2	10	ระดับปานกลาง
อัลกอริทึมดีแอลพี	3	4	3	3	3	16	ระดับสูง
อัลกอริทึมอะโมอีบา	3	4	3	4	3	17	ระดับสูง
อัลกอริทึมเรป	4	4	3	3	4	18	ระดับสูง

ค่าคะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวจากตารางที่ 5 นั้นได้มาจากการพิจารณาและศึกษาตามเอกสารงานวิจัย [2-8] ซึ่งเป็นค่าตามทฤษฎี โดยเมื่อจำแนกไปตามระดับความเป็น

ส่วนตัวที่กำหนดไว้จะได้ว่า ระดับต่ำได้แก่ ไม่ใช้อัลกอริทึม ระดับปานกลางได้แก่ อัลกอริทึมซีเทียมและซีอปลอม และอัลกอริทึมมิกซ์โซน และระดับสูงได้แก่ อัลกอริทึมดีแอลพี อัลกอริทึมอะโมอีบา และอัลกอริทึมเรป

5. การจำแนกรูปแบบการสื่อสารของยานพาหนะภายใต้ความเป็นส่วนตัวแบบหลายระดับ

จากรูปแบบการสื่อสารของยานพาหนะทั้ง 3 รูปแบบ [2] อันได้แก่ การสื่อสารระหว่างยานพาหนะกับยานพาหนะ การสื่อสารระหว่างยานพาหนะกับอุปกรณ์ และการสื่อสารระหว่างยานพาหนะกับบริการ สามารถแบ่งเป็นสถานการณ์ย่อยได้ 8 สถานการณ์ซึ่งจะนำมาจำแนกโดยกำหนดค่าคะแนนให้กับรูปแบบการสื่อสารต่างๆ ตามปัจจัยของความต้องการความเป็นส่วนตัว 5 ปัจจัยซึ่งมีรายละเอียดตามตารางที่ 6

ตารางที่ 6 การวิเคราะห์คะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวของรูปแบบการสื่อสารเพื่อจำแนกระดับความเป็นส่วนตัว

รูปแบบการสื่อสาร	พิกัด	ชื่อ	คุณสมบัติ	ข้อมูลผู้ขับ	สถานะ	คะแนนรวม	ระดับความเป็นส่วนตัว
การสื่อสารระหว่างยานพาหนะกับยานพาหนะ (วีทูวี : V2V)							
การบอกสถานะของยานพาหนะ	1	2	0	1	4	8	ระดับปานกลาง
การบอกสถานะของคนขับ	1	3	2	4	1	11	ระดับปานกลาง
การบอกตำแหน่งที่ตั้ง	4	3	2	2	1	12	ระดับปานกลาง
การสื่อสารส่วนบุคคล	4	4	4	4	4	20	ระดับสูง
การสื่อสารระหว่างยานพาหนะกับอุปกรณ์ (วีทูไอ : V2I)							
การแจ้งเตือนแบบสาธารณะ	0	0	0	2	1	3	ระดับต่ำ
การแจ้งเตือนแบบส่วนบุคคล	2	4	3	4	2	15	ระดับสูง
การสื่อสารระหว่างยานพาหนะกับบริการ (วีทูเอส : V2S)							
การลงทะเบียนจากบริการ	1	4	3	3	1	12	ระดับปานกลาง
การรับส่งข้อมูลจากบริการ	3	4	1	2	3	13	ระดับปานกลาง

ค่าคะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวจากตารางที่ 6 นั้นได้มาจากการพิจารณาและศึกษาตามเอกสารงานวิจัย [2-8] ซึ่งเป็นค่าตามทฤษฎีเช่นเดียวกับการจำแนกอัลกอริทึมในหัวข้อก่อนหน้านี้ โดยประกอบไปด้วยระดับต่ำได้แก่ สถานการณ์การแจ้งเตือนแบบสาธารณะ ระดับปานกลางได้แก่ สถานการร์การบอกสถานะของยานพาหนะ การบอกสถานะของคนขับ การบอกตำแหน่งที่ตั้ง การลงทะเบียนจากบริการ และการรับส่งข้อมูลจากบริการ และระดับสูงได้แก่ สถานการณ์การสื่อสารส่วนบุคคล และการแจ้งเตือนแบบส่วนบุคคล

6. การรักษาความเป็นส่วนตัวภายใต้ความเป็นส่วนตัวแบบหลายระดับ

จากการจำแนกอัลกอริทึมและรูปแบบการสื่อสารของยานพาหนะตามระดับความเป็นส่วนตัวในหัวข้อก่อนหน้านี้ สามารถนำมาใช้ในการรักษาความเป็นส่วนตัวของยานพาหนะภายใต้พื้นฐานของความเป็นส่วนตัวแบบหลายระดับ โดยอัลกอริทึมที่ใช้ในการปิดบังข้อมูลจะปรับเปลี่ยนไปตามสถานการณ์และรูปแบบการสื่อสาร ณ ขณะใดขณะหนึ่งโดยมีรายละเอียดอย่างสรุปตามตารางที่ 7

ตารางที่ 7 การแจกแจงระดับความเป็นส่วนตัวโดยจำแนกตามอัลกอริทึมและรูปแบบการสื่อสารของยานพาหนะ

ระดับความเป็นส่วนตัว	อัลกอริทึม	รูปแบบการสื่อสาร	
ระดับสูง	อัลกอริทึมดีแอลพี (คะแนน: 16) อัลกอริทึมอะโมอีบา (คะแนน: 17) อัลกอริทึมเรป (คะแนน: 18)	การสื่อสารแบบวีทูวี	การสื่อสารส่วนบุคคล (คะแนน: 20)
		การสื่อสารแบบวีทูไอ	การแจ้งเตือนแบบส่วนบุคคล (คะแนน: 15)
ระดับปานกลาง	อัลกอริทึมซื่อเทียมและซื่อปลอม (คะแนน: 9) อัลกอริทึมมิกซ์โซน (คะแนน: 10)	การสื่อสารแบบวีทูวี	การบอกสถานะของยานพาหนะ (คะแนน: 8)
			การบอกสถานะของคนขับ (คะแนน: 11)
			การบอกตำแหน่งที่ตั้ง (คะแนน: 12)
		การสื่อสารแบบวีทูเอส	การลงทะเบียนจากบริการ (คะแนน: 12)
			การรับส่งข้อมูลจากบริการ (คะแนน: 13)
ระดับต่ำ	ไม่ใช้อัลกอริทึม (คะแนน: 0)	การสื่อสารแบบวีทูไอ	การแจ้งเตือนแบบสาธารณะ (คะแนน: 3)

จากตารางที่ 7 ซึ่งได้แจกแจงระดับความเป็นส่วนตัวโดยจำแนกตามอัลกอริทึมและรูปแบบการสื่อสารของยานพาหนะ โดยเมื่อมีสถานการณ์หรือการใช้งานของยานพาหนะตามช่วงเวลาเข้ามา กระบวนการป้องกันและปิดบังความเป็นส่วนตัวของข้อมูลตามแนวความคิดของงานวิจัยเรื่องนี้ก็จะเริ่มขึ้นภายใต้ระดับความเป็นส่วนตัวที่ได้เลือกไว้ และจะสลับสับเปลี่ยนไปตามรูปแบบการสื่อสารที่เปลี่ยนไปตามช่วงเวลา

7. การวัดประสิทธิภาพการทำงานเชิงทฤษฎี

การวัดประสิทธิภาพการทำงานของวิธีการป้องกันและปิดบังข้อมูลของยานพาหนะบนพื้นฐานของความเป็นส่วนตัวแบบหลายระดับนี้จะใช้วิธีการคำนวณตามทฤษฎีโดยมีสมการคำนวณค่าโอเวอร์เฮด (Overhead) เป็นดังนี้

$$\text{Overhead} = \frac{\sum_{i=1}^{n} \text{Score}(E_i)}{n} \quad (1)$$

จากสมการที่ 1 กำหนดให้ E_i คือสถานการณ์ที่ i ซึ่งเกิดขึ้นในกระบวนการสื่อสารของยานพาหนะ $\text{Score}(E_i)$ คือค่าคะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวในสถานการณ์ที่ i และ n คือจำนวนของสถานการณ์ทั้งหมดที่เกิดขึ้น ซึ่งจากข้อมูลของงานวิจัย [2-8] พบว่าเมื่อมีค่าความสามารถและความต้องการในความเป็นส่วนตัวสูงขึ้นก็จะทำให้ค่าโอเวอร์เฮดสูงขึ้นตามไปด้วย โดยในการวัดประสิทธิภาพในครั้งนี้ได้ใช้สถานการณ์พื้นฐาน 8 สถานการณ์จากรูปแบบการสื่อสารของยานพาหนะที่กล่าวไว้ในหัวข้อก่อนหน้านี้ โดยกำหนดให้ความน่าจะเป็นของการเกิดสถานการณ์ทั้ง 8 สถานการณ์นี้มีอย่างเท่าเทียมกันและเป็นอิสระต่อกัน ซึ่งค่าโอเวอร์เฮดที่คำนวณได้ปรากฏตามตารางที่ 8

ตารางที่ 8 การคำนวณค่าโอเวอร์เฮดของอัลกอริทึม

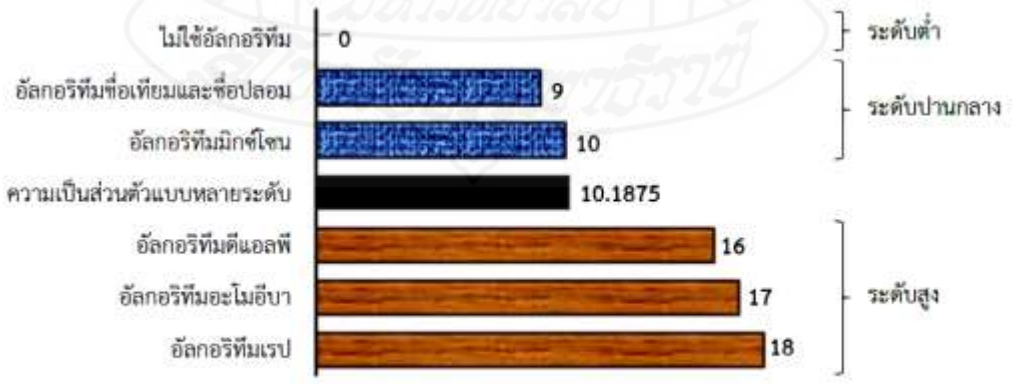
อัลกอริทึม	ค่าโอเวอร์เฮด
ไม่ใช้อัลกอริทึม	$\frac{0+0+0+0+0+0+0+0}{8}=0.0$
อัลกอริทึมชื่อเทียมและชื่อปลอม	$\frac{9+9+9+9+9+9+9+9}{8}=9.0$
อัลกอริทึมมิกซ์โซน	$\frac{10+10+10+10+10+10+10+10}{8}=10.0$
อัลกอริทึมดีแอลพี	$\frac{16+16+16+16+16+16+16+16}{8}=16.0$
อัลกอริทึมอะโมอีบา	$\frac{17+17+17+17+17+17+17+17}{8}=17.0$
อัลกอริทึมเรป	$\frac{18+18+18+18+18+18+18+18}{8}=18.0$

จากค่าโอเวอร์เฮดในตารางที่ 8 เป็นค่าที่ได้จากการคำนวณโดยการเลือกใช้อัลกอริทึมเพียงหนึ่งอัลกอริทึมตลอดทั้ง 8 สถานการณ์ ต่อไปนี้จะเป็นการคำนวณค่าโอเวอร์เฮดจากการเลือกใช้และปรับเปลี่ยนอัลกอริทึมไปตามระดับความเป็นส่วนตัวทั้ง 3 ระดับที่ได้กำหนดไว้ก่อนหน้านี้ ซึ่งมีรายละเอียดตามตารางที่ 9

ตารางที่ 9 การคำนวณค่าโอเวอร์เฮดโดยการปรับเปลี่ยนอัลกอริทึมไปตามระดับความเป็นส่วนตัว

กรณีการประมวลผล	ค่าโอเวอร์เฮด
กรณีที่ดีที่สุด (Best-Case)	$\frac{9+9+9+16+0+16+9+9}{8}=9.625$
กรณีที่เลวร้ายที่สุด (Worst-Case)	$\frac{10+10+10+18+0+18+10+10}{8}=10.75$
กรณีเฉลี่ย (Average-Case)	$\frac{9.625+10.75}{2}=10.1875$

จากตารางที่ 9 ปรากฏค่าโอเวอร์เฮดเฉลี่ยอยู่ที่ 10.1875 ซึ่งมีค่ามากกว่าการไม่ใช่อัลกอริทึม อัลกอริทึมชื่อเทียมและชื่อปลอม และอัลกอริทึมมิกซ์โซน แต่มีค่าน้อยกว่าอัลกอริทึมดีแอลพี อัลกอริทึมอะโมอีบา และอัลกอริทึมเรป ดังแสดงกราฟการเปรียบเทียบประสิทธิภาพของอัลกอริทึมตามรูปที่ 3



รูปที่ 3 กราฟการเปรียบเทียบค่าโอเวอร์เฮดของอัลกอริทึมต่างๆ กับความเป็นส่วนตัวแบบหลายระดับ

8. บทสรุปและแนวทางการวิจัยในอนาคต

งานวิจัยเรื่องนี้ได้นำเสนอความเป็นส่วนตัวแบบหลายระดับอันได้แก่ ระดับสูง ระดับปานกลาง และระดับต่ำ เพื่อใช้ในการป้องกันและปิดบังข้อมูลของยานพาหนะในเครือข่ายวาเน็ต โดยระดับความเป็นส่วนตัวแต่ละระดับนั้นจะมีอัลกอริทึมการป้องกันและปิดบังที่แตกต่างกันตามความเหมาะสมของสถานการณ์และกระบวนการสื่อสารของยานพาหนะ ณ ขณะใดขณะหนึ่ง และสามารถปรับเปลี่ยนไปตามสภาพความเป็นจริงของการสื่อสาร โดยจากการคำนวณค่าโอเวอร์เฮดตามทฤษฎีพบว่ากระบวนการป้องกันและปิดบังข้อมูลของยานพาหนะภายใต้ความเป็นส่วนตัวแบบหลายระดับนี้มีประสิทธิภาพในการทำงานที่ดีกว่ากระบวนการป้องกันและปิดบังแบบเดิม แต่อย่างไรก็ตามงานวิจัยเรื่องนี้ยังคงมีการวิจัยอย่างต่อเนื่องในอนาคตโดยการทดลองกับระบบจำลองที่กำหนดสภาพแวดล้อมและกระบวนการทำงานเสมือนจริงเพื่อวัดประสิทธิภาพเชิงปฏิบัติการอีกครั้งหนึ่ง ทั้งยังต้องกำหนดวิธีการคัดเลือกและสับเปลี่ยนอัลกอริทึมที่มีความน่าเชื่อถือมากยิ่งขึ้นในอนาคต

9. กิตติกรรมประกาศ

งานวิจัยเรื่องนี้ได้รับการสนับสนุนจากทุนอุดหนุนสำหรับการทำวิจัยในระดับบัณฑิตศึกษาประจำภาคปลาย ปีการศึกษา 2556 มหาวิทยาลัยสุโขทัยธรรมาธิราช

10. เอกสารอ้างอิง

[1] Chow, C.Y. Mokbel, M.F. He, T. (2011). A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks. *IEEE Transactions on Mobile Computing*, vol.10, no.1, 2011.

[2] Schoch, E. Kargl, F. Weber, M. and Leinmuller, T. (2008). Communication Patterns in VANETs. *IEEE Communications Magazine*, Volume 46, Issue 11, November 2008.

[3] Calandriello, G. Papadimitratos, P. Hubaux, J.P. and Lioy, A. (2007). Efficient and Robust Pseudonymous Authentication in VANET. *Proceedings of 4th ACM International Workshop on Vehicular Ad-Hoc Networks (VANET 2007)*, Montreal, Canada, September 10, 2007.

[4] Gerlach, M. and Guttler, F. (2007). Privacy in VANET using Changing Pseudonyms-Ideal and Real. *Proceedings of IEEE 65th Vehicular Technology Conference (VTC 2007)*, Dublin, Ireland, April 2007.

[5] Freudiger, J. Raya, M. and Félegyházi, M. (2007). Mix Zones for Location Privacy in Vehicular Networks. *Proceedings of First International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS 2007)*, Vancouver, British Columbia, August 14, 2007.

[6] Sampigethaya, K. Li, M. Huang, L. and Poovendran, R. (2007). AMOEBA: Robust Location Privacy Scheme for VANET. *IEEE Journal on Selected Areas in Communications*, Volume 25, Issue 8, 2007.

[7] Wasef A. and Shen, X.S. (2010). REP: Location Privacy for VANETs Using Random Encryption Periods. *Journal on Mobile Networks and Applications Archive*, Volume 15, Issue 1, 2010.

[8] Song, J.H. Wong, V.W.S. and Leung, V.C. (2010). Wireless Location Privacy Protection in Vehicular Ad-Hoc Networks. *Journal of Mobile Networks and Applications Archive*, Volume 15, Issue 1, 2010.

บรรณานุกรม

บรรณานุกรม

Abumansoor, O., Boukerche, A. & Landfeldt, B. (2011). *Privacy Preserving Neighborhood Awareness in Vehicular Ad Hoc Networks.* 7th ACM symposium on QoS and security for wireless and mobile networks.

Alganas, A., Lin, X. & Grami, A. (2011). *EVSE: An Efficient Vehicle Social Evaluation Scheme with Location Privacy Preservation for Vehicular Communications.* IEEE International Conference on Communications (ICC 2011), Kyoto, Japan.

Ashok, V. G., Gongjun, Y., Olariu, S. & Gupta, A. (2010). *Privacy Aware Localization in VANET.* IEEE 7th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2010), San Francisco, CA, USA.

Burmester, M., Magkos, E. & Chrissikopoulos, V. (2008). *Strengthening Privacy Protection in VANETs.* IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB 2008).

Calandriello, G., Papadimitratos, P., Hubaux, J. P., & Lioy, A. (2007). *Efficient and Robust Pseudonymous Authentication in VANET.* 4th ACM International Workshop on Vehicular Ad-Hoc Networks (VANET 2007), Montreal, Canada.

Chaurasia, B. K., Verma, S., Tomar, G. S. & Bhaskar, S.M. (2008). *Pseudonym Based Mechanism for Sustaining Privacy in VANETs.* 1st International Conference on Computational Intelligence, Communication Systems and Networks.

Chow, C.Y., Mokbel, M.F., He, T. (2011). *A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks.* IEEE Transactions on Mobile Computing, vol.10, no.1.

CVIS. (2012). Retrieved from http://www.cvisproject.org/.

Data Communication in VANETs. (2015). Retrieved from http://www.stonevariety.com/0031313/vanet.pdf.

DSRC. (2012). Retrieved from http://161.200.184.9/webelarning/elearning%20Computer53/Bluetooth/File/0_DSRC.html.

Ezell, S. (2010). *Intelligent Transportation Systems.* The Information Technology & Innovation Foundation (ITIF).

Freudiger, J., Raya, M. & Félegyházi, M. (2007). *Mix Zones for Location Privacy in Vehicular Networks.* 1st International ICST Workshop on Wireless Networking for Intelligent Transportation Systems, Vancouver, British Columbia.

Gerlach, M., & Guttler, F. (2007). *Privacy in VANETs using Changing Pseudonyms - Ideal and Real.* IEEE 65th Vehicular Technology Conference (VTC 2007), Dublin, Ireland.

Gosman, C., Dobre, C. & Cristea, V. (2010). *A Security Protocol for Vehicular Distributed Systems.* 12th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing.

Haas, J. J., Hu, Y. C. & Laurenti, N. (2011). *Low-Cost Mitigation of Privacy Loss due to Radiometric Identification.* 8th ACM International Workshop on Vehicular Inter-Networking (VANET 2011).

Hoh, B., Gruteser, M., Herring, R., Ban, J., Work, D., Herrera, J. C., Bayen, A. M., Annavaram, M. & Jacobso, Q. (2008). *Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring.* 6th International Conference on Mobile Systems, Applications, and Services (MobiSys 2008), Breckenridge, CO, USA.

Hoh, B., Gruteser, M., Xiong, H. & Alrabady, A. (2007). *Preserving Privacy in GPS Traces via Uncertainty-Aware Path Cloaking.* 14th ACM Conference on Computer and Communications Security, Alexandria, Virginia, USA.

InteliliDrive. (2012). Retrieved from http://www.intellidriveusa.org/.

Keardsri, W., Kritpolviman, K. & Wilailux, K. (2014). *Defining Privacy Levels for Location Protection and Anonymization in Vehicular Ad-Hoc Network.* ASEAN Undergraduate Conference in Computing 2014 (AUCC 2014).

Keardsri, W., Kritpolviman, K. & Wilailux, K. (2015). *Multi-Levels Privacy-Preserving for Location Monitoring System in VANET.* 1st National Conference on Technology for National Development (TECHCON 2015), Bangkok, Thailand.

Kenney, J. B. (2011). *Dedicated Short-Range Communications (DSRC) Standards in the United States.* Proceedings of the IEEE, Volume 99, Issue 7.

Kim, W. (2009). *Research and Development of UbiquitousTransportation Systems Research and Development of UbiquitousTransportation.* Korea Aerospace University Presentation.

Kompfner, P. (2009). *CVIS: Cooperative Vehicle-Infrastructure Systems.* White Paper 2009.

Kulachai, W. (2015). *Intelligent Transport Systems.* Retrieved from http://www.trafficpolice.go.th/.

Lee, S. K. (2009). *A Proposal for the standardization of u-ITS as ITS 2.0 by ISO/TC 204.* White Paper 2009.

Li, M., Sampigethaya, K., Huang, L. & Poovendran, R. (2006). *Swing & Swap: User-Centric Approaches Towards Maximizing Location Privacy.* 5th ACM Workshop on Privacy in Electronic Society, Alexandria, Virginia, USA.

Lu, R., Lin, X., Liang, X. & Shen, X. (2010). *Sacrificing the Plum Tree for the Peach Tree: A Socialspot Tactic for Protecting Receiver-location Privacy in VANET.* IEEE Global Telecommunications Conference (GLOBECOM 2010), Miami, FL, USA.

Lu, R., Lin, X., Luan, T. H., Liang, X. & Shen, X. (2011). *Anonymity Analysis on Social Spot based Pseudonym Changing for Location Privacy in VANETs.* IEEE International Conference on Communications (ICC 2011), Kyoto, Japan.

Poochaya, S. (2010). *Data Rate Enhancement of Dedicated Short Range Communication for Intelligence Transportation System using Mimo Technique.* Master Thesis in Telecommunication Engineering, Suranaree University of Technology.

Prathombutr, P. (2010). *Communications in ITS - The Car-Talk Project.* Car Talk Presentation.

Prathombutr, P. & Panjatanasak, S. (2006). *Intelligent Transport System in Thailand.* White Paper 2006.

Qian, Y., Lu, K. & Moayeri, N. (2008). *A Secure VANET MAC Protocol for DSRC Applications.* IEEE Global Telecommunications Conference.

Ren, D., Du, S. & Zhu, H. (2011). *A Novel Attack Tree Based Risk Assessment Approach for Location Privacy Preservation in the VANETs.* IEEE International Conference on Communications (ICC 2011), Kyoto, Japan.

Sampigethaya, K., Li, M., Huang, L. & Poovendran, R. (2007). *AMOEBA: Robust Location Privacy Scheme for VANET.* IEEE Journal on Selected Areas in Communications, Volume 25, Issue 8.

Scheuer, F., Brecht, M. & Federrath, H. (2010). *A privacy-aware location service for VANETs using Chaum's mixes.* IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2010), Niagara Falls, ON, Canada.

Smartway Team. (2007). *ITS Introduction Guide Shift from Legacy Systems to Smartway.* White Paper 2007.

Smith, B., Venkatanarayana, R., Park, H., Goodall, N., Datesh, J. & Skerrit, C. (2010). *IntelliDrive Traffic Signal Control Algorithms.* White Paper 2010.

Song, J. H., Wong, V. W. S. & Leung, V. C. (2010). *Wireless Location Privacy Protection in Vehicular Ad-Hoc Networks.* Journal of Mobile Networks and Applications archive, Volume 15, Issue 1.

Vehicular Ad-hoc Network: VANET. (2015). Retrieved from https://sites.google.com/site/internetworkingmanet/vanet.

Wasef, A. & Shen, X. (2010). *REP: Location Privacy for VANETs Using Random Encryption Periods.* Journal on Mobile Networks and Applications Archive, Volume 15, Issue 1.

Weerasinghe, H., Fu, H. & Leng, S. (2010). *Anonymous Service Access for Vehicular Ad Hoc Networks.* 6th International Conference on Information Assurance and Security, Xi'ian China.

Weerasinghe, H., Fu, H. & Leng, S. (2011). *Enhancing Unlinkability in Vehicular Ad Hoc Networks.* IEEE International Conference on Intelligence and Security Informatics (ISI 2011), Beijing, China.

Yang, Q., Lim, A., Ruan, X. & Qin, X. (2010). *Location Privacy Protection in Contention Based Forwarding for VANETs.* IEEE Global Telecommunications Conference (GLOBECOM 2010), Miami, FL, USA.

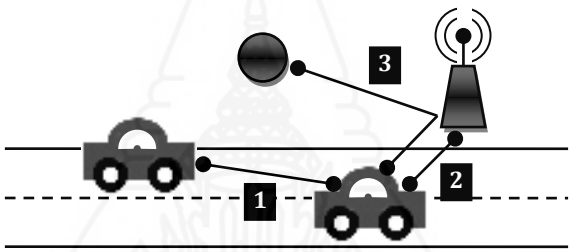
บทที่ 1
บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันรูปแบบการสื่อสารด้วยเทคโนโลยีไร้สาย (Wireless Technology) กำลังได้รับความนิยมและมีบทบาทมากยิ่งขึ้นในอนาคตอันใกล้ โดยในยุคเริ่มแรกของการสื่อสารด้วยเทคโนโลยีไร้สายเป็นเพียงการสื่อสารระหว่างเครื่องคอมพิวเตอร์ทั่วไปเท่านั้น แต่ในปัจจุบันและในอนาคตการสื่อสารด้วยเทคโนโลยีไร้สายกำลังกลายเป็นการสื่อสารระหว่างอุปกรณ์ต่างๆ มากมาย และอุปกรณ์เหล่านั้นก็สามารถเชื่อมต่อผ่านทางระบบไร้สายอยู่ตลอดเวลาและทั่วทุกหนทุกแห่ง จนกลายเป็นที่มาของเทคโนโลยีใหม่ที่เรียกว่าอินเทอร์เน็ตในทุกสิ่ง (Internet of Things: IoT) โดยอุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการสื่อสารได้แก่ คอมพิวเตอร์ แท็บเล็ต (Tablet) สมาร์ทโฟน (Smartphone) เซ็นเซอร์ (Sensor) รวมถึงรถยนต์หรือยานพาหนะอีกด้วย ซึ่งเทคโนโลยีของการสื่อสารแบบไร้สายในยานพาหนะนั้นเริ่มแรกถูกผนวกรวมกับระบบขนส่งและจราจรอัจฉริยะ (Intelligent Transport System: ITS) แต่ในต่อมาก็ได้แตกแขนงออกเป็นเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ (Vehicular Ad-Hoc Network: VANET) โดยสาขาวิชาทางด้านเครือข่ายไร้สายเฉพาะกิจของยานพาหนะนี้ได้เกิดขึ้นในช่วง 15 ปีที่ผ่านมา และยังอยู่ในช่วงของการทำวิจัยในประเด็นต่างๆ อย่างต่อเนื่อง หนึ่งในนั้นคือประเด็นทางด้านความเป็นส่วนตัวของตำแหน่งที่ตั้ง (Location Privacy) ซึ่งประเด็นดังกล่าวมีเป้าหมายและวัตถุประสงค์เพื่อป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะ เมื่อยานพาหนะเคลื่อนที่ไป ณ สถานที่ตั้งหรือตำแหน่งต่างๆ ในแผนที่

การติดตามตำแหน่งที่ตั้งของยานพาหนะ (Vehicle Location Tracking) และการตรวจสอบตำแหน่งที่ตั้งของยานพาหนะ (Vehicle Location Monitoring) เป็นกระบวนการหนึ่งที่ตรวจสอบว่ายานพาหนะแต่ละคันนั้นอยู่ ณ ตำแหน่งใดในแผนที่ ซึ่งการตรวจสอบตำแหน่งที่ตั้งนั้นมีทั้งข้อดีและข้อเสีย โดยถ้านำไปใช้ในการตรวจหาตำแหน่งของยานพาหนะเพื่อทำให้ทราบว่ายานพาหนะคันที่สนใจนั้นอยู่ ณ บริเวณใด หรือใช้ในการติดตามโจรผู้ร้ายก็จะเป็นประโยชน์อย่างยิ่ง แต่ในทางกลับกันถ้านำไปใช้เพื่อพยายามจะสอดส่องหรือแอบดูข้อมูลของยานพาหนะคันอื่นๆ ว่ากำลังเคลื่อนที่ไป ณ พิกัดใดในแผนที่ทางภูมิศาสตร์ กระบวนการดังกล่าวถือเป็นการละเมิดความ

เป็นส่วนตัวของยานพาหนะและของผู้ขับขี่ยานพาหนะ ในขณะเดียวกันการสื่อสารระหว่างยานพาหนะ (Vehicle Communications) บนท้องถนนในแต่ละช่วงเวลานั้นอาจมีรูปแบบการสื่อสารที่แตกต่างกันไปตามการขับขี่และสถานการณ์ต่างๆ ของยานพาหนะได้ดังแสดงในรูปภาพที่ 1.1 ซึ่งสถานการณ์เหล่านั้นก็ต้องการความเป็นส่วนตัวของตำแหน่งที่ตั้งที่แตกต่างกันออกไปด้วย เช่น รถตำรวจ รถดับเพลิง และรถฉุกเฉินของโรงพยาบาล ที่ไม่ต้องการความเป็นส่วนตัวเลยหรือต้องการความเป็นส่วนตัวน้อยมาก รถของผู้ใช้ตามท้องถนนทั่วไปที่ต้องการความเป็นส่วนตัวในระดับปานกลาง และรถของหน่วยสืบราชการลับที่ต้องการความเป็นส่วนตัวสูง เป็นต้น จะเห็นว่าสถานการณ์ต่างๆ ที่ได้กล่าวมานั้นมีระดับความเป็นส่วนตัว (Privacy Level) ที่แตกต่างกันไป ดังนั้นจึงต้องมีการจัดรูปแบบการป้องกันความเป็นส่วนตัวให้สอดคล้องกับสถานการณ์และระดับความเป็นส่วนตัวเหล่านั้นอย่างเหมาะสมด้วยเช่นกัน



1. การสื่อสารระหว่างยานพาหนะกับยานพาหนะ
2. การสื่อสารระหว่างยานพาหนะกับอุปกรณ์
3. การสื่อสารระหว่างยานพาหนะกับบริการ

ภาพที่ 1.1 รูปแบบการสื่อสารในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

จากรูปแบบการสื่อสารของยานพาหนะทั้ง 3 รูปแบบมีรายละเอียดของสถานการณ์ในการสื่อสารต่างๆ ดังต่อไปนี้

