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

Marc Jayson Baucas, *Student Member, IEEE,* Stephen Andrew Gadsden, *Senior Member, IEEE,* Petros Spachos, *Senior Member, IEEE*

***Abstract*—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. This paper proposes a low-end design that reinforces the security of a home network. It uses private blockchain technology and localization via RSSI-based trilateration. We investigated the benefits of private blockchains over their public counterpart, and we improve the precision of the localization algorithm by testing it against different wireless technologies. The results conclude that using a private blockchain with a WiFi-based communication system produces the most efficient iteration of the proposed design.**

***Index Terms*—Smart Home Monitoring, Kalman Filter, Private Blockchain, Indoor Localization, RSSI, Internet of Things**

I. Introduction

Several smart home services relying on using Internet of Things (IoT) devices. 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 [1]. However, many home networks fall victim to attackers that infiltrate the server and tamper with it. Also, aside from the standard data router, these networks lack a dedicated administrator to regulate their connected devices. To address these issues, a secure network administrator is needed [2]. By doing so, it can remain safe and monitored properly against security breaches.

This work focuses on creating a low-end solution to manage the devices attempting to access the network. We use the built-in trust-based protocol of private blockchains to create a tamper-proof and secure administrator. Also, due to its architecture, we can automate the network for more efficient management. However, using this technology limits it to track what goes in and out of the network. Therefore, it cannot pinpoint the source of malicious activity in terms of location [3]. To address this, we propose the use of a location-based filter via distance trilateration using the Received Signal Strength Indicator (RSSI). Trilateration-based indoor localization allows the network to pinpoint any device that is within the working radius of the network [4]. To further improve the precision of the collected RSSI values, we chose to incorporate Kalman filtering to manage the raw data [5].

Marc Jayson Baucas, Stephen Andrew Gadsden and Petros Spachos are with the School of Engineering, University of Guelph, Canada, N1G 2W1.

II. Background and Motivation

A. Smart home security based on IoT

Smart homes are an implementation of IoT systems within a home network [2]. It is a wireless home network that provides services and applications developed for improved health, comfort, and user safety [1]. However, this amount of data within it is vulnerable to intrusive attacks in terms of regulating device access [3]. Therefore, by adding a secure medium that monitors the devices attempting to access the network, data can remain private.

Smart homes have become a popular option for modern households. However, due to this increase in interest, security attacks towards remote monitoring and control are introduced [6]. An example is client impersonation. Client impersonation is when a malicious user can infiltrate and compromise the privacy of a homeowner. As a result, they gain complete control over their remote services. Our paper suggests solutions to fortify the security of smart home networks against such attacks.

In [3], they proposed a three-layer intrusion detection system (IDS) that uses a supervised machine learning approach to detect cyber-attacks on IoT networks. As for [7], they take a different approach by suggesting blockchains to regulate their proposed IDS. 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. Therefore, our proposed framework adapts to these designs using indoor localization via RSSI trilateration via Kalman filtering to add the ability to trace the sources of the attack.

B. Blockchain

Blockchains are data structures composed of a chain of blocks that are cryptographically linked [8]. It can be a historical tamper-proof ledger for data and transaction management [9]. This design is more useful in IoT architectures due to its ability to preserve the integrity of the network's data [10] [11]. Blockchains can also 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 [12]. Also, 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.

There are two models of authentication in blockchains: public and private [13]. A public blockchain relies on a proof-

of-work system [14]. This system requires incoming users to solve a provided algorithm to grant them voting rights to be in the mining process. Executing this complex algorithm requires high processing power, which is not ideal for IoT devices due to their processor constraints [13]. On the other hand, a private blockchain uses a built-in trust-based access layer to authorize users [9]. This feature eliminates the need for a proof-of-work system [15]. However, as the ledger grows, latency becomes an issue. Therefore, there is a visible trade between the two blockchains in terms of latency and resource management [10]. Since our proposed network is for a smaller group of users and low-end devices, a private blockchain is better. However, we integrate RSSI-based indoor localization via trilateration to further improve the detection system of the network.

C. RSSI-based Indoor Localization via Trilateration

Wireless indoor localization is a concept of determining the location of a point of interest (POI) within a controlled environment [4]. It takes advantage of the signal characteristics that devices provide to estimate the location of each device [16]. One of the most commonly used signal features is the RSSI value. This value is a metric for the power of a wireless signal.

