Security Challenges of ZigBee Network in IoT

M Rayhan Ahmed Mithu, Gustavo Angeles, Advisor: Dr. Ambareen Siraj, Dr. Nan Guo
Department of Computer Science, Tennessee Tech University

ABSTRACT

- As the industry is leaning towards smart technology with the idea of products controlling their own production environment, more and more must be thought on the security issues of this advancement.
- One of the major component of moving towards the smart industry is the communication network. ZigBee is becoming a very popular choice of communication network in the industry as it cheap and consumes very littlie resources.
- In this project we experimented the implementation of ZigBee in industry and the security challenges of the network. We identify some vulnerabilities of the network and propose countermeasure. Since Zigbee networks are low powered, we have considered the scenario to be close proximity attacks or insider attacks. These kinds of attacks can detriment the productivity in the industry, by adding a node that congests the network or by removing one, and losing the data needed to continue production. Gathering information can lead to leaks if the information gathered by the attacker is sensitive.
- We will implement Intrusion Detection Systems (IDS) within the ZigBee network. Then analyze compatibility of the IDS in the network and results of the implementation.

RESEARCH CHALLENGE AND OBJECTIVES

ZigBee is a very low powered and minimal resource consuming communication network. The network consists of multiple nodes, and a coordinator. The coordinator is responsible to manage the network that includes sending and receiving data from the nodes..

- The **challenge** is that ZigBee devices do not have enough resources to perform security check while transferring data.
- Our **objective** is to provide a mechanism to ensure security in the network. An anomaly based IDS to identify malicious information and detecting the attacking node responsible for sending that malicious information.
- We have divided our implementation in three phases.
  - **Phase 1: Environment Setup**
  - **Phase 2: Implement Attacking Scenario**
  - **Phase 3: Intrusion Detection System**

PHASE 1: ENVIRONMENT SETUP

We created a mock IoT environment with sensors and a hub. We have used a start topology, since it is widely used in the industry. We have used a Raspberry Pi 3 as the network coordinator and Arduino for the other nodes in our environment. We collected information from different sensors and the data was uploaded in the Microsoft Azure cloud.

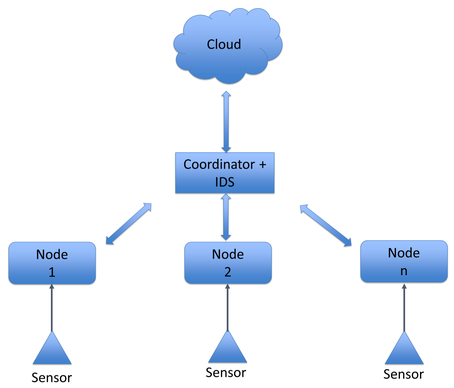
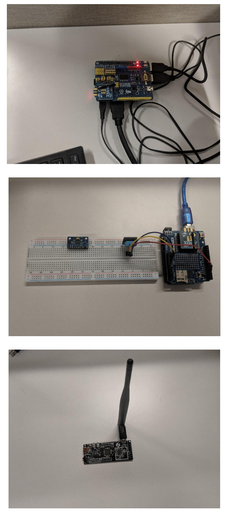


Fig: Environment Topology



PHASE 2: IMPLEMENT ATTACKING SCENARIO

We have identified three attacking scenarios for the experiment. Each of the attacking scenario violets one of the CIA (Confidentiality, Integrity, Availability) tirade of security. In order to perform some of our attacking scenarios we have used the KillerBee sniffer.

- **Attacking scenario 1 (Confidentiality):** Our first attacking scenario violates confidentiality of the communication network. We introduce a second malicious coordinator in the network which collects information from the nodes. Each node broadcasts to all the coordinator available in the network. This attack uses this vulnerability and gather information without authorization. We also used the sniffer to gather information.
- **Attacking scenario 2 (Integrity):** In this attacking scenario we send malicious and wrong information to the coordinator which violates integrity. The sniffer was used to inject data in the network as well.
- **Attacking scenario 3 (Availability):** We perform a DoS attack in order to deny services to the legitimate nodes. This violates availability as the coordinator is overwhelmed with data from the attacking node and cannot process information from the legitimate nodes.

PHASE 3: INTRUSION DETECTION SYSTEM

In our experiment we gather two different data sets.

- **Legitimate dataset:** Data collected from our IoT environment before implementing any attacking scenario.
- **Malicious dataset:** The data set is created with the data collected during the implementation of attacking scenarios.

Proposed anomaly based IDS:

- Trained with legitimate dataset
- Create models of authorized communication
- Detect unauthorized communication and identify malicious node

Parameters to check valid communication:

- Packet length, delay, ratio
- RSSI
- Error rate

FUTURE WORK

- Design anomaly based Intrusion Detection System
- Implement IDS in environment and gather results
- Test real time intrusion detection in the environment
- Analyze performance of IDS with successful detection rate
- Identify malicious node and send instruction to the coordinator

REFERENCES

- H. Lasi et al, "Industry 4.0," Business & Information Systems Engineering, vol. 6, (4), pp. 239-242, 08/01, 2014.
- N. Vidgren et al, "Security threats in ZigBee-enabled systems" in 2013 46th Hawaii International Conference on System Sciences, 2013, pp. 5132-5138.
- E. Ronen et al, "IoT Goes Nuclear" Security and Privacy (SP), 2017 IEEE Symposium on, pp. 195-212, 2017
- O. Olawumi et al, "Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned," Hybrid Intelligent Systems (HIS), 2014 14th International Conference on, pp. 199-206, 2014.

The project is funded by Cybersecurity Education Research and Outreach Center (CEROC), Tennessee Tech University