1. การสื่อสารระหว่างยานพาหนะกับยานพาหนะหรือวีทูวี (Vehicle to Vehicle: V2V) เป็นรูปแบบการสื่อสารระหว่างยานพาหนะตั้งแต่สองคันขึ้นไปที่แลกเปลี่ยนข้อมูลต่างๆ ระหว่างกัน โดยตัวอย่างของการสื่อสารประเภทนี้ได้แก่ การแสดงสถานการณ์หรือพฤติกรรมบางอย่างของยานพาหนะ ณ ขณะที่ขับขี่ เช่น การเลี้ยวซ้ายเลี้ยวขวา การเพิ่มลดความเร็ว การบอกตำแหน่งที่ตั้ง การแจ้งบอก “มือใหม่หัดขับ” เป็นต้น ซึ่งสถานการณ์หรือพฤติกรรมเหล่านี้จะมีความเป็นส่วนตัวในการสื่อสารที่แตกต่างกันไป

2. การสื่อสารระหว่างยานพาหนะกับอุปกรณ์หรือวีทูไอ (Vehicle to Infrastructure: V2I) เป็นรูปแบบการสื่อสารระหว่างยานพาหนะกับเครื่องมือสื่อสารและอุปกรณ์ควบคุมต่างๆ ที่ติดตั้งบริเวณรายรอบถนน โดยอาจจะเป็นเสาสัญญาณข้างถนน อุปกรณ์หรือเครื่องมือที่ติดอยู่บนเกาะกลางถนน โดยตัวอย่างของการสื่อสารประเภทนี้ได้แก่ การแสดงข้อมูลบางอย่างของอุปกรณ์ข้างถนนกับยานพาหนะ เช่น การแจ้งเตือนเขตชุมชน การแจ้งเตือนเขตโรงเรียน การแจ้งเตือนก่อนถึงสี่แยก เป็นต้น ซึ่งการแสดงข้อมูลเหล่านี้จะมีความเป็นส่วนตัวในการสื่อสารที่แตกต่างกันไป

3. การสื่อสารระหว่างยานพาหนะกับบริการหรือวีทูเอส (Vehicle to Service: V2S) เป็นรูปแบบการสื่อสารระหว่างยานพาหนะกับผู้ให้บริการต่างๆ ที่อยู่ห่างจากบริเวณพื้นที่ถนน โดยตัวอย่างของการสื่อสารประเภทนี้ได้แก่ การรับส่งข้อมูลจากบริการที่มีหลากหลายรูปแบบ เช่น ข้อความ เพลง เสียง วีดิโอ เป็นต้น ซึ่งรูปแบบข้อมูลที่แตกต่างกันเหล่านี้ก็จะต้องมีรูปแบบของความเป็นส่วนตัวในการสื่อสารที่แตกต่างกันไป

จากความรู้ในประเด็นของการป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะเมื่อได้ศึกษาถึงงานวิจัยที่เกี่ยวข้องพบว่า พบว่าช่วงเริ่มต้นนั้นได้ใช้การปิดบังชื่อหรือปิดบังข้อมูลของยานพาหนะให้กลายเป็นชื่อเทียม (Pseudonym) (Gerlach & Guttler, 2007) และชื่อปลอม (Anonym) (Calandriello, Papadimitratos, Hubaux & Lioy, 2007) โดยเป็นอัลกอริทึมอย่างง่ายที่นำมาใช้ในช่วง 10 ปีที่ผ่านมา ซึ่งใช้เทคนิคการเข้ารหัส (Encryption) และเทคนิคการแฮช (Hashing) ในการปิดบังข้อมูลทำให้การติดตามข้อมูลของยานพาหนะทำได้ยากขึ้น ทั้งยังไม่สามารถทราบถึงชื่อหรือข้อมูลจริงของยานพาหนะนั้นได้ แต่การใช้ชื่อเทียมและชื่อปลอมได้ถูกกำหนดให้กับยานพาหนะแต่ละคันอย่างถาวรทำให้สุดท้ายสามารถคาดเดาถึงข้อมูลจริงของยานพาหนะนั้นได้ในที่สุด งานวิจัยต่อมามีการนำเสนอหลักการที่เรียกว่ามิกซ์โซน (Mix-Zone) (Freudiger, Raya & Félegyházi, 2007) ซึ่งเป็นอัลกอริทึมที่มีการแลกเปลี่ยนกุญแจที่ใช้ในการเข้ารหัสของข้อมูล ซึ่งจะแบ่งพื้นที่ต่างๆ ในแผนที่ออกเป็นมิกซ์โซนหลายมิกซ์โซน โดยแต่ละมิกซ์โซนจะมีกุญแจการเข้ารหัสเพื่อใช้ในการปิดบังข้อมูลที่แตกต่างกันออกไป ยานพาหนะจะต้องใช้กุญแจในการปิดบังข้อมูลที่แตกต่างกันไปตามมิกซ์โซนปัจจุบันที่กำลังเคลื่อนที่ไปถึง ทำให้ชื่อของยานพาหนะมีการเปลี่ยนแปลงแบบพลวัต (Dynamic) อยู่ตลอดเวลา แต่อย่างไรก็ตามการสื่อสารของยานพาหนะยังต้องใช้กระบวนแบบบรอดคาสท์ซึ่งมีการปล่อยสัญญาณอย่างต่อเนื่อง ทำให้ยังสามารถติดตามเส้นทางของยานพาหนะนั้นจากสัญญาณที่ปล่อยออกมาได้ดังเดิมถึงแม้ว่าจะมีการเปลี่ยนแปลงชื่อก็ตาม เพียงแต่การเดาชื่อหรือข้อมูลจริงของยานพาหนะนั้นทำได้ยากขึ้นเท่านั้น งานวิจัยต่อมาจึงได้นำเสนอหลักการที่เรียกว่าอะโมอีบ้า (AMOEBA) (Sampigethaya, Li, Huang & Poovendran, 2007) ซึ่งเป็นอัลกอริทึมที่กำหนดให้ยานพาหนะแต่ละคันมีการปล่อยสัญญาณบรอด

คาสท์แบบเป็นช่วงที่ไม่ต่อเนื่องโดยกำหนดให้มีช่วงเงียบ (Silent Period) และช่วงปล่อยสัญญาณ (Broadcast Period) จึงทำให้การติดตามข้อมูลของยานพาหนะเกิดการขาดช่วงจังหวะและยากยิ่งขึ้นต่อการติดตามเส้นทาง นอกจากนี้ยังใช้กระบวนการสื่อสารผ่านทางหัวหน้ากลุ่ม (Group Leader) ของเขตพื้นที่ที่ยานพาหนะกำลังเคลื่อนที่อยู่ ณ ปัจจุบันเพื่อเป็นตัวแทนในการแลกเปลี่ยนข้อมูล อัลกอริทึมอะโมอีบ้านี้มีข้อเสียคือมีโอเวอร์เฮดในการประมวลผลที่สูงมาก จึงมีงานวิจัยต่อมาได้นำเอาแนวคิดของอะโมอีบ้าไปประยุกต์ใช้โดยการเพิ่มหลักการเข้ารหัสชื่อแบบสุ่มหรือเรป (Random Encryption Period: REP) (Wasef, & Shen, 2010) ซึ่งจะมีการปรับปรุงระยะเวลาในการเงียบและระยะเวลาในการส่งสัญญาณเป็นแบบสุ่ม โดยกำหนดกุญแจการเข้ารหัสที่เป็นตัวเลขสุ่มแล้วปล่อยสัญญาณตามคาบที่ถูกระบุด้วยตัวเลขสุ่มนั้น ทำให้ชื่อเทียมหรือชื่อปลอมของยานพาหนะมีการเปลี่ยนแปลงไปแบบที่ไม่สามารถคาดเดาได้ ยากต่อการติดตามข้อมูลยิ่งขึ้น แต่อย่างไรก็ตามงานวิจัยนี้ก็เพิ่มโอเวอร์เฮดในการประมวลผลให้สูงยิ่งขึ้นตามไปด้วย งานวิจัยต่อมาคือดีแอลพี (Density-based Location Privacy: DLP) (Song, Wong, & Leung, 2010) ซึ่งเกิดขึ้นในช่วงเวลาเดียวกับงานวิจัยของ Wasef et al. (2010) ได้นำเอาหลักการของอะโมอีบ้าไปประยุกต์ใช้เช่นกันแต่จะมีการพิจารณาถึงความหนาแน่น (Density) ของเขตพื้นที่ใกล้เคียงว่ามีปริมาณของยานพาหนะมากน้อยเพียงใด ซึ่งถ้ามีปริมาณยานพาหนะที่มากเกินกว่าค่าเกณฑ์ (Threshold) ที่กำหนดไว้ก็จะทำการเปลี่ยนชื่อเทียมและชื่อปลอมของยานพาหนะนั้นทันที เพราะยิ่งมีปริมาณของยานพาหนะในเขตพื้นที่หนึ่งๆ เพิ่มขึ้นก็จะทำให้ค่าความเป็นส่วนตัวลดน้อยลง โดยงานวิจัยนี้สามารถปกป้องความเป็นส่วนตัวของข้อมูลได้เป็นอย่างดีแต่การประมวลผลยังมีค่าโอเวอร์เฮดที่สูงมากเช่นเดิมทำให้ยังคงขาดประสิทธิภาพในการทำงาน

จากงานวิจัยที่ได้กล่าวไปทั้งหมดนั้น มีการคำนึงถึงปัจจัยทางด้านความเป็นส่วนตัว (Privacy) เพียงอย่างเดียวเท่านั้น ซึ่งต้องการจะหาวิธีการทุกวิถีทางเพื่อที่จะป้องกันความเป็นส่วนตัวให้ได้มากที่สุดเท่าที่จะทำได้ ทำให้เกิดโอเวอร์เฮดที่สูงมากในการประมวลผล ซึ่งในสภาพความเป็นจริงนั้นการสื่อสารมีหลากหลายสถานการณ์ เช่น รถฉุกเฉินพาคนเจ็บส่งโรงพยาบาลที่ไม่ต้องการความเป็นส่วนตัวเลย หรือรถที่ขับธรรมดาที่ต้องการความเป็นส่วนตัวมาก เป็นต้น โดยในแต่ละสถานการณ์นั้นก็มีความต้องการความเป็นส่วนตัวที่แตกต่างกันไป บางสถานการณ์ต้องการความเป็นส่วนตัวสูง บางสถานการณ์ต้องการความเป็นส่วนตัวต่ำ บางสถานการณ์ไม่ต้องการความเป็นส่วนตัวเลย นั่นคือการป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งอาจจะไม่จำเป็นในบางสถานการณ์ก็ได้ ดังนั้นงานวิจัยเรื่องนี้จึงได้นำเสนอสิ่งที่เรียกว่า การสลับโหมดความเป็นส่วนตัวหรือพริมส์ (Privacy Mode Switching: PriMS) เพื่อปรับเปลี่ยนความต้องการความเป็นส่วนตัวของตำแหน่งที่ตั้งให้เป็นไปตามความเหมาะสมของสถานการณ์การสื่อสารและการเคลื่อนที่ของ

ยานพาหนะ ทั้งนี้เพื่อลดโอเวอร์เฮดในการประมวลผล และเพิ่มประสิทธิภาพในการทำงานให้สูงขึ้น ทั้งยังสามารถป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะได้อย่างเหมาะสมที่สุดอีกด้วย

แนวคิดและกระบวนการวิจัยของงานวิจัยเรื่องนี้ได้กำหนดให้มีระดับความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะเป็น 3 ระดับ ได้แก่ ระดับสูง (High) ระดับกลาง (Medium) และระดับต่ำ (Low) ซึ่งในแต่ละระดับก็จะมีความเหมาะสมกับสถานการณ์การสื่อสารของยานพาหนะที่แตกต่างกันออกไป และได้กำหนดอัลกอริทึม (Algorithm) และวิธีการป้องกันความเป็นส่วนตัวตามระดับความเป็นส่วนตัวทั้ง 3 ระดับนั้นโดยเลือกใช้อัลกอริทึมที่เหมาะสมที่สุดที่ได้จากงานวิจัยก่อนหน้านี้มาประยุกต์ใช้กับระดับความเป็นส่วนตัวทั้ง 3 ระดับ พร้อมทั้งสร้างและนำเสนออัลกอริทึมพริมส์ (PriMS) ที่เป็นการรวมกระบวนการเลือกระดับความเป็นส่วนตัวและกระบวนการเลือกใช้อัลกอริทึมที่เหมาะสมเข้าด้วยกัน โดยจะมีการสลับโหมดความเป็นส่วนตัวไปตามสถานการณ์ที่เหมาะสมของระดับความเป็นส่วนตัวที่กำหนดไว้ ซึ่งอาจเป็นการสลับโหมดแบบปรับด้วยตัวเอง (Manual Mode) และการสลับโหมดแบบอัตโนมัติ (Automatic Mode) ตามพฤติกรรมและช่วงเวลาของการสื่อสารรูปแบบต่างๆ

2. วัตถุประสงค์ของการวิจัย

2.1 เพื่อกำหนดแบบแผน (Scheme) การป้องกันและปิดบังความเป็นส่วนของตำแหน่งที่ตั้งอย่างมีประสิทธิภาพโดยแบ่งตามระดับความเป็นส่วนตัว (Privacy Level) ของเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

2.2 เพื่อนำเสนออัลกอริทึม (Algorithm) การสลับโหมดความเป็นส่วนตัวสำหรับเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

3. ขอบเขตของการวิจัย

3.1 อัลกอริทึมการสลับโหมดความเป็นส่วนตัวนั้นเป็นการใช้หรือนำเอาวิธีการป้องกันความเป็นส่วนตัวแบบต่างๆ ที่ถูกนำเสนอขึ้นก่อนหน้านี้มาประยุกต์ใช้ โดยไม่ได้ต้องการคิดวิธีการป้องกันขึ้นมาใหม่อย่างสิ้นเชิง

3.2 การทดสอบระบบจะกระทำอยู่ภายใต้ตัวจำลองทางเครือข่าย (Network Simulator) ด้วยซอฟต์แวร์ที่ผู้วิจัยได้พัฒนาขึ้น โดยไม่ได้มีการทดสอบกับระบบจริงแต่อย่างใด

3.3 ลักษณะโมเดลถนนที่ใช้จะประกอบไปด้วย 2 แบบ ได้แก่ โมเดลถนนแบบแมนแฮทตัน (Manhattan) และโมเดลถนนแบบทางอิสระ (Freeway)

3.4 รูปแบบของการสื่อสารต่างๆ ของเครือข่ายไร้สายเฉพาะกิจของยานพาหนะในงานวิจัยนี้จะเกิดขึ้นอย่างอิสระโดยมีความน่าจะเป็นในการเกิดอย่างเท่าเทียมกัน เช่น การบอกสถานะ การแจ้งเตือน การเรียกใช้บริการ จะมีโอกาสในการเกิดอย่างเท่าเทียมกันเสมอ เป็นต้น

3.5 สภาวะแวดล้อมของระบบเครือข่ายไร้สายเฉพาะกิจของยานพาหนะของงานวิจัยเรื่องนี้ได้กำหนดให้ไม่มีสภาวะที่ขัดข้องในระบบการสื่อสารใดๆ และไม่มีปัญหาในการค้นหาเส้นทางแต่อย่างใด

3.6 ในการคำนวณประสิทธิภาพการทำงานของของเครือข่ายไร้สายเฉพาะกิจของยานพาหนะในงานวิจัยนี้จะไม่คำนึงถึงกำลัง (Power) และกำหนดให้ค่าทรัพยากร (Resources) อื่นๆ ของระบบมีค่าคงที่

4. ขั้นตอนและวิธีดำเนินการวิจัย

4.1 ศึกษาข้อมูลเอกสารและงานวิจัยที่เกี่ยวข้องกับประเด็นทางด้านความเป็นส่วนตัวในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

4.2 ศึกษาเครื่องมือการจำลองของระบบการสื่อสารในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

4.3 วิเคราะห์ประเด็นทางด้านความเป็นส่วนของตำแหน่งที่ตั้งของเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

4.4 กำหนดและให้นิยามระดับความเป็นส่วนตัวที่ใช้ในการป้องกันและปิดบังความเป็นส่วนของตำแหน่งที่ตั้งสำหรับเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

4.5 กำหนดแบบแผนการป้องกันและปิดบังความเป็นส่วนของตำแหน่งที่ตั้งสำหรับเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

4.6 นำเสนออัลกอริทึมการสลับโหมดความเป็นส่วนตัวสำหรับเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

4.7 จำลองระบบการสื่อสารเพื่อทดสอบผลลัพธ์ตามอัลกอริทึมการสลับโหมดความเป็นส่วนตัวสำหรับเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

4.8 ปรับปรุงและแก้ไขอัลกอริทึมให้สามารถทำงานได้อย่างมีประสิทธิภาพและสอดคล้องกับความเป็นส่วนตัวของตำแหน่งที่ตั้ง

4.9 สรุปผลการวิจัยและตีพิมพ์บทความจากงานวิจัย

4.10 เรียบเรียงและจัดรูปเล่มทำวิทยานิพนธ์

5. ประโยชน์ที่คาดว่าจะได้รับ

5.1 ได้แบบแผนการป้องกันความเป็นส่วนของตำแหน่งที่ตั้งอย่างมีประสิทธิภาพภายใต้การจำแนกระดับความเป็นส่วนตัวที่เหมาะสม สำหรับเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

5.2 ได้อัลกอริทึมพริมส์ ที่เป็นการสลับโหมดความเป็นส่วนตัวสำหรับเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

5.3 ได้เข้าใจถึงกระบวนการสื่อสารในเครือข่ายไร้สารเฉพาะกิจของยานพาหนะอย่างแท้จริงว่ามีความต้องการในระดับความเป็นส่วนตัวมากน้อยเพียงใด และมีความจำเป็นแค่ไหนที่จะต้องป้องกันและปิดบังความเป็นส่วนตัว

6. ผลการตีพิมพ์บทความจากงานวิจัย

ส่วนหนึ่งของวิทยานิพนธ์เรื่องนี้ได้รับการตีพิมพ์ในประชุมวิชาการระดับชาติและระดับนานาชาติตามเอกสารในภาคผนวก โดยมีรายละเอียดดังต่อไปนี้

6.1 บทความเรื่อง “การกำหนดระดับความเป็นส่วนตัวสำหรับการป้องกันและปิดบังตำแหน่งที่ตั้งในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ (Defining Privacy Levels for Location Protection and Anonymization in Vehicular Ad-Hoc Network)” โดย วงศ์ยศ เกิดศรี ขจิตพรรณ กฤตพลวิมาน และ กรกช วิไลลักษณ์ ตีพิมพ์ในรายงานการประชุมวิชาการระดับภูมิภาคเอเชียตะวันออกเฉียงใต้ 2nd ASEAN Undergraduate Conference in Computing (AUC^2 2014) ณ จังหวัดชลบุรี ระหว่างวันที่ 20-21 กุมภาพันธ์ พ.ศ. 2557

6.2 บทความเรื่อง “การรักษาความเป็นส่วนตัวแบบหลายระดับของระบบตรวจสอบตำแหน่งที่ตั้งในวาเน็ต (Multi-Level Privacy-Preserving for Location Monitoring System in VANET)” โดย วงศ์ยศ เกิดศรี ขจิตพรรณ กฤตพลวิมาน และ กรกช วิไลลักษณ์ ตีพิมพ์ในรายงานการประชุมทางวิชาการและนำเสนอผลงานวิจัยระดับชาติครั้งที่ 1 ภายใต้หัวข้อเทคโนโลยีเพื่อการพัฒนาชาติ 1st National Conference on Technology for National Development (TECHCON 2015) ณ วิทยาลัยเทคโนโลยีสยาม กรุงเทพมหานคร ในวันที่ 11 กรกฎาคม พ.ศ. 2558

บทที่ 2
วรรณกรรมที่เกี่ยวข้อง

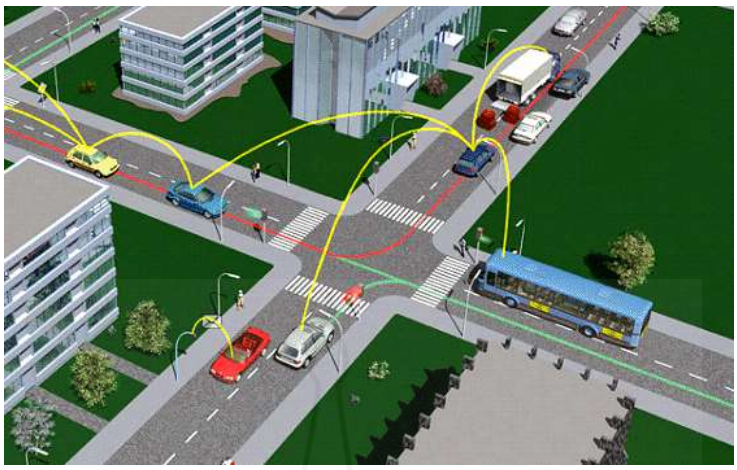
จากเนื้อหาในบทก่อนหน้านี้ได้กล่าวเกริ่นนำถึงที่มาและความสำคัญของงานวิจัยเรื่องนี้ไปแล้ว ต่อไปนี้จะอธิบายในส่วนของทฤษฎีที่เกี่ยวข้องและงานวิจัยที่เกี่ยวข้องกับงานวิจัยเรื่องนี้ ซึ่งประกอบไปด้วยส่วนของระบบขนส่งและจราจรอัจฉริยะ เครือข่ายไร้สายเฉพาะกิจของยานพาหนะ โปรโทคอลในการสื่อสารของยานพาหนะ ระบบตรวจสอบและติดตามตำแหน่งที่ตั้งของยานพาหนะ และบทวิจารณ์งานวิจัยต่างๆ ที่เกี่ยวข้องโดยมีรายละเอียดดังต่อไปนี้

1. ทฤษฎีที่เกี่ยวข้อง

1.1 ระบบขนส่งและจราจรอัจฉริยะ (Intelligent Transport System: ITS)

ระบบขนส่งและจราจรอัจฉริยะ (Ezell, 2010) (Kulachai, 2015) เป็นระบบที่มีการใช้เทคโนโลยีด้านระบบคอมพิวเตอร์และเทคโนโลยีทางการสื่อสารมาใช้กับการจัดการจราจรและการขนส่ง ทั้งนี้เพื่อเป็นการเพิ่มความปลอดภัยในการเดินทาง เพิ่มประสิทธิภาพในการจัดการจราจร และต้องการให้เกิดผลกระทบต่อสิ่งแวดล้อมให้น้อยที่สุด ระบบขนส่งและจราจรอัจฉริยะประกอบไปด้วย 6 ระบบที่สำคัญคือ ระบบการจัดการจราจร ระบบการให้ข้อมูลข่าวสารการเดินทาง ระบบความปลอดภัยในยานพาหนะและการจัดการเหตุฉุกเฉิน ระบบการบริหารจัดการรถสินค้า ระบบการจัดการรถขนส่งสาธารณะ และระบบชำระค่าผ่านทางอัตโนมัติ โดยมีรายละเอียดดังต่อไปนี้

1.1.1 ระบบการจัดการจราจร (Traffic Management System) เกี่ยวข้องกับการควบคุมการจราจรและสัญญาณไฟจราจร โดยการนำเอาเทคโนโลยีชั้นสูงทั้งในด้านฮาร์ดแวร์และซอฟต์แวร์มาใช้ในการควบคุมสัญญาณไฟจราจรให้มีประสิทธิภาพ นอกจากนั้นยังรวมถึงการจัดการกับอุบัติเหตุหรืออุบัติการณ์ต่างๆ โดยการใช้เซ็นเซอร์ และเทคโนโลยีทางการสื่อสารเพื่อตรวจสอบการเกิดอุบัติเหตุ และที่สำคัญอย่างยิ่งคือ ระบบดังกล่าวจะมีการนำเทคโนโลยีด้านการตรวจตรา เช่น การนำเอาอุปกรณ์สำหรับตรวจนับจำนวนยานพาหนะมาใช้ เพื่อให้การคำนวณรอบสัญญาณไฟมีความสอดคล้องกับปริมาณการจราจรในแต่ละทิศทางของทางแยกและตรงกับเวลาจริงมากที่สุด ดังแสดงไว้ในรูปภาพที่ 2.1



ภาพที่ 2.1 การจัดการจราจรในระบบขนส่งและจราจรอัจฉริยะ

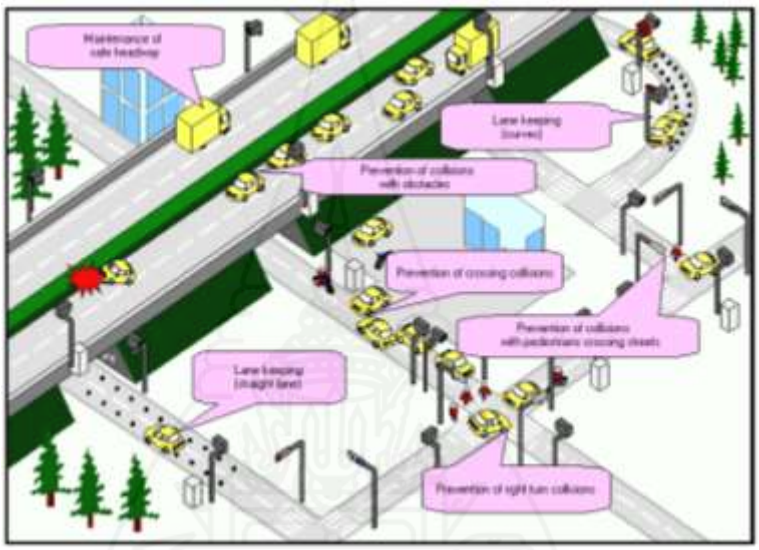
ที่มา: http://www.geoexpertsolutions.com/images/ITS.gif

1.1.2 ระบบสารสนเทศของการเดินทาง (Traveling Information System) ระบบดังกล่าวนี้เป็นการให้ข้อมูลข่าวสารก่อนการเดินทาง ระบบแนะนำเส้นทางติดตั้งในรถยนต์ การให้ข้อมูลข่าวสารขณะเดินทางเกี่ยวกับอุบัติเหตุและอุบัติการณ์ต่างๆ ตลอดจนสภาพถนน สภาพการจราจรและสภาพแวดล้อม โดยใช้เทคโนโลยีด้านวิทยุสื่อสาร ป้ายสลับข้อความ อินเทอร์เน็ต การรายงานข่าวทางโทรทัศน์และการให้ข้อมูลส่วนบุคคล เป็นต้น ดังแสดงในรูปภาพที่ 2.2

ภาพที่ 2.2 การส่งข้อมูลและสารสนเทศในระบบขนส่งและจราจรอัจฉริยะ

ที่มา: http://mubbisherahmed.files.wordpress.com/2011/11/etsi-its.jpg

1.1.3 ระบบความปลอดภัยในยานพาหนะ (Vehicular Safety) เป็นระบบที่ช่วยในการเพิ่มความปลอดภัยในการขับขี่ยานพาหนะบนท้องถนน โดยจะประกอบด้วยเทคโนโลยีในการควบคุมความเร็วอัตโนมัติ การเตือนการชน การหลีกเลี่ยงการชน เครื่องมือป้องกันหรือเตือนกรณีผู้ขับขี่ง่วงนอน ตลอดจนการส่งสัญญาณขอความช่วยเหลือ เป็นต้น ส่วนระบบการจัดการอุบัติเหตุหรือกรณีฉุกเฉินนั้น สามารถดำเนินการได้โดยการใช้เทคโนโลยีการบอกตำแหน่งยานพาหนะอัตโนมัติ ดังแสดงในรูปภาพที่ 2.3

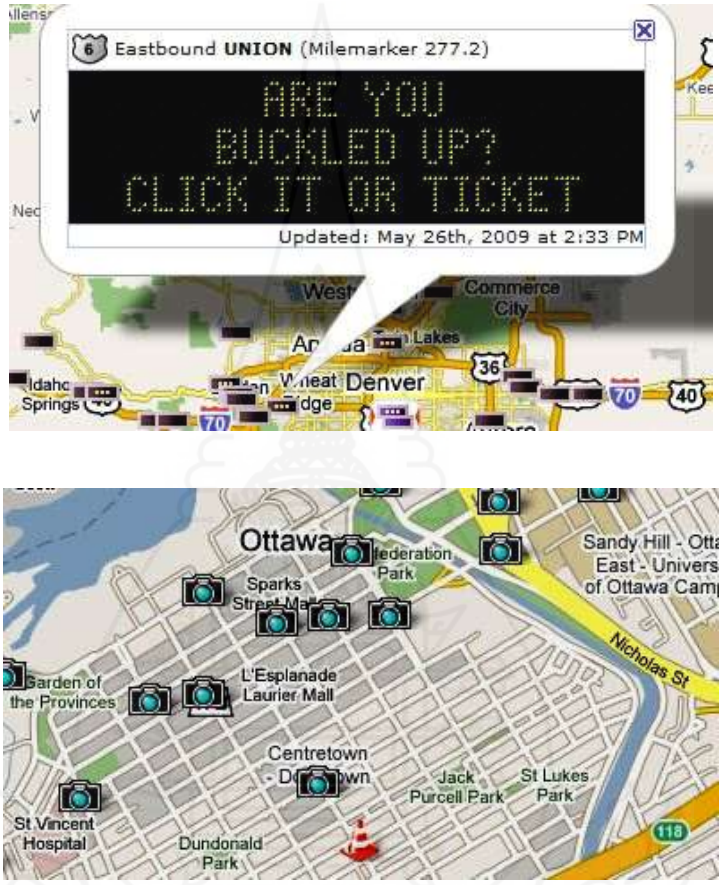


ภาพที่ 2.3 ความปลอดภัยของยานพาหนะในระบบขนส่งและจราจรอัจฉริยะ
ที่มา: http://www.mlit.go.jp/road/ITS/Policy/h12/image2.gif

1.1.4 ระบบการบริหารจัดการรถสินค้า (Cargo Car Management System) เป็นระบบที่มีวัตถุประสงค์หลักในการเพิ่มผลผลิตและเพิ่มความปลอดภัยในด้านอุตสาหกรรมและระบบการขนส่งสินค้า โดยการปรับปรุงการจดทะเบียน การออกใบอนุญาต การจัดเก็บภาษีและขั้นตอนการขนส่งสินค้า โดยมีการใช้เทคโนโลยีในการตรวจปล่อยรถแบบอิเล็กทรอนิกส์ (Electronic Clearance) การจัดการและติดตามรถบรรทุกที่นำส่งสินค้า ตลอดจนการตรวจสอบความปลอดภัยในการจัดสิ่งสินค้าในอุตสาหกรรมต่างๆ ซึ่งระบบดังกล่าวไม่ได้เกี่ยวข้องโดยตรงต่อการแก้ไขปัญหาจราจร แต่เป็นระบบที่ส่งผลดีทางอ้อมต่อการจัดการจราจร

