Smart Homes

Smart Homes: From Research to Industry

A.J. Brush
Microsoft

Jeannie Albrecht
Williams College

Mike Hazas
Lancaster University

Robert Miller
Microsoft

Smart homes innovations are both a research topic and an industry reality. In this article, we highlight smart home research from the Proceedings of the ACM Journal on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT) presented at the September 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and smart home industry updates from the CES conference in January 2020.

Do you have a smart device in your home? A smart speaker, thermostat, camera. lighting or perhaps an internet connected scale? The widespread adoption of home wireless networking caused a boom in the creation of internet connected home devices from security cameras to smart speakers. Consumers' recent willingness to install smart home devices inspires researchers to continue building novel sensors and developing methods to make devices more secure and encourages companies make new smart home devices available for purchase.

In this article, we share recent smart home innovations from both research and industry. First, we highlight home sensing and security research published in the ACM Journal on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT) and presented at the UbiComp conference in September 2019. Health sensing is a particularly active area of research as advances in sensing technology could help with detection and treatment of health conditions, but also raise concerns around comfort, practicality, and privacy. Particularly relevant to smart home research are efforts to monitor people's sleep quality. In the Smart Home Sleep Monitoring section we highlight findings from two different research approaches. Phyjama's [1] is a wearable system that embeds sensors in pajamas while TagSleep[2] places RFID tags and readers into the bedroom environment. Unfortunately, the increasing number of smart home devices installed in homes make them an attractive target for hackers. Thus, researchers are working on approaches to make devices more secure. In the Smart Home Security Update section, we highlight the REVOLT system[3], in which researchers use signals from audio and wifi data to detect and prevent voice replay attacks.

For companies working on smart homes technology, a key industry event is CES. Held every January in Las Vegas, CES has over 4,500 exhibitors from the well-established to the start-ups and is attended by more than 175,000 people[1]. Walking the exhibition halls, you feel like a kid in the gadget candy store. In the Smart Home Industry Update section, first-time attendee Robert Miller shares his.

SMART HOME SLEEP MONITORING

The widespread adoption of smart home technologies encourages the design and implementation of new sensors, providing a wide range of additional data sources to augment existing data streams. Some of these sensors even go beyond measuring aspects of the home itself, such as temperature, electricity, and water usage, and aim to monitor aspects of the human occupants, including their sleep patterns. In this section we highlight interesting and promising research results on sleep sensor design and implementation in smart homes.

Measuring the sleep behavior of occupants in smart homes is a challenging problem for many reasons. There are health benefits to being able to accurately monitor sleep behavior, however concerns about comfort and privacy have prevented widespread adoption of sophisticated sensors. Recent work by Ali Kiaghadi, Seyedeh Homeyounfar, Jeremy Gummeson, Trisha Andrew, and Deepak Ganeson at the University of Massachusetts Amherst that appeared in an IMWUT article titled “Phyjama: Physiological Sensing via Fiber-enhanced Pyjamas”[1] investigates new ways to measure the physiological aspects of sleeping occupants, such as breathing and heart rates, using sensor-augmented sleepwear called “phyjamas.” Since pajamas in general are designed to be worn comfortably, Kiaghadi et al developed a distributed set of sensors for augmenting loose-fitting sleepwear. Together, these sensors can be used to accurately monitor the breathing and heart rates of their wearers while they sleep.

The Phyjamas proposed sensor suite consists of new fabric-based pressure sensors combined with triboelectric sensors that are activated by changes in physical contact. The sensors are carefully stitched into pajamas in the form of textile patches, and then connected using silver-plated nylon thread shielded in cotton. The wires coming from each patch eventually lead to a small button-sized circuit board that is discretely sewn into the pajamas where a normal button would typically appear. Since people tend to move around and sleep in different positions, the data provided from an individual sensor patch can be unreliable. However, using data collected from multiple sensors, Kiaghadi et al. were able to detect heartbeat peaks, breathing rates, and sleep postures with high levels of accuracy across many different sleep positions. These advances will be particularly helpful for monitoring elderly patients whom frequently suffer from sleep disorders.