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 [17].

However, wireless signals are still subject to noise as the number of potential sources of interference within an area increases [17]. Therefore, to ensure that the localization of these points of interest is accurate, Kalman filtering is used.

A Kalman filter (KF) is an estimating algorithm commonly used for linear systems [5], [18]. Some of its variations like the Extended Kalman or the Unscented Kalman Filter usually veers toward a non-linear system [19]. A standard KF was selected to model this algorithm due to the linearity of distance and localization via RSSI. This selection also benefits the device since it requires less processor power to carry out the algorithm. Since we intend the frequent usage of the trilateration algorithm within the framework, a less complex equation is better in terms of scalability and long-term use.

A standard KF uses the state estimate ($\widehat{x}$) and the state estimate covariance (P). The state estimate is the predicted future value of the system. Meanwhile, the state estimate covariance is the approximated accuracy of the state estimate. The filtering process of a KF is composed of two steps; the predicting and updating step.

The prediction step estimates the next state estimate and covariance values of the system in its current time index, k. This process is:

$$\begin{aligned} \widehat{x}_{k+1|k} &= A_k \widehat{x}_k + B_k u_k \\ P_{k+1|k} &= A_k P_k A_k^T + Q_k \end{aligned} \tag{1}$$

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

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

$$K_{k+1} = P_{k+1|k} C_{k+1}^T (C_{k+1} P_{k+1|k} C_{k+1}^T + R_{k+1})^{-1} \tag{2}$$

This equation introduces the measurement sensitivity (C) and measurement error covariance (R). Next, the resulting values are the indexed final state estimates and covariance values of the system. This finalization process as it incorporates the measured input (z) is:

$$\begin{aligned} \widehat{x}_{k+1|k+1} &= \widehat{x}_{k+1|k} + K_{k+1}(z_{k+1} - H_{k+1}\widehat{x}_{k+1|k}) \\ P_{k+1|k+1} &= (1 - K_{k+1}H_{k+1}) P_{k+1|k} (1 - K_{k+1}H_{k+1})^T \\ &\quad + K_{k+1} R_{k+1} K_{k+1}^T \end{aligned} \tag{3}$$

This process is recursive to produce an estimated representation of the filtered data.

III. Methodology

A. Overview

The proposed design focuses on a low-end access level implementation for smart home networks. This access layer is composed of two components to manage the devices within the network. The first component uses a private blockchain to determine any unrecognized devices attempting to connect to the network. It can create a list of all the trusted devices based on the stored information on the server. As a result, the network can manage which connected devices can access and contribute to its stored data. However, this type of protection towards unauthorized access may not be enough to keep the network protected.

The second component will use localization to gain more information about the source of the attack. It is to determine the general location of the device. This filter will allow the ledger to keep track of the projected positions of the devices. It uses anchors that pinpoint the location of connecting devices via trilateration. To further increase the accuracy of the process, we decided to incorporate a simple Kalman filter. By integrating estimation theory into the design, the localization of devices can allow more accurate monitored node positions around the sensing network.

The resulting network model starts with the main network router. Around it is the anchors that include a copy of the blockchain implemented to a home network. This cluster encompasses the unit that will regulate and manage the device authorization as the administrative head. Around each anchor are the smart appliances and devices that attempt to access the different home network services. With these components, this paper proposes low-end access and device managing system for smaller sensing networks.

B. System Components

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. Also, 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.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LNET.2021.3070270, IEEE Networking Letters

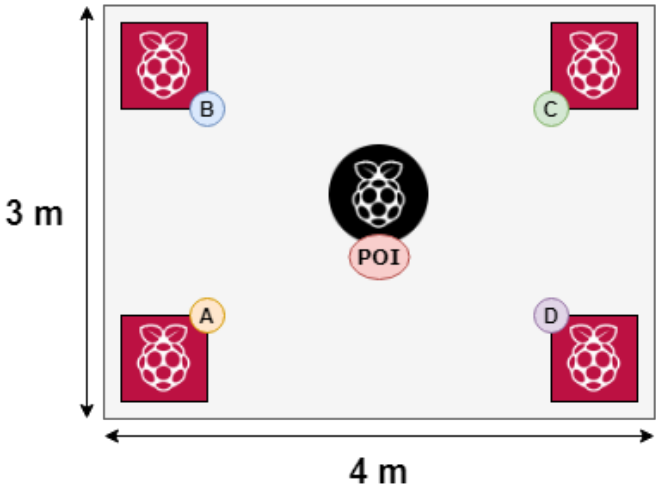

Fig. 1: Room setup for access layer testbed showing anchor locations and point of interest.

