Indoor Localization Using 802.11 WiFi and IoT Edge Nodes

*Ahmad Salman, *Samy El-Tawab, *Zachary Yorio, and **Amr Hilal
* College of Integrated Science and Engineering, James Madison University
** Research and Informatics Division, University Libraries, Virginia Tech
{salmanaa, eltawass, yoriozp}@jmu.edu, ahilal@vt.edu

***Abstract*—The growing affordability and power of the Internet of Things (IoT) technology are enabling researchers to find solutions to problems in all aspects of life. One of these applications is health-care facilities where medical doctors and other medical staff members are in an environment that often needs to locate at moments a patient or other health specialists. In this paper, we propose a solution for the Localization of health Center Assets Through an IoT Environment (*LoCATE*) system, which allows tracking patients and medical staff in near real time. *LoCATE* makes use of the current 802.11 wireless networks within a health-care facility and edge node technology as its tracking technique. The edge nodes continuously communicate with the infrastructure's wireless network Access Points (APs)in a non-intrusive manner. The data, collected from the APs by the edge nodes, is processed by a calculation algorithm based on the signal strength to locate the person in possession of the edge node within a reasonable range of variability. We also address privacy and security concerns regarding the system and the proposed solution. Our solution shows accuracy and reliability in locating the nodes as well as cost efficiency and ease of portability.**

***Index Terms*—IoT (Internet of Things); Cyber-Physical System; Cloud Computing**

I. Introduction

Health-care providers are continually competing to provide the best possible service to their patients. In the United States, in particular, health-care has been the subject of much debate regarding the actual cost of treatment in health-care facilities. As technology advances, practitioners gain access to new technologies that replace outdated methods of treatment and increase the capabilities of health-care facilities which make use of these new technologies. There are various products available to health-care facility management that attempt to solve the issues of locating a medical staff member or a patient in a real-time. However, many of these systems require additional work from medical staffs, forcing individual staff members to input into an electronic form the location and status of a particular patient, which is monitored by a centralized party. This can be of an issue to health-care practitioners, particularly nurses, who commonly handle multiple patients at one time causing miss reporting important information for a specific patient via the electronic system and leading to longer waiting times and a potentially less than satisfactory patient experience. The *LoCATE* system solution seeks to minimize additional and unnecessary work for the medical staff while alleviating many of the issues that patients commonly experience, including those mentioned previously. Our system uses lightweight, low-cost IoT edge nodes connected to an 802.11 wireless network to provide a near real-time method for tracking both patients and practitioners. It also includes security measures to assure the full confidentiality and privacy of patients and their medical records to comply with government regulations and law acts related to that issue.

The remaining of the paper is organized as follows, in Section II we discuss related work on the topic of indoor localization techniques already in use by other researchers or industries. Section III-B explains the details of our edge node's design including both the hardware and software that enables our system. Our methods of data collection and analysis of the current state of the LoCATE system are discussed in IV. We address security and privacy concerns of the system in Section VI. Finally, conclusions and plans for future work are outlined in Section VII.

II. Related Work

Several studies on indoor localization techniques have been conducted [1], [2], [3], [4]. Some researchers use Wireless Sensor Networks (WSNs) with low-power Bluetooth beacons or RFID tags [5]. While other researchers use other techniques such as device-free detection [6], [7]. For example, Lu et al. [8] created a WSN using Wireless Local Area Network (WLAN) inside a hospital using smartphones as nodes. The issue with this approach is that some hospitals have a "no cell phone" policy for staff members, especially for those who work in operation room areas. Many studies have explored the usage of body area WSNs such as the study conducted by Boulmalf et al. [9] which used Android technology to create a lightweight, portable middle-ware. Klingbeil et al. [10] developed a WSN that included network designs, localization algorithms, and experimental results from the deployed network. Quite a few studies were made on IoT environments in healthcare settings or other environments [11]. Islam et al. [12] examine IoT-based healthcare technologies and their characteristics. The survey discusses the security of IoT and proposes its model to minimize the security risks as well as the current trends, policies, and challenges within the IoT healthcare sector. Our study shows that the characteristics of the building facility maybe in favor of one solution over the others. In case of big healthcare hospitals, the use of WLAN signal strength to calculate the location, would be the best option for the given

978-1-5386-8509-9/18/$31.00

situation since the WiFi infrastructure and APs are already installed in almost every healthcare facility.