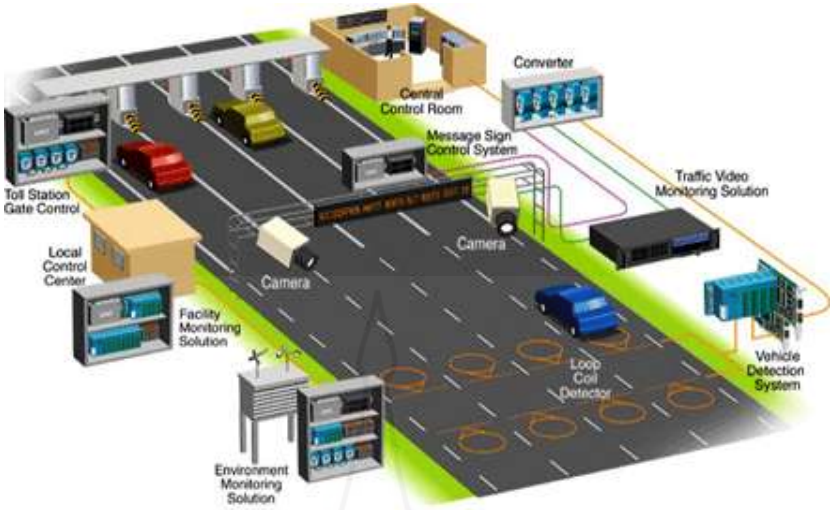
1.1.5 ระบบการจัดการรถขนส่งสาธารณะ (Public Car Management System) เป็นระบบที่ใช้เทคโนโลยีในการบอกตำแหน่งหรือจีพีเอส (GPS) ของยานพาหนะอัตโนมัติ ซึ่งจะเป็น

ประโยชน์ต่อประชาชนผู้ที่ขับขี่ยานพาหนะ และผู้ใช้บริการยานพาหนะได้สามารถทราบถึงเวลาในการรอรถโดยสารสาธารณะ และทราบถึงตำแหน่งของรถโดยสารสาธารณะ ณ เวลาปัจจุบันว่าอยู่ที่บริเวณใดในแผนที่ ทำให้สามารถบริหารจัดการเวลาการเดินทางได้ดียิ่งขึ้น นอกจากนี้ก็ยังมีการให้สิทธิแก่รถโดยสารสาธารณะที่แยกสัญญาณไฟ เป็นต้น ดังแสดงในรูปภาพที่ 2.4



ภาพที่ 2.4 การจัดการรถขนส่งสาธารณะในระบบขนส่งและจราจรอัจฉริยะ
ที่มา: http://googlemapsmania.blogspot.com/2009/05/denver-and-ottawa-traffic-conditions.html

1.1.6 ระบบชำระค่าผ่านทางพิเศษ (Expressway Payment System) เป็นระบบการจ่ายเงินค่าโดยสารแก่รถโดยสารสาธารณะและการเก็บค่าผ่านทางแบบอิเล็กทรอนิกส์ โดยการใช้บัตรสมาร์ตการ์ด (Smart Card) โดยที่ผู้ขับขี่ยานพาหนะไม่ต้องจอดรถเพื่อจ่ายเงินให้กับเจ้าหน้าที่เก็บเงิน แต่จะใช้เทคโนโลยีของอาร์เอฟไอดี (RFID) และเทคโนโลยีเซ็นเซอร์ในการส่งข้อมูลการชำระค่าผ่านทางไปยังระบบการชำระเงิน ดังแสดงในรูปภาพที่ 2.5



ภาพที่ 2.5 การเก็บค่าผ่านทางพิเศษในระบบขนส่งและจราจรอัจฉริยะ

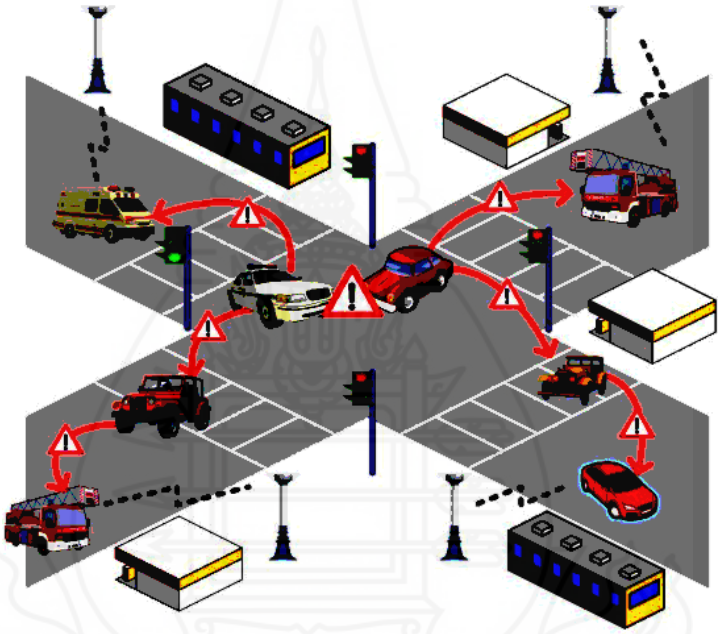
ที่มา: http://www.tech-faq.com/wp-content/uploads/images/Intelligent-Transportation-Systems.gif

1.2 เครือข่ายไร้สายเฉพาะกิจของยานพาหนะ (Vehicular Ad-hoc Network: VANET)

เครือข่ายไร้สายเฉพาะกิจของยานพาหนะหรือวาเน็ต (Vehicular Ad-hoc Network: VANET, 2015) (Data Communication in VANETs, 2015) เป็นงานวิจัยสาขาหนึ่งในอุตสาหกรรมยานยนต์ที่ใช้เทคโนโลยีการสื่อสารไร้สาย และการขับขี่ยานยนต์เข้าด้วยกัน โดยมีวัตถุประสงค์เพื่อช่วยในเรื่องการรักษาความปลอดภัยบนท้องถนน และสามารถติดต่อสื่อสารข้อมูล ข่าวสารการจราจร บนท้องถนน การติดต่อสื่อสารกันได้ระหว่างยานยนต์ ในการขับขี่จะช่วยให้ การเดินทางมีความสะดวกสบาย และ มีความปลอดภัยในชีวิต ทรัพย์สิน มากขึ้น โดยเราสามารถแลกเปลี่ยนข้อมูลข่าวสารต่างๆ ได้ตลอดเวลา โดยการรับส่ง ข้อมูลข่าวสารการจราจร ผ่านทางเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

เครือข่ายไร้สายเฉพาะกิจของยานพาหนะพัฒนามาจากเครือข่ายเคลื่อนที่เฉพาะกิจ โดยมีการติดตั้งอุปกรณ์สื่อสารแบบไร้สายตามเทคโนโลยี IEEE 802.11 ไว้ ภายในรถยนต์ ทำให้รถยนต์สามารถติดต่อสื่อสารกันและแบ่งปันข้อมูลการจราจรระหว่างกันได้ และเนื่องจากรถยนต์เคลื่อนที่ด้วยความเร็วที่สูงจึงส่งผลให้รูปแบบการเชื่อมต่อของรถยนต์ที่อยู่ภายในเครือข่ายเปลี่ยนแปลงอย่างรวดเร็ว ดังนั้นจึงได้ มีการพัฒนาโพรโทคอลค้นหาเส้นทางสำหรับเครือข่ายไร้สายเฉพาะกิจของยานพาหนะขึ้นมาโดยเฉพาะ

โพรโทคอลค้นหาเส้นทางสำหรับเครือข่ายไร้สายเฉพาะกิจของยานพาหนะที่พัฒนาขึ้นในปัจจุบันนั้นจัดอยู่ในกลุ่มของโพรโทคอลที่ทำการค้นหาเส้นทางแบบฐานตำแหน่ง (Position-based Routing Protocols) กล่าวคือ จะอาศัยข้อมูลตำแหน่งซึ่งได้มาจากส่วนให้บริการตำแหน่ง (Location Service) ข้อมูลตำแหน่งดังกล่าวนั้นได้ แก่ ตำแหน่งปัจจุบัน ของโหนดต้นทาง (Source Node) โหนดเพื่อนบ้าน (Neighbor node) และโหนดปลายทาง (Destination Node) เพื่อใช้ในการตัดสินใจเลือกโหนดส่งต่อ (Forwarding node) แพ็กเก็ตข้อมูลไปยังโหนดปลายทางที่ต้องการ โดยภาพรวมของการสื่อสารในเครือข่ายไร้สายของยานพาหนะปรากฏดังในรูปภาพที่ 2.6



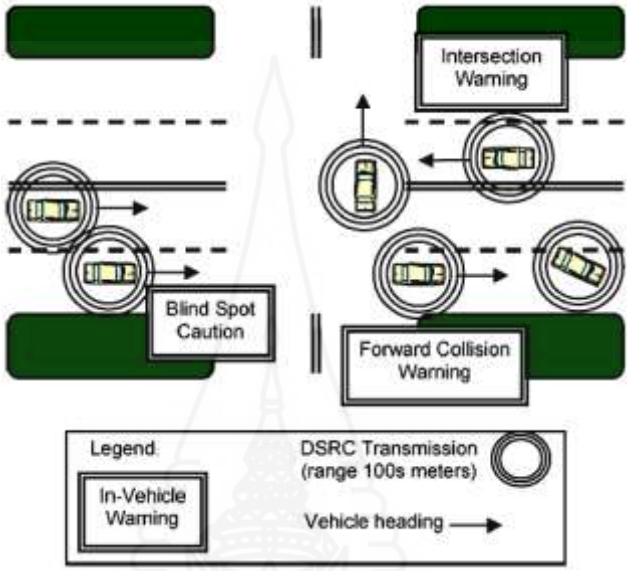
ภาพที่ 2.6 เครือข่ายไร้สายเฉพาะกิจของยานพาหนะ

ที่มา: http://www.ics.uci.edu/~keldefra/figs/vanet.gif

1.3 โปรโทคอลในการสื่อสารของยานพาหนะ (Vehicle Communications)

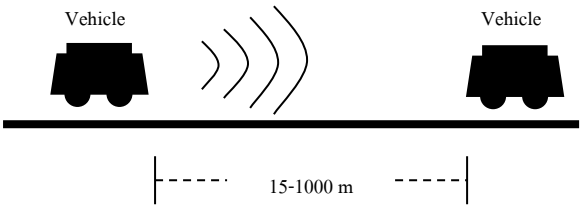
การสื่อสารของยานพาหนะนั้นโดยทั่วไปจะเป็นการสื่อสารในระยะใกล้ๆ ในช่วงเวลาสั้นๆ ซึ่งโปรโทคอลที่นิยมกับแพร่หลายในกระบวนการสื่อสารประเภทนี้ได้แก่ โปรโทคอลดีเอสอาร์ซี (Dedicated Short Range Communications: DSRC) (Kenney, 2011) (DSRC, 2012) (Poochaya, 2010) (Qian, Lu & Moayeri, 2008) เป็นโปรโทคอลที่ใช้ในการสื่อสารระยะสั้นถึงระยะกลางของเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ โดยมีขอบเขตระยะการสื่อสารอยู่ที่ 15-1000

เมตร มีความเร็วในการรับส่งข้อมูลอยู่ที่ 0.5-27 Mbps และมีช่วงความถี่ของสัญญาณอยู่ที่ 12-75 MHz ดังตัวอย่างในรูปภาพที่ 2.8 โดยอยู่ภายใต้มาตรฐานของ IEEE 802.11p หรือ Wireless Access in Vehicular Environments: WAVE

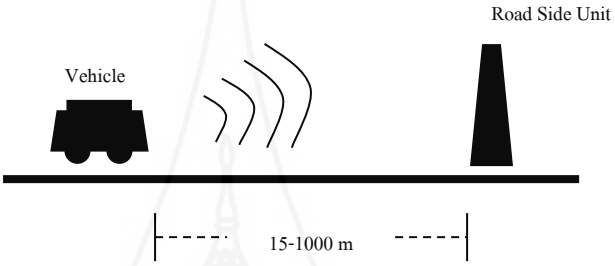


ภาพที่ 2.7 ขอบเขตการสื่อสารของโปรโทคอลดีเอสอาร์ซี (Kenney, 2011)

จากรูปภาพที่ 2.7 ขอบเขตการสื่อสารของโปรโทคอลดีเอสอาร์ซีจะอยู่ในระยะใกล้ถึงระยะกลางทั้งนี้เพื่อเป็นการส่งข้อมูลที่ต้องการความรวดเร็ว เช่น บอกข้อมูลการขับขี่ แจ้งเตือนเมื่อมีการเข้าใกล้วัตถุต่างๆ เป็นต้น โปรโทคอลดีเอสอาร์ซีเป็นมาตรฐานและเทคโนโลยีที่สำคัญในระบบขนส่งและจราจรอัจฉริยะ ซึ่งใช้กับรูปแบบการสื่อสารหลัก 3 รูปแบบได้แก่ การสื่อสารระหว่างยาน พาหนะกับยานพาหนะ (V2V) การสื่อสารระหว่างยานพาหนะกับอุปกรณ์ (V2I) และการสื่อสารระหว่างยานพาหนะกับบริการ (V2S) ดังรูปภาพที่ 2.8 และ รูปภาพที่ 2.9 ทั้งนี้เพื่อต้องการบริหารจัดการระบบขนส่งและจราจรให้มีประสิทธิภาพสูงสุดโดยคำนึงถึงความสะดวกรวดเร็ว การประหยัดเวลา ความปลอดภัย และการใช้พลังงานและเชื้อเพลิงที่คุ้มค่า



ภาพที่ 2.8 การสื่อสารระหว่างยานพาหนะกับยานพาหนะด้วยโปรโทคอลดีเอสอาร์ซี



ภาพที่ 2.9 การสื่อสารระหว่างยานพาหนะกับอุปกรณ์ด้วยโปรโทคอลดีเอสอาร์ซี

มาตรฐานของเทคโนโลยีการสื่อสารระยะใกล้สำหรับระบบขนส่งและจราจรอัจฉริยะสามารถแบ่งออกได้เป็น 3 มาตรฐาน (Kenney, 2011) ซึ่งแยกตามกลุ่มของประเทศที่ใช้งานได้ดังนี้

1) มาตรฐานที่ใช้ในทวีปอเมริกาเหนือ เป็นมาตรฐานเอเอสทีเอ็ม (American Society for Testing and Material: ASTM) ซึ่งอยู่บนช่วงความถี่ 5.9 GHz ภายใต้มาตรฐาน IEEE 802.11p หรือ WAVE ซึ่งเป็นมาตรฐานที่มีวัตถุประสงค์หลักเพื่อต้องการรองรับการติดต่อสื่อสารระหว่างยานพาหนะที่เคลื่อนที่ด้วยความเร็วสูงอย่างมีประสิทธิภาพ โดยมาตรฐานนี้มีการพัฒนาต่อยอดมาจากมาตรฐาน IEEE 802.11a หรือ ASTM E2213-03 โดยมีการใช้ข้อดีของการมอดูเลชัน (Modulation) แบบโอเอฟดีเอ็ม (OFDM) ที่มีความทนทานต่อสภาพการจางหายไปของสัญญาณอันเนื่องมาจากที่สัญญาณมีหลายเส้นทางจึงก่อให้เกิดปัญหาดังกล่าวขึ้น โดยวิธีแบบโอเอฟดีเอ็ม จะเป็นการเพิ่มช่วงเวลาของอักขระขึ้นเป็น 2 เท่าของมาตรฐาน IEEE 802.11a ทำให้ผู้ส่งและผู้รับสามารถติดต่อสื่อสารกันได้ในสภาพช่องสัญญาณที่ผู้ส่งหรือผู้รับมีการเคลื่อนที่ด้วยความเร็วสูงได้ โดยรายละเอียดของข้อมูลพารามิเตอร์ต่างๆ ถูกกำหนดไว้ในตารางที่ 2.1 ชุดพารามิเตอร์สำหรับมาตรฐาน IEEE 802.11p

ตารางที่ 2.1 ชุดพารามิเตอร์สำหรับมาตรฐาน IEEE 802.11p

พารามิเตอร์	ค่ามาตรฐานที่ใช้
Frequency Band	5.9 GHz
Modulation Type	BPSK, QPSK
Data Transmission Rate	3-27 mbps
Number of Data Subcarrier	52
Number of FFT Length	64
Number of Cyclic Prefix	32
OFDM Symbol Duration	8 μs

2) มาตรฐานที่ใช้ในทวีปยุโรป เป็นมาตรฐานในชื่อเซ็นดีเอสอาร์ซี (CEN-DSRC) ซึ่งถูกกำหนดขึ้นมาเพื่อใช้งานในระบบขนส่งและจราจรอัจฉริยะสำหรับกลุ่มประเทศในทวีปยุโรป โดยจะเป็นมาตรฐานที่กำหนดคุณลักษณะของระบบขนส่งและจราจรอัจฉริยะที่ผู้ใช้งานสามารถนำมาตรฐานดังกล่าวไปใช้อ้างอิงในการออกแบบระบบขนส่งและจราจรอัจฉริยะและเทคโนโลยีที่เกี่ยวข้องกับระบบขนส่งและจราจรอัจฉริยะได้ โดยมีชุดพารามิเตอร์ดังแสดงไว้ในตารางที่ 2.2

ตารางที่ 2.2 ชุดพารามิเตอร์สำหรับมาตรฐานเซ็นดีเอสอาร์ซี (CEN-DSRC)

พารามิเตอร์	ค่ามาตรฐานที่ใช้
Frequency Band	5.8 GHz
Communication System	Passive
Maximum Data Transmission Rate	500 kbps (Downlink) 250 kbps (Uplink)
Communication Range	15 m
Maximum Power	RSE:33 dBm OBE:-15 dBm

3) มาตรฐานที่ใช้ในประเทศญี่ปุ่น มาตรฐานของประเทศญี่ปุ่นถูกกำหนดขึ้นมาโดยองค์กรเออาร์ไอบี (Association of Radio Industrial and Business: ARIB) ซึ่งเป็นองค์กรที่มีหน้าที่ในการกำหนดมาตรฐานต่างๆ ในอุตสาหกรรมโทรคมนาคมของประเทศญี่ปุ่น โดยทางเอ

อาร์ไอบี ได้กำหนดมาตรฐาน ARIB STDT55 ขึ้นมาเพื่อเป็นตัวกำหนดคุณลักษณะพื้นฐานของระบบขนส่งและจราจรอัจฉริยะให้มีมาตรฐานที่เด่นชัด และนอกจากนั้นก็ยังได้พัฒนามาตรฐาน ARIB STD-T75 ขึ้นมาเพื่อนำไปใช้เป็นมาตรฐานหลักในการออกแบบระบบขนส่งและจราจรอัจฉริยะ และการพัฒนาเทคโนโลยีต่างๆ ทางด้านการสื่อสารของระบบขนส่งและจราจรอัจฉริยะของประเทศญี่ปุ่น ดังแสดงรายละเอียดข้อมูลค่าพารามิเตอร์มาตรฐานในตารางที่ 2.3

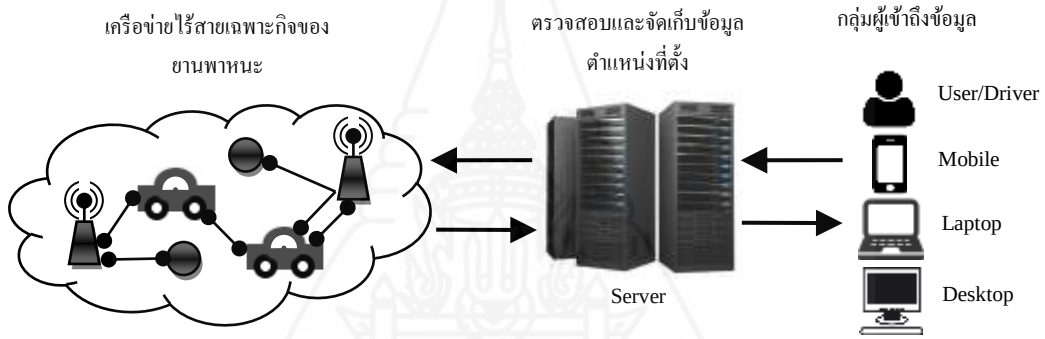
ตารางที่ 2.3 ชุดพารามิเตอร์สำหรับมาตรฐาน ARIB STD-T75

พารามิเตอร์	**ค่ามาตรฐานที่ใช้**
Frequency Band	5.8 GHz
Modulation Type	ASK, QPSK
Data Transmission Rate	1 Mbps for ASK 4 Mbps for QPSK
Communication	TDMA/FDD
Power Supplied to RSU Antenna	10 m to 30 m = 300 mW
Power Supplied to OBU Antenna	Less than 10 mW

จากมาตรฐานเออาร์ไอบีที่ใช้ในประเทศญี่ปุ่นนั้นมีคุณลักษณะที่แตกต่างกับมาตรฐานของกลุ่มประเทศในทวีปยุโรปและทวีปอเมริกาเหนือ โดยจะไม่มีการนำเอาเทคโนโลยีโอเอฟดีเอ็ม (OFDM) เข้ามาใช้งานในระบบ เนื่องจากในประเทศญี่ปุ่นนั้นมีการใช้งานระบบขนส่งและจราจรอัจฉริยะเป็นแบบเฉพาะเจาะจงในระบบใดระบบหนึ่งเท่านั้น นั้นคือระบบการเก็บค่าผ่านทางอัตโนมัติ ซึ่งเป็นระบบที่ไม่ต้องการอัตราเร็วของการส่งข้อมูลมากนัก โดยในการติดต่อสื่อสารระหว่างผู้ส่งที่ติดตั้งอุปกรณ์สื่อสารไว้ภายในยานพาหนะกับผู้รับที่ติดตั้งระบบการรับข้อมูลอยู่ที่อุปกรณ์นั้นกระทำภายใต้ความเร็วต่ำ เพราะยานพาหนะจะมีการหยุดหรือชะลอความเร็วเมื่อผ่านมายังช่องเก็บค่าผ่านทางอัตโนมัติ ด้วยเหตุนี้จึงไม่มีความจำเป็นที่จะต้องนำเทคโนโลยีโอเอฟดีเอ็ม (OFDM) มาใช้งานร่วมกับระบบขนส่งและจราจรอัจฉริยะตามมาตรฐานเออาร์ไอบี

1.4 ระบบตรวจสอบและติดตามตำแหน่งที่ตั้งของยานพาหนะ (Vehicle Location Monitoring and Tracking System)

ระบบตรวจสอบตำแหน่งที่ตั้งของยานพาหนะ (Chow, Mokbel & He, 2011) เป็นระ-บบที่ใช้สำหรับติดตามและจัดเก็บข้อมูลเส้นทางและตำแหน่งที่ตั้งของยานพาหนะในระบบเอาไว้ในฐานข้อมูลกลางเพื่อใช้ในกระบวนการตรวจสอบตำแหน่งที่ตั้งของยานพาหนะเพื่อจะได้ทราบตำแหน่งพิกัดปัจจุบันของยานพาหนะแต่ละคันในแผนที่ทางภูมิศาสตร์ โดยมีกระบวนการทำงานดังรูปภาพที่ 2.10 ซึ่งประกอบไปด้วย 3 ส่วนได้แก่เครือข่ายไร้สายเฉพาะกิจของยานพาหนะ เครื่องมือตรวจสอบและจัดเก็บตำแหน่งที่ตั้งของยานพาหนะ และผู้ใช้งานในระบบ ที่อาจจะเป็นตัวบุคคล หรืออาจจะเป็นเครื่องมือสื่อสารต่างๆ



ภาพที่ 2.10 ระบบตรวจสอบและติดตามตำแหน่งที่ตั้งของยานพาหนะ

ระบบตรวจสอบตำแหน่งที่ตั้งของยานพาหนะจะมีส่วนหนึ่งที่เป็นการติดตามตำแหน่งที่ตั้งของยานพาหนะโดยใช้สัญญาณจีพีเอส (Global Positioning System: GPS) โดยจีพีเอสนั้นเป็นเทคโนโลยีในการบอกตำแหน่งที่ตั้งบนพื้นโลกซึ่งอาศัยหลักการคำนวณสัญญาณความถี่ที่ส่งมาจากดาวเทียมต่างๆ ซึ่งโคจรอยู่รอบโลก ทำให้ทราบถึงตำแหน่งที่ตั้ง ณ จุดใดจุดหนึ่งที่มีการรับสัญญาณได้ โดยทั่วไปจะนำตำแหน่งที่ตั้งจากจีพีเอสนี้ไปแสดงร่วมกับโปรแกรมแสดงแผนที่ทำให้ผู้ใช้งานสามารถติดตามตำแหน่งของยานพาหนะหรืออุปกรณ์ต่างๆ ได้ตลอดเวลา

2. งานวิจัยที่เกี่ยวข้อง

งานวิจัยที่เกี่ยวข้องกับการสื่อสารของยานพาหนะนั้นเกิดขึ้นมาพร้อมกับเทคโนโลยีเครือข่ายไร้สาย (Wireless Network) (Lee, 2009) (Kim, 2009) ซึ่งเกิดเป็นแนวคิดของระบบขนส่งและจราจรอัจฉริยะ (Intelligent Transport System: ITS) และพัฒนาต่อเนื่องมาจนถึงปัจจุบันและอนาคตกลายเป็น ระบบขนส่งและจราจรอัจฉริยะแบบทั่วทุกหนทุกแห่ง (Ubiquitous Intelligent Transport System: u-ITS) ซึ่งเป็นกระบวนการติดต่อสื่อสารของยานพาหนะกับอุปกรณ์สื่อสารทุกรูปแบบ โดยในช่วงเวลาดังกล่าวได้มีนิยามศัพท์คำหนึ่งเกิดขึ้นมานั่นคือ ยานพาหนะพูดได้ (Car Talk) ซึ่งความจริงแล้วกระบวนการของยานพาหนะพูดได้นั้นเป็นส่วนหนึ่งของระบบขนส่งและจราจรอัจฉริยะที่ต้องการทำให้ยานพาหนะสามารถติดต่อสื่อสารหรือส่งข้อมูลไปยังยานพาหนะคันอื่นๆ ได้ หรือสามารถติดต่อสื่อสารกับอุปกรณ์ได้ ซึ่งได้มีโครงการที่เกี่ยวข้องกับรถพูดได้นี้เกิดขึ้นทั่วทุกภูมิภาคของโลก โดยแบ่งออกเป็น 4 โครงการที่สำคัญดังต่อไปนี้

โครงการอินเทลลิไดรว์ (IntelliDrive) (Smith, Venkatanarayana, Park, Goodall, Datesh & Skerrit, 2010) (InteliliDrive, 2012) เป็นโครงการพัฒนาระบบขนส่งและจราจรอัจฉริยะของประเทศสหรัฐอเมริกา โดยได้มีการกำหนดอัลกอริทึมที่ใช้ในการควบคุมสัญญาณการสื่อสารของยานพาหนะบนท้องถนนให้สามารถสื่อสารกันได้อย่างถูกต้อง และมีความปลอดภัยทั้งข้อมูลในการสื่อสารและผู้ขับขี่ โดยโครงการนี้มีผู้สนับสนุนคือ U.S. Department of Transportation (USDOT) ซึ่งใช้งบประมาณ 2.6 ล้านเหรียญสหรัฐฯ และใช้เวลาในการดำเนินงานประมาณ 3 ปีคือ ช่วงปี ค.ศ. 2009-2011

โครงการซีวีไอเอส (CVIS: Cooperative Vehicle-Infrastructure Systems) (Kompfner, 2009) (CVIS, 2012) เป็นโครงการใหญ่โครงการหนึ่งของทวีปยุโรป โดยเป็นการร่วมมือของกลุ่มประเทศในยุโรป เพื่อพัฒนาอุปกรณ์ต้นแบบของระบบขนส่งและจราจรอัจฉริยะที่ใช้ในการติดต่อสื่อสารของยานพาหนะบนท้องถนน โดยโครงการดังกล่าวมีกลุ่มผู้ร่วมพัฒนาทั้งหมด 61 กลุ่มที่ประกอบไปด้วยองค์กรทางการศึกษา และองค์กรทางภาคอุตสาหกรรมซึ่งกระจายตัวกันไปทั่วทั้งทวีปยุโรป โดยได้รับเงินสนับสนุนโครงการจากสหพันยุโรป (European Commission: EU) เป็นจำนวนเงิน 22 ล้านเหรียญยูโร แต่งบประมาณจริงที่เกิดขึ้นคือ 41 ล้านเหรียญยูโร โครงการเริ่มในปี ค.ศ. 2006 และสิ้นสุดในต้นปี ค.ศ. 2010

โครงการสมาร์ทเวย์ (Smartway) (Smartway Team, 2007) เป็นโครงการพัฒนาระบบขนส่งและจราจรอัจฉริยะของประเทศญี่ปุ่น ซึ่งเน้นการสื่อสารของยานพาหนะบนทางด่วนหรือถนนที่ต้องใช้ความเร็วสูง ทั้งนี้เพื่อลดอุบัติเหตุที่จะเกิดขึ้น และเพื่อให้การขับขี่ยานพาหนะมีความ

เป็นระเบียบเรียบร้อยมากยิ่งขึ้น โดยโครงการนี้มีผู้สนับสนุนคือ National Institute for Land and Infrastructure Management ซึ่งใช้เวลาในการดำเนินงานประมาณ 2 ปีคือ ช่วงปี ค.ศ. 2006-2007

โครงการคาร์ทอล์ค (CarTalk) (Prathombutr, 2010) เป็นโครงการพัฒนาระบบขนส่งและจราจรอัจฉริยะของประเทศไทย ซึ่งเป็นการสร้างอุปกรณ์ต้นแบบในการสื่อสารของยานพาหนะกับยานพาหนะ โดยเน้นถึงระบบความปลอดภัยบนท้องถนนเป็นหลัก โดยโครงการนี้มีผู้สนับสนุนคือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center: NECTEC) และมีผู้ร่วมโครงการเป็นสถาบันการศึกษา 3 แห่งได้แก่ สถาบันเทคโนโลยีแห่งเอเชีย (AIT) มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ และมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี ซึ่งใช้งบประมาณ 9 ล้านบาท และใช้เวลาในการดำเนินงานประมาณ 2 ปีในช่วงที่ 1 คือปี ค.ศ. 2009-2010 และมีโครงการในการพัฒนาในช่วงที่ 2 ต่อไปในอนาคต

จากโครงการทั้ง 4 โครงการที่ได้กล่าวมานี้ล้วนแล้วแต่สนับสนุนในกระบวนการของยานพาหนะพูดได้หรือกระบวนการสื่อสารของยานพาหนะทั้งสิ้น ซึ่งจะเห็นได้ว่ากระบวนการดังกล่าวกำลังถูกพัฒนาไปสู่มาตรฐานและการใช้งานจริงในอนาคต ดังนั้นจึงจำเป็นต้องคำนึงถึงประเด็นต่างๆ ที่เกี่ยวข้องในการสื่อสารเหล่านั้น เช่น ความเป็นส่วนตัวในการสื่อสาร ความมั่นคงในการสื่อสาร และ การสื่อสารเพื่อความปลอดภัยทางถนน เป็นต้น ซึ่งงานวิจัยเรื่องนี้ได้เจาะลงไปในประเด็นเรื่องความเป็นส่วนตัวของตำแหน่งที่ตั้ง (Location Privacy) ของยานพาหนะโดยมีรายละเอียดของงานวิจัยที่เกี่ยวข้องดังต่อไปนี้

