บทคัดย่อ

ความปลอดภัยในระบบไวร์เลสเซ็นเซอร์เนตเวิร์คมีความท้าทายเป็นอย่างยิ่ง เนื่องจากความแตกต่างของระบบไวร์เลสเซ็นเซอร์เนตเวิร์ค กับระบบเนตเวิร์คแบบปรกติที่เราใช้อยู่ในปัจจุบัน ข้อแตกต่างที่กล่าวมานี้มีอยู่ 2 ประการหลักๆ คือ ประการแรกไวร์เลสเซ็นเซอร์มีข้อจำกัดในเรื่องของทรัพยากรในหลายๆ ด้าน เช่น พลังงาน (พลังงานจากแหล่งจ่าย), ความสามารถของตัวประมวลผล และความจุของช่องสื่อสาร ประการที่สองคือ ไวร์เลสเซ็นเซอร์มีความเสี่ยงต่อการถูกโจมตีทางกายภาพ เช่นการถูกยึดครองหรือดัดแปลงโหนด ดังนั้นการรักษาความปลอดภัยด้วยการเข้ารหัสข้อมูลเพียงอย่างเดียวจึงไม่เพียงพอ ในระบบไวร์เลสเซ็นเซอร์เนตเวิร์คเราควรที่จะมีระบบในการตรวจจับผู้บุกรุกด้วย และวิธีตรวจจับนี้จะต้องใช้ทรัพยากรในระบบไม่มากจนเกินไป เพราะด้วยข้อจำกัดของไวร์เลสเซ็นเซอร์เนตเวิร์คดังที่กล่าวมาในขั้นต้น

โครงงานนี้จึงมีเป้าหมายที่จะพัฒนาความปลอดภัยในระบบไวร์เลสเซ็นเซอร์เนตเวิร์ค (Security System for WSNs) ที่ใช้ทรัพยากรเพียงเล็กน้อย โดยสามารถตรวจจับการโจมตีแบบซิงค์โฮลได้เป็นหลัก (Sinkhole) บนพื้นฐานการทำงานของ ค่าความแรงของสัญญาณของข้อมูลที่ได้รับ (Received Signal Strength Indicator: RSSI) ซึ่งวิธีตรวจจับนี้ต้องใช้การทำงานร่วมกับโหนดตรวจสอบพิเศษ (Extra Monitor: EM) ซึ่งแยกออกมาจากโหนดต่างๆ โดยเรานำค่าความแรงของสัญญาณของข้อมูลที่ได้รับ (RSSI) ที่ส่งมาจาก EM โหนดจำนวน 4 โหนด มาคำนวณหาตำแหน่งของไวร์เลสเซ็นเซอร์ทั้งหมดในระบบ โดยกำหนดให้เบสสเตชั่นเป็นจุดเริ่มต้น (0,0) โดยในที่นี้เราจะทดลองการทำงานทั้งหมดผ่านโปรแกรมจำลองการทำงาน (Simulator) เพื่อทดสอบว่าการตรวจจับวิธีนี้จะมีความแม่นยำสูงเพียงใด