III. System Design

The *LoCATE* system is comprised of edge nodes (IoT devices), a database server, and a mobile user application. The edge nodes are used as tracking devices made up of Raspberry Pi Zero with USB WiFi dongles for network monitoring capabilities. The edge nodes monitor the APs in the system and calculate the location based on the signal strength of the AP within connection range at any given time and update any change in location to the server database. The database holds tracking information for each node and is cross-referenced with the patients and staff information database to identify the person being tracked using a given node. The system gets smarter by only sending the data when the location changes. A person (node) staying in the same place does not need to update the database.

A. System Architecture

An architecture diagram for the LoCATE system is shown in Fig. 1. The edge nodes operates in the following two modes of operation: *Monitoring mode*: Where the node scans nearby APs to check for signal strength and use the gathered data to calculate locations; and *Data upload mode*: This mode is when the node detects a **significate** change in location based on the calculated data and updates the database with the new information.

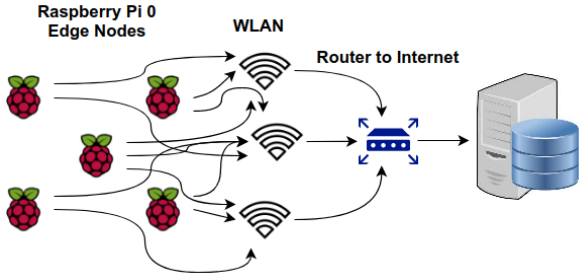

Fig. 1. LoCATE system architecture diagram

B. Edge Node Design

1) Hardware: The current design of the *LoCATE* system makes use of an IoT device (Raspberry Pi zero). Currently for testing purposes, a Raspberry Pi 0 W is used. The edge node consists of a wireless USB dongles. The dongle has the ability to switch into monitoring mode and picks out specific packets known as beacon frames on networks. Finally, in order to keep the system mobile, a rechargeable lithium battery pack powers the Raspberry Pi via its micro USB port. This will supply the edge node with power for roughly 6 to 8 hours. Our current working model is shown in Fig. 2.

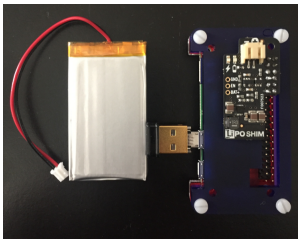

Fig. 2. Edge node design utilizing the compact Raspberry Pi Zero hardware.

2) Software: The edge node uses the following software components to monitor, parse, and push data to our database: Raspbian OS, Python Scripts, BASH Shell Scripts, Tshark Wireless Network Analyzer and Crontab Job Scheduler. The Crontab schedule allows the edge node to run the necessary scripts that scan for access points in range, parse the date, time, and signal strength from data packets, then submit the collected data to a local database server. For testing, this is set to occur twice a minute to reach almost real-time tracking with low cost infrastructure. To help improve the accuracy of the localization algorithm, a network channel hopping script also runs during the Tshark scans. This helps the node pick up more access points in the area that may be broadcasting on different channels. To store node tracing data, the *LoCATE* system utilizes a local MySQL database server.

IV. Data Collection

Once the node was operational, multiple trials were conducted to determine the accuracy and consistency of the calculated distances from access points. Fig. 3 shows a map of the area within the ISAT/CS building located at James Madison University which was used to conduct trial data. The green circles denote locations of ceiling-mounted access points and the spots labeled with red numbers are where the node was placed for various increments of time to collect data. Multiple trials with collection times of one, two, and four minutes were conducted at these four spots. Distances were measured from these spots to nearby access points so that calculated averages of distances done by the node could be compared to expected values.

V. Results and Analysis

After data analysis from the database, our results show a table with each trial's results based on which Media Access Control (MAC) addresses were detected at which spots. These results are shown in Table I. Empty cells in the table indicate that no data packets were collected for that access point during the specific trial. We noticed the trend of more complete data being collected the longer the node was able to stay in a location. We conclude that our access point channel hopping script needs more than one minute in order to scan for all access points in range properly. The trials with two-minute scan durations showed much more consistency in data collection, with four-minute intervals even slightly more reliable than that.