In another article from IMWUT, Chen Liu, Jie Xiong, Lin Cai, Lin Feng, Xiaojiang Chen, and Dingyi Fang took a different approach to analyzing the sleep behavior of smart home occupants in their paper titled “Beyond Respiration: Contactless Sleep Sound-Activity Recognition Using RF Signals.[2]” Unlike Phyjamas, which focused on making wearable sensors, Liu et al. avoided comfort and privacy issues by designing a system called TagSleep that uses only RFID tags and readers. The RFID devices are deployed in the bedroom, but are not attached to the occupants themselves. Further, since only RF signals are used, the authors avoid privacy concerns that arise when using audio or video devices in bedrooms.

TagSleep relies on a novel two-layer sensing scheme to accurately recognize snore, cough, or somniloquy as well as sleep posture in smart home occupants. They attach three RFID tags and one RFID reader to locations on each side of the bed, forming a somewhat rectangular plane across the bed. As occupants exhibit specific sleep events, including snoring, coughing, and somniloquy, they are able to observe phase variations in the RF signals due to changes in the chest movement and breathing rate during these activities. They use the signal reflection from nearby walls and furniture to enhance the phase change caused by respiration and thereby

[1] CES factsheet, https://cdn.ces.tech/ces/media/pdfs/2020/ces2020_factsheet_9-23.pdf

improve the accuracy of their results. Thus, the first layer of their sensing scheme measures changes in respiration, while the second layer uses this information to identify sleep sound-activities and postures. Four different common sleep positions are considered in their evaluation. They measure the effectiveness of several different classifier algorithms in their article and show that high levels of accuracy for both sleep sound-activity and sleep posture recognition are possible.

When combined with sensors that measure the home environment, research that measures physiological aspects of occupants, such as sleep behavior using TagSleep or Phyjamas, enable more sophisticated and accurate automation in smart homes. Research on sensor design, more broadly, continues to explore many ways to provide a richer sensing environment.

SMART HOME SECURITY RESEARCH

As the adoption of smart home devices rises so does the number of security incidents, from smart home cameras passwords being hacked to people being surprised by what their smart speakers have recorded and uncertain who might have access to their data. While companies are taking a variety of steps to address security concerns including encouraging unique passwords, two-step authentication, and providing additional user controls, researchers are also working on technical innovations to make devices more secure. In their IMWUT journal paper, "Combating Replay Attacks Against Voice Assistants,"[3] authors Swadhin Pradhan, Wei Sun, Ghufran Baig and Lili Qiu from the University of Texas, Austin describe an approach to prevent *voice replay attacks*, where an attacker plays previously recorded (or synthesized) audio to a smart speaker device.

Pradhan et al.'s system aims to prevent three types of replay attacks: a) *remote voice replay*, where an attacker gains access to a speaker in the home and plays recorded or synthesized audio, b) *local voice replay*, where an attacker in the home near the speaker can directly replay audio, and c) *sophisticated replay* where the attacker plays back recorded audio and mimics the breathing patterns of someone speaking the audio. To detect these three situations, the REplay-resilient VOice Legitimacy Tester (REVOLT) system uses signals from both voice and WiFi channels.

REVOLT first runs a voice module with pre-trained machine learning models to check if the audio spoken to a smart speaker is pre-recorded. Using the ASV2017 dataset and their own data collected from 10 users, the authors demonstrate that the high frequency data of replayed audio differs from live audio because replayed audio goes through additional audio conversion steps as it is recorded and then replayed through speakers. Thus, replayed audio can be detected using several spectral features of the audio. In parallel to testing if the voice audio is live, REVOLT determines the direction of the audio source and points the device's WiFi directional antenna toward the source to enable detection of human breathing. By detecting breathing, the system can check if a human is present and if the breathing patterns are synchronized with the audio. This ensures that a human is speaking the audio and helps prevent sophisticated replay attacks. Using their datasets and extensive analysis, the authors determine the best features for detecting pre-recorded audio and how best to detect human presence and breathing patterns for users within 2 meters of a device.

Any system based on machine learning must always balance the false positive rate (incorrectly allowing replayed audio to be treated as a live voice) with the false negative rate (denying a real user's command). For REVOLT, the authors define two security levels: a) Casual for commands like playing music where a low false negative rate would be preferred and b) Critical for commands such as controlling locks or access to personal data where a low false positive rate is desired. They then show an end-to-end evaluation with two sets of parameters that achieves these goals.

