XÁC THỰC DỰA TRÊN CHỨNG MINH KHÔNG CÓ KIẾN THỨC THẾ HỆ TIẾP THEO CHO MẠNG CẢM BIẾN KHÔNG DÂY SỬ DỤNG GIẢI PHÁP DỰA TRÊN LƯỚI

Vũ Anh Hào

Trường Đại học Công nghệ Thông tin - Đại học Quốc gia TP.HCM

What ?

Đề xuất một mô hình bảo mật trong quá trình xác thực giữa các nút cảm biến và trạm của mạng cảm biến không dây. Trong đó sử dụng là Zero-knowledge Proof dựa trên giải pháp lưới (lattice-based) để đảm bảo an toàn cho hệ thống xác thực trước những mối đe dọa của tấn công bình thường và tấn công lượng tử.

Why ?

Những thách thức trong việc bảo mật hệ thống mạng cảm biến không dây, đặc biệt là quá trình xác thực các nút cảm biến.

Chống lại các cuộc tấn công giả mạo, nghe lén và phá khóa bằng các kỹ thuật tấn công lượng tử.

Overview

Trong hệ thống mạng cảm biến không dây nút cảm biến rất dễ bị tấn công. Do đó, quá trình xác thực đóng vai trò quan trọng trong việc định danh và phát hiện những tấn công giả mạo vào hệ thống.

Zero-knowledge Proof (ZKP) có thể giải quyết được nhiều vấn đề bảo mật của WSN. Các giải pháp dựa trên lưới (lattice-based) có thể ngăn chặn các cuộc tấn công lượng tử.

ZKP dựa trên lattice-based được xem là state-of-the-art trong việc chống lại các tấn công từ máy tính thông thường và máy tính lượng tử và trở thành một lựa chọn an toàn và bền vững trong IoT và WSN.

Description

Mô hình bảo mật cho hệ thống Mạng cảm biến không dây

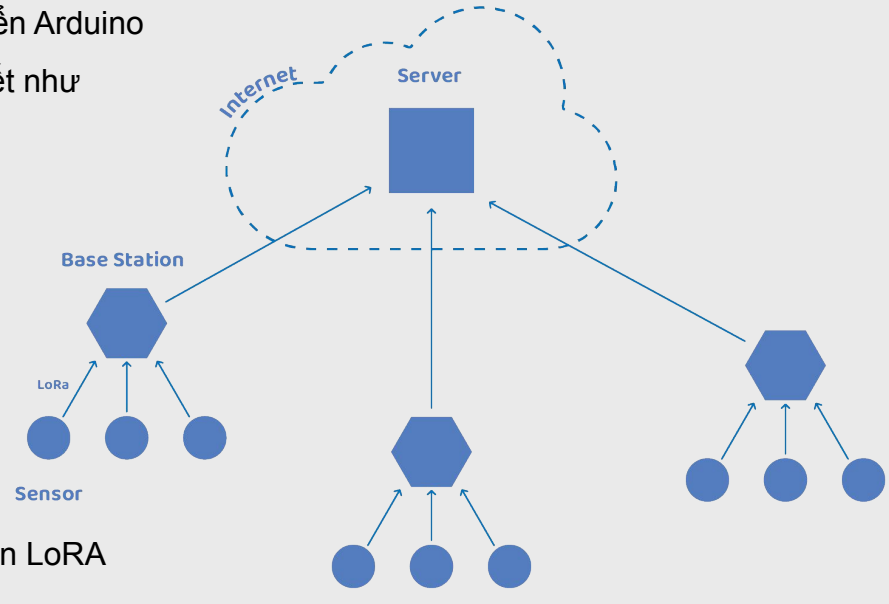
Mạng cảm biến không dây thu thập thông tin thời tiết bao gồm các nút cảm biến, trạm (base station) và máy chủ trung tâm.

Nút cảm biến sử dụng mạch điều khiển Arduino được kết nối với các cảm biến thời tiết như nhiệt độ, độ ẩm, lượng mưa,...

Các nút cảm biến cần mang thông tin định danh (id), fingerprint của chính nó và một số thông tin về các nút lân cận nhằm phục vụ cho việc chứng minh

Giao tiếp với trạm thông qua bộ truyền LoRA

Trạm là một bộ máy tính mini Raspberry PI, có chức năng xác thực các nút cảm biến kết nối trực tiếp tới trạm



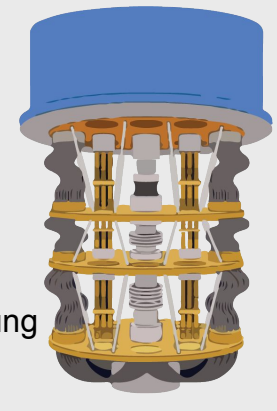
Đánh giá hiệu quả

Ngăn chặn các cuộc tấn công thường thấy

- Clone Attack
- Man-In-The-Middle Attack
- Replay Attack

Ngăn chặn các cuộc tấn công lượng tử

- Sử dụng các phương trình toán để phân tích, chứng minh tính đúng đắn của hệ thống khi đối mặt với các cuộc tấn công lượng tử.



NII

Vũ Anh Hào – Trường Đại học Công nghệ Thông tin - Đại học Quốc gia TP.HCM
TEL : 0338 929 592 Email : haova.17@grad.uit.edu.vn