Fig. 3. Predetermined locations in James Madison University's ISAT/CS building used to test *LoCATE* edge nodes

TABLE I
DISTANCES OBSERVED IN FEET FROM ACCESS POINTS VIA MONITORING WITH CHANNEL HOPPING ENABLED.

MACs	1 Min Intervals		2 Min Intervals		4 Min Intervals	
	Trial 1	Trial 2	Trial 1	Trial 2	Trial 1	Trial 2
Spot 1						
9a:60			35.96	37.5	45.2	49.92
9c:c0	22.73	12.55	25.46	10.3	21.8	15.37
81:60	46.73	49.92		49.1	48.3	46.5
42:60				31.8	47.7	32.25
Spot 2						
42:60			15.11	19.6	16	19.39
44:a0			27.51	24.33	22.5	32.34
49:00	26.78	31.87	24.07	20.5	23.3	30.28
4b:e0			16.64	16.8	17.2	13.8
81:60	49.38		39.85	49.9	34.8	46.96
Spot 3						
aa:e0			49.4	41.7	35.9	45.3
43:60	24.7	31.72	30.6	31.9	26.2	16.88
44:60	42.11	40.96	40.8	20.5	25.8	31.49
49:00	31.19	24.21	10.1	23.7		20.46
5a:60			41.9	46	40.1	44.66
5e:60			13.8 2	18	18.9	14.75
Spot 4						
43:60	23.2	16.73	10.5	11.6	11.9	7.53
44:60	49.7	48.36	44.6	34.7	41.8	40.73
49:00			42.9		49.9	49.54
5e:60			45.9	47.7	49.9	37.72

Because of this consistency, we chose the four-minute interval data to perform trimmed mean analysis on our four-minute interval trials. In Table II, calculated averages for a ten and twenty percent trim from the top and bottom of the data sets are shown. Any blank cells in the table denote that not enough data was present for those MAC addresses during the specified trials for the trimming function to successfully calculate the new mean. We expected to see the averages come closer to the expected and approximated distances from the spots to the access points, but instead, the means wavered back and forth with no real trend as the trimming increased. This lead us to believe that data packet outliers are not having a significant impact on our calculated distances and the implementation of a trimmed mean function in our code may not be necessary. Since our final goal for these nodes is to track what room a person is currently in, the deviation within a one-foot difference is negligible.

TABLE II
TRIMMED MEAN CALCULATIONS FOR DISTANCES IN FEET FROM 4 MINUTE MONITORING TRIALS.

MACs	4 Min Avg		10% Trim Mean		20% Trim Mean	
	Trial 1	Trial 2	Trial 1	Trial 2	Trial 1	Trial 2
Spot 1						
9a:60	45.2	49.92	45.15	49.92	44.78	49.92
9c:c0	21.8	15.37	21.92	15.61	21.91	15.91
81:60	48.3	46.5		46.58	49.15	46.72
42:60	47.7	32.25	48.45	32.04	48.95	32.04
Spot 2						
42:60	16	19.39	15.99	19.87	16.11	19.87
44:a0	22.5	32.34	22.16	32.51	21.53	32.51
49:00	23.3	30.28	23.22	30.09	23.15	30.09
4b:e0	17.2	13.8	17.26	13.92	17.41	13.92
81:60	34.8	46.96	35.15	47.06	35.29	47.07
Spot 3						
aa:e0	35.9	45.3	36.13	45.35	36.13	45.7
43:60	26.2	16.88	26.17	16.88	26.16	16.94
44:60	25.8	31.49		31.63	26.16	31.69
49:00		20.46		19.81		18.95
5a:60	40.1	44.66	40.27	44.67	40.09	44.85
5e:60	18.9	14.75	18.86	14.93	18.82	14.94
Spot 4						
43:60	11.9	7.53	11.23	7.51	11.27	7.52
44:60	41.8	40.73	42.06	40.78	42.36	40.77
49:00	49.9	49.54		49.92		49.92
5e:60	49.9	37.72		37.55		37.12

Our results examined the percent error trends of our trials which were calculated according to the following formula

$$Er = \frac{(D_a - D_{exp})}{D_{exp}} * 100$$

Where Er is the error percentage, D_a is the actual measured distance, and D_{expt} is the expected distance. Table III provides the MAC addresses of access points on the same floor as the node during the trials, which can more accurately be used to approximate distances and location.