In summary, by exploiting the differences between the original and replayed voice signals and detecting the impact of human breathing on WiFi signals, the REVOLT system can detect replay attacks without requiring users to carry any additional hardware. Smart home security research will continue to be important as smart speakers and voice assistants try move beyond being used primarily for playing music or answering questions to become places where customers do more

sensitive interactions from online shopping to controlling smart home security devices or accessing more personal data such as their email.

SMART HOME INDUSTRY UPDATE

The CES conference every January offers a fascinating window into commercial activities in the smart home space. We asked our guest author, Robert Miller, a first-time visitor to CES to walk the smart home floor and share his experience.

"*After what felt like several hours of being lost at sea in a crowd of attendees, slots machines, and exhibit booths, I finally found my way to the Smart Home space on level 2 of the Sands Expo (hosted in the Venetian). The Sands Expo had a very modern-day bazaar / startup vibe to it. I couldn't walk more than a few feet without getting distracted by an obscure piece of smart home tech or being offered a 1-1 product demo by an all too eager exhibitor.*

Security solutions were well represented. A variety of options for sensors, flood lights, smart locks, and camera systems were all on display. I even stumbled across a set of security products for the non-humans in your home. SureFlap, a smart pet door works with your pet's microchip to ensure it's in fact your family pooch (or kitty) coming in for that late-night snack. The maker, SurePetcare[2], also offers smart feeders and activity trackers. They pair with the company's companion app where you can configure notifications, set activity goals, and view detailed analysis of your pet's daily habits – inside and outside of your home.

Beyond home security, it was interesting to see the number of traditional home hardware components that are becoming smart. For example, The U by Moen™ Smart Faucet[3] pairs with your smart speaker to bring voice commanding to your kitchen sink. You can turn the facet on or off using your voice, you can also ask for precise temperatures, amounts, and even set routines, e.g. "pour a bottle of warm water for the baby." Moen also offers The Flo Smart Water Shutoff, a smart valve that connects inline to your home's main water supply. You can configure the valve to monitor use, alert if an anomaly is detected, and even cutoff supply in the event of an emergency. I also saw many choices for built-in smart electrical outlets which seemed like a better replacement option for my existing outlets than the plug-in accessories widely available today. Companies were showing smart options for pretty much every part of your home: lights, toilets, facets, meters, garage door openers, etc.

The CES Tech East exhibits hosted in the Las Vegas Convention Center are where many of the well-known brands like Google, Samsung and GoPro have their booths. Here companies seemly spared no expense on their exhibits and I felt a little underdressed approaching some of the booths in my sneakers, jeans, and ballcap. I managed to see Samsung's new home robot Ballie[4]. Unfortunately, due to the incredibly popularity of the booth, I didn't get to experience a demo or get any closer than a conference room's length away. According to Samsung, Ballie is a smart home assistant that "transforms living spaces into experience-spaces." The softball sized robot can follow you around the home, take pictures, detect intruders, and help with your fitness routines. While I was perusing Samsung's space, an unexpected highlight was the newest iteration of The Frame tv[5]. Samsung showed a few new sizes and introduced a subscription service, Art Mode 3.0 that rotates curated art tailored to the owner's taste. I found the screen very impressive, at first glance I thought I was looking at an authentic work of art and had to inch in closer to get a better look before I could tell it was a display. All in all, CES was a great time. I encourage anyone who has a love for technology or works in the industry to attend at least once."

2 SurePetcare, https://www.surepetcare.com/en-US
3 Moen Smart Home, https://www.moen.com/smart-home
4 Samsung Ballie, https://news.samsung.com/us/samsung-ballie-ces-2020/
5 Samsung The Frame, https://www.samsung.com/us/televisions-home-theater/tvs/the-frame/

CONCLUSION

Rapid adoption by consumers of smart home devices is driving research and industry innovations. To learn more about IMWUT journal and UbiComp conference, please visit their websites at https://dl.acm.org/journal/imwut and http://ubicomp.org/ubicomp2020/. UbiComp 2020 will be held from September 12-16th in Cancun, Mexico collocated with ACM International Symposium on Wearable Computers (ISWC'20). To take in future smart home industry advances, CES 2021 will be held Jan. 6-9, 2021 in Las Vegas. Visit their website at https://www.ces.tech/

