1. บทคัดย่อ

ในปัจจุบันเครือข่ายอุปกรณ์ส่งสัญญาณได้รับความสนใจเป็นอย่างมาก เนื่องจากหน่วยประมวลผลขนาดเล็กมีราคาต่ำลง จึงมีการติดตั้งหน่วยประมวลผลบนอุปกรณ์ส่งสัญญาณชนิดต่าง ๆ เพื่อให้อุปกรณ์เหล่านี้ทำงานร่วมกันได้ในระบบต่าง ๆ เช่น ระบบควบคุมสัญญาณจราจร ระบบเฝ้าสังเกตสภาวะแวดล้อม ระบบพยากรณ์อากาศ ฯลฯ ลักษณะสำคัญประการหนึ่งของหลายระบบที่มีการนำอุปกรณ์ส่งสัญญาณมาใช้คือ ระบบเหล่านี้จะมีการกระจายอุปกรณ์ส่งสัญญาณไว้ในพื้นที่ที่สนใจศึกษาเพื่อให้อุปกรณ์เหล่านี้เก็บข้อมูลต่าง ๆ เพื่อนำไปทำการวิเคราะห์ต่อไป เป็นที่แน่นอนว่า ในระบบที่มีภารกิจที่สำคัญนั้น ควรมีการยืนยันความน่าเชื่อถือของข้อมูลเหล่านี้ (เช่น ในระบบที่ใช้ในทางการทหาร หรือในระบบวัดสภาวะแวดล้อมในโรงงานปฏิกรณ์ปรมาณู) การปกป้องข้อมูลเหล่านี้ จำเป็นต้องพึ่งพาเทคโนโลยีในทางศาสตร์แห่งการสื่อสารอย่างปลอดภัยเป็นอย่างยิ่ง ความท้าทายที่สำคัญอย่างหนึ่งคือ การนำเทคโนโลยีเหล่านี้มาปรับใช้ในระบบที่มีการใช้อุปกรณ์ส่งสัญญาณที่มีหน่วยประมวลผลขนาดเล็กและมีความสามารถจำกัด ในโครงการนี้ คณะผู้วิจัยได้ทำการออกแบบวิธีการและโปรโตคอลที่สามารถนำมาใช้ในระบบอุปกรณ์ส่งสัญญาณได้ วิธีการและโปรโตคอลที่ออกแบบได้แก่ รหัสยืนยันความแท้จริงของข้อมูลแบบนิรนาม ระบบแคพช่า และระบบลายเซ็นอิเล็กทรอนิกส์แบบผลรวม โดยทั้งสามสิ่งนี้ มีการทำงานที่มีประสิทธิภาพ อีกทั้งทางคณะผู้วิจัยยังได้เขียนข้อพิสูจน์ทางคณิตศาสตร์ เพื่อยืนยันว่าระบบเหล่านี้ให้ความปลอดภัยในการทำงานได้จริงอีกด้วย

คำสำคัญ: ศาสตร์แห่งการสื่อสารอย่างปลอดภัย การพิสูจน์ความปลอดภัย รหัสยืนยันความแท้จริงของข้อมูล แคพช่า ลายเซ็นอิเล็กทรอนิกส์ อุปกรณ์ส่งสัญญาณ

Abstract

There has been much interest in sensor network applications in recent years. With decreasing prices of processors as one of the major driving forces, many applications now equip sensors with processors and let them cooperate to achieve a common goal. Applications of this type include traffic control, eco-system monitoring, and forecasting systems. The most common applications involve scattering sensors in some environment so that they can gather data for further analysis. Clearly, in mission-critical applications, it is undesirable to gather data that are unreliable or potentially-corrupt (maliciously or otherwise). The need to protect information communicated among the sensors can only be addressed by cryptography. The challenge is to adapt cryptographic technology to the special needs of sensor network applications. Under this grant, we have designed schemes and protocols that can be applied to sensor network applications. The schemes and protocols we investigated are blind message authentication codes, CAPTCHAs (Completely Automated Public Turing tests to tell Computers and Humans Apart), and aggregate signatures. The proposed schemes and protocols are not only efficient but also provably secure.

Keywords: cryptography, security proofs, message authentication codes, CAPTCHAs, digital signatures, sensor networks