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 - 220202014

Tóm tắt

- **Lớp: CS2205.CH1702**
- **Link Github:** https://github.com/haova/CS2205.APR2023
- **Link YouTube video:** https://youtu.be/A6guSq1apTA
- **Họ và Tên: Vũ Anh Hào**

Giới thiệu

Sự gia tăng các nguy cơ mất an toàn thông tin trong IoT và WSN.

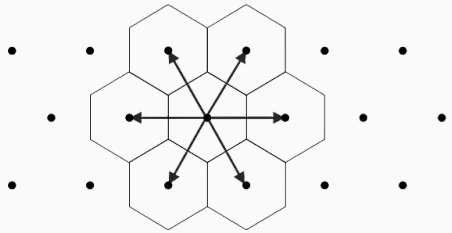
Cần những kỹ thuật xác thực vừa gọn nhẹ lại vừa đảm bảo an toàn.

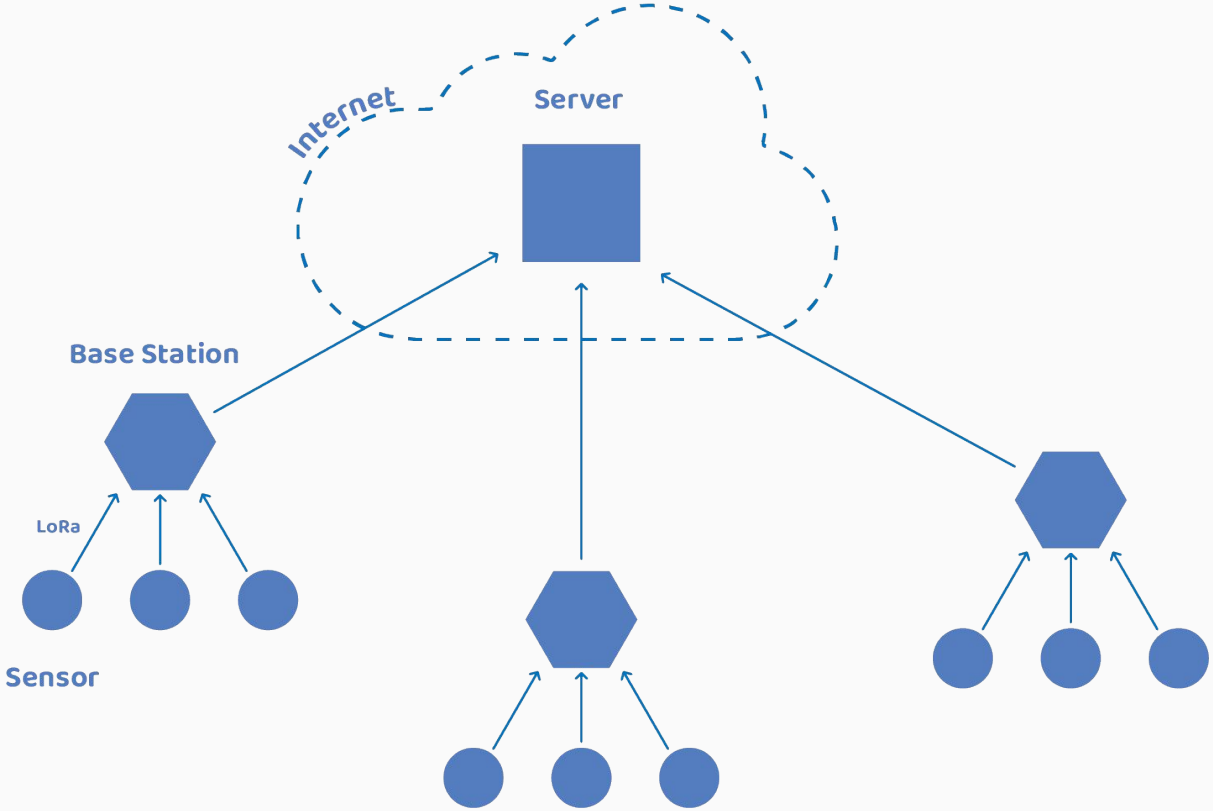
Wireless Sensor Network Security

- **Data**
  - Confidentiality
  - Integrity
- **Communication channel**
  - Security architecture
  - Key management system
- **Sensors**
  - Authentication
  - Access control

Giới thiệu

- 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.
- Zero-knowledge Proof lattice-based.