งานวิจัยในประเด็นเรื่องความเป็นส่วนตัวของตำแหน่งที่ตั้ง (Location Privacy) บนเครือข่ายไร้สายเฉพาะกิจของยานพาหนะนั้นได้ถูกวิจัยเพิ่มมากขึ้นเรื่อยๆ ในปัจจุบัน เพราะเนื่องจากประเด็นดังกล่าวเป็นประเด็นวิจัยที่ใหม่และสามารถนำเอาแนวคิดและทฤษฎีต่างๆ เข้าไปประยุกต์ใช้ได้อย่างหลากหลาย โดยกระบวนการสื่อสารของยานพาหนะ เป็นกระบวนการสื่อสารแบบเฉพาะกิจรูปแบบหนึ่งที่จะต้องมีโปรโทคอลคอยสนับสนุนในการสื่อสารข้อมูล ได้แก่ โปรโทคอลดีเอสอาร์ซี (Kenney, 2011) ซึ่งกระบวนการทำงานของโปรโทคอลดังกล่าวจำเป็นต้องคำนึงถึงความมั่นคง (Security) ความเป็นส่วนตัว (Privacy) และความปลอดภัย (Safety) ในการสื่อสารอยู่เสมอ

ความเป็นส่วนตัวของตำแหน่งที่ตั้งเป็นประเด็นหนึ่งที่เกิดขึ้น ณ ขณะที่ยานพาหนะมีการขับเคลื่อนไปยังพื้นที่ต่างๆ โดยทั่วไปแล้วยานพาหนะจะใช้หลักการบรอดคาสท์ท์ (Broadcast) ในการติดต่อสื่อสารทั้งการรับและการส่งข้อมูล ซึ่งกระบวนการดังกล่าวอาจสามารถถูกติดตามข้อมูล และถูกติดตามเส้นทางของยานพาหนะ (Vehicle Tracking) ได้ ดังนั้นจึงมีนักวิจัยมากมาย

(Freudiger et al., 2007) (Sampigethaya et al., 2007) (Wasef et al., 2010) (Song et al., 2010) ได้นำเสนอกระบวนการป้องกันความเป็นส่วนตัวในตำแหน่งที่ตั้งขึ้น เพื่อไม่ให้สามารถติดตามเส้นทางของยานพาหนะได้อย่างเป็นสาธารณะ โดยหลักการปิดบังชื่ออย่างง่ายได้ถูกนำเสนอขึ้นในช่วง 10 ปีที่ผ่านมาซึ่งได้แก่ การใช้ชื่อเทียม (Pseudonym) และชื่อปลอม (Anonym) (Calandriello et al., 2007) (Gerlach et al., 2007) ในการปิดบังข้อมูลของยานพาหนะ

Calandriello et al. (2007) ได้แสดงให้เห็นถึงประสิทธิภาพของการใช้ชื่อเทียมและชื่อปลอมว่ามีความแตกต่างกันอย่างไรบ้าง โดยพบว่ากระบวนการประมวลผลของชื่อเทียมมีอัลกอริทึมที่ไม่ซับซ้อน แต่จะไม่แข็งแรงในการป้องกันความเป็นส่วนตัวของข้อมูล ในขณะที่กระบวนการประมวลผลของชื่อปลอมมีอัลกอริทึมที่ซับซ้อน แต่ก็มีความแข็งแรงต่อการป้องกันความเป็นส่วนของข้อมูล ดังนั้นจึงจำเป็นต้องเลือกและพิจารณาว่าการปิดบังชื่อแบบใดที่เหมาะสมในการสื่อสาร ซึ่งจะขึ้นอยู่กับข้อมูลและสถานการณ์การสื่อสาร ณ ขณะนั้น โดยที่ชื่อเทียมและชื่อปลอมจะถูกกำหนดให้กับยานพาหนะแต่ละคันแบบถาวรซึ่งอาจสามารถค้นหาและคาดเดาชื่อจริงของยานพาหนะได้ จึงทำให้ Gerlach et al. (2007) ได้เสนอให้มีกระบวนการเปลี่ยนชื่อเทียมและชื่อปลอมของยานพาหนะขึ้น ซึ่งกระบวนการเปลี่ยนชื่อนี้จะกระทำก็ต่อเมื่อมีการเปลี่ยนสถานการณ์ในการสื่อสารใหม่ และกระบวนการเปลี่ยนชื่อปลอมและชื่อเทียมนี้ได้ถูกสนับสนุนโดยงานวิจัยของ Hoh et al. (2007) และ Hoh et al. (2008) ที่ทำการเปลี่ยนเวลาและตำแหน่งที่ตั้งของข้อมูลที่ได้จากการตรวจจับจาก GPS เพื่อไม่ให้รู้ถึงระยะเวลาจริงและเส้นทางจริงในการขับขี่ของยานพาหนะ โดยจะแสดงข้อมูลอยู่ในรูปของเส้นการเดินทางเสมือน (Virtual Trip Lines) ซึ่งหลักการดังกล่าวนี้ก็สอดคล้องกับงานวิจัยของ Li et al. (2006) และ Chaurasia et al. (2008) ที่ได้ทำการปรับเปลี่ยนข้อมูลของยานพาหนะไม่ว่าจะเป็นข้อมูลของตัวยานพาหนะเองหรือข้อมูลของผู้ขับขี่ไปตามความจำเป็นในการสื่อสาร ณ ช่วงเวลาหนึ่งๆ โดยที่ตัวผู้ขับขี่เป็นผู้พิจารณาในการปรับเปลี่ยนระดับข้อมูลเหล่านั้น ทั้งนี้ก็เพื่อเป็นการป้องกันความเป็นส่วนตัวในตำแหน่งที่ตั้งของยานพาหนะและของผู้ขับขี่นั่นเอง

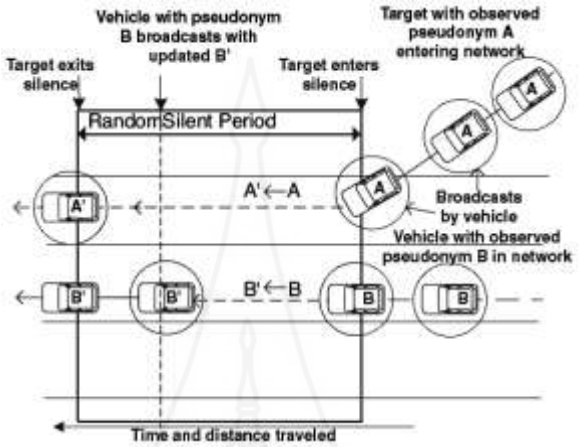
การทำให้กระบวนการติดตามเส้นทางของยานพาหนะมีการติดตามที่ยากขึ้นนั้นก็จะต้องมีกระบวนทางด้านการเข้ารหัสลับ (Cryptography) มาประมวลผลร่วมกับกระบวนการสื่อสาร ซึ่ง Burmester et al. (2008) ได้ยกตัวอย่างถึงกระบวนการปิดบังข้อมูล กระบวนการเข้ารหัสข้อมูล และกระบวนการปลอมแปลงข้อมูล ซึ่งกระบวนการเหล่านี้ช่วยทำให้การสื่อสารข้อมูลไม่มีความต่อเนื่อง ทำให้ไม่สามารถเชื่อมโยงข้อมูลของเส้นทางการสื่อสารของยานพาหนะแต่ละคันได้ ซึ่ง Yang et al. (2010) ได้นำเสนอการค้นหาเส้นทาง (Routing) ของยานพาหนะโดยใช้โปรโทคอล Dummy-based Location Privacy Protection (DBLPP) Routing Protocol ซึ่งจะเป็นโปรโทคอลที่

ค้นหาเส้นทางที่ไม่มีอยู่จริงหรือเส้นทางปลอม โดยที่มีการปิดบังเส้นทางจริงของการสื่อสารเอาไว้ ซึ่งทำให้ไม่สามารถทราบและเชื่อมโยงถึงข้อมูลตำแหน่งที่ตั้งจริงของยานพาหนะได้ ซึ่งหลักการดังกล่าวสอดคล้องกับงานของ Lu et al. (2010) ที่นำเสนอการส่งแพ็คเก็ตข้อมูลการสื่อสารของยานพาหนะโดยใช้เทคนิค “Sacrificing the Plum Tree for the Peach Tree” ซึ่งมีการปิดบังเส้นทางจริงของยานพาหนะ ณ ขณะที่มีการค้นหาเส้นทาง นอกเหนือจากนี้ Scheuer et al. (2010) ก็ได้นำเสนอหลักการที่คล้ายๆ กันในการค้นหาเส้นทางโดยใช้เทคนิค Chaum’s mixes ซึ่งเป็นการเพิ่มและปรับปรุงกระบวนการสื่อสารในเครือข่ายเฉพาะกิจของยานพาหนะให้มีความมั่นคงและปลอดภัยมากยิ่งขึ้น

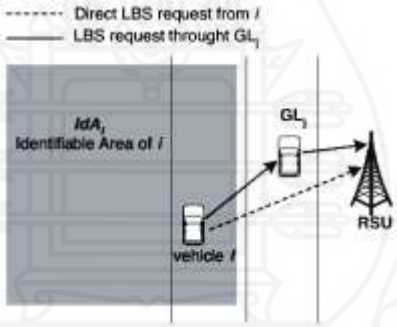
งานวิจัยในช่วง 3 ปีที่ผ่านมาเริ่มมีการประยุกต์ใช้แนวคิดทางด้านความเป็นส่วนตัวของตำแหน่งที่ตั้งบนยานพาหนะมากยิ่งขึ้นซึ่งงานวิจัยส่วนใหญ่จะนำเสนออยู่ในรูปแบบของโปรโทคอลหรืออัลกอริทึมที่ใช้สำหรับปิดบังข้อมูล และค้นหาข้อมูลของยานพาหนะ เช่น Gosman et al. (2010) นำเสนอโปรโทคอลที่สามารถป้องกันและต่อต้านการถูกโจมตีในการสื่อสารข้อมูล Weerasinghe et al. (2010) และ Weerasinghe et al. (2011) นำเสนอโปรโทคอล Anonymous Online Service Access (AOSA) ที่สามารถซ่อนการเชื่อมโยงการสื่อสารของยานพาหนะได้ ทำให้ไม่สามารถรู้ถึงเส้นทางหรือกระบวนการสื่อสารของยานพาหนะคันใดคันหนึ่งได้ทั้งหมด Haas et al. (2011) นำเสนออัลกอริทึมในการทำให้ความเป็นส่วนตัวของยานพาหนะถูกสูญเสียไปให้น้อยที่สุด Ren et al. (2011) นำเสนอวิธีการประเมินความเสี่ยงในประเด็นด้านความเป็นส่วนของตำแหน่งที่ตั้งของยานพาหนะ Alganas et al. (2011) นำเสนอหลักการที่คล้ายกับ Ren et al. (2011) นั่นคือการประเมินสภาพแวดล้อมการสื่อสารของยานพาหนะว่ามีโอกาสที่จะเปิดเผยตำแหน่งที่ตั้งได้มากน้อยเพียงใด และ Lu et al. (2011) นำเสนอผลการวิเคราะห์ถึงความเป็นชื่อนิรนามของยานพาหนะในประเด็นตำแหน่งที่ตั้งว่ามีได้มากน้อยเพียงใด เป็นต้น และนอกเหนือจากนั้นก็ยังมีการนำเสนอกระบวนการป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะที่มีความฉลาดยิ่งขึ้น เช่นมีการรับรู้ถึงเหตุการณ์หรือข้อมูลที่เกิดขึ้นเพื่อใช้สำหรับกระบวนการป้องกันความเป็นส่วนตัว เช่น งานวิจัยของ Ashok et al. (2010) และ Abumansoor et al. (2011) เป็นต้น

จากการศึกษางานวิจัยทั้งหมดตามที่ได้กล่าวมานั้น มีงานวิจัยที่เป็นประเด็นหลักของความเป็นส่วนตัวในตำแหน่งที่ตั้งอยู่ 4 งานวิจัย ได้แก่ งานวิจัยของ Sampigethaya et al. (2007) ที่นำเสนออัลกอริทึม AMOEBA ซึ่งกำหนดให้ยานพาหนะแต่ละคันมีช่วงเวลาของการปล่อยสัญญาณที่แตกต่างกันตามช่วงเวลาที่กำหนด และมีช่วงเวลาเงียบ (Silent Period) โดยจะไม่มีการปล่อยสัญญาณใดๆ เลย ดังนั้นการติดตามตำแหน่งของยานพาหนะก็จะทำได้ยากยิ่งขึ้นดังแสดงรายละเอียดการทำงานในรูปภาพที่ 2.11 นอกจากนี้ในการสื่อสารกับบริการต่างๆ หรืออุปกรณ์ต่างๆ

ข้างถนนนั้นจะไม่ได้มีการสื่อสารกันระหว่างยานพาหนะกับอุปกรณ์เหล่านั้นแต่จะมีการส่งผ่านทางตัวแทนหรือหัวหน้ากลุ่มของเขตพื้นที่ที่ยานพาหนะกำลังเคลื่อนที่อยู่ ณ ปัจจุบันดังแสดงในรูปภาพที่ 2.12 ทั้งนี้ก็เพื่อปิดบังไม่ให้อุปกรณ์รับรู้ข้อมูลจริงของยานพาหนะแต่ละคัน



ภาพที่ 2.11 การปล่อยสัญญาณร่วมกับการหยุดปล่อยสัญญาณของยานพาหนะ

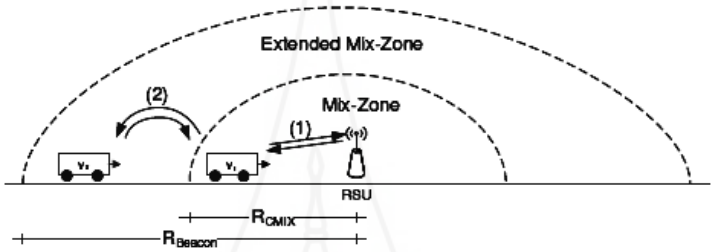


ภาพที่ 2.12 การสื่อสารระหว่างตัวแทนกลุ่มของยานพาหนะกับอุปกรณ์

จากรูปภาพที่ 2.11 แสดงให้เห็นว่ายานพาหนะ A และ B มีช่วงของการปล่อยสัญญาณและช่วงของการเงียบหรือการหยุดปล่อยสัญญาณที่แตกต่างกันทั้งนี้เพื่อทำให้ขาดความต่อเนื่องในการติดตามเส้นทางและตำแหน่งที่ตั้งของยานพาหนะนั่นเอง และจากรูปภาพที่ 2.12 แสดงให้เห็นว่ายานพาหนะที่เป็นตัวแทนของกลุ่มเท่านั้นที่สามารถติดต่อกับอุปกรณ์ได้โดยตรง แต่อย่างไรก็ตามวิธี AMOEBA ดังกล่าวมีข้อเสียคือเมื่อช่วงเวลาเงียบยาวนานจนเกินไปก็จะทำให้ไม่สามารถติดตามตำแหน่งของยานพาหนะได้เลย เพราะข้อมูลของการปล่อยสัญญาณจะเกิดการขาดตอนมาก

จนเกินไปจนเกิดความไม่ต่อเนื่อง และการไว้ใจหัวหน้ากลุ่มมากจนเกินไปอาจจะก่อให้เกิดความเสี่ยงในการสื่อสารได้ด้วยเช่นเดียวกัน

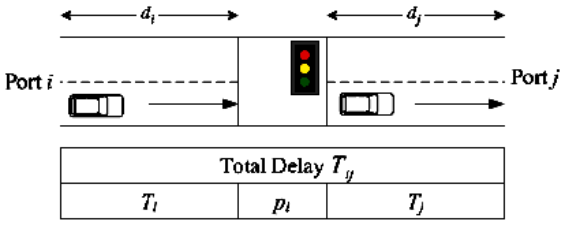
Freudiger et al. (2007) จึงได้นำเสนอหลักการเปลี่ยนตำแหน่งที่ตั้งโดยใช้วิธีการแบบ Mix-Zone ซึ่งจะมีกระบวนการเปลี่ยนกุญแจที่ใช้ในการเข้ารหัสข้อมูลตามตำแหน่งที่ตั้งของยานพาหนะไปเรื่อยๆ ตามเขตพื้นที่ที่ยานพาหนะนั้นเคลื่อนที่ไปถึง ดังแสดงรายละเอียดในรูปภาพที่ 2.13



ภาพที่ 2.13 การกำหนดโซนและการส่งต่อข้อมูลไปยังต่างโซน

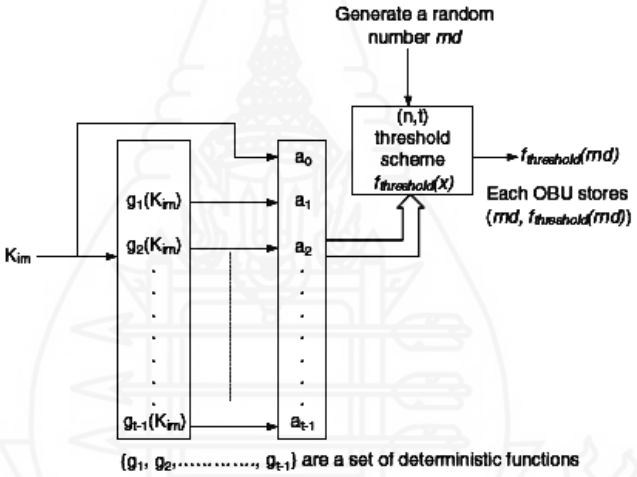
จากรูปภาพที่ 2.13 มีการกำหนด Mix-Zone โดยที่การสื่อสารระหว่างยานพาหนะกับอุปกรณ์จะใช้กุญแจการเข้ารหัส V_1 และ เมื่อยานพาหนะเคลื่อนที่ออกไปยังนอก Mix-Zone ก็จะทำการส่งต่อกุญแจการเข้ารหัส V_1 นี้ไปยังส่วนที่เป็น Extended Mix-Zone ซึ่งใช้กุญแจการเข้ารหัส V_2 ซึ่งภายในขอบเขตพื้นที่ของเสากระจายสัญญาณหนึ่งๆ นั้นอาจจะมี Mix-Zone หลายๆ Mix-Zone อยู่ภายใน แต่อย่างไรก็ตามหลักการดังกล่าวยังมีความปลอดภัยไม่เพียงพอ และยังเป็นการเพิ่มการประมวลผลให้กับหน่วยประมวลผลกลางของยานพาหนะและของเสาข้างถนนมากยิ่งขึ้น และกระบวนการดังกล่าวก็ยังต้องมีการบรอดคาสท์อยู่ตลอดเวลาดังเช่นการสื่อสารในระยะเริ่มต้น

หลังจากนั้น Song et al. (2010) ได้นำเสนออัลกอริทึม Density-based Location Privacy (DLP) ซึ่งเป็นการกำหนดเวลาในการเปลี่ยนชื่อปลอมหรือเปลี่ยนข้อมูลของยานพาหนะ พร้อมทั้งการปรับปรุงโหนดของยานพาหนะเพื่อนบ้านให้มีขอบเขตในการรับข้อมูลตำแหน่งที่ตั้งของยานพาหนะแต่ละคันที่จำกัดดังแสดงรายละเอียดในรูปภาพที่ 2.14 งานวิจัยดังกล่าวมีลักษณะคล้ายกับงานวิจัยของ Freudiger et al. (2007) ที่ยังต้องใช้หลักการบรอดคาสท์อยู่ตลอดเวลา เพียงแต่มีการกำหนดระยะเวลาเพิ่มเติมเข้ามาในการที่จะตัดสินใจว่าเมื่อใดที่ยานพาหนะจะต้องเปลี่ยนชื่อปลอม ซึ่งจะกำหนดให้เป็น Density Zone



ภาพที่ 2.14 การกำหนดเวลาหน่วงในการเปลี่ยนข้อมูลของยานพาหนะ

หลังจากนั้น Wasef et al. (2010) จึงได้นำเสนออัลกอริทึม REP ซึ่งมีแนวคิดในการปรับปรุงระยะเวลาในการเงียบและระยะเวลาในการส่งข้อมูลโดยใช้หลักของการสุ่มช่วงเวลาหรือคาบในการเข้ารหัสข้อมูล (Random Signal Encryption) หลักการทำงานปรากฏดังในรูปภาพที่ 2.15



ภาพที่ 2.15 การกำหนดตัวเลขสุ่มที่ใช้ในการเข้ารหัสและปล่อยสัญญาณ

จากรูปภาพที่ 2.15 เป็นการกำหนดกุญแจที่เป็นตัวเลขสุ่มที่ใช้สำหรับการเข้ารหัสข้อมูลและใช้ในการปล่อยสัญญาณตามคาบที่ถูกระบุโดยตัวเลขสุ่มนั้น ซึ่งวิธีการดังกล่าวจะทำให้สามารถติดตามข้อมูลของยานพาหนะได้ยากขึ้น แต่ในขณะเดียวกันก็ยังสามารถติดตามเส้นทางของยานพาหนะได้ตามรูปแบบการเงียบที่แตกต่างกันของยานพาหนะแต่ละคันได้ดังเดิม แต่ข้อเสียของวิธีการทำงานดังกล่าวก็คือ เมื่อมีการส่งข้อมูลในแต่ละช่วงเวลาจะต้องมีการสุ่มเพื่อเข้ารหัสข้อมูลอยู่ตลอดเวลาซึ่งจะทำให้เกิดโอเวอร์เฮด (Overhead) สูงในการประมวลผล

จากงานวิจัยที่ได้กล่าวไปทั้งหมดนั้น มีการคำนึงถึงปัจจัยทางด้านความเป็นส่วนตัว (Privacy) เพียงอย่างเดียวเท่านั้น ซึ่งต้องการจะหาวิธีการทุกวิถีทางเพื่อที่จะป้องกันความเป็น

ส่วนตัวให้ได้มากที่สุดเท่าที่จะทำได้ ทำให้เกิดโอเวอร์เฮดที่สูงมากในการประมวลผล ซึ่งในสภาพความเป็นจริงนั้นการสื่อสารมีหลากหลายสถานการณ์ เช่น รถฉุกเฉินพาคนเจ็บส่งโรงพยาบาลที่ไม่ต้องการความเป็นส่วนตัวเลย หรือรถธรรมดาที่ต้องการความเป็นส่วนตัวมาก เป็นต้น โดยในแต่ละสถานการณ์นั้นก็มีความต้องการความเป็นส่วนตัวที่แตกต่างกันไป บางสถานการณ์ต้องการความเป็นส่วนตัวสูง บางสถานการณ์ต้องการความเป็นส่วนตัวต่ำ บางสถานการณ์ไม่ต้องการความเป็นส่วนตัวเลย นั่นคือการป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งอาจจะไม่จำเป็นในทุกสถานการณ์ก็ได้ ดังนั้นงานวิจัยเรื่องนี้จึงได้นำเสนอสิ่งที่เรียกว่า การสลับโหมดความเป็นส่วนตัว (Privacy Mode Switching: PriMS) (Keardsri, Kritpolviman, & Wilailux, 2014) (Keardsri, Kritpolviman, & Wilailux, 2015) เพื่อปรับเปลี่ยนความต้องการความเป็นส่วนตัวของตำแหน่งที่ตั้งให้เป็นไปตามความเหมาะสมของสถานการณ์การสื่อสารและการเคลื่อนที่ของยานพาหนะ ทั้งนี้เพื่อลดโอเวอร์เฮดในการประมวลผล และเพิ่มประสิทธิภาพในการทำงานให้สูงขึ้น ทั้งยังสามารถป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะได้อย่างเหมาะสมที่สุดอีกด้วย

บทที่ 3
วิธีดำเนินการวิจัย

จากทฤษฎีและงานวิจัยที่เกี่ยวข้องที่ได้กล่าวไปแล้วในบทก่อนหน้านี้ ต่อไปจะนำเสนอรายละเอียดของแนวคิดการทำงานของระบบ และวิธีการดำเนินการวิจัยที่ได้ออกแบบและพัฒนาขึ้นสำหรับงานวิจัยเรื่องนี้ โดยประกอบไปด้วยแนวคิดของงานวิจัย ประชากรและกลุ่มตัวอย่าง ระดับความเป็นส่วนตัว ปัจจัยสำหรับกำหนดระดับความเป็นส่วนตัว อัลกอริทึมในการป้องกันและปิดบังความเป็นส่วนตัว รูปแบบการสื่อสารของยานพาหนะ การป้องกันความเป็นส่วนตัวภายใต้ระดับความเป็นส่วนตัว โดยมีรายละเอียดดังต่อไปนี้

1. แนวคิดของงานวิจัย

จากงานวิจัยทั้งหมดที่กล่าวไว้ในบทที่ 2 พบว่า อัลกอริทึมต่างๆ ที่นำเสนอขึ้นในช่วงที่ผ่านมา มีแนวคิดการป้องกันและปิดบังความเป็นส่วนตัวโดยมุ่งเน้นไปในเรื่องของการรักษาความเป็นส่วนตัวให้ได้มากที่สุดเพียงอย่างเดียว จึงทำให้ขั้นตอนการปิดบังข้อมูลและตำแหน่งที่ตั้งของยานพาหนะมีความซับซ้อนมากยิ่งขึ้น เกิดค่าโอเวอร์เฮดในการประมวลผลที่สูงมาก ซึ่งเมื่อพิจารณาถึงสภาพความเป็นจริงในการสื่อสารของยานพาหนะพบว่า มีหลากหลายรูปแบบและสถานการณ์ที่แตกต่างกัน โดยในแต่ละสถานการณ์นั้นก็มีความต้องการความเป็นส่วนตัวที่แตกต่างกันด้วย บางสถานการณ์ต้องการความเป็นส่วนตัวสูง บางสถานการณ์ต้องการความเป็นส่วนตัวต่ำ บางสถานการณ์ไม่ต้องการความเป็นส่วนตัวเลย ดังนั้นงานวิจัยนี้จึงได้กำหนดให้มีระดับความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะเป็น 3 ระดับ ได้แก่ ระดับสูง ระดับปานกลาง และระดับต่ำ ซึ่งในแต่ละระดับก็จะมีความเหมาะสมกับสถานการณ์การสื่อสารของยานพาหนะที่แตกต่างกันออกไป และได้กำหนดอัลกอริทึม และวิธีการป้องกันความเป็นส่วนตัวตามระดับความเป็นส่วนตัวทั้ง 3 ระดับโดยเลือกใช้อัลกอริทึมที่เหมาะสมที่สุดที่ได้จากงานวิจัยก่อนหน้านี้มาประยุกต์ใช้กับระดับความเป็นส่วนตัวทั้ง 3 ระดับ พร้อมกับการสลับโหมดความเป็นส่วนตัว (Privacy Mode Switching: PriMS) เพื่อปรับเปลี่ยนความต้องการความเป็นส่วนตัวของตำแหน่งที่ตั้งให้เป็นไปตามความเหมาะสมของสถานการณ์การสื่อสารและการเคลื่อนที่ของยานพาหนะ ทั้งนี้เพื่อลดโอเวอร์เฮดในการประมวลผล และเพิ่มประสิทธิภาพในการทำงานให้สูงขึ้น ทั้งยังสามารถป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะได้อย่างเหมาะสมที่สุดอีกด้วย

2. ประชากรและกลุ่มตัวอย่าง

งานวิจัยเรื่องนี้กระทำอยู่ภายใต้ระบบจำลอง (Simulation) ทั้งหมดโดยไม่มีการทดสอบกับระบบจริงแต่อย่างใด โดยเริ่มต้นได้กำหนดแบบแผน (Scheme) และรายละเอียดของสถานการณ์ (Situations) ในการสื่อสารของยานพาหนะขึ้นมา แล้วจัดกลุ่มสถานการณ์ต่างๆ ตามระดับความเป็นส่วนตัวที่เหมาะสม ดังนั้นประชากรและกลุ่มตัวอย่างทั้งหมดจะเป็นข้อมูลจากโปรแกรมจำลองระบบโดยแบ่งออกเป็น 3 ส่วนดังนี้

2.1 ยานพาหนะ (Vehicles) คือยานพาหนะที่ขับในระบบจำลองซึ่งจะถูกสร้างด้วยโปรแกรมจำลองโดยการสุ่มแล้วจัดเป็นกลุ่มการทดลองจำนวน 6 กลุ่ม ได้แก่ กลุ่มที่มีจำนวนยานพาหนะ 50 คัน 100 คัน 150 คัน 200 คัน 250 คัน และ 300 คัน ตามลำดับ

2.2 อุปกรณ์ข้างถนน (Roadside Units) คืออุปกรณ์ที่ติดตั้งติดหรือชิดกับพื้นที่ของถนน เช่น เสารับส่งสัญญาณไวไฟ (Wi-Fi) อุปกรณ์ตรวจจับความเร็ว กล้องตรวจจับแผ่นป้ายทะเบียน เป็นต้น ซึ่งประชากรในส่วนนี้จะกำหนดให้มีจำนวนคงที่ไม่มีการเปลี่ยนแปลง

2.3 บริการ (Services) คือผู้ให้บริการต่างๆ ผ่านทางเครือข่ายไร้สาย ซึ่งอยู่ห่างจากพื้นที่ของถนนเข้าไปในพื้นที่ของสิ่งปลูกสร้างอื่นๆ เช่น บริการข้อมูลการจราจร บริการข้อมูลสภาพอากาศ เป็นต้น ซึ่งประชากรในส่วนนี้จะกำหนดให้มีจำนวนคงที่ไม่มีการเปลี่ยนแปลง

3. ระดับความเป็นส่วนตัว

งานวิจัยเรื่องนี้ได้กำหนดระดับความเป็นส่วนตัว (Privacy Levels) ในการป้องกันและปิดบังตำแหน่งที่ตั้งของยานพาหนะออกเป็น 3 ระดับ ดังรายละเอียดตามตารางที่ 3.1

ตารางที่ 3.1 การจำแนกระดับความเป็นส่วนตัว

ระดับ	นิยาม	ตัวอย่างสถานการณ์
สูง (High)	เป็นระดับความเป็นส่วนตัวที่ต้องการความเป็นส่วนตัวสูง โดยข้อมูลของยานพาหนะจะต้องถูกป้องกันและปิดบังในระดับสูง และมีอัลกอริทึมที่ซับซ้อนในการประมวลผล โดยผู้ที่ไม่ได้รับอนุญาตให้เข้าถึงข้อมูลดังกล่าวจะไม่สามารถเปิดเผย ติดตาม และย้อนรอยได้	ยานพาหนะของหน่วยสืบราชการลับ ยานพาหนะขนเงินของธนาคารที่ต้องการความเป็นส่วนตัวสูง

ตารางที่ 3.1 (ต่อ)