TABLE III
DISTANCES FROM SPOTS TO ACCESS POINTS IN FEET.

	MACs in Range	Distance
Spot 1		
	9c:c0	16
	81:60	50
	42:60	56
Spot 2		
	42:60	25
	44:a0	30
	49:00	25
	4b:e0	15
	81:60	35
Spot 3		
	43:60	35
	44:60	25
	49:00	20
Spot 4		
	43:60	18
	44:60	30
	49:00	35

In Fig. 4, the results for spot 1 can be seen. For both trials, our results show a consistent trend of positive errors, ranging

from about twenty to fifty percent. The primary explanation for this is structural impediments in the surrounding floor plan such as walls or doors, encumbering packet transmission from access point to edge node.

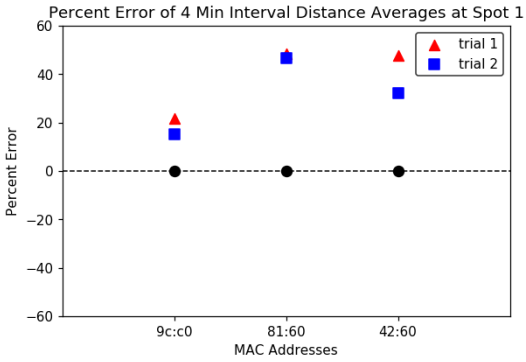

Fig. 4. Percent error calculated for all access point MAC addresses in range at spots 1 for 4 minute interval scan trials.

Fig. 5 presents the percent error calculations for spot 2. Since this spot was more centralized in the middle of a long hallway, we see that the error range is more tightly grouped around the expected value, or zero. The errors fluctuate between positive and negative percentages, showing the fluid nature of signal strength that we expected.

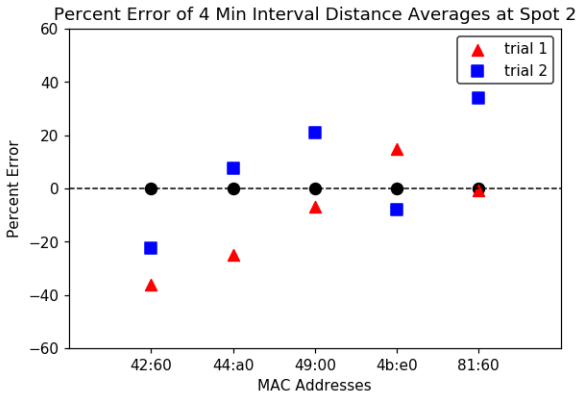

Fig. 5. Percent error calculated for all access points MAC addresses in range at spot 2 for 4 minute interval scan trials.

A similar but more exaggerated fluctuation in error can be seen in Fig. 6. More of the nearby access points at this spot are behind walls and around corners, increase the fluctuation. It is also worth noting that the access point with MAC address ending in ”49:00” was not picked up by the edge node during trial 1, explaining the lack of a red triangle in the graph.

Some of the most consistent data collections were seen in Fig. 7. Both trials had practically the same amount of error for access points with MACs ending in ”44:60” and ”49:00”. These results show that the node is capable of consistency, reliability and that we can improve the distance calculation in feet from signal strength in dBm. The actual distance from the access point is also important to consider when looking at

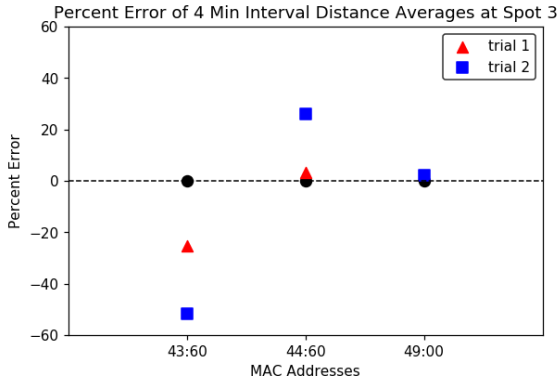

Fig. 6. Percent error calculated for all access point MAC addresses in range at spot 3 for 4 minute interval scan trials.

these errors. Even the relative thirty-five and sixty percent error from MAC address ”43:60” at spot 4 is only the difference of about nine feet. For the purpose of this research, this was enough to map a person to the correct room they are located in at the hospital setting with a great accuracy.

