Research Paper Presentation

Yuvraj Singh Shekhawat

CS20BTECH11057

Title and authors

Title

IoT-based Smart Home Device Monitor Using Private Blockchain Technology and Localization

Authors

1. Marc Jayson Baucas, Student Member, IEEE
2. Stephen Andrew Gadsden, Senior Member, IEEE
3. Petros Spachos, Senior Member, IEEE

Abstract

1. Internet of Things (IoT)-based smart home applications are rising in popularity. However, this trend attracts malicious activity, which causes cost-efficient security to be in high demand.
2. This paper proposes a low-end design that reinforces the security of a home network.
3. It uses private blockchain technology and localization via RSSI-based trilateration.
4. We improve the precision of the localization algorithm by testing it against different wireless technologies.
5. The results conclude that using a private blockchain with a WiFi-based communication system produces the most efficient iteration of the proposed design

Definitions

- **IOT** : The Internet of Things (IoT) refers to a system of interrelated, internet-connected objects that are able to collect and transfer data over a wireless network without human intervention.
- **Blockchain Technology** : A system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.
- **RSSI** : Received Signal Strength Indicator is a measurement of the power present in a received radio signal.

Abbreviations

Introduction

1. Several smart home services relying on using Internet of Things (IOT) devices.
2. Implemented services such as remove surveillance and personal data storage create a network of devices that provide control over the different smart systems within the house.
3. Many home networks fall victim to attackers that infiltrate the server and tamper with it
4. We use the built-in protocol of private blockchains to create a tamper-proof and secure administrator.
5. However it cannot pinpoint the source of malicious activity in terms of location.
6. To improve this, we propose the use of a location based filter via distance trilateration using the Received Signal Strength Indicator (RSSI).
7. To further improve the precision of the collected RSSI values, we chose to incorporate Kalman filtering to manage the raw data.

Smart-Home security based on IOT

1. It is a wireless home network that provides services and applications developed for improved health, comfort, and user safety
2. The amount of data within it is vulnerable to intrusive attacks in terms of regulating device access. Therefore, by adding a secure medium that monitors the devices attempting to access the network, data can remain private.
3. By using client impersonation Hackers can gain complete control over the remote services.
4. A three-layer intrusion detection system (IDS) is proposed that uses a supervised machine learning approach to detect cyber-attacks on IoT networks. Although these designs, on their own, can detect an attack without knowing where the attack is coming from, it is not possible to implement further prevention.
5. Therefore, our proposed framework adapts to these designsusing indoor localization via RSSI trilateration via Kalman filtering to add the ability to trace the sources of the attack.

Blockchain

1. Blockchains are data structures composed of a chain of blocks that are cryptographically linked.
2. Blockchains can automate their processing with the incorporation of smart contracts. A smart contract is a term-based transaction protocol with a defined function and an assigned activation agreement.
3. Blockchains use a consensus process called *Mining* to determine the actions and changes carried out within their system. We plan to use this process to filter and give access to connecting devices in the network.
4. There are two models of authentication in Blockchains: public and private.
5. A public blockchain relies on a proof of-work system. This system requires incoming users to solve a provided algorithm to grant them voting rights to be in the mining process.

6. Executing this complex algorithm requires high processing power, which is not ideal for IOT devices due to their processor constraints.
7. A private Blockchain uses a built-in trust-based access layer to authorize users. This feature eliminates the need for a proof-of-work system but as the ledger grows, latency becomes an issue.
8. Therefore, there is a visible trade between the two blockchains in terms of latency and resource management. Since our proposed network is for a smaller group of users and low-end devices, a private blockchain is better.
9. We will integrate RSSI-based indoor localization via trilateration to further improve the detection system of the network.

RSSI-based Indoor Localization via Trilateration

1. Wireless Indoor localization is a concept of determining the location of a point of interest (POI) within a controlled environment.
2. Trilateration is a method that is for localization. It uses the distances between a point of interest and three known points also known as anchor nodes, to solve for the position of this point on a 2-dimensional plane.
3. However, wireless signals are still subject to noise as the number of potential sources of interference within an area increases. Therefore, to ensure that the localization of these points of interest is accurate, Kalman filtering is used.
4. A Kalman filter (KF) is an estimating algorithm commonly used for linear systems. A standard KF was selected to model this algorithm due to the linearity of distance and localization via RSSI.
5. A standard KF uses the state estimate ($\hat{x}$) and the state estimate covariance (P). The state estimate is the predicted future value of the system. The state estimate covariance is the approximated accuracy of the state estimate.

6. The filtering process of a KF is composed of two steps: the predicting and updating step.
7. The prediction step estimates the next state estimate and covariance values of the system in its current time index, k. The process is

$$\hat{x}_{k+1|k} = A_k \hat{x}_k + A_k u_k \tag{1}$$

$$P_{k+1|k} = A_k P_k {A_k}^T + Q_k \tag{2}$$

Using the system model (A), measurement model (B), control input (u) and noise covariance (Q).