ระดับ	นิยาม	ตัวอย่างสถานการณ์
ปานกลาง (Medium)	เป็นระดับความเป็นส่วนตัวที่ต้องการความเป็นส่วนตัวปานกลาง โดยข้อมูลของยานพาหนะจะถูกป้องกันและปิดบังในบางส่วนที่จำเป็น และมีอัลกอริทึมที่ไม่ซับซ้อนมากในการประมวลผล โดยผู้ที่ไม่ได้รับอนุญาตให้เข้าถึงข้อมูลดังกล่าวจะไม่สามารถเปิดเผย ติดตาม และย้อนรอยข้อมูลที่สำคัญได้ แต่อาจสามารถทราบถึงข้อมูลบางอย่างที่เป็นข้อมูลพื้นฐานได้	ยานพาหนะของผู้ใช้ตามท้องถนนทั่วไปที่ต้องการความเป็นส่วนตัวในระดับปานกลาง
ต่ำ (Low)	เป็นระดับความเป็นส่วนตัวที่ต้องการความเป็นส่วนตัวต่ำ โดยข้อมูลของยานพาหนะจะไม่ถูกป้องกันและปิดบัง หรือถ้ามีความจำเป็นในการปิดบังก็จะใช้เพียงอัลกอริทึมอย่างง่ายในการประมวลผล โดยผู้ที่เกี่ยวข้องสามารถเข้าถึงข้อมูลดังกล่าวได้อย่างเปิดเผยทั้งยังสามารถติดตามและย้อนรอยข้อมูลได้	ยานพาหนะสาธารณะ เช่น รถตำรวจ รถดับ-เพลิง และรถฉุกเฉินที่ไม่ต้องการความเป็นส่วนตัวหรือต้องการความเป็นส่วนตัวต่ำ

จากระดับความเป็นส่วนตัวของตำแหน่งที่ตั้งของยาน พาหนะทั้ง 3 ระดับจะนำมากำหนดช่วงคะแนน เพื่อใช้ในการจัดกลุ่มอัลกอริทึมและจัดกลุ่มรูปแบบของการสื่อสารของยานพาหนะเพื่อให้สอดคล้องและเหมาะสมกับระดับความเป็นส่วนตัวที่กำหนดขึ้นให้มากที่สุด โดยจะได้กล่าวไว้ในหัวข้อถัดไป

4. ปัจจัยสำหรับกำหนดระดับความเป็นส่วนตัว

เมื่อกำหนดระดับความเป็นส่วนตัวในการป้องกันและปิดบังความเป็นส่วนตัวของข้อมูลของยานพาหนะเป็น 3 ระดับแล้ว ต่อไปจะเป็นการกำหนดปัจจัยต่างๆ ของยานพาหนะที่จะนำมาพิจารณาเพื่อจำแนกและจัดกลุ่มระดับความเป็นส่วนตัวที่เหมาะสมโดยจากการศึกษางานวิจัยที่เกี่ยวข้องสามารถแบ่งปัจจัยต่างๆ เป็น 5 ปัจจัยดังรายละเอียดต่อไปนี้

4.1 พิกัด (Position) เป็นข้อมูลพิกัดหรือตำแหน่งของยานพาหนะ เช่น พิกัดละติจูด พิกัดลองจิจูด อยู่บนทางด่วน อยู่กลางสี่แยก เป็นต้น

4.2 ชื่อ (Name) เป็นชื่อเรียกขานหรือชื่อที่ใช้สำหรับการอ้างอิงของยานพาหนะ เช่น ชื่อเรียก หมายเลขทะเบียน เป็นต้น

4.3 คุณสมบัติ (Properties) เป็นข้อมูลคุณสมบัติต่างๆ ของยานพาหนะ เช่น สี รุ่น ยี่ห้อ จำนวนที่นั่ง ความแรงของเครื่องยนต์ เป็นต้น

4.4 ข้อมูลผู้ขับขี่ (Driver) เป็นข้อมูลผู้ขับขี่ยานพาหนะ เช่น ชื่อ เพศ อายุ น้ำหนัก ส่วนสูง หมายเลขบัตรประจำตัวประชาชน หมายเลขใบขับขี่ เป็นต้น

4.5 สถานะ (Status) เป็นสถานะของยานพาหนะ เช่น เลี้ยวซ้าย เลี้ยวขวา เดินหน้า ถอยหลัง เร่งความเร็ว ลดความเร็ว เป็นต้น

จากปัจจัยปัจจัย 5 ปัจจัยในการพิจารณาความต้องการความเป็นส่วนตัว สามารถนำมากำหนดค่าระดับคะแนนที่เป็นระดับความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะได้ 5 ระดับ โดยมีค่าคะแนนตั้งแต่ 0-4 ดังรายละเอียดในตารางที่ 3.2

ตารางที่ 3.2 คะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัว

ระดับความสามารถ	คะแนน
ระดับมากที่สุด	4
ระดับมาก	3
ระดับปานกลาง	2
ระดับน้อย	1
ระดับน้อยที่สุด	0

การให้คะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวของแต่ละอัลกอริทึมและรูปแบบการสื่อสารตามปัจจัยที่กำหนดไว้นั้นจะใช้เกณฑ์การให้คะแนนที่มาจากการศึกษาคุณสมบัติของอัลกอริทึมและรูปแบบการสื่อสารต่างๆ จากรายละเอียดที่ระบุไว้ในเอกสารงานวิจัยและเอกสารทางวิชาการที่เกี่ยวข้องพร้อมทั้งการปรึกษาผู้เชี่ยวชาญ โดยเมื่อกำหนดค่าคะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวให้กับแต่ละอัลกอริทึมและรูปแบบการสื่อสารตามปัจจัยที่กำหนดไว้เรียบร้อยแล้วก็จะนำค่าคะแนนที่ได้ทุกปัจจัยมารวมกันเป็นค่าคะแนนรวมแล้วแบ่งเป็นช่วงคะแนนเพื่อใช้ในการจัดกลุ่มอัลกอริทึม

และรูปแบบการสื่อสารตามระดับความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะที่เหมาะสม โดยช่วงคะแนนดังกล่าวแสดงไว้ในตารางที่ 3.3

ตารางที่ 3.3 ช่วงคะแนนของระดับความเป็นส่วนตัว

ระดับความเป็นส่วนตัว	ช่วงคะแนน
ระดับสูง	14 - 20
ระดับปานกลาง	7 - 13
ระดับต่ำ	0 - 6

จากช่วงคะแนนที่กำหนดขึ้นตามตารางที่ 3.3 จะนำมาใช้ในการจัดกลุ่มอัลกอริทึมและรูปแบบการสื่อสารพร้อมทั้งแจกแจงค่าคะแนนตามรายละเอียดในตารางที่ 3.4 และตารางที่ 3.5 ของหัวข้อถัดไป

5. อัลกอริทึมการป้องกันและปิดบังความเป็นส่วนตัว

จากการศึกษาอัลกอริทึมการป้องกันและปิดบังความเป็นส่วนตัวของตำแหน่งที่ตั้งของยานพาหนะในหัวข้องานวิจัยที่เกี่ยวข้องมาแล้วนั้น ผู้วิจัยได้เลือกอัลกอริทึมที่สำคัญสำหรับนำมาใช้ในงานวิจัยเรื่องนี้ทั้งหมด 5 อัลกอริทึมดังรายละเอียดต่อไปนี้

5.1 อัลกอริทึมชื่อเทียมและชื่อปลอม (Pseudonym and Anonym Algorithm)

เป็นอัลกอริทึมการป้องกันและปิดบังข้อมูลอย่างง่ายที่นำมาใช้ในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะในช่วง 10 ปีที่ผ่านมา ซึ่งใช้เทคนิคการเข้ารหัส (Encryption) และเทคนิคการแฮช (Hashing) ในการปิดบังข้อมูล

5.2 อัลกอริทึมมิกซ์โซน (Mix-Zone Algorithm)

เป็นอัลกอริทึมการเปลี่ยนตำแหน่งที่ตั้งโดยการแลก เปลี่ยนกุญแจที่ใช้ในการเข้ารหัสข้อมูลของตำแหน่งที่ตั้ง ซึ่งจะแบ่งพื้นที่ต่างๆ ในแผนที่ออกเป็นมิกซ์โซนหลายมิกซ์โซน โดยแต่ละมิกซ์โซนจะมีกุญแจการเข้ารหัสเพื่อใช้ในการปิดบังข้อมูลของตำแหน่งที่ตั้งที่แตกต่างกันออกไป ยานพาหนะจะต้องใช้กุญแจในการปิดบังข้อมูลที่แตกต่างกันไปตามมิกซ์โซนปัจจุบันที่กำลังเคลื่อนที่ไปถึง

5.3 อัลกอริทึมอะโมอีบา (AMOEBA Algorithm)

เป็นอัลกอริทึมที่กำหนดให้ยานพาหนะแต่ละคันมีช่วงเวลาของการปล่อยสัญญาณที่แตกต่างกันตามช่วงเวลาที่กำหนดไว้ และมีช่วงเวลาเงียบ (Silent Period) ที่จะไม่มีการปล่อยสัญญาณใดๆ จึงทำให้การติดตามตำแหน่งของยานพาหนะทำได้ยากยิ่งขึ้น นอกจากนี้ยังใช้กระบวนการสื่อสารผ่านทางตัวแทนหรือหัวหน้ากลุ่มของเขตพื้นที่ที่ยานพาหนะกำลังเคลื่อนที่อยู่ ณ ปัจจุบันเพื่อปิดบังข้อมูลจริงของยานพาหนะแต่ละคัน

5.4 อัลกอริทึมเรป (REP Algorithm)

เป็นอัลกอริทึมที่มีการทำงานคล้ายกับอัลกอริทึมอะโมอีบาแต่มีการปรับปรุงระยะเวลาในการเงียบและระยะเวลาในการส่งข้อมูลโดยใช้หลักของการสุ่มคาบเวลาในการเข้ารหัสข้อมูล (Random Encryption Period) โดยกำหนดกุญแจที่เป็นตัวเลขสุ่มที่ใช้สำหรับการเข้ารหัสและใช้ในการปล่อยสัญญาณตามคาบที่ถูกระบุด้วยตัวเลขสุ่มนั้น

5.5 อัลกอริทึมดีแอลพี (DLP Algorithm)

เป็นอัลกอริทึมที่มีการปิดบังข้อมูลของตำแหน่งที่ตั้งของยานพาหนะโดยพิจารณาความหนาแน่นของยานพาหนะเพื่อนบ้านที่อยู่ใกล้เคียงกัน เพื่อให้มีขอบเขตการรับส่งข้อมูลระหว่างยานพาหนะที่จำกัด โดยถ้ามีความหนาแน่นของยานพาหนะเพื่อนบ้านมากเกินขอบเขตที่กำหนดไว้ก็จะต้องทำการเข้ารหัสข้อมูลใหม่อีกครั้ง

นอกจากอัลกอริทึมทั้ง 5 อัลกอริทึม พบว่าในบางช่วงเวลาของการสื่อสารของยานพาหนะนั้นอาจไม่จำเป็นที่จะต้องใช้อัลกอริทึมใดเลยในการป้องกันและปิดบังตำแหน่งที่ตั้ง เพราะในกระบวนการสื่อสารดังกล่าวต้องการความเป็นสาธารณะแทนความเป็นส่วนตัว ซึ่งจากปัจจัยในการพิจารณาความต้องการความเป็นส่วนตัวที่กล่าวไว้ในหัวข้อก่อนหน้านี้ สามารถนำมาใช้ในการจัดกลุ่มอัลกอริทึมได้ตามรายละเอียดในตารางที่ 3.4

ตารางที่ 3.4 คะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวของอัลกอริทึม

อัลกอริทึม	พิกัด	ชื่อ	คุณสมบัติ	ข้อมูลผู้ขับขี่	สถานะ	คะแนนรวม	ระดับความเป็นส่วนตัว
ไม่ใช้อัลกอริทึม	0	0	0	0	0	0	ระดับต่ำ
ชื่อเทียม ชื่อปลอม	1	3	2	2	1	9	ระดับปานกลาง

ตารางที่ 3.4 (ต่อ)

อัลกอริทึม	พิกัด	ชื่อ	คุณสมบัติ	ข้อมูลผู้ขับขี่	สถานะ	คะแนนรวม	ระดับความเป็นส่วนตัว
ไม่ใช้อัลกอริทึม	0	0	0	0	0	0	ระดับต่ำ
ชื่อเทียม ชื่อปลอม	1	3	2	2	1	9	ระดับปานกลาง
มิกซ์โซน	1	3	2	2	2	10	ระดับปานกลาง
ดีแอลพี	3	4	3	3	3	16	ระดับสูง
อะโมอีบา	3	4	3	4	3	17	ระดับสูง
เรป	4	4	3	3	4	18	ระดับสูง

ค่าคะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวจากตารางที่ 5 นั้นได้มาจากการพิจารณาและศึกษาตามเอกสารงานวิจัย ซึ่งเป็นค่าตามทฤษฎี โดยเมื่อจำแนกไปตามระดับความเป็นส่วนตัวที่กำหนดไว้จะได้ว่า ระดับต่ำได้แก่ ไม่ใช้อัลกอริทึม ระดับปานกลางได้แก่ อัลกอริทึมชื่อเทียมและชื่อปลอม และอัลกอริทึมมิกซ์โซน และระดับสูงได้แก่ อัลกอริทึมดีแอลพี อัลกอริทึมอะโมอีบา และอัลกอริทึมเรป

6. รูปแบบการสื่อสารของยานพาหนะ

รูปแบบการสื่อสารของยานพาหนะสามารถจำแนกออกได้เป็น 3 รูปแบบหลักได้แก่ การสื่อสารระหว่างยานพาหนะกับยานพาหนะหรือวีทูวี (V2V) การสื่อสารระหว่างยานพาหนะกับอุปกรณ์หรือวีทูไอ (V2I) และการสื่อสารระหว่างยาน พาหนะกับบริการหรือวีทูเอส (V2S) โดยในแต่ละรูปแบบหลักก็จะแบ่งเป็นรูปแบบการสื่อสารย่อยได้อีกหลายรูปแบบ ซึ่งมีรายละเอียดดังต่อไปนี้

6.1 การสื่อสารระหว่างยานพาหนะกับยานพาหนะ

เป็นการสื่อสารระหว่างยานพาหนะตั้งแต่สองคันขึ้นไปที่มาแลกเปลี่ยนข้อมูลและสถานะระหว่างกัน เช่น การเลี้ยวซ้ายเลี้ยวขวา การเดิน หน้าถอยหลัง การเพิ่มลดความเร็ว การบอกตำแหน่งที่ตั้ง การบอกสถานะของคนขับ เป็นต้น

6.2 การสื่อสารระหว่างยานพาหนะกับอุปกรณ์

เป็นการสื่อสารระหว่างยานพาหนะกับเครื่องมือสื่อสารและอุปกรณ์ควบคุมต่างๆ ที่ติดตั้งบริเวณรอบถนน อาจจะเป็นเสาข้างถนนหรือเครื่องมือที่ติดอยู่บนถนน เช่น การแจ้งเตือนเขตชุมชน การแจ้งเตือนเขตโรงเรียน การแจ้งเตือนก่อนถึงสี่แยก เป็นต้น

6.3 การสื่อสารระหว่างยานพาหนะกับบริการ

เป็นการสื่อสารระหว่างยานพาหนะกับผู้ให้บริการต่างๆ ที่อยู่ห่างจากบริเวณพื้นที่ถนน เช่น การรับส่งข้อมูลจากบริการของผู้ให้บริการในรูปแบบของข้อความ รูปภาพ เพลง เสียง วีดิโอ ภาพเคลื่อนไหว เป็นต้น

จากรูปแบบการสื่อสารของยานพาหนะทั้ง 3 รูปแบบสามารถนำมาจัดกลุ่มโดยกำหนดค่าคะแนนให้กับรูปแบบการสื่อสารต่างๆ ตามปัจจัยของความต้องการความเป็นส่วนตัว 5 ปัจจัย ได้แก่ การป้องกันและปิดบังพิกัด ชื่อ คุณสมบัติ ข้อมูลผู้ขับ และสถานะของยานพาหนะ ซึ่งมีรายละเอียดตามตารางที่ 3.5

ตารางที่ 3.5 คะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวของรูปแบบการสื่อสาร

รูปแบบการสื่อสาร	พิกัด	ชื่อ	คุณสมบัติ	ข้อมูลผู้ขับ	สถานะ	รวม	ระดับความเป็นส่วนตัว
การสื่อสารระหว่างยานพาหนะกับยานพาหนะ							
การบอกสถานะของยานพาหนะ	1	2	0	1	4	8	ระดับปานกลาง
การบอกสถานะของคนขับ	1	3	2	4	1	11	ระดับปานกลาง
การบอกตำแหน่งที่ตั้ง	4	3	2	2	1	12	ระดับปานกลาง
การสื่อสารส่วนบุคคล	4	4	4	4	4	20	ระดับสูง
การสื่อสารระหว่างยานพาหนะกับอุปกรณ์							
การแจ้งเตือนแบบสาธารณะ	0	0	0	2	1	3	ระดับต่ำ

ตารางที่ 3.5 (ต่อ)

รูปแบบการสื่อสาร	พิกัด	ชื่อ	คุณสมบัติ	ข้อมูลผู้ขับ	สถานะ	รวม	ระดับความเป็นส่วนตัว
การแจ้งเตือนแบบส่วนบุคคล	2	4	3	4	2	15	ระดับสูง
การสื่อสารระหว่างยานพาหนะกับบริการ							
การลงทะเบียนจากบริการ	1	4	3	3	1	12	ระดับปานกลาง
การรับส่งข้อมูลจากบริการ	3	4	1	2	3	13	ระดับปานกลาง

ค่าคะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวจากตารางที่ 3.5 นั้นได้มาจากการพิจารณาและศึกษาตามเอกสารงานวิจัย ซึ่งเป็นค่าตามทฤษฎีเช่นเดียวกับการจำแนกอัลกอริทึมในหัวข้อก่อนหน้านี้ โดยประกอบไปด้วยระดับต่ำได้แก่ สถานการณ์การแจ้งเตือนแบบสาธารณะ ระดับปานกลางได้แก่ สถานการร์การบอกสถานะของยานพาหนะ การบอกสถานะของคนขับ การบอกตำแหน่งที่ตั้ง การลงทะเบียนจากบริการ และการรับส่งข้อมูลจากบริการ และระดับสูงได้แก่ สถานการณ์การสื่อสารส่วนบุคคล และการแจ้งเตือนแบบส่วนบุคคล

7. การป้องกันความเป็นส่วนตัวภายใต้ระดับความเป็นส่วนตัว

จากการจัดกลุ่มอัลกอริทึมและรูปแบบการสื่อสารของยานพาหนะตามระดับความเป็นส่วนตัวในหัวข้อก่อนหน้านี้ สามารถนำมาใช้ในกระบวนการป้องกันและปิดบังตำแหน่งที่ตั้งของยานพาหนะแบบใหม่ที่อยู่บนพื้นฐานของระดับความเป็นส่วนตัวนั้น โดยอัลกอริทึมที่ใช้ในการปิดบังจะปรับเปลี่ยนไปตามสถานการณ์และรูปแบบการสื่อสาร ณ ขณะใดขณะหนึ่งโดยมีรายละเอียดดังตารางที่ 3.6

ตารางที่ 3.6 การแจกแจงระดับความเป็นส่วนตัวโดยจำแนกตามอัลกอริทึมและรูปแบบการสื่อสารของยานพาหนะ

รูปแบบการสื่อสาร	คะแนนรวม	ระดับความเป็นส่วนตัว	อัลกอริทึม
การสื่อสารระหว่างยานพาหนะกับยานพาหนะ			
การบอกสถานะของยานพาหนะ	8	ระดับปานกลาง	อัลกอริทึมชื่อเทียมและชื่อปลอม (9) อัลกอริทึมมิกซ์โซน (10)
การบอกสถานะของคนขับ	11	ระดับปานกลาง	อัลกอริทึมชื่อเทียมและชื่อปลอม (9) อัลกอริทึมมิกซ์โซน (10)
การบอกตำแหน่งที่ตั้ง	12	ระดับปานกลาง	อัลกอริทึมชื่อเทียมและชื่อปลอม (9) อัลกอริทึมมิกซ์โซน (10)
การสื่อสารส่วนบุคคล	20	ระดับสูง	อัลกอริทึมอะโมอีบา (17) อัลกอริทึมเรป (18) อัลกอริทึมดีแอลพี (16)
การสื่อสารระหว่างยานพาหนะกับอุปกรณ์			
การแจ้งเตือนแบบสาธารณะ	3	ระดับต่ำ	ไม่ใช้อัลกอริทึม (0)
การแจ้งเตือนแบบส่วนบุคคล	15	ระดับสูง	อัลกอริทึมอะโมอีบา (17) อัลกอริทึมเรป (18) อัลกอริทึมดีแอลพี (16)
การสื่อสารระหว่างยานพาหนะกับบริการ			
การลงทะเบียนจากบริการ	12	ระดับปานกลาง	อัลกอริทึมชื่อเทียมและชื่อปลอม (9) อัลกอริทึมมิกซ์โซน (10)
การรับส่งข้อมูลจากบริการ	13	ระดับปานกลาง	อัลกอริทึมชื่อเทียมและชื่อปลอม (9) อัลกอริทึมมิกซ์โซน (10)

จากตารางที่ 3.6 ซึ่งได้แจกแจงระดับความเป็นส่วนตัวโดยจำแนกตามอัลกอริทึมและรูปแบบการสื่อสารของยานพาหนะ โดยเมื่อมีสถานการณ์หรือการใช้งานของยานพาหนะตามช่วงเวลาเข้ามา กระบวนการป้องกันและปิดบังความเป็นส่วนตัวของข้อมูลตามแนวความคิดของงานวิจัยเรื่องนี้ก็จะเริ่มขึ้นภายใต้ระดับความเป็นส่วนตัวที่ได้เลือกไว้ และจะสลับสับเปลี่ยนไปตามรูปแบบการสื่อสารที่เปลี่ยนไปตามช่วงเวลา

จากข้อมูลการป้องกันและปิดบังตำแหน่งที่ตั้งบนพื้นฐานของระดับความเป็นส่วนตัวในตารางที่ 3.6 สามารถนำมาเขียนเป็นรหัสเทียม (Pseudocode) ได้ดั งนี้

```
1   Function protectLocation(event)
2      score ← checkEventScore(event)
3      If score between 0 to 6
4         algor ← callLowLevel()
5      Else If score between 7 to 13
6         algor ← callMediumLevel()
7      Else If score between 14 to 20
8         algor ← callHighLevel()
9      Else
10        algor ← null
11     End If
12     anonymizeData(algor)
13  End Function
```

เมื่อพิจารณาจากรหัสเทียมจะเห็นว่าเมื่อมีสถานการณ์เข้ามาในการบวนการป้องกันและปิดบังข้อมูลของยานพากนะ ก็จะถูกนำมาพิจารณาค่าคะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวและตรวจสอบช่วงคะแนนเพื่อกำหนดอัลกอริทึมที่เหมาะสมในการป้องกันและปิดบังข้อมูล ตามรายละเอียดของตารางที่ 3.3 ในหัวข้อก่อนหน้านี้

จากการกำหนดระดับความเป็นส่วนตัวและกระบวนการป้องกันและปิดบังความเป็นส่วนตัวของข้อมูลภายใต้ระดับความเป็นส่วนตัวที่ได้กล่าวไว้ในบทนี้ จะเข้าสู่กระบวนการวัดผลและประเมินประสิทธิภาพในการทำงานซึ่งกล่าวไว้ในบทถัดไป

บทที่ 4
ผลการวิเคราะห์ข้อมูล

จากกระบวนการดำเนินการวิจัยในบทที่ผ่านมาทำให้เห็นถึงแนวคิด ขั้นตอน และกระบวนการต่างๆ ของงานวิจัยเรื่องนี้ ต่อไปจะเป็นผลการวิเคราะห์ข้อมูล และผลลัพธ์ที่ได้จากการทดลองในระบบจำลอง ซึ่งประกอบไปด้วย 2 ส่วนหลักได้แก่ การวัดประสิทธิภาพและวิเคราะห์การทำงานเชิงทฤษฎี (Theoretical Analysis) และการวัดประสิทธิภาพและวิเคราะห์การทำงานเชิงปฏิบัติการ (Experimental Analysis) โดยมีรายละเอียดดังต่อไปนี้

1. การวัดประสิทธิภาพและวิเคราะห์การทำงานเชิงทฤษฎี

การวัดประสิทธิภาพการทำงานของวิธีการป้องกันและปิดบังข้อมูลของยานพาหนะบนพื้นฐานของอัลกอริทึมพริมพ์นี้จะใช้วิธีการคำนวณตามทฤษฎีโดยมีสมการคำนวณค่าโอเวอร์เฮด (Overhead) ได้ดังสมการต่อไปนี้

$$\text{Overhead} = \frac{\sum_{i=1}^{n} \text{Score}(E_i)}{n} \quad \ldots (1)$$

จากสมการที่ 1 กำหนดให้ E_i คือสถานการณ์ที่ i ซึ่งเกิดขึ้นในกระบวนการสื่อสารของยานพาหนะ $\text{Score}(E_i)$ คือค่าคะแนนความสามารถและความต้องการในการป้องกันและปิดบังความเป็นส่วนตัวในสถานการณ์ที่ i และ n คือจำนวนของสถานการณ์ทั้งหมดที่เกิดขึ้น ซึ่งจากข้อมูลของงานวิจัยที่เกี่ยวข้องพบว่า เมื่อมีค่าความสามารถและความต้องการในความเป็นส่วนตัวสูงขึ้นก็จะทำให้ค่าโอเวอร์เฮดสูงขึ้นตามไปด้วย โดยในการวัดประสิทธิภาพในครั้งนี้ได้ใช้สถานการณ์พื้นฐาน 8 สถานการณ์ ($n = 8$) จากรูปแบบการสื่อสารของยานพาหนะที่กล่าวไว้ในหัวข้อก่อนหน้านี้ซึ่งประกอบไปด้วย (1) การบอกสถานะของยานพาหนะ (2) การบอกสถานะของคนขับ (3) การบอกตำแหน่งที่ตั้ง (4) การสื่อสารส่วนบุคคล (5) การแจ้งเตือนแบบสาธารณะ (6) การแจ้งเตือนแบบส่วนบุคคล (7) การลงทะเบียนจากบริการ และ (8) การรับส่งข้อมูลจากบริการ โดยกำหนดให้ความน่าจะเป็นของการเกิดสถานการณ์ทั้ง 8 สถานการณ์นี้มีอย่างเท่าเทียมกันและเป็นอิสระต่อกัน ซึ่งค่าโอเวอร์เฮดที่คำนวณได้ปรากฏตามตารางที่ 4.1

ตารางที่ 4.1 การคำนวณค่าโอเวอร์เฮดของอัลกอริทึมตามทฤษฎี

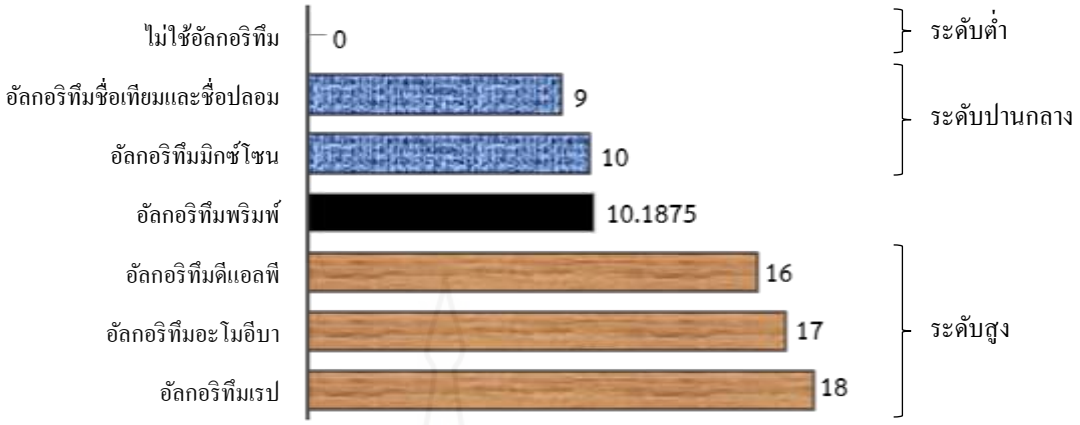
อัลกอริทึม	ค่าโอเวอร์เฮด
ไม่ใช้อัลกอริทึม	$\frac{0+0+0+0+0+0+0+0}{8}=0.0$
อัลกอริทึมชื่อเทียมและชื่อปลอม	$\frac{9+9+9+9+9+9+9+9}{8}=9.0$
อัลกอริทึมมิกซ์โซน	$\frac{10+10+10+10+10+10+10+10}{8}=10.0$
อัลกอริทึมดีแอลพี	$\frac{16+16+16+16+16+16+16+16}{8}=16.0$
อัลกอริทึมอะโมอีบา	$\frac{17+17+17+17+17+17+17+17}{8}=17.0$
อัลกอริทึมเรป	$\frac{18+18+18+18+18+18+18+18}{8}=18.0$

จากค่าโอเวอร์เฮดในตารางที่ 4.1 เป็นค่าที่ได้จากการคำนวณโดยการเลือกใช้อัลกอริทึมเพียงหนึ่งอัลกอริทึมตลอดทั้ง 8 สถานการณ์ ต่อไปนี้จะเป็นการคำนวณค่าโอเวอร์เฮดจากการเลือกใช้และปรับเปลี่ยนอัลกอริทึมไปตามระดับความเป็นส่วนตัวทั้ง 3 ระดับที่ได้กำหนดไว้ก่อนหน้านี้ ซึ่งมีรายละเอียดตามตารางที่ 4.2

ตารางที่ 4.2 การคำนวณค่าโอเวอร์เฮดโดยการปรับเปลี่ยนอัลกอริทึมไปตามระดับความเป็นส่วนตัว

กรณีการประมวลผล	ค่าโอเวอร์เฮด
กรณีที่ดีที่สุด (Best-Case)	$\frac{9+9+9+16+0+16+9+9}{8}=9.625$
กรณีที่เลวร้ายที่สุด (Worst-Case)	$\frac{10+10+10+18+0+18+10+10}{8}=10.75$
กรณีเฉลี่ย (Average-Case)	$\frac{9.625+10.75}{2}=10.1875$

จากตารางที่ 4.2 ปรากฏค่าโอเวอร์เฮดเฉลี่ยอยู่ที่ 10.1875 ซึ่งมีค่ามากกว่าการไม่ใช้อัลกอริทึม อัลกอริทึมชื่อเทียมและชื่อปลอม และอัลกอริทึมมิกซ์โซน แต่มีค่าน้อยกว่าอัลกอริทึมดีแอลพี อัลกอริทึมอะโมอีบา และอัลกอริทึมเรป ดังแสดงกราฟการเปรียบเทียบประสิทธิภาพของอัลกอริทึมตามรูปภาพที่ 4.1