REFERENCES

1. Ali Kiaghadi, Seyedeh Zohreh Homayounfar, Jeremy Gummeson, Trisha Andrew, and Deepak Ganesan, "Phyjama: Physiological Sensing via Fiber-enhanced Pyjamas," In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies" Vol. 3, No. 3* September 2019, https://doi.org/10.1145/3351247
2. Chen Liu, Jie Xiong, Lin Cai, Lin Feng, Xiaojiang Chen, and Dingyi Fang, "Beyond Respiration: Contactless Sleep Sound-Activity Recognition Using RF Signals", In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies" Vol. 3, No. 3* September 2019, https://doi.org/10.1145/3351254
3. Swadhin Pradhan, Wei Sun, Ghufran Baig, Lili Qui, "Combating Replay Attacks Against Voice Assistants," In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies" Vol. 3, No. 3* September 2019, https://doi.org/10.1145/3351258

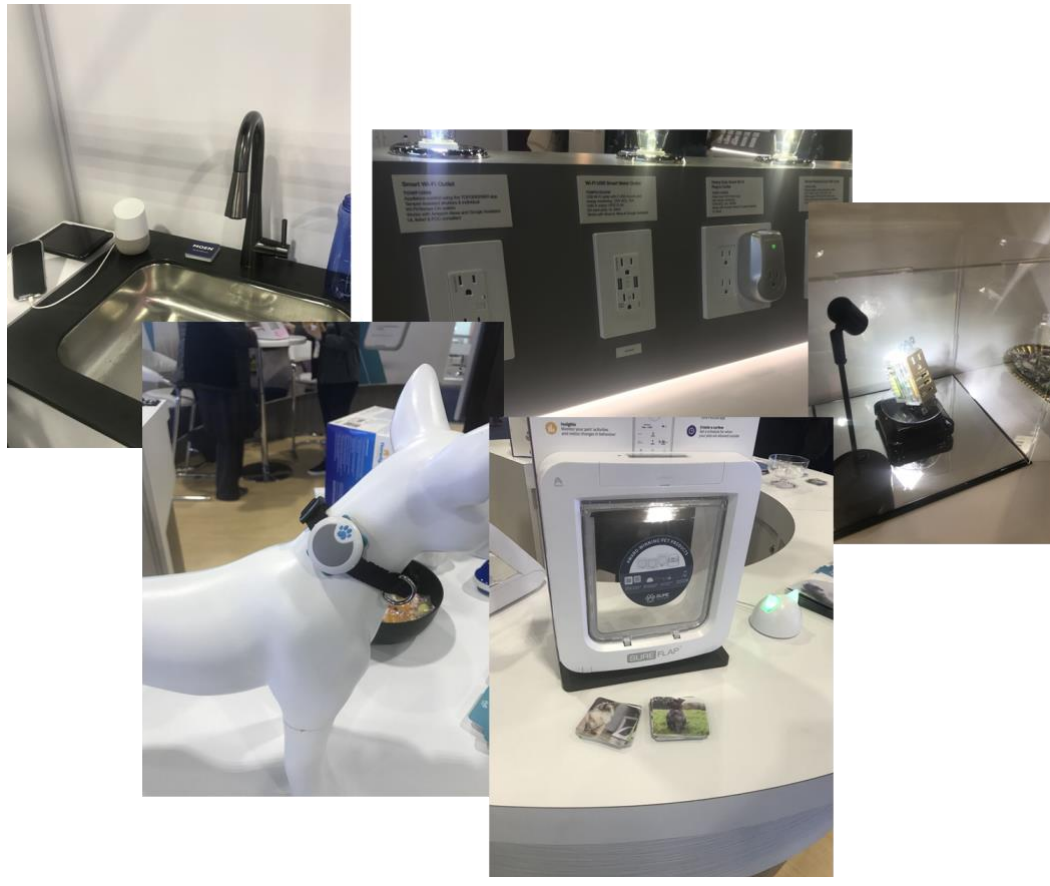
ABOUT THE AUTHORS

A.J. Brush is a Principal Program Manager at Microsoft. Contact her at ajbrush@microsoft.com.

Jeannie Albrecht is a Professor and Chair of the Department of Computer Science at Williams College. Contact her at jeannie@cs.williams.edu.

Robert Miller is a Principal Program Manager at Microsoft. Contact him at romill@microsoft.com

PICTURE OPTIONS:




ROYOLE