8. The updating step is carried out by first solving for the Kalman gain (K) as:

$$K_{k+1} = P_{k+1|k} {C_{k+1}}^T \left(C_{k+1} P_{k+1|k} {C_{k+1}}^T + R_{k+1} \right) \tag{3}$$

9. This equation introduces the measurement sensitivity (C) and measurement error covariance (R).

System Components

6. The proposed design uses Raspberry Pi 3 Model B's as its main centre of operations for data filtering. It serves as the anchors that create the perimeter around the network. We selected this device due to its modularity and rapid prototyping.
7. The Pis were to represent the devices and appliances within a smart home. Some smart devices have the bare minimum to have a compact and optimized design. Therefore, to simulate these low-cost devices, we chose to use a Pi.
8. We programmed each Pi with the same Raspbian-Jesse OS image. We used Python 3.7 in incorporating software components needed in the design. These main parts include the blockchain and the Kalman filter.
9. The blockchain component is programmed using python initialized upon executing the Pi. Each blockchain contains the same configuration and list of trusted devices.

10. Within each anchor are its unique identifier and geographical position on the network.
11. We embedded the Kalman filter within the blockchain class as a smart contract triggered by a data transaction. The RSSI values is for calculating the location of each device.

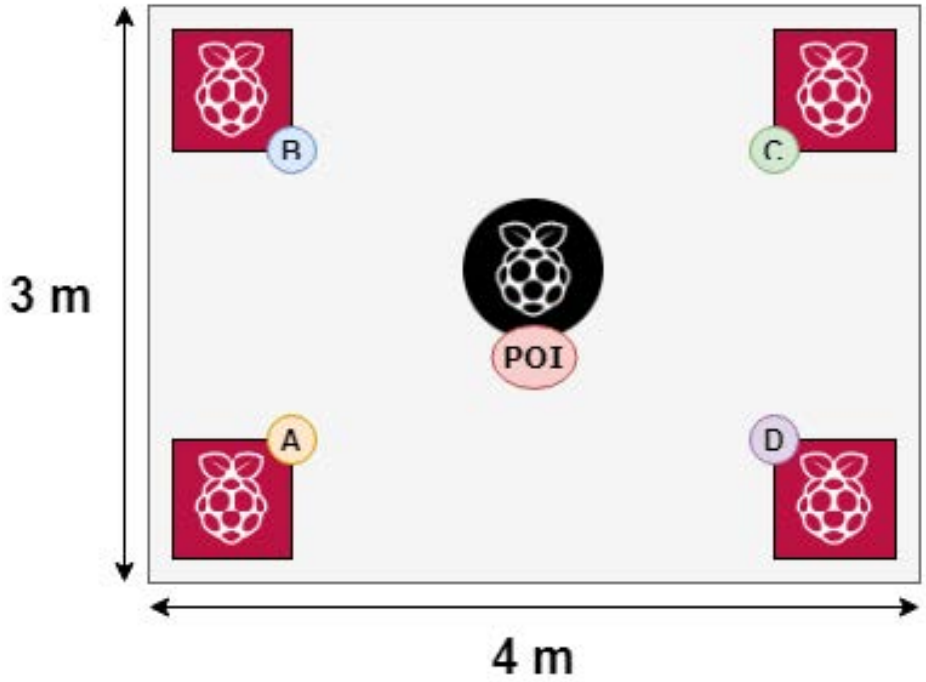

Figure: Room setup for access layer testbed showing anchor locations and point of interest

Testbed

1. We tested each aspect of the access layer separately to optimize the proposed design. More Pis can be added to the testbed to model more complex infrastructures but that will disturb the plausibility of the design foundation.
2. The first test compares efficiency of public and private blockchains. The metric used is the memory, processor usage, and execution time. The test is designed with a device requesting access to the server through an anchor. Each anchor consults the blockchain with which users are allowed to connect.
3. For the public blockchain, it processes the request through proof of work. As for private blockchains, the anchor will attempt to consult through the trusted ledger. We preloaded the blockchains with the identification of devices that are authorized to access the network.

1. Obtaining the physical memory usage was through a python library called memory-profiler. Meanwhile, we used the built-in CPU usage Monitor of the Pi to get the processor usage. As for execution time, it is the elapsed time between a device sends a request and the anchor responds.