ภาพที่ 4.1 กราฟการเปรียบเทียบค่าโอเวอร์เฮดของอัลกอริทึมต่างๆ กับอัลกอริทึมพริมส์

จากรูปภาพที่ 4.1 อัลกอริทึมพริมส์มีค่าโอเวอร์เฮดเฉลี่ยอยู่ที่ 10.1875 ซึ่งมีค่าน้อยกว่าค่าโอเวอร์เฮดของอัลกอริทึมดีแอลพี อัลกอริทึมอะโมอีบา และอัลกอริทึมเรป ซึ่งล้วนแล้วแต่เป็นอัลกอริทึมที่มีประสิทธิภาพในการป้องกันและปิดบังข้อมูลที่สูงแต่มีค่าโอเวอร์เฮดที่สูงด้วยเช่นกัน และเมื่อพิจารณาถึงประสิทธิภาพของอัลกอริทึมพริมพ์เชิงทฤษฎีจะพบว่าประสิทธิภาพการทำงานมีไม่ด้อยไปกว่าอัลกอริทึมทั้ง 3 ที่ได้กล่าวไปข้างต้น เพราะมีการเลือกใช้อย่างผสมผสานและสลับสับเปลี่ยนอัลกอริทึมทั้ง 3 เข้าด้วยกันตามความเหมาะสม รวมถึงการเลือกไม่ใช้อัลกอริทึมอัลกอริทึมชื่อเทียมและชื่อปลอม และอัลกอริทึมมิกซ์โซนในการประมวลผลตามความเหมาะสมกับรูปแบบการสื่อสารของยานพาหนะอีกด้วย

2. การวัดประสิทธิภาพและวิเคราะห์การทำงานเชิงปฏิบัติการ

การวัดประสิทธิภาพและวิเคราะห์การทำงานเชิงปฏิบัติการนั้นประกอบไปด้วยการวัดค่าต่าง ๆ 3 ค่า ได้แก่ ค่าโอเวอร์เฮดเฉลี่ยของการประมวลผล (Average of Overhead) โดยมีสูตรในการคำนวณดังสมการที่ 2 ค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัว (Probability of Privacy Protection and Anonymization) โดยมีสูตรในการคำนวณดังสมการที่ 3 และค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัว (Efficiency Ratio of Privacy Protection and Anonymization) โดยมีสูตรในการคำนวณดังสมการที่ 4 ตามลำดับ

$$\text{Overhead} = \frac{\sum_{i=1}^{n} \text{Time}(E_i)}{n} \quad \ldots (2)$$

จากสมการที่ 2 กำหนดให้ E_i คือสถานการณ์ที่ i ซึ่งเกิดขึ้นในกระบวนการสื่อสารของยานพาหนะ $\text{Time}(E_i)$ คือเวลาที่ใช้ในการป้องกันและปิดบังความเป็นส่วนตัวในสถานการณ์ที่ i ตามอัลกอริทึมที่กำหนด และ n คือจำนวนของสถานการณ์ทั้งหมดที่เกิดขึ้น

$$\text{Probability} = \frac{|D|}{|S|} \quad \ldots (3)$$

จากสมการที่ 3 กำหนดให้ D คือข้อมูลของยานพาหนะที่ไม่ถูกเปิดเผยหรือสามารถปิดบังความเป็นส่วนตัวได้ และ S คือข้อมูลของยานพาหนะทั้งหมดที่ใช้ในการติดสื่อสารและรับส่งข้อมูลโดยอาจจะเป็นข้อมูลที่ถูกเปิดเผยและไม่ถูกเปิดเผยความเป็นส่วนตัว

$$\text{Efficiency Ratio} = \frac{\text{Probability}}{\text{Overhead}} \quad \ldots (4)$$

จากสมการที่ 4 กำหนดให้ Probability คือความน่าจะเป็นที่สามารถป้องกันและปิดบังความเป็นส่วนตัวได้ และ Overhead คือเวลาที่ใช้ในการป้องกันและปิดบังความเป็นส่วนตัวตามสถานการณ์และอัลกอริทึมที่กำหนด

การวัดค่าประสิทธิภาพการทำงานเชิงปฏิบัติการนั้นกระทำภายใต้ระบบจำลองที่ได้สร้างขึ้นเพื่อทดสอบประสิทธิภาพการทำงาน และเปรียบเทียบผลลัพธ์ว่าสอดคล้องไปตามประสิทธิภาพการทำงานเชิงทฤษฎีมากน้อยเพียงใด โดยมีรายละเอียดดังต่อไปนี้

2.1 โมเดลของถนนที่ใช้ในการทดลอง

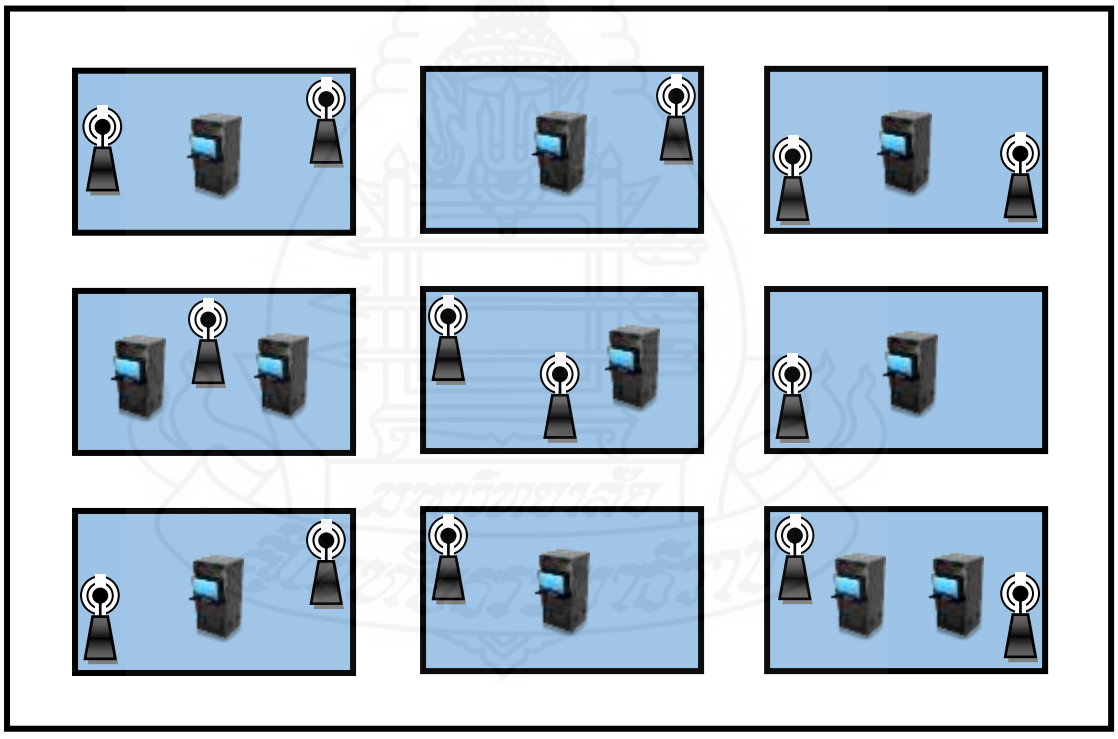
งานวิจัยเรื่องนี้ได้ใช้โมเดลของถนน 2 รูปแบบได้แก่ โมเดลถนนแบบแมนแฮทตัน (Manhattan) และโมเดลถนนแบบแบบทางอิสระ (Freeway) ดังแสดงในรูปภาพที่ 4.3 และ รูปภาพที่ 4.4 ตามลำดับ โดยกำหนดรูปสัญลักษณ์ต่างๆ เพื่อใช้ในการแสดงในแผนที่ของถนนดังแสดงตามรูปภาพที่ 4.2

อุปกรณ์ข้างถนน (Roadside Unit: RSU)

เครื่องแม่ข่ายที่เป็นผู้ให้บริการ (Services)

ภาพที่ 4.2 รูปสัญลักษณ์ต่างๆ ที่ปรากฏบนโมเดลถนน

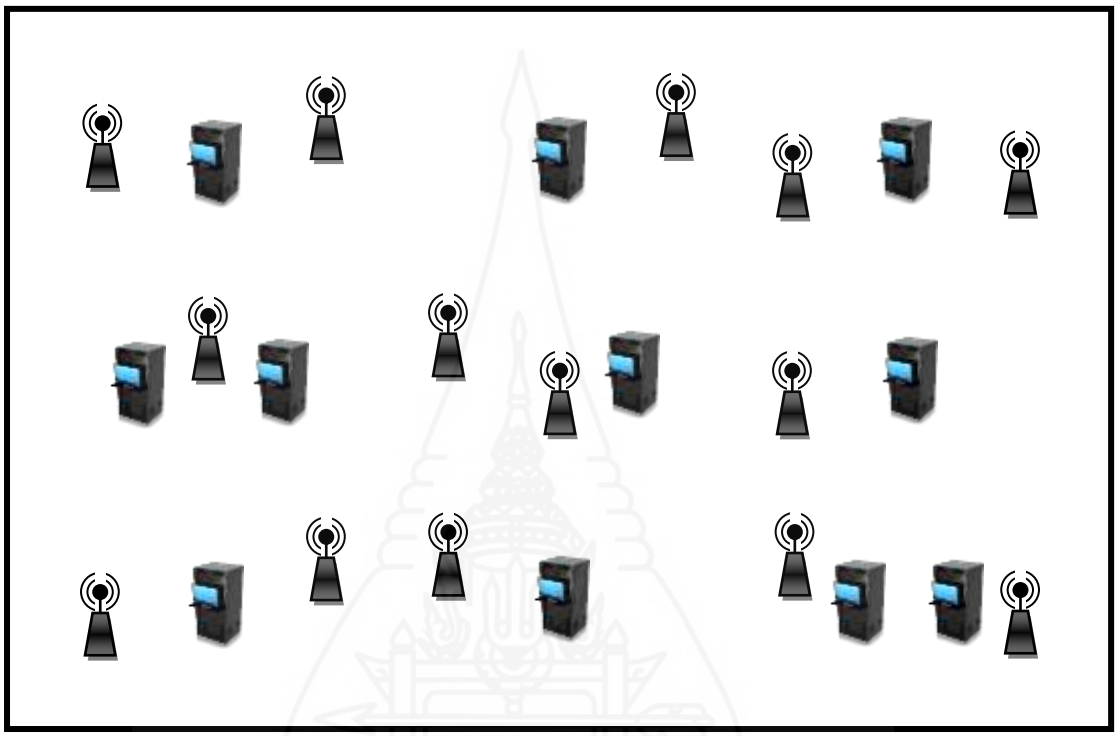
2.1.1 โมเดลถนนแบบแมนแฮทตัน (Manhattan) จะมีลักษณะเป็นถนนที่ทอดยาวเส้นตรงและวางเป็นระเบียบตามแนวยาวและแนวขวางของแผนที่ โดยแบ่งออกเป็นบล็อก (Block) และกำหนดขอบเขตของขอบถนนอย่างชัดเจน โดยงานวิจัยเรื่องนี้ได้กำหนดตำแหน่งของอุปกรณ์ข้างถนน (Roadside Unit: RSU) พร้อมทั้งเครื่องแม่ข่ายที่เป็นผู้ให้บริการ (Services) ต่างๆ เอาไว้ตามรายละเอียดในรูปภาพที่ 4.3



ภาพที่ 4.3 โมเดลถนนแบบแมนแฮทตัน

2.1.2 โมเดลถนนแบบทางอิสระ (Freeway) จะมีลักษณะเป็นถนนที่มีความเป็นอิสระในการเคลื่อนที่โดยจะไม่มีบล็อก (Block) กั้นเพื่อกำหนดขอบเขตของถนนแต่อย่างใด ทำให้

ยานพาหนะสามารถเคลื่อนที่ได้อย่างอิสระไปทั่วทุกทิศทุกทางของแผนที่ได้ ซึ่งโมเดลดังกล่าวได้จัดวางตำแหน่งของอุปกรณ์ข้างถนน (Roadside Unit: RSU) และเครื่องแม่ข่ายที่เป็นผู้ให้บริการ (Services) ต่างๆ เช่นเดียวกับโมเดลก่อนหน้านี้ ดังแสดงตามรูปภาพที่ 4.4



ภาพที่ 4.4 โมเดลถนนแบบทางอิสระ

2.2 ผลการทดลองตามแบบจำลอง

งานวิจัยเรื่องนี้ได้ทำการวัดค่าต่างๆ อันได้แก่ ค่าโอเวอร์เฮดเฉลี่ย (Average of Overhead) ค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัว (Probability of Privacy Protection and Anonymization) และค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัว (Efficiency Ratio of Privacy Protection and Anonymization) โดยมีรายละเอียดดังต่อไปนี้

กำหนดให้ N คือ จำนวนของยานพาหนะ
Non-Algor คือ ไม่ใช้อัลกอริทึม
Pseudonym คือ อัลกอริทึมชื่อเทียมและชื่อปลอม
Mix-Zone คือ อัลกอริทึมมิกซ์โซน

AMOEBA คือ อัลกอริทึมอะโมอีบา

DLP คือ อัลกอริทึมดีแอลพี

REP คือ อัลกอริทึมเรป

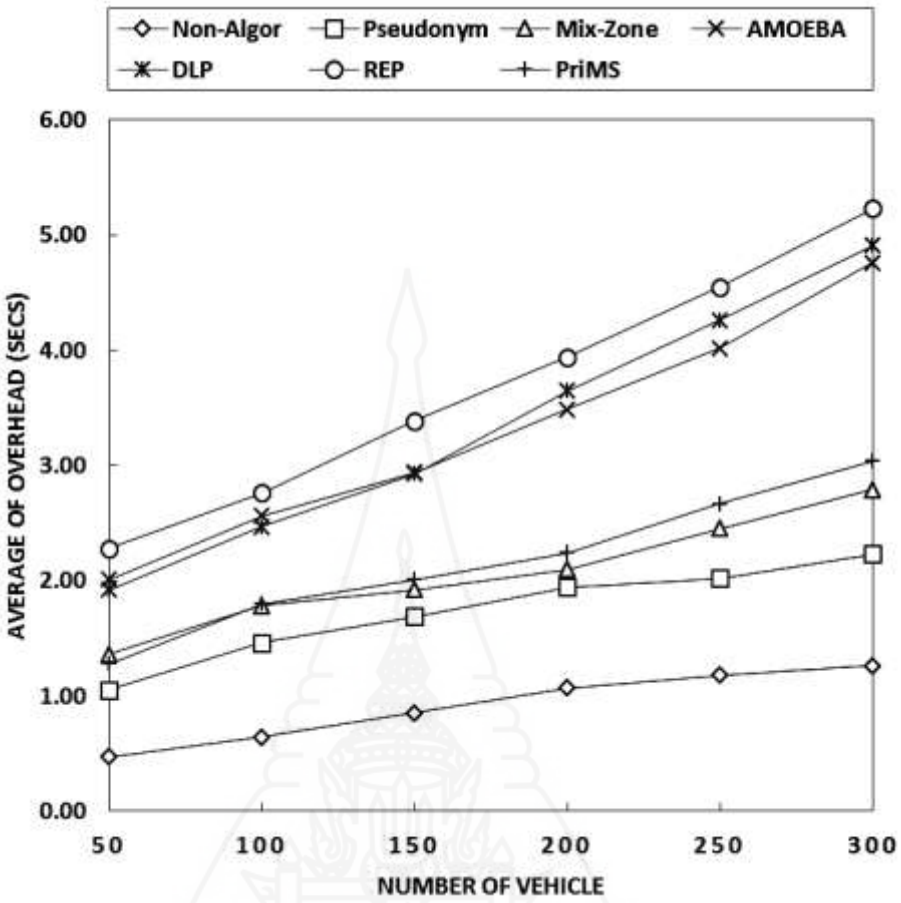
PriMS คือ อัลกอริทึมพริมส์

กำหนดให้รูปแบบและสถานการณ์การสื่อสารทั้ง 8 รูปแบบที่กล่าวไว้ในหัวข้อก่อนหน้านี้มีโอกาสเกิดขึ้นได้อย่างสุ่ม (Random) โดยมีความความน่าจะเป็นในการเกิดเหตุการณ์ต่างๆ อย่างเท่าเทียมกัน

2.2.1 ผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ย (Average of Overhead) กับจำนวนยานพาหนะ (Number of Vehicle) บนโมเดลถนนแบบแมนแฮทตัน โดยกำหนดค่าความน่าจะเป็นของการเกิดเหตุการณ์ต่างๆ ในผลการทดลองเท่ากับ 0.5 ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.3 และกราฟเปรียบเทียบผลการทดลองตามรูปภาพที่ 4.5

ตารางที่ 4.3 ผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ยกับจำนวนยานพาหนะบนโมเดลถนนแบบแมนแฮทตัน

N	Non-Algor	Pseudonym	Mix-Zone	AMOEBA	DLP	REP	PriMS
50	0.47	1.05	1.36	2.01	1.92	2.28	1.28
100	0.64	1.46	1.78	2.56	2.47	2.76	1.80
150	0.85	1.69	1.92	2.94	2.93	3.39	2.01
200	1.07	1.94	2.10	3.49	3.65	3.94	2.24
250	1.18	2.02	2.45	4.02	4.26	4.55	2.67
300	1.26	2.23	2.79	4.76	4.91	5.23	3.04



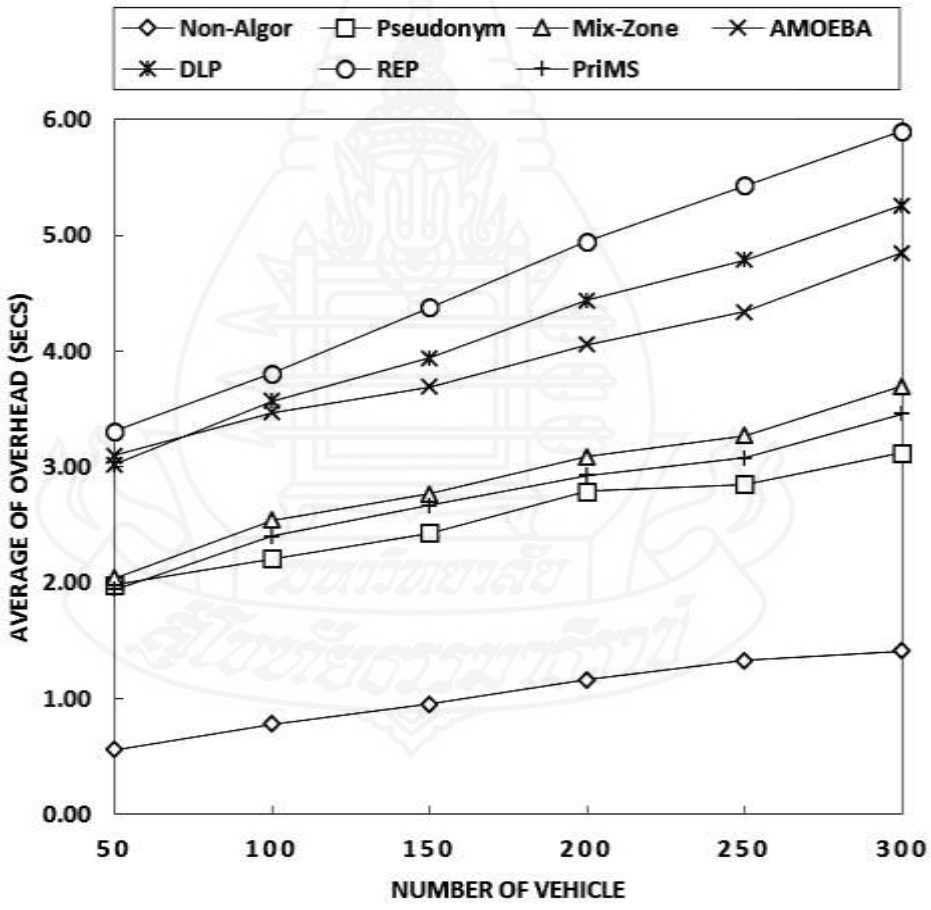
ภาพที่ 4.5 กราฟเปรียบเทียบผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ยกับจำนวนยานพาหนะบนโมเดลถนนแบบแมนแฮทตัน

จากรายละเอียดในตารางที่ 4.3 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.5 นั้นจะเห็นว่าอัลกอริทึมพริมส์ นั้นมีค่าโอเวอร์เฮดเฉลี่ยอยู่ในระดับปานกลาง กล่าวคือค่าโอเวอร์เฮดเฉลี่ยมีค่าที่ต่ำกว่าอัลกอริทึมเรป อัลกอริทึมอะโมอีบา และอัลกอริทึมดีแอลพี แต่สูงกว่าอัลกอริทึมมิกซ์โซน อัลกอริทึมชื่อเทียมและชื่อปลอม และไม่ใช้อัลกอริทึม

2.2.2 ผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ย (Average of Overhead) กับจำนวนยานพาหนะ (Number of Vehicle) บนโมเดลถนนแบบทางอิสระ โดยกำหนดค่าความน่าจะเป็นของการเกิดเหตุการณ์ต่างๆ ในผลการทดลองเท่ากับ 0.5 ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.4 และกราฟเปรียบเทียบผลการทดลองตามรูปภาพที่ 4.6

ตารางที่ 4.4 ผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ยกับจำนวนยานพาหนะบนโมเดลถนนแบบทางอิสระ

N	Non-Algor	Pseudonym	Mix-Zone	AMOEBA	DLP	REP	PriMS
50	0.56	1.98	2.04	3.10	3.02	3.31	1.94
100	0.78	2.21	2.54	3.47	3.57	3.81	2.40
150	0.95	2.43	2.77	3.69	3.94	4.38	2.67
200	1.16	2.79	3.09	4.06	4.44	4.95	2.93
250	1.33	2.85	3.27	4.34	4.79	5.43	3.08
300	1.41	3.12	3.70	4.85	5.26	5.90	3.46



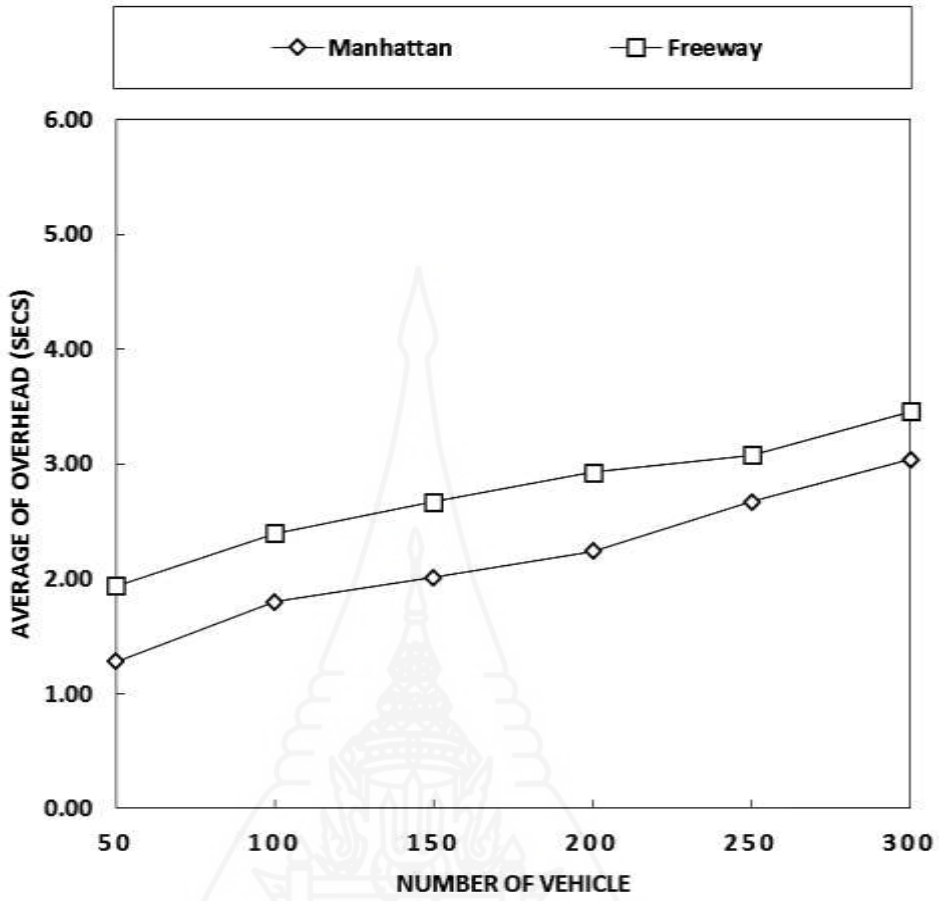
ภาพที่ 4.6 กราฟเปรียบเทียบผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ยกับจำนวนยานพาหนะบนโมเดลถนนแบบทางอิสระ

จากรายละเอียดในตารางที่ 4.4 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.6 นั้นจะเห็นว่าอัลกอริทึมพริมส์ นั้นมีค่าโอเวอร์เฮดเฉลี่ยอยู่ในระดับปานกลางเช่นเดียวกับโมเดลถนนแบบแมนแฮทตันแต่มีค่าโอเวอร์เฮดเฉลี่ยที่ต่ำกว่า กล่าวคือค่าโอเวอร์เฮดเฉลี่ยมีค่าที่ต่ำกว่าอัลกอริทึมเรป อัลกอริทึมอะโมอีบา อัลกอริทึมดีแอลพี และอัลกอริทึมมิกซ์โซน แต่สูงกว่าอัลกอริทึมชื่อเทียมและชื่อปลอม และไม่ใช้อัลกอริทึม

2.2.3 ผลการทดลองเปรียบเทียบระหว่างค่าโอเวอร์เฮดเฉลี่ย (Average of Overhead) กับจำนวนยานพาหนะ (Number of Vehicle) ของโมเดลถนนแบบแมนแฮทตัน และโมเดลถนนแบบทางอิสระในอัลกอริทึมพริมส์ โดยกำหนดค่าความน่าจะเป็นของการเกิดเหตุการณ์ต่างๆ ในผลการทดลองเท่ากับ 0.5 ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.5 และกราฟเปรียบ เทียบผลการทดลองตามรูปภาพที่ 4.7

ตารางที่ 4.5 ผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ยกับจำนวนยานพาหนะของโมเดลถนนแบบแมนแฮทตันและโมเดลถนนแบบทางอิสระในอัลกอริทึมพริมส์

N	Manhattan	Freeway
50	1.28	1.94
100	1.80	2.40
150	2.01	2.67
200	2.24	2.93
250	2.67	3.08
300	3.04	3.46



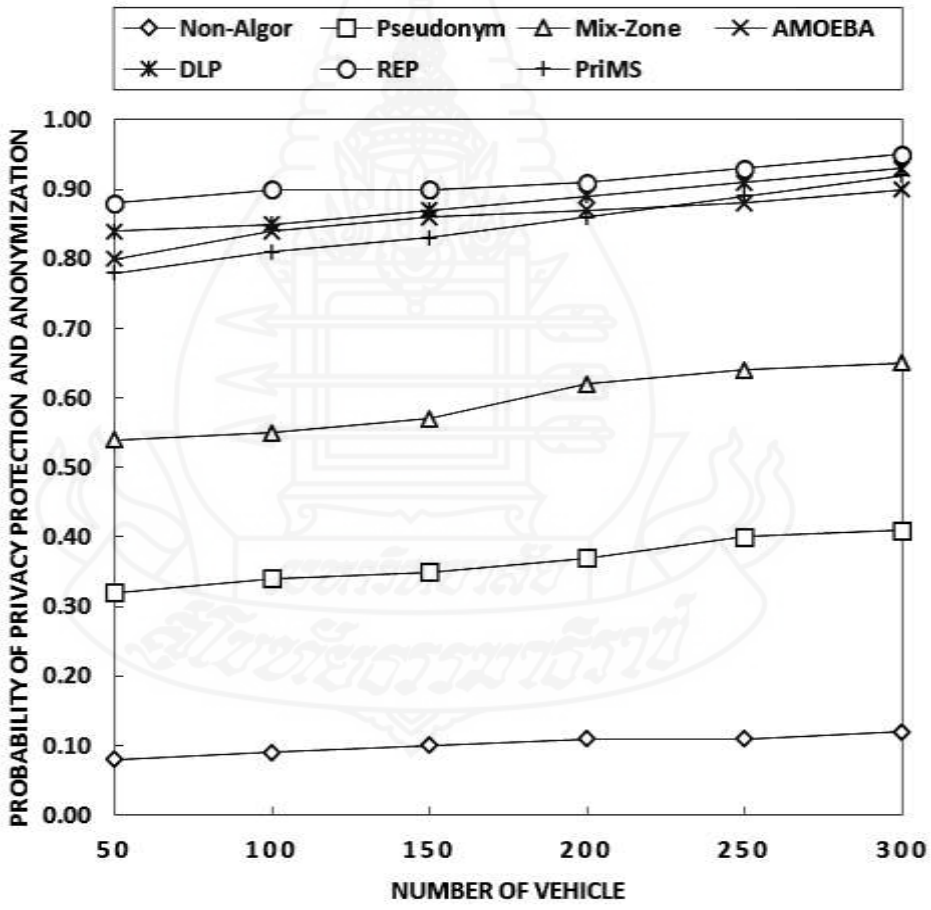
ภาพที่ 4.7 กราฟเปรียบเทียบผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ยกับจำนวนยานพาหนะของโมเดลถนนแบบแมนแฮทตันและโมเดลถนนแบบทางอิสระในอัลกอริทึมพริมส์

จากรายละเอียดในตารางที่ 4.5 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.7 นั้นจะเห็นว่าค่าโอเวอร์เฮดเฉลี่ยของอัลกอริทึมพริมส์ ในโมเดลถนนแบบแมนแฮทตันนั้นมีค่าต่ำกว่าค่าโอเวอร์เฮดเฉลี่ยของอัลกอริทึมพริมส์ ในโมเดลถนนแบบทางอิสระ

2.2.4 ผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัว (Probability of Privacy Protection and Anonymization) กับจำนวนยานพาหนะ (Number of Vehicle) บนโมเดลถนนแบบแมนแฮทตัน โดยกำหนดค่าความน่าจะเป็นของเหตุการณ์ที่อาจถูกเปิดเผยข้อมูลเท่ากับ 0.5 ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.6 และกราฟเปรียบเทียบผลการทดลองตามรูปภาพที่ 4.8

ตารางที่ 4.6 ผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวกับจำนวนยานพาหนะบนโมเดลถนนแบบแมนแฮทตัน

N	Non-Algor	Pseudonym	Mix-Zone	AMOEBA	DLP	REP	PriMS
50	0.08	0.32	0.54	0.80	0.84	0.88	0.78
100	0.09	0.34	0.55	0.84	0.85	0.90	0.81
150	0.10	0.35	0.57	0.86	0.87	0.90	0.83
200	0.11	0.37	0.62	0.87	0.89	0.91	0.86
250	0.11	0.40	0.64	0.88	0.91	0.93	0.89
300	0.12	0.41	0.65	0.90	0.93	0.95	0.92