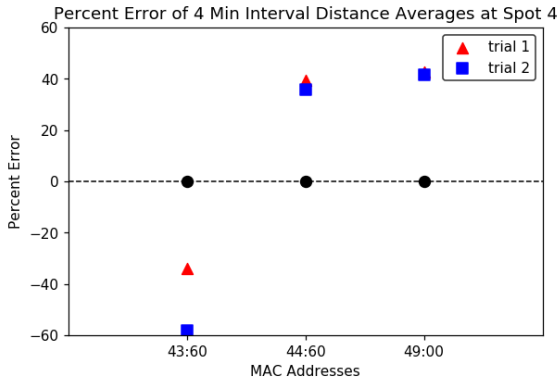

Fig. 7. Percent error calculated for all access point MAC addresses in range at spot 4 for 4 minute interval scan trials.

VI. Privacy and Security

Privacy and security is critical for these types of tracking systems [13]. Patients, upon check-in, are assigned an available edge node. The node is recorded, along with their personal information, into a database record. During the patients' stay at the hospital, the location of the patient is updated, and sent to an access-controlled database. If administrative personnel, with access to patients' information, wishes to locate a patient or track their location history, they can do so by locating the node number associated with the designated patient and look for the latest node update in the nodes' database. We are not concerned about protecting the data of patients and medical staff when they are on the hospital's servers as, along with medical and personal information, they should be well secured in order to comply with the Health Insurance Portability and Accountability Act (HIPAA) [14]. Our concerns are more towards securing the edge nodes and the APs against attacks

such as spoofing and side-channel analysis. We will address some of these attacks in the following subsections and the countermeasures we took to protect the system.

A. Protecting the data

Even though the nodes themselves do not carry any personal data for the patients, they can still reveal medical information such as the operation/surgery they are undergoing or the medical tests they are performing based on their location in the hospital. For these reasons, the location history on the node's memory needs to be protected as well as when it is being uploaded to the server. We use the authenticated encryption AES-128-GCM as described in [15]. Using authenticated encryption allows the server to authenticate the nodes when receiving updates from them while providing data confidentiality.

The AES implementation uses masking and randomization techniques described in [16] to protect against side-channel attacks such as Simple Power Analysis (SPA) and Differential Power Analysis (DPA) [17]. This way if an attacker gets physical access to one of the nodes, they wont be able to extract the data assuming a reasonable amount of gathered power traces.

Finally, the encryption keys for AES-128 are generated using a True Random Number Generator (TRNG) and are updated after every use, i.e., after a patient's check-out and before a new patient's check-in.

B. Edge Nodes and Access Point Spoofing

An Attacker can spoof the MAC address of one of the access points making the nodes make wrong calculations regarding the location. or the attacker can also spoof one of the node's MAC address and try to upload the wrong data o the server. To prevent these two attacks, we use 802.1x authentication to insure that the nodes are authenticated periodically and independently making it harder to authenticate a spoofed node. If an access point is spoofed, the location calculation algorithm on the node will be able to detect the spoofed access point through comparisons to the history of data obtained from that access point.

VII. Conclusions and Future Work

We implemented a reliable tracking system using WiFi and low-cost IoT edge nodes. We showed that distance calculation from packet signal strength is consistent, but not always accurate. However, it can be sufficient in a healthcare facility where rooms size is large enough. We highlight on the privacy and security of the data collected, and solutions for cyber-attacks against the edge nodes. With the use of edge nodes, there is enough storage space to expand on computing capabilities. Since all of the processing is done on the node, it shows that there is the capability to do much more (e.g., a patient medical record could be kept on the node that travels around with them). Future work on the project includes power consumption analysis, improve the tracking system by implementing elements of machine learning to be able to predict locations of medical staff members or patients being tracked with a LoCATE edge node.

