บทที่ 5

สรุปผลการศึกษา

งานวิจัยนี้นำเสนอระบบ Detecting and Slowing Down Spam E-mail System (DSDSE) เพื่อลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจากเครื่องที่เป็นบอตเน็ต โดยประยุกต์เทคนิคการตรวจสอบบอตเน็ตจากพฤติกรรมการสอบถามข้อมูล Domain Name ผ่านระบบ Domain Name System (DNS) และเทคนิคการตรวจสอบความผิดปรกติในการส่งจดหมายอิเล็กทรอนิกส์ มาวิเคราะห์ร่วมกัน เมื่อพบสิ่งผิดปรกติตามเงื่อนไขที่กำหนด ระบบจะทำการควบคุม Bandwidth ตามประวัติการใช้งานก่อนหน้านั้น จากผลการทดลองพบว่าระบบ DSDSE สามารถตรวจพบเครื่องที่เป็นบอตเน็ตที่กำลังส่งจดหมายอิเล็กทรอนิกส์สแปม และสามารถลดปริมาณการส่งออกจดหมายอิเล็กทรอนิกส์สแปมได้ เมื่อเปรียบเทียบกับปริมาณข้อมูลก่อนการติดตั้งระบบ DSDSE

5.1 สรุปผลการทดสอบสมมุติฐาน

สรุปผลสมมุติฐาน จำนวน 2 ข้อ จากผลลัพธ์ และผลการทดสอบสมมุติฐานในบทที่ 4 ดังนี้

5.1.1 สรุปผลการทดสอบสมมุติฐานที่ 1

สมมุติฐานที่ 1 กล่าวไว้ว่า “พฤติกรรมการสอบถามข้อมูล Domain Name เดียวกันของกลุ่มเครื่องคอมพิวเตอร์ ผ่านระบบ DNS และความผิดปรกติในการส่งจดหมายอิเล็กทรอนิกส์สามารถระบุได้ว่าเป็นพฤติกรรมของบอตเน็ตที่ส่งจดหมายอิเล็กทรอนิกส์สแปม” จากแนวคิดของ Choi ในการตรวจสอบกลุ่มเครื่องที่มีพฤติกรรมการร้องขอให้ตรวจสอบ Domain Name เดียวกันจากระบบ DNS มีความสัมพันธ์กับกลุ่มเครื่องคอมพิวเตอร์ที่เป็นบอตเน็ต ซึ่งกำลังติดต่อกับ Domain Name นั้น เพื่อรอรับคำสั่งในการทำงาน ร่วมกับการพิจารณาความผิดปรกติของการส่งจดหมายอิเล็กทรอนิกส์โดยอาศัยค่า Threshold ที่เหมาะสม สามารถระบุได้ว่าเครื่องใดที่เป็นบอตเน็ตและกำลังส่งจดหมายอิเล็กทรอนิกส์สแปม

5.1.2 **สรุปผลการทดสอบสมมุติฐานที่** 2

สมมุติฐานที่ 2 กล่าวไว้ว่า"การลดอัตราการส่งข้อมูลภายใน Bandwidth ของเครื่องที่ระบุว่าเป็นบอตเน็ตและมีพฤติกรรมส่งจดหมายอิเล็กทรอนิกส์สแปม สามารถช่วยลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมได้" เมื่อพิจารณากราฟผลลัพธ์การควบคุม Bandwidth ในบทที่ 4 ทั้ง 3 รูปแบบ พบว่าระบบ DSDSE สามารถทำการลดอัตราการส่งออกจดหมายอิเล็กทรอนิกส์สแปม ได้ทั้ง 3 วิธี ซึ่งระบบที่พัฒนาขึ้นช่วยให้มีการนำ Bandwidth ส่วนที่สูญเสียไปจากการใช้งานในการส่งจดหมายอิเล็กทรอนิกส์สแปมกลับคืนมาใช้ให้เป็นประโยชน์ด้านอื่นต่อไปได้

5.2 **ข้อเสนอแนะแนวทางการพัฒนาต่อ**

สำหรับงานวิจัยในอนาคตควรที่จะทำการศึกษาเพิ่มเติม คือ เรื่องการหานโยบายการลดอัตรา Bandwidth ในปริมาณที่เหมาะสมกับเครือข่ายในลักษณะต่างๆ ซึ่งจะช่วยให้ระบบการใช้งานเครือข่ายมีภาพรวมการใช้งานที่ดีขึ้น แม้ว่าระบบกำลังประสบปัญหาอยู่ก็ตาม