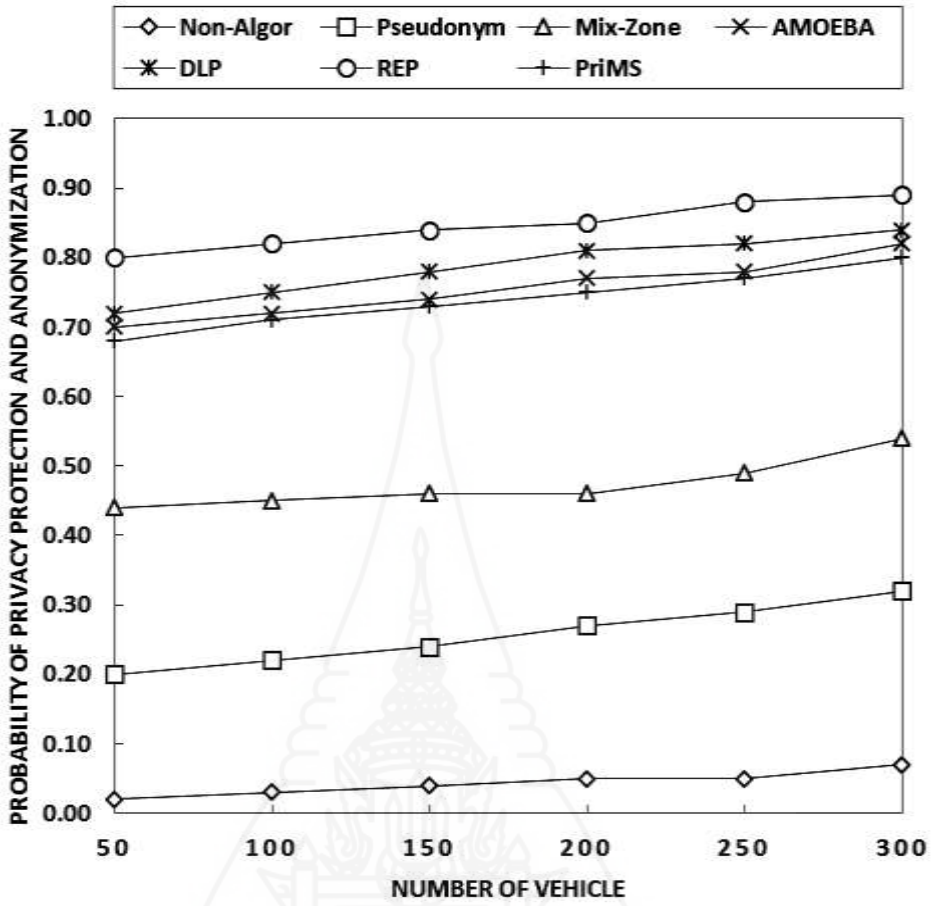
ภาพที่ 4.8 กราฟเปรียบเทียบผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวกับจำนวนยานพาหนะบนโมเดลถนนแบบแมนแฮทตัน

จากรายละเอียดในตารางที่ 4.6 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.8 นั้นจะเห็นว่าอัลกอริทึมพริมส์ นั้นมีค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวอยู่ในกลุ่มสูง ซึ่งมีค่าความน่าจะเป็นใกล้เคียงกับอัลกอริทึมเรป อัลกอริทึมอะโมอีบา และอัลกอริทึมดีแอลพี

2.2.5 ผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัว (Probability of Privacy Protection and Anonymization) กับจำนวนยานพาหนะ (Number of Vehicle) บนโมเดลถนนแบบทางอิสระ โดยกำหนดค่าความน่าจะเป็นของเหตุการณ์ที่อาจถูกเปิดเผยข้อมูลเท่ากับ 0.5 ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.7 และกราฟเปรียบเทียบผลการทดลองตามรูปภาพที่ 4.9

ตารางที่ 4.7 ผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวกับจำนวนยานพาหนะบนโมเดลถนนแบบทางอิสระ

N	Non-Algor	Pseudonym	Mix-Zone	AMOEBA	DLP	REP	PriMS
50	0.02	0.20	0.44	0.70	0.72	0.80	0.68
100	0.03	0.22	0.45	0.72	0.75	0.82	0.71
150	0.04	0.24	0.46	0.74	0.78	0.84	0.73
200	0.05	0.27	0.46	0.77	0.81	0.85	0.75
250	0.05	0.29	0.49	0.78	0.82	0.88	0.77
300	0.07	0.32	0.54	0.82	0.84	0.89	0.80



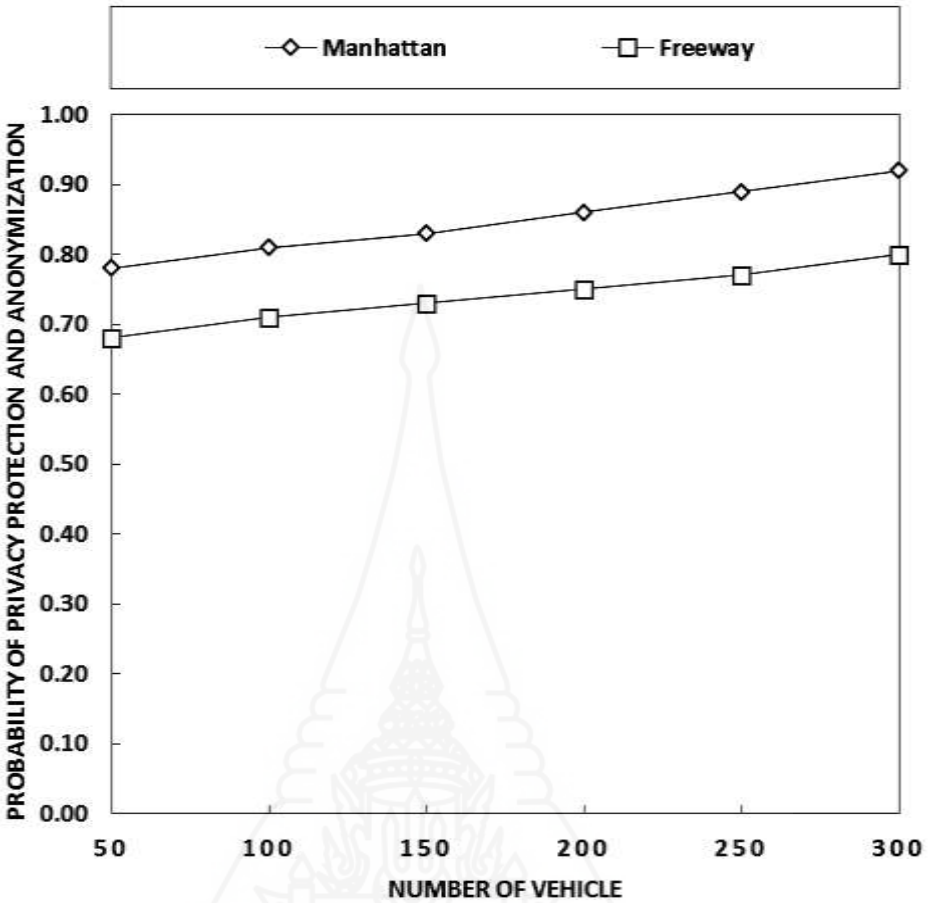
ภาพที่ 4.9 กราฟเปรียบเทียบผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวกับจำนวนยานพาหนะบนโมเดลถนนแบบทางอิสระ

จากรายละเอียดในตารางที่ 4.7 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.9 นั้นจะเห็นว่าอัลกอริทึมพริมส์ นั้นมีค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวอยู่ในกลุ่มสูงเช่นเดียวกับโมเดลถนนแบบแมนแฮทตัน ซึ่งมีค่าใกล้เคียงกับอัลกอริทึมเรป อัลกอริทึมอะโมอีบา และอัลกอริทึมดีแอลพี

2.2.6 ผลการทดลองเปรียบเทียบระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัว (Probability of Privacy Protection and Anonymization) กับจำนวนยานพาหนะ (Number of Vehicle) ของโมเดลถนนแบบแมนแฮทตัน และโมเดลถนนแบบทางอิสระในอัลกอริทึมพริมส์ โดยกำหนดค่าความน่าจะเป็นของเหตุการณ์ที่อาจถูกเปิดเผยข้อมูลเท่ากับ 0.5 ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.8 และกราฟเปรียบ เทียบผลการทดลองตามรูปภาพที่ 4.10

ตารางที่ 4.8 ผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวกับจำนวนยานพาหนะของโมเดลถนนแบบแมนแฮทตันและโมเดลถนนแบบทางอิสระในอัลกอริทึมพริมส์

N	Manhattan	Freeway
50	0.78	0.68
100	0.81	0.71
150	0.83	0.73
200	0.86	0.75
250	0.89	0.77
300	0.92	0.80



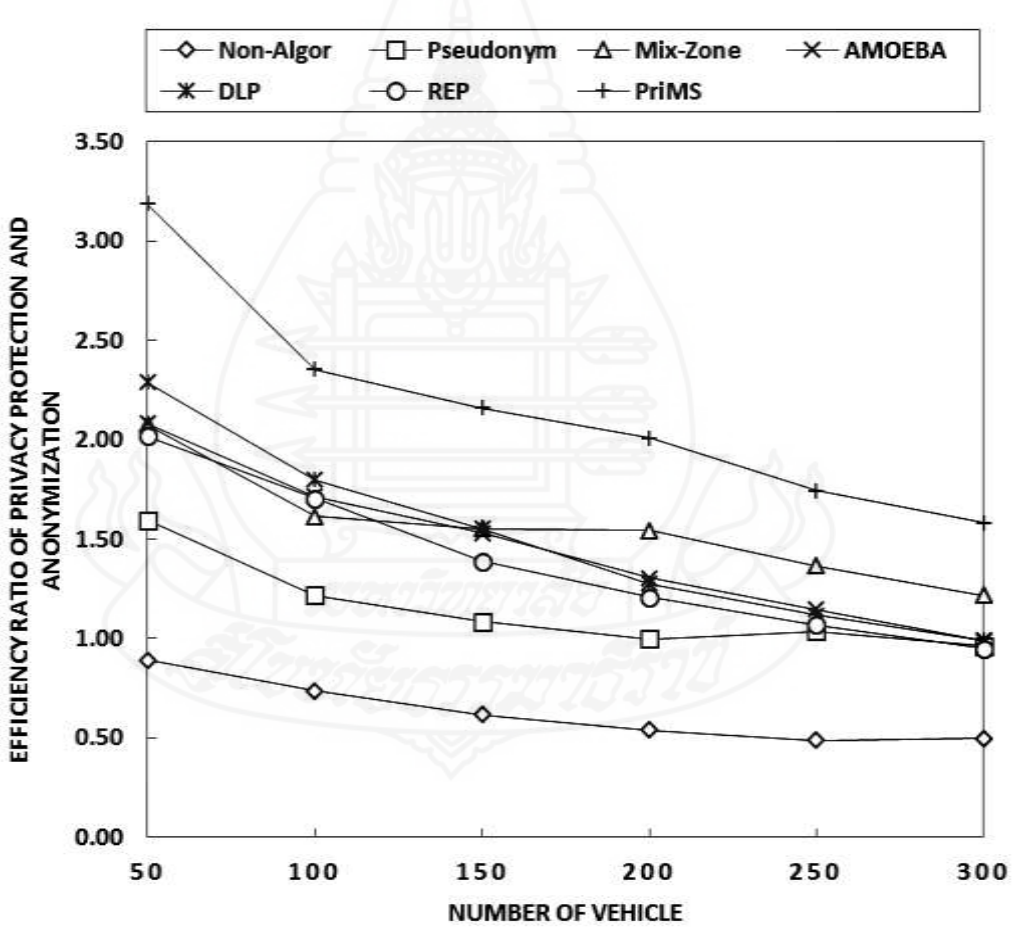
ภาพที่ 4.10 กราฟเปรียบเทียบผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวกับจำนวนยานพาหนะของโมเดลถนนแบบแมนแฮทตันและโมเดลถนนแบบทางอิสระในอัลกอริทึมพริมส์

จากรายละเอียดในตารางที่ 4.8 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.10 นั้นจะเห็นว่าค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวของอัลกอริทึมพริมส์ ในโมเดลถนนแบบแมนแฮทตันนั้นมีค่าสูงกว่าค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวของอัลกอริทึมพริมส์ ในโมเดลถนนแบบทางอิสระ

2.2.7 ผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัว (Efficiency Ratio of Privacy Protection and Anonymization) กับจำนวนยานพาหนะ (Number of Vehicle) บนโมเดลถนนแบบแมนแฮทตัน ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.9 และกราฟเปรียบเทียบผลการทดลองตามรูปภาพที่ 4.11

ตารางที่ 4.9 ผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวกับจำนวนยานพาหนะบนโมเดลถนนแบบแมนแฮทตัน

N	Non-Algor	Pseudonym	Mix-Zone	AMOEBA	DLP	REP	PriMS
50	1.22	1.62	1.72	1.80	1.71	2.35	1.22
100	1.08	1.55	1.53	1.55	1.39	2.16	1.08
150	1.00	1.54	1.30	1.28	1.21	2.01	1.00
200	1.04	1.37	1.14	1.12	1.07	1.74	1.04
250	0.96	1.22	0.99	0.99	0.95	1.58	0.96
300	1.22	1.62	1.72	1.80	1.71	2.35	1.22



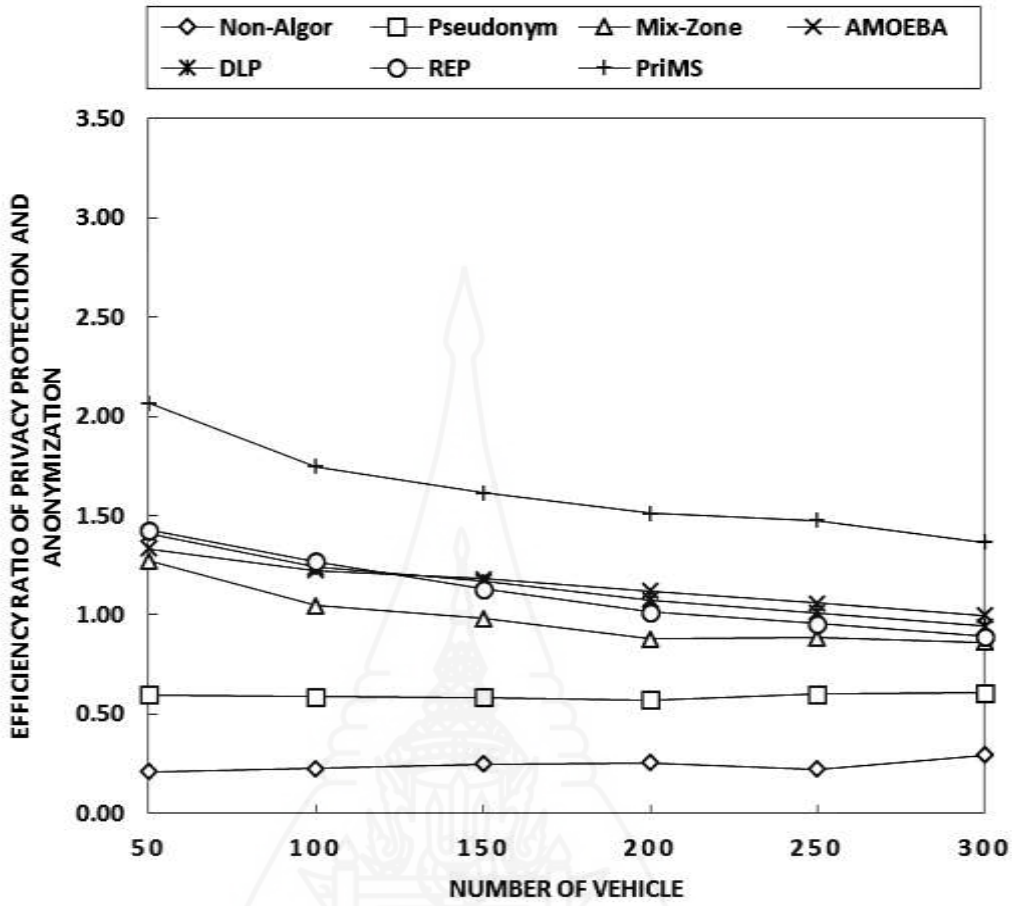
ภาพที่ 4.11 กราฟเปรียบเทียบผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวกับจำนวนยานพาหนะบนโมเดลถนนแบบแมนแฮทตัน

จากรายละเอียดในตารางที่ 4.9 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.11 นั้นจะเห็นว่าอัลกอริทึมพริมส์ นั้นมีค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวสูงที่สุดเมื่อเทียบกับอัลกอริทึมอื่นๆ เพราะอัลกอริทึมพริมส์ มีค่าโอเวอร์เฮดเฉลี่ยที่ต่ำแต่มีค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวที่สูง

2.2.8 ผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัว (Efficiency Ratio of Privacy Protection and Anonymization) กับจำนวนยานพาหนะ (Number of Vehicle) บนโมเดลถนนแบบแบบทางอิสระ ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.10 และกราฟเปรียบเทียบผลการทดลองตามรูปภาพที่ 4.12

ตารางที่ 4.10 ผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวกับจำนวนยานพาหนะบนโมเดลถนนแบบทางอิสระ

N	Non-Algor	Pseudonym	Mix-Zone	AMOEBA	DLP	REP	PriMS
50	0.21	0.60	1.27	1.33	1.41	1.43	2.07
100	0.23	0.59	1.05	1.22	1.24	1.27	1.75
150	0.25	0.58	0.98	1.18	1.17	1.13	1.61
200	0.25	0.57	0.88	1.12	1.08	1.01	1.51
250	0.22	0.60	0.88	1.06	1.01	0.96	1.48
300	0.29	0.61	0.86	1.00	0.94	0.89	1.36



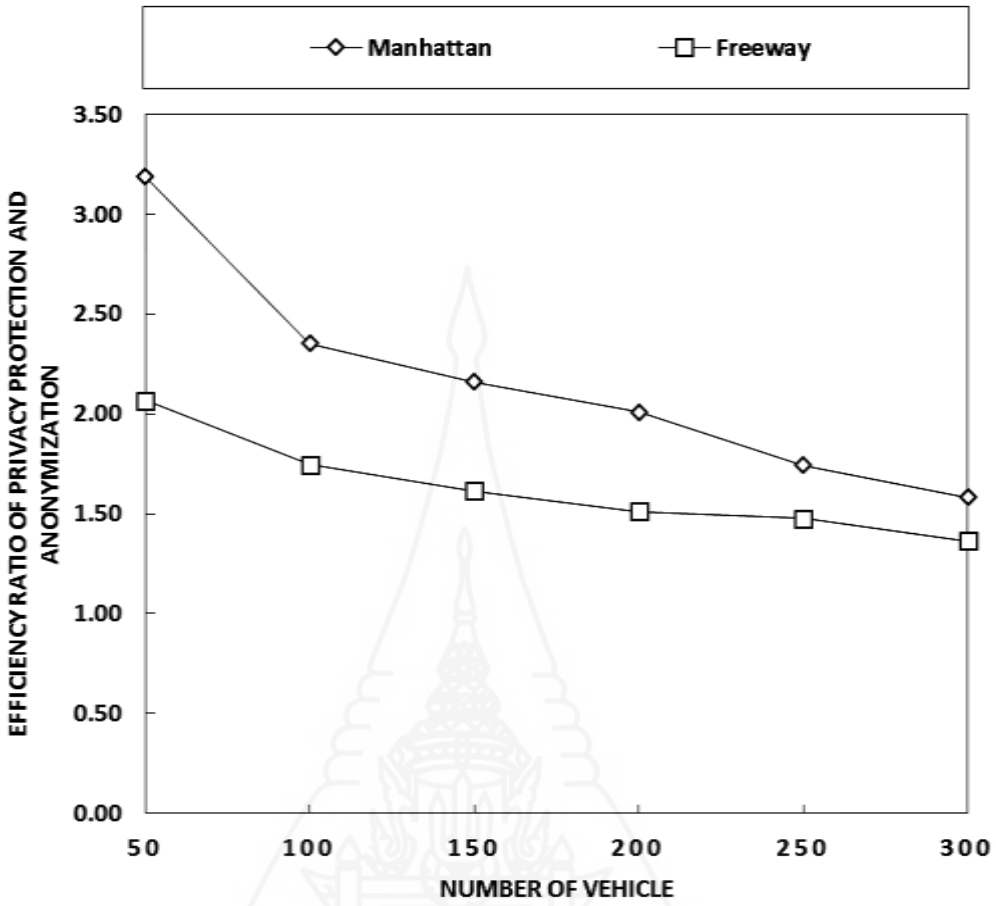
ภาพที่ 4.12 กราฟเปรียบเทียบผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวกับจำนวนยานพาหนะบนโมเดลถนนแบบทางอิสระ

จากรายละเอียดในตารางที่ 4.10 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.12 นั้นจะเห็นว่าอัลกอริทึมพริมส์ นั้นมีค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวสูงที่สุดเมื่อเทียบกับอัลกอริทึมอื่นๆ เช่นเดียวกับโมเดลถนนแบบแมนแฮทตัน เพราะมีค่าโอเวอร์เฮดเฉลี่ยที่ต่ำแต่มีค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวที่สูง

2.2.9 ผลการทดลองเปรียบเทียบระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัว (Efficiency Ratio of Privacy Protection and Anonymization) กับจำนวนยานพาหนะ (Number of Vehicle) ของโมเดลถนนแบบแมนแฮทตัน และโมเดลถนนแบบทางอิสระในอัลกอริทึมพริมส์ ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.11 และกราฟเปรียบ เทียบผลการทดลองตามรูปภาพที่ 4.13

ตารางที่ 4.11 ผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวกับจำนวนยานพาหนะของโมเดลถนนแบบแมนแฮทตันและโมเดลถนนแบบทางอิสระในอัลกอริทึมพริมส์

N	Manhattan	Freeway
50	3.19	2.07
100	2.35	1.75
150	2.16	1.61
200	2.01	1.51
250	1.74	1.48
300	1.58	1.36



ภาพที่ 4.13 กราฟเปรียบเทียบผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวกับจำนวนยานพาหนะของโมเดลถนนแบบแมนแฮทตันและโมเดลถนนแบบทางอิสระในอัลกอริทึมพริมส์

จากรายละเอียดในตารางที่ 4.11 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.13 นั้นจะเห็นว่าค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวของอัลกอริทึมพริมส์ ในโมเดลถนนแบบแมนแฮทตันนั้นมีค่าสูงกว่าค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวของอัลกอริทึมพริมส์ ในโมเดลถนนแบบทางอิสระ

2.3 ผลการทดลองตามแบบจำลองโดยการสมมุติสถานการณ์การสื่อสาร

ในส่วนนี้ได้มีการสมมุติสถานการณ์การสื่อสารของยานพาหนะขึ้นเพื่อใช้วัดค่าประสิทธิภาพในการทำงานของอัลกอริทึมพริมส์ โดยมีรายละเอียดดังต่อไปนี้

2.3.1 สถานการณ์การสื่อสาร

รถของหน่วยกู้ภัยแห่งหนึ่งได้รับแจ้งว่ามีอุบัติเหตุเกิดขึ้นบนถนนสายหนึ่งจึงได้เปิดสัญญาณไซเรนเพื่อเดินทางไปยังจุดเกิดเหตุ โดยระหว่างทางนั้นได้มีการรายงานสถานะของรถ เช่น เลี้ยวซ้าย เลี้ยวขวา รายงานตำแหน่งที่ตั้งทางภูมิศาสตร์ของรถ และยังมีการสื่อสารส่วนบุคคลเพื่อแจ้งข้อมูลผู้ขับขี่รถ และข้อมูลแพทย์และเจ้าหน้าที่ที่ร่วมเดินทางมา จนเมื่อรถมาถึงที่เกิดเหตุได้มีเจ้าหน้าที่ทำการถ่ายรูปภาพเพื่อใช้เก็บหลักฐานต่างๆ แล้วส่งต่อผ่านทางบริการ 3G ไปยังศูนย์ควบคุมการเกิดอุบัติเหตุบนท้องถนน หลังจากนั้นเจ้าหน้าที่ได้นำตัวผู้บาดเจ็บขึ้นรถทันทีเพื่อนำตัวไปส่งโรงพยาบาล โดยตลอดเส้นทางนั้นได้เปิดสัญญาณไซเรนเพื่อแจ้งเตือนและขอทางแก่ผู้ใช้รถใช้ถนนที่ตามเส้นทางที่รถผ่าน

2.3.2 การวิเคราะห์สถานการณ์การสื่อสารตามลำดับเหตุการณ์

การวิเคราะห์สถานการณ์การข้างต้นนั้นมีรายละเอียดตามตารางที่ 4.12 และมีผลการทดลองของค่าโอเวอร์เฮดเฉลี่ย ค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัว และค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวกับจำนวนยานพาหนะดังรายละเอียดดังต่อไปนี้

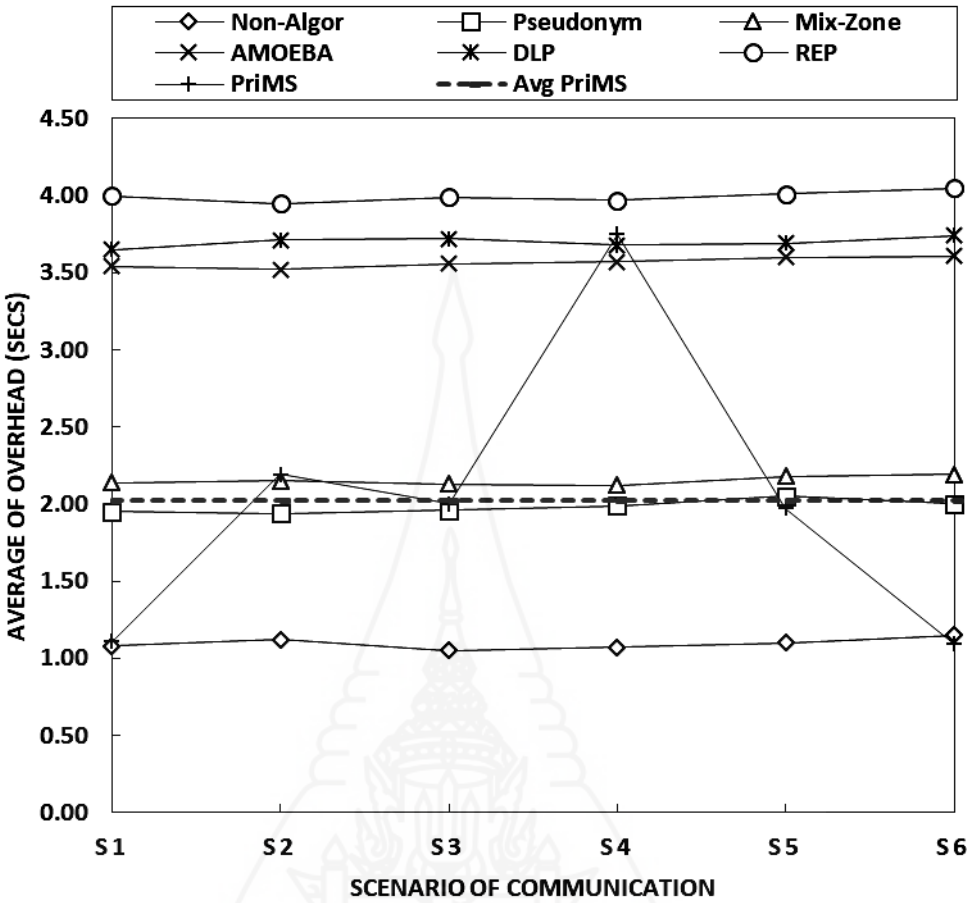
ตารางที่ 4.12 การวิเคราะห์สถานการณ์การสื่อสารตามลำดับเหตุการณ์

สถานการณ์ย่อย	รูปแบบการสื่อสาร	ระดับความเป็นส่วนตัว
S1 เปิดสัญญาณไซเรน	V2I	ระดับต่ำ
S2 แลกเปลี่ยนสถานะของรถให้กับรถคันอื่น	V2V	ระดับปานกลาง
S3 แลกเปลี่ยนตำแหน่งที่ตั้งให้กับรถคันอื่น	V2V	ระดับปานกลาง
S4 การสื่อสารส่วนบุคคลระหว่างรถกับรถ	V2V	ระดับสูง
S5 ส่งรูปภาพผ่านทางบริการ 3G	V2S	ระดับปานกลาง
S6 เปิดสัญญาณไซเรน	V2I	ระดับต่ำ

2.3.3 ผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ยกับสถานการณ์ของการสื่อสารบนโมเดลถนนแบบแมนแฮทตัน โดยกำหนดค่าความน่าจะเป็นของการเกิดเหตุการณ์ต่างๆ ในผลการทดลองเท่ากับ 0.5 ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.13 และกราฟเปรียบเทียบผลการทดลองตามรูปภาพที่ 4.14

ตารางที่ 4.13 ผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ยกับสถานการณ์ของการสื่อสารบนโมเดลถนนแบบแมนแฮทตัน (กำหนดให้ N = 200)

Scenario	**Non-Algor**	**Pseudonym**	**Mix-Zone**	**AMOEBA**	**DLP**	**REP**	**PriMS**
S1	1.08	1.95	2.14	3.54	3.65	4.00	1.11
S2	1.12	1.94	2.15	3.52	3.71	3.95	2.19
S3	1.05	1.96	2.13	3.56	3.72	3.99	2.00
S4	1.07	1.99	2.12	3.57	3.68	3.97	3.75
S5	1.10	2.05	2.18	3.60	3.69	4.01	1.97
S6	1.15	2.00	2.19	3.61	3.74	4.05	1.09
Avg.	1.10	1.98	2.15	3.57	3.70	4.00	2.02



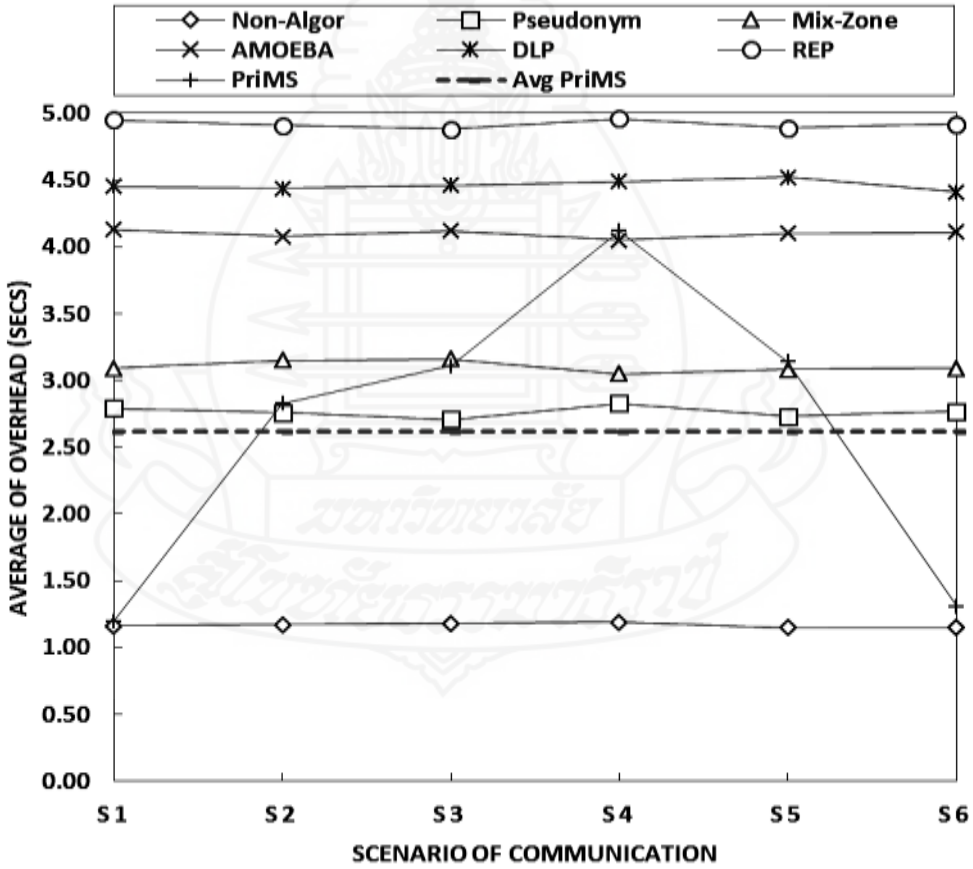
ภาพที่ 4.14 กราฟผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ยกับสถานการณ์ของการสื่อสารบนโมเดลถนนแบบแมนแฮทตัน