Blockchain Type	**Memory Usage (MB)**	**CPU Usage(%)**	**Execution Time (**
Private	12.20	11	0.00021
Public	12.37	25	25.89

Table: Memory usage and execution time results of the blockchain tests

2. We carried out the second test by focusing on the localization via a trilateration filter. We will decide between BLE, WiFi, or ZigBee to maximize the capabilities of the Kalman filter We set up the BLE transmissions using the built-in Bluetooth drivers within the Pis.
3. We calculated the distance with parameters calibrated based on the hardware specifications of the wireless components used with the Pis.
4. All technologies used a 2.00 Path Loss Factor. For the system loss constant, BLE uses -56, WiFi uses -45, and XBee uses 18. To compare the precision of the different wireless technologies, we calculated the Root Mean Squared Error (RMSE) as

$$RMSE = \sqrt{\frac{\sum_1^n (P_i - O_i)^2}{n}} \tag{4}$$

where P represents the predicted value and O is the observed under n time samples. RMSE highlights the impact of the Kalman filter in maintaining the consistency of the distance calculations.

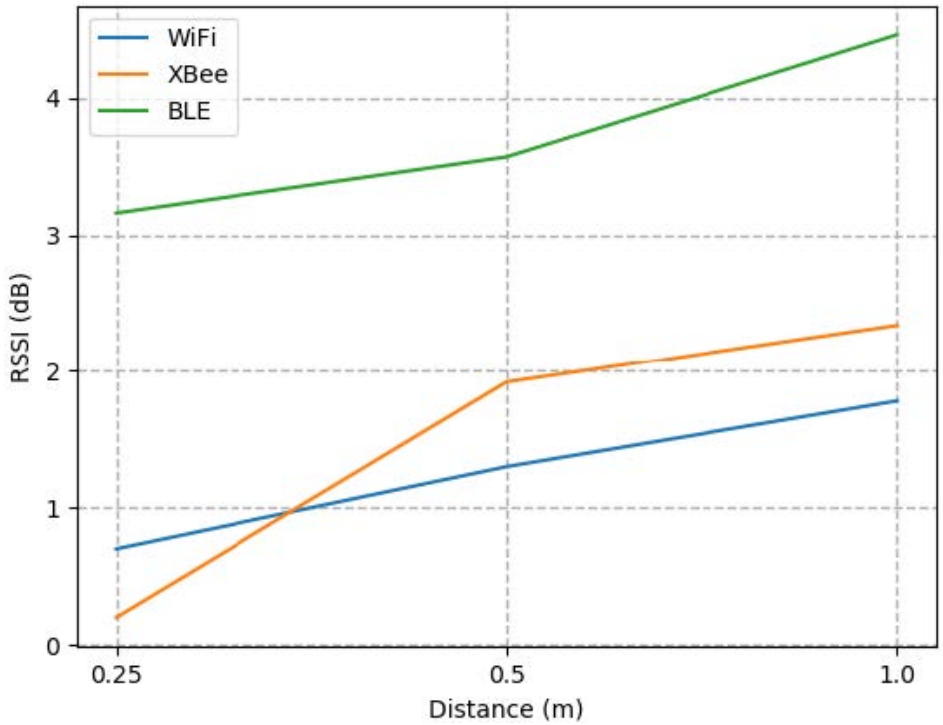

Figure: RMSE of RSSI values from WiFi, XBee, and BLE

Blockchain evaluation

1. We conducted test for blockchain comparison of the anchor accessing each blockchain type. The 20 iterations of the test gave nearly same result in Table I.
2. In terms of memory usage, both types of blockchains use relatively the same amount of memory. However, accessing the private blockchain takes 14% less CPU usage than its public counterpart. This difference shows how private blockchains take fewer resources to run on the Raspberry Pi.
3. A transaction between the anchor and the public blockchain takes 25 seconds. Meanwhile, the private blockchain is 0.21 milliseconds.
4. Due tothe expected volume of transactions between the anchor and the blockchain, a lower resource demand and execution time is better. Therefore, choosing to use private blockchains in the proposed design proves to be better.

Frame Title

1. We tested the proposed design based on its precision in estimating the distance between an anchor and a point of interest. The testbed has the device at varying distances from the anchor on a flat plane.
2. The values used in the tests were: 0.25, 0.50 and 1m.
3. The RSSI RMSE results of each wireless technology are shown in Fig. 2 as collected over 100 samples.
4. Comparing the three technologies, XBee had the best results in terms of distances closer to the device but failed in RSSI consistency.
5. For BLE, it showed the most inconsistent RSSI values among the three.
6. Meanwhile, WiFi yielded the most consistent RSSI reported among the three technologies. Overall, WiFi had the best results in minimizing the effect of the actual distance to the precision of the calculated value.

Conclusion

1. The proposed design is a combination of private blockchain technology and localization via RSSI-based trilateration. It aims to create an access layer that can increase the security of home networks.
2. We conducted two tests to check which technologies were more optimal. The first was to compare the presented types of blockchains for memory usage, CPU usage and execution times. The results show that private blockchains proved to be better for the design.
3. The second test checks which communication medium among BLE, WiFi, and ZigBee yielded the most precise RSSI generation. The results showed that WiFi stayed the most consistent.
4. Therefore, the design is more optimized by integrating private blockchains over public and WiFi for RSSI measurements. Overall, the design has proven its plausibility as an access layer that reinforces security for smart home networks.