

## 344-491 สัมมนาวิชาการทางวิทยาการคอมพิวเตอร์

เรื่อง	Exploring The Security Vulnerabilities of LoRa		
ผู้สัมมนา	นาย กอบเดช ภูกลาง		รหัสนักศึกษา 5710210024
	นาย อนุรักษ์ ไทยสงค์		รหัสนักศึกษา 5710210797
วันที่	วันที่ 1 เดือน พฤศจิกายน 2559		เวลา 14.30 – 15.15 น.
สถานที่	ห้อง CS201 ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่		

---

### บทคัดย่อ

ในการเชื่อมต่อสื่อสารข้อมูลในอุปกรณ์ IoT นั้นส่วนใหญ่จะใช้มาตรฐานการสื่อสารหรือโปรโตคอลระยะใกล้เช่น Bluetooth, Wi-Fi หรือ ZigBee ทำให้มีข้อจำกัดด้านระยะทางที่ไม่ไกลมากเท่าที่ต้องการและถึงแม้ว่าจะมีเทคโนโลยี GSM ที่มีระยะการสื่อสารในระยะไกลแต่การสนับสนุนด้านการสื่อสารนั้นจะต้องมีค่าใช้จ่ายสูงโดยเฉลี่ย จึงไม่เหมาะกับการนำมาใช้เท่าที่ควร ดังนั้นเทคโนโลยีไร้สายระยะไกลและ low power wide area networks (LPWAN) จึงได้รับการพัฒนาเพื่อเติมช่องว่างระหว่างโปรโตคอลระยะใกล้และ GSM ซึ่งหนึ่งในนั้นที่กำลังนิยมและเป็นเทคโนโลยีที่ใหม่ก็คือ LoRa เป็นตัวแก้ปัญหาการสื่อสารระยะไกลและเรื่องของการใช้พลังงานที่ต่ำมากๆ ตอบโจทย์ของการด้าน IoT เป็นอย่างมาก

แต่ LoRa เป็นเทคโนโลยีที่ยังค่อนข้างใหม่การใช้งานจึงเห็นปัญหาได้น้อยเพราะยังไม่ได้วิเคราะห์เรื่องความปลอดภัยอย่างจริงจังมากนักซึ่งเป็นปัญหาที่สำคัญก่อนการนำไปใช้จริงกับอุปกรณ์ที่มีความเสี่ยงและต้องการความปลอดภัยสูง เพื่อป้องกันข้อผิดพลาดอันจะเกิดขึ้นในอนาคต เมื่อนำเทคโนโลยีเครือข่ายและอุปกรณ์ ของ LoRa มาใช้งานจริง

ในบทความนี้ผู้เขียนจะอธิบายถึงคุณสมบัติและลักษณะเฉพาะของเทคโนโลยี LoRa เพื่อการวิเคราะห์ช่องโหว่ใหม่ๆ ต่อการโจมตีด้านความปลอดภัย ซึ่งการตรวจสอบช่องโหว่ด้านความปลอดภัยที่อาจเกิดขึ้นใน LoRa นั้นจะวิเคราะห์เฉพาะเครือข่าย LoRa และช่องโหว่ในอุปกรณ์ LoRa ต่อการโจมตีที่แตกต่างกัน ซึ่งการวิเคราะห์ของบทความจะแสดงให้เห็นว่า การส่งข้อมูลระยะไกลของ LoRa มีความเสี่ยงที่จะเกิดการโจมตีด้านความปลอดภัยขึ้นในหลายกรณีและมีกรณีใดบ้าง

---

### เอกสารอ้างอิง

Emekcan Aras, Gowri Sankar Ramachandran, Piers Lawrence and Danny HughesiMinds - DistriNet, KU Leuven, 3001 Leuven, Belgium. Exploring The Security Vulnerabilities of LoRa. จาก <http://ieeexplore.ieee.org/document/7985777/?reload=true>