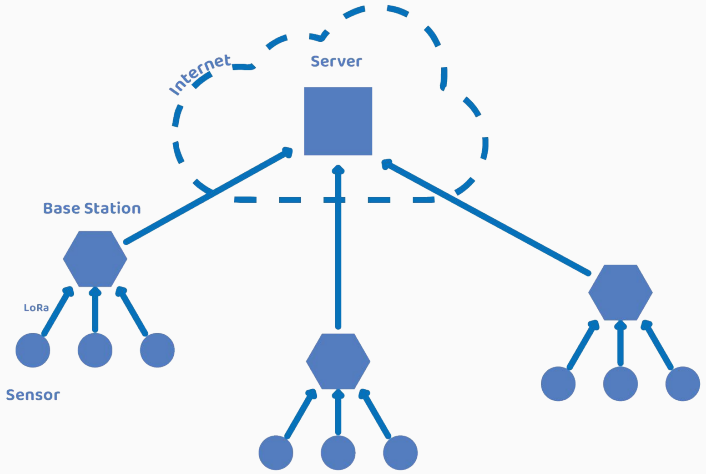
Mục tiêu

- Đề xuất mô hình bảo mật cho hệ thống Mạng cảm biến không dây với trung tâm là việc xác thực Zero-knowledge Proof dựa trên Lattice giữa các nút cảm biến và trạm.
- Đánh giá tính hiệu quả của hệ thống trong việc ngăn chặn các cuộc tấn công thường thấy trong hệ thống Mạng cảm biến không dây là: Clone Attack, Man in the Middle Attack và Reply Attack.
- Đánh giá tính hiệu quả của hệ thống trong việc ngăn chặn các cuộc tấn công lượng tử: Shor, Grover.

Nội dung và Phương pháp

Đề xuất mô hình

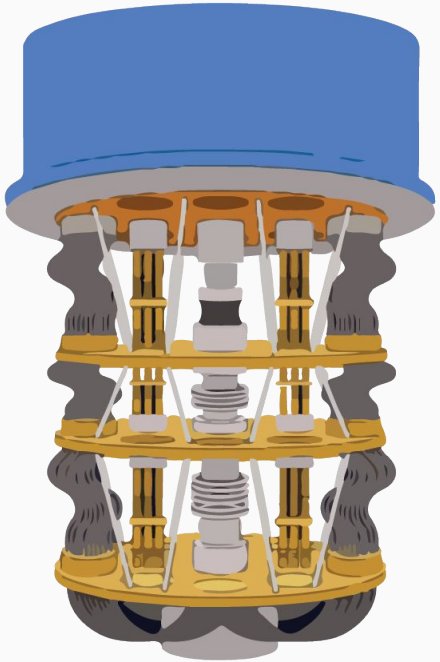
- Nghiên cứu, tìm hiểu các bài báo khoa học
- Thiết kế một mạng cảm biến không dây
- Giả lập hệ thống WSN
- Xây dựng WSN trên thiết bị thật
- Đảm bảo hệ thống WSN hoạt động bình thường



Nội dung và Phương pháp

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



Kết quả dự kiến

- Xây dựng được hệ thống Mạng cảm biến không dây thật với trung tâm là xác thực Zero-knowledge Proof dựa trên Lattice giữa các nút cảm biến và trạm.
- Hệ thống ngăn chặn và phát hiện các cuộc tấn công thường thấy trong hệ thống Mạng cảm biến không dây: Clone Attack, Man in the Middle Attack và Reply Attack.
- Hệ thống hiệu quả trong việc ngăn chặn các cuộc tấn công lượng tử: Shor, Grover.

Tài liệu tham khảo

[1] Arbia Riahi, Enrico Natalizio, Yacine Challal, Zied Chtourou:
A roadmap for security challenges in the Internet of Things. Digit. Commun. Networks 4(2): 118-137 (2018)

[2] Fangmin Sun, Zhan Zhao, Zhen Fang, Lidong Du, Zhihong Xu, Diliang Chen:
A Review of Attacks and Security Protocols for Wireless Sensor Networks. J. Networks 9(5): 1103-1113 (2014)

[3] Poornima M. Chanal, Mahabaleshwar S. Kakkasageri:
Security and Privacy in IoT: A Survey. Wirel. Pers. Commun. 115(2): 1667-1693 (2020)

[4] Siba K. Udgata, Alefiah Mubeen, Samrat L. Sabat:
Wireless Sensor Network Security Model Using Zero Knowledge Protocol. ICC 2011: 1-5

[5] Vadim Lyubashevsky, Ngoc Khanh Nguyen, Maxime Plançon:
Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. CRYPTO (2) 2022: 71-101

[6] Francisco Martín-Fernández, Pino Caballero-Gil, Cándido Caballero-Gil:
Authentication Based on Non-Interactive Zero-Knowledge Proofs for the Internet of Things. Sensors 16(1): 75 (2016)

[7] Feng Li, Bruce M. McMillin:
A Survey on Zero-Knowledge Proofs. Adv. Comput. 94: 25-69 (2014)