

บทคัดย่อ

ความปลอดภัยในระบบเครือข่ายเซ็นเซอร์แบบไร้สายมีความท้าทายเป็นอย่างยิ่ง เนื่องจากความแตกต่างของระบบเครือข่ายเซ็นเซอร์แบบไร้สาย กับระบบเนตเวิร์คแบบปกติที่เราใช้อยู่ในปัจจุบัน ข้อแตกต่างที่กล่าวมานี้มีอยู่ 2 ประการหลักๆ คือ ประการแรกเซ็นเซอร์แบบไร้สายมีข้อจำกัดในเรื่องของทรัพยากรในหลายๆ ด้าน เช่น พลังงาน (พลังงานจากแหล่งจ่าย), ความสามารถของตัวประมวลผล และความจุของช่องสื่อสาร ประการที่สองคือ เซ็นเซอร์แบบไร้สายมีความเสี่ยงต่อการถูกโจมตีทางกายภาพ เช่น การถูกยึดครอง หรือดัดแปลงโหนด ดังนั้นการรักษาความปลอดภัยด้วยการเข้ารหัสข้อมูลเพียงอย่างเดียวจึงไม่เพียงพอ ในระบบเครือข่ายเซ็นเซอร์แบบไร้สายเราควรที่จะมีระบบในการตรวจจับผู้บุกรุกด้วย และวิธีตรวจจับนี้จะต้องใช้ทรัพยากรในระบบไม่มากเกินไป เพราะด้วยข้อจำกัดของเครือข่ายเซ็นเซอร์แบบไร้สายดังที่กล่าวมาในข้างต้น

โครงการนี้จึงมีเป้าหมายที่จะพัฒนาความปลอดภัยในระบบเครือข่ายเซ็นเซอร์แบบไร้สาย (Security System for WSNs) ที่ใช้ทรัพยากรเพียงเล็กน้อย โดยสามารถตรวจจับการโจมตีแบบ Sinkhole และ Selective Forward ได้เป็นหลัก บนพื้นฐานการทำงานของค่าความแรงของสัญญาณของข้อมูลที่ได้รับ (Received Signal Strength Indicator: RSSI) ซึ่งวิธีการตรวจจับนี้ต้องใช้การทำงานร่วมกับโหนดตรวจจับพิเศษ (Extra Monitor: EM) ซึ่งแยกออกมาจากโหนดต่างๆ โดยเรานำค่าความแรงของสัญญาณของข้อมูลที่ได้รับ (RSSI) ที่ส่งมาจาก EM โหนดจำนวน 4 โหนด มาคำนวณหาตำแหน่งของเซ็นเซอร์แบบไร้สายทั้งหมดในระบบ โดยกำหนดให้เบสสเตชันเป็นจุดเริ่มต้น (0,0) โดยในที่นี้เราจะทดลองการทำงานทั้งหมดผ่านโปรแกรมจำลองการทำงาน (Simulator) เพื่อทดสอบว่าการตรวจจับวิธีนี้จะมีความแม่นยำสูง