Therefore, to simulate these low-cost devices, we chose to use a Pi.

We programmed each Pi with the same Raspbian-Jesse OS image. Also, we used Python 3.7 in incorporating software components needed in the design. These main parts include the blockchain and the Kalman filter. The blockchain component is programmed using python initialized upon executing the Pi. Each blockchain contains the same configuration and list of trusted devices. Within each anchor are its unique identifier and geographical position on the network. We embedded the Kalman filter within the blockchain class as a smart contract triggered by a data transaction. The RSSI values will is for calculating the location of each device.

IV. Results

A. Testbed

We tested each aspect of the access layer separately to optimize the proposed design. The testbed has four anchors arbitrarily placed around a room shown in Fig. 1. We recognize that more Pis can be added to the testbed to model more complex infrastructures. However, we chose to test our framework on simpler setups to ensure that the design foundation is plausible.

The first test compares public and private blockchains to determine which is more efficient at filtering devices. 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. For the public blockchain, it processes the request through proof of work. The algorithm used is a complex comparator using the nonce of the block. It will require the anchor to increment the nonce until it reaches the desired value with an arbitrary number of leading zero bits. Listing 1 shows the algorithm used. 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. Obtaining the physical memory usage was through

```
def proof_of_work(block, n):
  block.nonce = 0
  block_hash = sha256(block)
  while not block_hash[:n] = '0' * n:
    block.nonce += 1
    block_hash = sha256(block)
  return hash
```

Listing 1: Proof of work code abstraction.

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

TABLE I: Memory usage and execution time results of the blockchain tests.

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.

We carried out the second test by focusing on the localization via a trilateration filter. The created 4×3 m workspace simulates a room as the scope of the access layer, as shown in Fig. 1. We will decide between BLE, WiFi, or ZigBee to maximize the capabilities of the Kalman filter. These capabilities are on their accuracy in representing the distance between the anchor and the device. We set up the BLE transmissions using the built-in Bluetooth drivers within the Pis. As for WiFi, we used a WiFi-based network scanning python library called Rssi. Lastly, for ZigBee, a Digi XBee S2C module is installed with the python-XBee library. We calculated the distance with parameters calibrated based on the hardware specifications of the wireless components used with the Pis. 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:

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(P_i - O_i)^2}{n}} \tag{4}$$

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.

B. Blockchain evaluation

The blockchain comparison measures the memory usage, CPU usage, and elapsed time between the anchor consulting the blockchain and the moment it responds. We conducted the test for 20 iterations of the anchor accessing each blockchain type. Table I shows the results of testing for each blockchain technology.

In terms of memory usage, both types of blockchains use relatively the same amount of memory. These values show that running these blockchains on the anchor requires the same amount of allocated memory to access. However, accessing the private blockchain takes 14% less CPU usage than its public

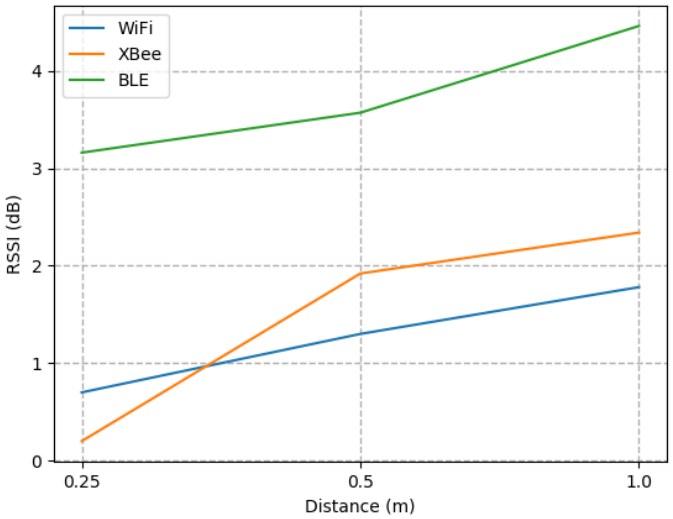

Fig. 2: RMSE of RSSI values from WiFi, XBee, and BLE.

counterpart. This difference shows how private blockchains take fewer resources to run on the Raspberry Pi. Also, a transaction between the anchor and the public blockchain takes 25 seconds. Meanwhile, the private blockchain is 0.21 milliseconds. This discrepancy in the execution time could be the proof of work required for the public blockchain. Due to the 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.