จากรายละเอียดในตารางที่ 4.13 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.14 นั้นจะเห็นว่าอัลกอริทึมพริมส์ นั้นมีค่าโอเวอร์เฮดเฉลี่ยอยู่ในระดับต่างๆ ตามสถานการณ์การสื่อสารที่เปลี่ยนแปลงไปอย่างเหมาะสมกับสภาพความเป็นจริงของโมเดลถนนแบบแมนแฮทตัน

2.3.4 ผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ยกับสถานการณ์ของการสื่อสารบนโมเดลถนนแบบทางอิสระ โดยกำหนดค่าความน่าจะเป็นของการเกิดเหตุการณ์ต่างๆ ในผลการทดลองเท่ากับ 0.5 ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.14 และกราฟเปรียบเทียบผลการทดลองตามรูปภาพที่ 4.15

ตารางที่ 4.14 ผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ยกับสถานการณ์ของการสื่อสารบนโมเดลถนนแบบทางอิสระ (กำหนดให้ N = 200)

Scenario	Non-Algor	Pseudonym	Mix-Zone	AMOEBA	DLP	REP	PriMS
S1	1.16	2.79	3.09	4.13	4.45	4.95	1.20
S2	1.17	2.76	3.15	4.08	4.44	4.91	2.83
S3	1.18	2.71	3.16	4.12	4.46	4.88	3.11
S4	1.19	2.83	3.05	4.05	4.49	4.96	4.12
S5	1.15	2.73	3.08	4.10	4.52	4.89	3.14
S6	1.15	2.77	3.09	4.11	4.41	4.92	1.31
Avg.	1.17	2.77	3.10	4.10	4.46	4.92	2.62



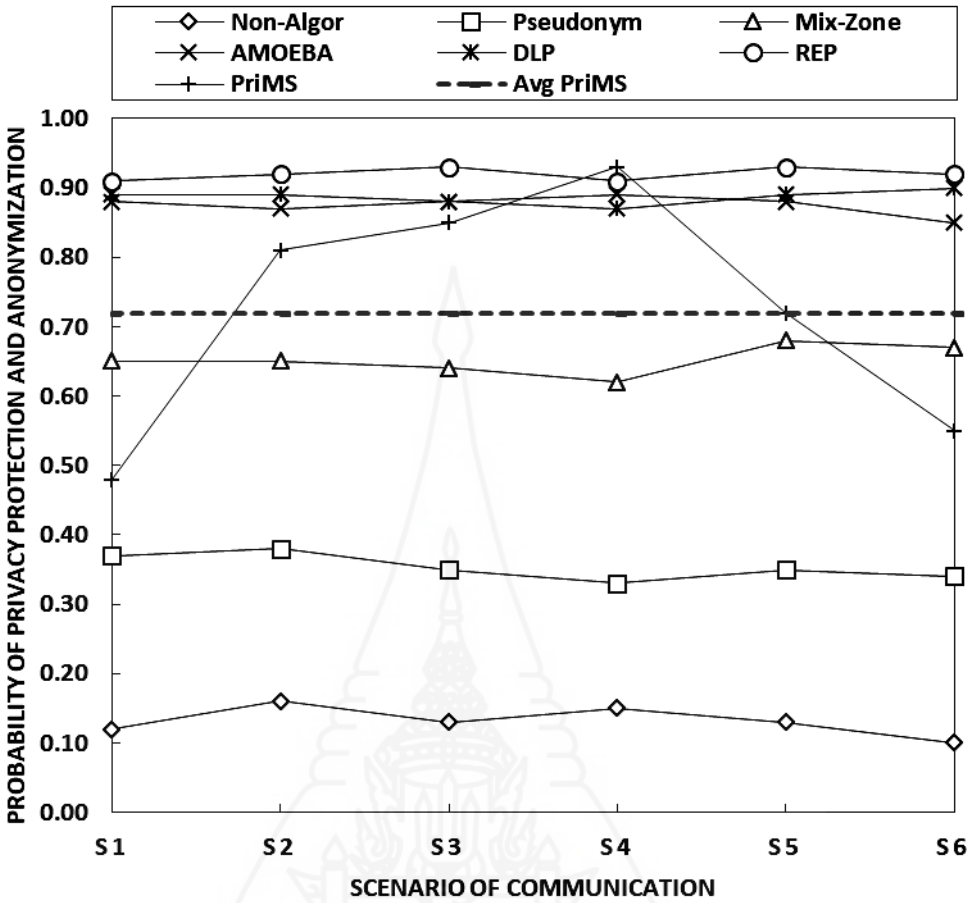
ภาพที่ 4.15 กราฟผลการทดลองระหว่างค่าโอเวอร์เฮดเฉลี่ยกับสถานการณ์ของการสื่อสารบนโมเดลถนนแบบทางอิสระ

จากรายละเอียดในตารางที่ 4.14 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.15 นั้นจะเห็นว่าอัลกอริทึมพริมส์ นั้นมีค่าโอเวอร์เฮดเฉลี่ยอยู่ในระดับต่างๆ ตามสถานการณ์การสื่อสารที่เปลี่ยนแปลงไปอย่างเหมาะสมกับสภาพความเป็นจริงของโมเดลถนนแบบทางอิสระ ซึ่งสอดคล้องกับผลการทดลองของโมเดลถนนแบบแมนแฮทตัน

2.3.5 ผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวกับสถานการณ์ของการสื่อสารบนโมเดลถนนแมนแฮทตัน โดยกำหนดค่าความน่าจะเป็นของการเกิดเหตุการณ์ต่างๆ ในผลการทดลองเท่ากับ 0.5 ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.15 และกราฟเปรียบเทียบผลการทดลองตามรูปภาพที่ 4.16

ตารางที่ 4.15 ผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวกับสถานการณ์ของการสื่อสารบนโมเดลถนนแมนแฮทตัน (กำหนดให้ N = 200)

Scenario	**Non-Algor**	**Pseudonym**	**Mix-Zone**	**AMOEBA**	**DLP**	**REP**	**PriMS**
S1	0.12	0.37	0.65	0.88	0.89	0.91	0.48
S2	0.16	0.38	0.65	0.87	0.89	0.92	0.81
S3	0.13	0.35	0.64	0.88	0.88	0.93	0.85
S4	0.15	0.33	0.62	0.89	0.87	0.91	0.93
S5	0.13	0.35	0.68	0.88	0.89	0.93	0.72
S6	0.10	0.34	0.67	0.85	0.90	0.92	0.55
Avg.	0.13	0.35	0.65	0.88	0.89	0.92	0.72



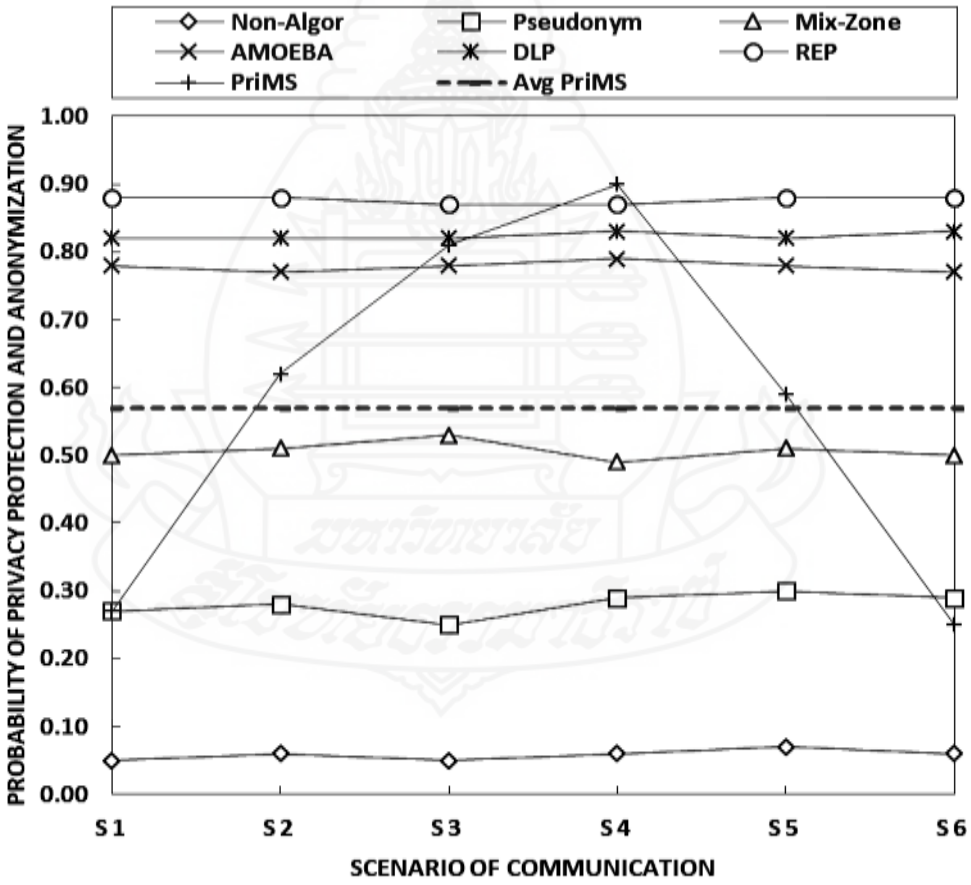
ภาพที่ 4.16 กราฟผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวกับสถานการณ์ของการสื่อสารบนโมเดลถนนแมนแฮทตัน

จากรายละเอียดในตารางที่ 4.15 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.16 นั้นจะเห็นว่าอัลกอริทึมพริมส์ นั้นมีค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวอยู่ในระดับต่างๆ ตามสถานการณ์การสื่อสารที่เปลี่ยนแปลงไปอย่างเหมาะสมกับสภาพความเป็นจริงของโมเดลถนนแบบแมนแฮทตัน

2.3.6 ผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวกับสถานการณ์ของการสื่อสารบนโมเดลถนนแบบทางอิสระ โดยกำหนดค่าความน่าจะเป็นของการเกิดเหตุการณ์ต่างๆ ในผลการทดลองเท่ากับ 0.5 ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.16 และกราฟเปรียบเทียบผลการทดลองตามรูปภาพที่ 4.17

ตารางที่ 4.16 ผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวกับสถานการณ์ของการสื่อสารบนโมเดลถนนแบบทางอิสระ (กำหนดให้ N = 200)

Scenario	Non-Algor	Pseudonym	Mix-Zone	AMOEBA	DLP	REP	PriMS
S1	0.05	0.27	0.50	0.78	0.82	0.88	0.27
S2	0.06	0.28	0.51	0.77	0.82	0.88	0.62
S3	0.05	0.25	0.53	0.78	0.82	0.87	0.81
S4	0.06	0.29	0.49	0.79	0.83	0.87	0.90
S5	0.07	0.30	0.51	0.78	0.82	0.88	0.59
S6	0.06	0.29	0.50	0.77	0.83	0.88	0.25
Avg.	0.06	0.28	0.51	0.78	0.82	0.88	0.57



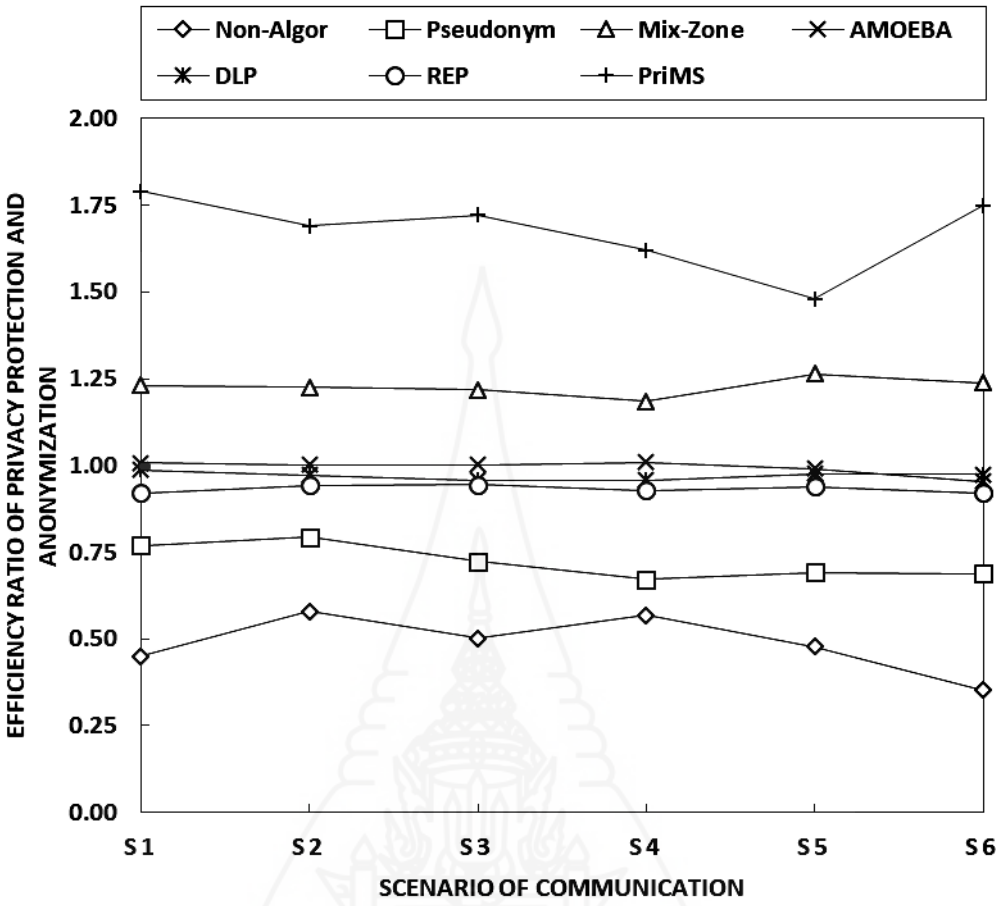
ภาพที่ 4.17 กราฟผลการทดลองระหว่างค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวกับสถานการณ์ของการสื่อสารบนโมเดลถนนแบบทางอิสระ

จากรายละเอียดในตารางที่ 4.16 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.17 นั้นจะเห็นว่าอัลกอริทึมพริมส์ นั้นมีค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวอยู่ในระดับต่างๆ ตามสถานการณ์การสื่อสารที่เปลี่ยนแปลงไปอย่างเหมาะสมกับสภาพความเป็นจริงของโมเดลถนนแบบทางอิสระ ซึ่งสอดคล้องกับผลการทดลองของโมเดลถนนแบบแมนแฮทตัน

2.3.7 ผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวกับสถานการณ์ของการสื่อสารบนโมเดลถนนแมนแฮทตัน โดยกำหนดค่าความน่าจะเป็นของการเกิดเหตุการณ์ต่างๆ ในผลการทดลองเท่ากับ 0.5 ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.17 และกราฟเปรียบเทียบผลการทดลองตามรูปภาพที่ 4.18

ตารางที่ 4.17 ผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวกับสถานการณ์ของการสื่อสารบนโมเดลถนนแมนแฮทตัน (กำหนดให้ N = 200)

Scenario	**Non-Algor**	**Pseudonym**	**Mix-Zone**	**AMOEBA**	**DLP**	**REP**	**PriMS**
S1	0.45	0.77	1.23	1.01	0.99	0.92	1.79
S2	0.58	0.79	1.22	1.00	0.97	0.94	1.69
S3	0.50	0.72	1.22	1.00	0.96	0.94	1.72
S4	0.57	0.67	1.18	1.01	0.96	0.93	1.62
S5	0.48	0.69	1.26	0.99	0.98	0.94	1.48
S6	0.35	0.69	1.24	0.95	0.97	0.92	1.75
Avg.	0.49	0.72	1.23	0.99	0.97	0.93	1.45



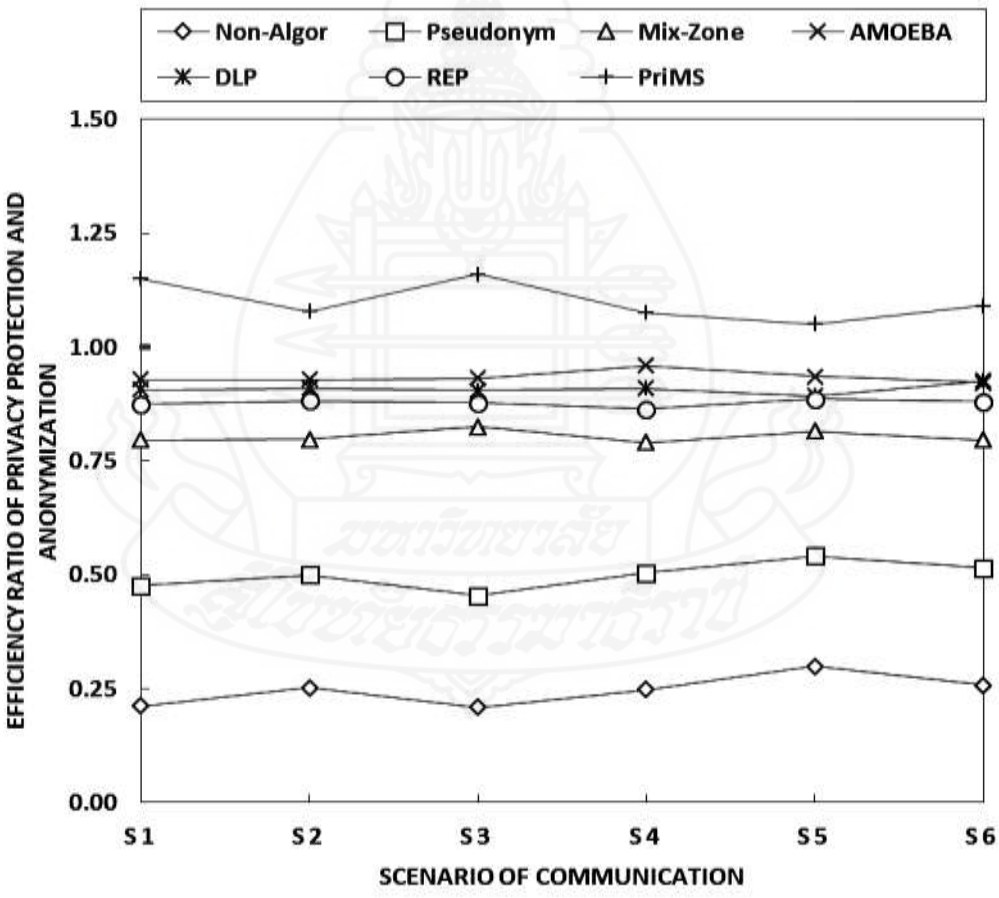
ภาพที่ 4.18 กราฟผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวกับสถานการณ์ของการสื่อสารบนโมเดลถนนแมนแฮทตัน

จากรายละเอียดในตารางที่ 4.17 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.18 นั้นจะเห็นว่าอัลกอริทึมพริมส์นั้นมีค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวบนโมเดลถนนแมนแฮทตันที่สูงที่สุดกว่าอัลกอริทึมอื่นๆ

2.3.8 ผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวกับสถานการณ์ของการสื่อสารบนโมเดลแบบทางอิสระ โดยกำหนดค่าความน่าจะเป็นของการเกิดเหตุการณ์ต่างๆ ในผลการทดลองเท่ากับ 0.5 ซึ่งปรากฏดังรายละเอียดตามตารางที่ 4.18 และกราฟเปรียบเทียบผลการทดลองตามรูปภาพที่ 4.19

ตารางที่ 4.18 ผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวกับสถานการณ์ของการสื่อสารบนโมเดลแบบทางอิสระ (กำหนดให้ N = 200)

Scenario	Non-Algor	Pseudonym	Mix-Zone	AMOEBA	DLP	REP	PriMS
S1	0.21	0.48	0.80	0.93	0.91	0.87	1.15
S2	0.25	0.50	0.80	0.93	0.91	0.88	1.08
S3	0.21	0.45	0.83	0.93	0.90	0.88	1.16
S4	0.25	0.50	0.79	0.96	0.91	0.86	1.07
S5	0.30	0.54	0.81	0.94	0.89	0.89	1.05
S6	0.26	0.52	0.80	0.92	0.93	0.88	1.09
Avg.	0.25	0.50	0.80	0.93	0.91	0.88	1.08



ภาพที่ 4.19 กราฟผลการทดลองระหว่างค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวกับสถานการณ์ของการสื่อสารบนโมเดลแบบทางอิสระ

จากรายละเอียดในตารางที่ 4.18 และกราฟเปรียบเทียบผลการทดลองในรูปภาพที่ 4.19 นั้นจะเห็นว่าอัลกอริทึมพริมส์นั้นมีค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวบนโมเดลถนนแบบทางอิสระที่สูงที่สุดกว่าอัลกอริทึมอื่นๆ ซึ่งสอดคล้องกับผลการทดลองของโมเดลถนนแมนแฮทตัน

จากผลการวัดประสิทธิภาพและวิเคราะห์การทำงานเชิงทฤษฎีและการทำงานเชิงปฏิบัติการจะเห็นได้ว่าค่าโอเวอร์เฮดเฉลี่ยและค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวของอัลกอริทึมพริมส์ มีค่าที่เหมาะสมตามสถานการณ์การสื่อสารของยานพาหนะ และค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวมีค่าที่สูงกว่าอัลกอริทึมอื่นๆ ซึ่งรายละเอียดโดยสรุปจะได้กล่าวไว้ในบทต่อไป

บทที่ 5
สรุปการวิจัย อภิปรายผล และข้อเสนอแนะ

จากการวิเคราะห์ข้อมูลและผลลัพธ์ของการทดลองที่ได้กล่าวไปแล้วในบทก่อนหน้านี้ ต่อไปจะเป็นการสรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ โดยมีรายละเอียดดังต่อไปนี้

1. สรุปการวิจัยและอภิปรายผล

งานวิจัยเรื่องนี้ได้นำเสนออัลกอริทึมการสลับโหมดความเป็นส่วนตัว (Privacy Mode Switching: PriMS) โดยได้กำหนดระดับความเป็นส่วนตัวขึ้นเพื่อใช้ในการปรับเปลี่ยนโหมดความเป็นส่วนตัวไปตามความเหมาะสมสำหรับการป้องกันและปิดบังตำแหน่งที่ตั้ง และข้อมูลที่สำคัญของยานพาหนะในเครือข่ายไร้สายเฉพาะกิจของยานพาหนะ โดยระดับความเป็นส่วนตัวแต่ละระดับนั้นจะมีอัลกอริทึมการป้องกันและปิดบังที่แตกต่างกันตามสถานการณ์จริงซึ่งคัดเลือกจากอัลกอริทึมต่างๆ ที่มีการนำเสนอไปก่อนหน้านี้โดยแบ่งออกเป็น 3 ระดับได้แก่

1) ระดับสูง (High Level) ประกอบไปด้วยอัลกอริทึมแรป อัลกอริทึมอะโมอีบา และอัลกอริทึมดีแอลพี

2) ระดับปานกลาง (Medium Level) ประกอบไปด้วย อัลกอริทึมมิกซ์โซน และอัลกอริทึมรหัสเทียมและรหัสปลอม

3) ระดับต่ำ (Low Level) ประกอบไปด้วย ไม่ใช้อัลกอริทึม

งานวิจัยเรื่องนี้ยังได้กำหนดระดับความเป็นส่วนตัวทั้ง 3 ระดับตามรูปแบบต่างๆ ในการสื่อสารของยานพาหนะ ณ ขณะใดขณะหนึ่ง เพื่อให้สามารถปรับเปลี่ยนไปตามสภาพความเป็นจริงของการสื่อสารได้อย่างเหมาะสม

จากการคำนวณค่าโอเวอร์เฮดตามทฤษฎีพบว่าแนวคิดการสลับโหมดความเป็นส่วนตัวของยานพาหนะภายใต้ระดับความเป็นส่วนตัวที่หลายระดับนี้มีประสิทธิภาพการทำงานที่ดีกว่ากระบวนการป้องกันและปิดบังแบบเดิมที่ใช้เพียงอัลกอริทึมใดอัลกอริทึมหนึ่ง กล่าวคือ ค่าโอเวอร์เฮดเฉลี่ยที่คำนวณได้จะมีค่ามากกว่าการไม่ใช่อัลกอริทึม อัลกอริทึมชื่อเทียมและชื่อปลอม และอัลกอริทึมมิกซ์โซน แต่มีค่าน้อยกว่าอัลกอริทึมดีแอลพี อัลกอริทึมอะโมอีบา และอัลกอริทึมแรป แต่อย่างไรก็ตามผลลัพธ์การทำงานเชิงทฤษฎีของแนวคิดนี้มีความสอดคล้องและเหมาะสมกับความต้องการในความเป็นส่วนตัวในการสื่อสารของยานพาหนะมากกว่าอัลกอริทึมอื่นๆ

จากการคำนวณค่าโอเวอร์เฮดตามการทดลองในระบบจำลองพบว่าแนวคิดการสลับโหมดความเป็นส่วนตัวนี้มีประสิทธิภาพการทำงานที่ดีกว่ากระบวนการป้องกันและปิดบังแบบเดิม ซึ่งสอดคล้องกับผลการทดลองตามทฤษฎี กล่าวคือ ค่าโอเวอร์เฮดเฉลี่ยจากการทดลองในโมเดลถนนแบบแมนแฮทตันและโมเดลถนนแบบเส้นทางอิสระมีค่าอยู่ในระดับปานกลาง แต่ค่าความน่าจะเป็นในการป้องกันและปิดบังความเป็นส่วนตัวอยู่ในระดับสูง และเมื่อคำนวณค่าอัตราประสิทธิภาพในการป้องกันและปิดบังความเป็นส่วนตัวพบว่าแนวคิดการสลับโหมดความเป็นส่วนตัวของงานวิจัยเรื่องนี้มีค่าสูงสุด

2. ข้อเสนอแนะแนวทางการทำวิจัยในอนาคต

ถึงแม้ว่างานวิจัยเรื่องนี้จะปรากฏผลการทดลองได้อย่างเป็นที่น่าพอใจตามที่กล่าวไว้ในหัวข้อก่อนนี้แล้วก็ตาม แต่ก็ยังมีข้อเสนอแนะและแนวทางในการทำวิจัยในอนาคตเพิ่มเติมดังต่อไปนี้

2.1 งานวิจัยเรื่องนี้ยังต้องมีการทดลองเพิ่มเติมในส่วนของการคัดเลือกอัลกอริทึมในกลุ่มความเป็นส่วนตัวระดับสูง และระดับปานกลางเพื่อคัดเลือกอัลกอริทึมที่เหมาะสมกับการสื่อสารของยานพาหนะในลักษณะเฉพาะ เนื่องจากระดับความเป็นส่วนตัวทั้งสองระดับดังกล่าวมีอัลกอริทึมหลายแบบให้เลือกใช้ ซึ่งยังไม่มีการระบุที่ชัดเจนว่าอัลกอริทึมใดควรใช้เมื่อใด โดยงานวิจัยเรื่องนี้ได้ตั้งสมมุติฐานเบื้องต้นเพียงแค่ว่าระดับความเป็นส่วนตัวต่างๆ จะถูกเลือกใช้แบบสุ่มอย่างอิสระ ซึ่งในสภาพความเป็นจริงอาจจะไม่เป็นเช่นนั้นก็ได้

2.2 ปัจจุบันได้มีการนำเสนออัลกอริทึมอื่นๆ ที่ใช้ในการป้องกันและปิดบังความเป็นส่วนตัวอีกหลายอัลกอริทึม ซึ่งงานวิจัยเรื่องนี้ยังไม่ได้นำมาใช้เปรียบเทียบและจัดกลุ่มตามแนวคิดการสลับโหมดความเป็นส่วนตัวและระดับความเป็นส่วนตัวทั้ง 3 ระดับ ซึ่งการทดลองเพิ่มเติมกับอัลกอริทึมที่หลากหลายจะทำให้เห็นถึงผลลัพธ์และประสิทธิภาพการทำงานในภาพรวมของแนวคิดการสลับโหมดความเป็นส่วนตัวของงานวิจัยนี้ได้มากยิ่งขึ้น

ประวัติผู้วิจัย

ชื่อ	ร้อยตำรวจเอก วงศ์ยศ เกิดศรี
วัน เดือน ปีเกิด	13 มิถุนายน 2526
สถานที่เกิด	อำเภอหาดใหญ่ จังหวัดสงขลา
ประวัติการศึกษา	
ระดับปริญญาตรี	ประกอบไปด้วย 9 สาขาได้แก่ วท.บ. (วิทยาการคอมพิวเตอร์) มหาวิทยาลัยสงขลานครินทร์ พ.ศ. 2549 บธ.บ. (การจัดการทั่วไป) มหาวิทยาลัยสุโขทัยธรรมาธิราช พ.ศ. 2551 ศ.บ. (เศรษฐศาสตร์ธุรกิจ) มหาวิทยาลัยสุโขทัยธรรมาธิราช พ.ศ. 2553 ศศ.บ. (สารสนเทศศาสตร์) มหาวิทยาลัยสุโขทัยธรรมาธิราช พ.ศ. 2554 ศศ.บ. (สื่อสารมวลชน) มหาวิทยาลัยรามคำแหง พ.ศ. 2554 ร.บ. มหาวิทยาลัยรามคำแหง พ.ศ. 2555 วท.บ. (เทคโนโลยีสารสนเทศและการสื่อสาร) มหาวิทยาลัยสุโขทัยธรรมาธิราช พ.ศ. 2557 ร.บ. (บริหารงานยุติธรรม) มหาวิทยาลัยรามคำแหง พ.ศ. 2558 รป.บ. (บริหารงานยุติธรรม) มหาวิทยาลัยสุโขทัยธรรมาธิราช พ.ศ. 2559
ระดับปริญญาโท	ประกอบไปด้วย 2 สาขาได้แก่ วท.ม. (วิทยาศาสตร์คอมพิวเตอร์) จุฬาลงกรณ์มหาวิทยาลัย พ.ศ. 2552 บธ.ม. (การตลาด) มหาวิทยาลัยรามคำแหง พ.ศ. 2556
ระดับปริญญาเอก	ประกอบไปด้วย 1 สาขาได้แก่ Ph.D. (Business Administration) IIC University of Technology, Cambodia, 2017
ที่อยู่ปัจจุบัน	5801/100 คาซ่าคอนโด อโศก-ดินแดง ถนนอโศก-ดินแดง แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
สถานที่ทำงาน	ศูนย์เฝ้าระวังและติดตามความเคลื่อนไหวทางสื่อสังคมออนไลน์ (ศฝส.) ตึก 1 ชั้น 20 ศูนย์ปฏิบัติการสำนักงานตำรวจแห่งชาติ (ศปก.ตร.) ถนนพระราม 1 แขวงปทุมวัน เขตปทุมวัน กรุงเทพมหานคร 10330