VIII. Acknowledgment

This work is supported by a 4-VA collaborative research grant between JMU and VT: https://4-va.org/james-madison-university/ Spring 2018. The authors would like to thank RMH Healthcare director of perioperative services Mr. Shawn Craddock for allowing us to tour and visit the facility. Authors would like to thank senior students: Nick Benedetto, Brendan Colton, and Nick Reist.

References

[1] H. Wang, S. Sen, A. Elgohary, M. Farid, M. Youssef, and R. R. Choudhury, "No need to war-drive: Unsupervised indoor localization," in *Proceedings of the 10th international conference on Mobile systems, applications, and services*. ACM, 2012, pp. 197–210.

[2] F. Adib, Z. Kabelac, and D. Katabi, "Multi-Person Localization via RF Body Reflections." in *NSDI*, 2015, pp. 279–292.

[3] M. S. Bargh and R. de Groote, "Indoor localization based on response rate of bluetooth inquiries," in *Proceedings of the first ACM international workshop on Mobile entity localization and tracking in GPS-less environments*. ACM, 2008, pp. 49–54.

[4] T. D. McAllister, S. El-Tawab, and M. H. Heydari, "Localization of Health Center Assets Through an IoT Environment (LoCATE)," in *2017 Systems and Information Engineering Design Symposium (SIEDS)*, April 2017, pp. 132–137.

[5] M. Altini, D. Brunelli, E. Farella, and L. Benini, "Bluetooth indoor localization with multiple neural networks," in *IEEE 5th International Symposium on Wireless Pervasive Computing 2010*, May 2010, pp. 295–300.

[6] Y. Wang, K. Wu, and L. M. Ni, "Wifall: Device-free fall detection by wireless networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 2, pp. 581–594, 2017.

[7] A. Saeed, A. E. Kosba, and M. Youssef, "Ichnaea: A low-overhead robust WLAN device-free passive localization system," *IEEE Journal of selected topics in signal processing*, vol. 8, no. 1, pp. 5–15, 2014.

[8] C.-H. Lu, H.-H. Kuo, C.-W. Hsiao, Y.-L. Ho, Y.-H. Lin, and H.-P. Ma, "Localization with WLAN on smartphones in hospitals," in *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)*, Oct 2013, pp. 534–538.

[9] M. Boulmalf, A. Belgana, T. Sadiki, S. Hussein, T. Aouam, and H. Harroud, "A lightweight middleware for an e-health WSN based system using Android technology," in *2012 International Conference on Multimedia Computing and Systems*, May 2012, pp. 551–556.

[10] L. Klingbeil and T. Wark, "A Wireless Sensor Network for Real-Time Indoor Localisation and Motion Monitoring," in *2008 International Conference on Information Processing in Sensor Networks (ipsn 2008)*, April 2008, pp. 39–50.

[11] M. Tellez, S. El-Tawab, and H. M. Heydari, "Improving the security of wireless sensor networks in an IoT environmental monitoring system," in *2016 IEEE Systems and Information Engineering Design Symposium (SIEDS)*, April 2016, pp. 72–77.

[12] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[13] C. Bradley, S. El-Tawab, and M. H. Heydari, "Security analysis of an IoT system used for indoor localization in healthcare facilities," in *2018 Systems and Information Engineering Design Symposium (SIEDS)*, April 2018, pp. 147–152.

[14] U. S. of America, *Health Insurance Portability and Accountability Act (HIPAA)*, 1996.

[15] National Institute of Standards and Technology, *NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. pub-NIST, November 2007.

[16] S. Tillich, C. Herbst, and S. Mangard, in *Applied Cryptography and Network Security*. Springer Berlin Heidelberg, 2007, pp. 141–157.

[17] A. Salman, A. Ferozpuri, E. Homsirikamol, P. Yalla, J. P. Kaps, and K. Gaj, "A scalable ecc processor implementation for high-speed and lightweight with side-channel countermeasures," in *2017 International Conference on ReConFigurable Computing and FPGAs (ReConFig)*, Dec 2017, pp. 1–8.