C. Localization filter evaluation

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. The values used in the tests were; 0.25, 0.50 and 1 m. The RSSI RMSE results of each wireless technology are shown in Fig. 2 as collected over 100 samples.

Based on the obtained metrics, the consistency of the RSSI decreased as the distance between the device and the anchor increased. As a result, when the actual distance increases, the preciseness of the theoretical value decreases. Comparing the three technologies, XBee had the best results in terms of distances closer to the device. However, it could not maintain a reasonable trend in RSSI consistency as the actual distance increased. For BLE, it showed the most inconsistent RSSI values among the three. This observation shows how it is the least ideal in terms of precision. Meanwhile, WiFi yielded the most consistent RSSI reported among the three technologies. Overall, WiFi had the best results in minimizing the effects of the actual distance to the precision of the calculated value.

V. Conclusion

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. 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. 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. 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.

References

[1] M. Collotta and G. Pau, "A novel energy management approach for smart homes using bluetooth low energy," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 12, pp. 2988–2996, 2015.

[2] W. Li, T. Logenthiran, V. Phan, and W. L. Woo, "A novel smart energy theft system (sets) for iot-based smart home," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5531–5539, 2019.

[3] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, 2019.

[4] S. Sahin, H. Ozcan, and K. Kucuk, "Smarttag: An indoor positioning system based on smart transmit power scheme using active tags," *IEEE Access*, vol. 6, pp. 23500–23510, 2018.

[5] J. Wang, R. Zhu, and S. Liu, "A differentially private unscented kalman filter for streaming data in iot," *IEEE Access*, vol. 6, pp. 6487–6495, 2018.

[6] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[7] S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir, and M. Imran, "Investigating smart home security: Is blockchain the answer?," *IEEE Access*, vol. 8, pp. 117802–117816, 2020.

[8] L. Zhou, L. Wang, Y. Sun, and P. Lv, "Beekeeper: A blockchain-based iot system with secure storage and homomorphic computation," *IEEE Access*, vol. 6, pp. 43472–43488, 2018.

[9] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, April 2018.

[10] W. Yang, E. Aghasian, S. Garg, D. Herbert, L. Disiuta, and B. Kang, "A survey on blockchain-based internet service architecture: Requirements, challenges, trends, and future," *IEEE Access*, vol. 7, pp. 75845–75872, 2019.

[11] G. Li, M. Dong, L. T. Yang, K. Ota, J. Wu, and J. Li, "Preserving edge knowledge sharing among iot services: A blockchain-based approach," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 4, no. 5, pp. 653–665, 2020.

[12] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, Nov 2019.

[13] M. Alaslani, F. Nawab, and B. Shihada, "Blockchain in iot systems: End-to-end delay evaluation," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8332–8344, Oct 2019.

[14] M. Rahouti, K. Xiong, and N. Ghani, "Bitcoin concepts, threats, and machine-learning security solutions," *IEEE Access*, vol. 6, pp. 67189–67205, 2018.

[15] M. J. Baucas and P. Spachos, "Permissioned blockchain-driven internet of things gateway using bluetooth low energy," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[16] Y. Shu, Y. Huang, J. Zhang, P. Coué, P. Cheng, J. Chen, and K. G. Shin, "Gradient-based fingerprinting for indoor localization and tracking," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 4, pp. 2424–2433, 2016.

[17] S. Sadowski and P. Spachos, "Rssi-based indoor localization with the internet of things," *IEEE Access*, vol. 6, pp. 30149–30161, 2018.

[18] H.H. Afshari, S.A. Gadsden, and S. Habibi, "Gaussian filters for parameter and state estimation: A general review of theory and recent trends," *Signal Processing*, vol. 135, pp. 218–238, 2017.

[19] I. Ullah, Y. Shen, X. Su, C. Esposito, and C. Choi, "A localization based on unscented kalman filter and particle filter localization algorithms," *IEEE Access*, vol. 8, pp. 2233–2246, 2020.