SCTE·ISBE CABLE-TEC EXPO 2019 NEW ORLEANS, LA SEPT. 30-OCT. 3

2019 Fall Technical Forum SCTE·ISBE • NCTA • CABLELABS

New Sensing Techniques For Advanced IoT Applications

A Technical Paper prepared for SCTE•ISBE by

Arun Ravisankar
Senior Engineer, Comcast Labs
Comcast Corporation
1800 Arch St, Philadelphia, Pa 19103
Phone: 2152867558
Arun_Ravisankar@comcast.com

Table of Contents

List of Figures

Introduction

History is witness to the evolution of civilizations and how humans continue to discover and innovate things that would propel everyone to newer levels of technological advances, as we aspire to attain a higher intellectual state. Industrial revolutions are key indicators of how humankind continues to seek techniques that would improve lifestyles and bring advancement to civilization. IoT (Internet of Things) applications play a significant role in providing peace of mind to customers/users and help improve lifestyles. Residential IoT applications bring peace of mind to customers by offering security applications or improving lifestyle by offering a suite of home automation applications that enable users with a worry-free experience that also optimize usage of resources. Commercial and Industrial IoT applications help organizations increase productivity and help optimize resources.

Regardless of IoT application type, there are some major components that power them and help provide all the services that these applications are designed and intended for. Figure 1 shows the components that typically make up an IoT application. All these components play an integral role in providing the desired result.

Rules would define how applications would act on data sent from sensors. Rules form the basic construct of IoT applications. For example, rules set on a home automation application to determine the next course of action if a motion sensor detects a motion event.

Algorithms would analyze sensor data and provide insights that could be used in predictive analysis and advanced applications

Sensors are devices that interface with the physical world, and usually to convert physical parameters (for ex: temperature, humidity, magnetic field, light, sound, etc.) to electrical signals which a machine can understand and a software program can process.

Sensors on an automobile are vital in determining the health of important components and also are an integral part of the systems that provide reliable information for autonomous driving. Numerous sensors also aid the safe operation of airplanes.

This paper focuses on the role of sensors that are vital in providing the information necessary for software algorithms to process and apply the rules that govern the application's features. We examine how new sensors and sensing techniques could take these applications to a higher scale of efficiency.

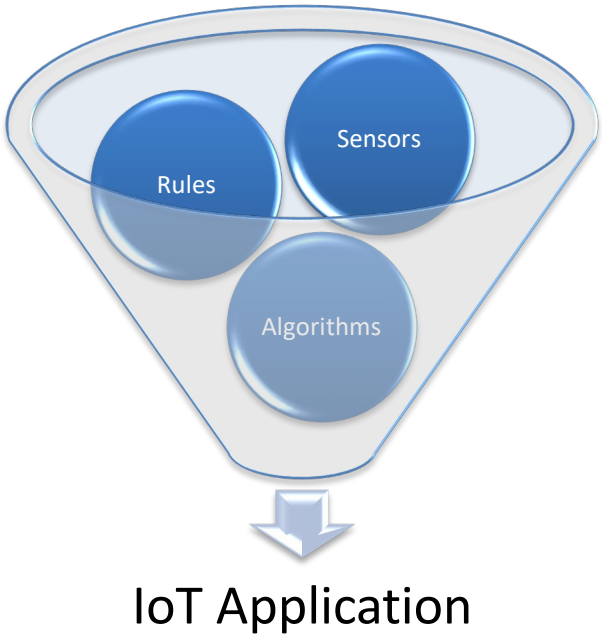

Figure 1 - Components of a Typical IoT Application

Sensors in IoT

IoT applications influence both residential and commercial landscapes and are an important aspect of the business services they offer -- be it providing peace of mind by protecting the customer's house, or by maintaining the production line at a factory. Sensors in these systems provide critical information that can determine further courses of action in the system.

Sensor choice, positioning and the data model depend on the product use cases and design. In-home security applications, for example Xfinity Home, use various types of sensors in a home to detect anomalies towards providing comprehensive security. The following are some of the sensors used in a typical home security application, which are depicted in Figure 2.

1. Motion Sensors
2. Door/Window Sensors
3. Security Cameras
4. Safety sensors (like smoke detectors)
5. Thermostats
6. Catastrophe sensors, for fires, floods, and weather-related dangers.

Most operators provide smart home applications packaged with sensors and detectors, like motion sensors, door window sensors, door locks, fire sensors, flood sensors and others as shown in Figure 3. The motion sensor is a passive infrared sensor (PIR). This sensor uses infrared to sense motion and sends data to a central control unit over a Zigbee network. The sensor detects motion events and passes this information over to the controller, which in turn processes it and translates it to a specific data model. The rules engine processes and determines if there is a need to send alerts. The door/window sensor uses magnetic fields between two ends of the sensor to signal when it is open or closed. Smoke detectors look

out for the presence of certain particles in the environment and generate alerts when those particles are present.

Figure 2 - Sensors used in a home security application

With advances in technology, most home appliances include a range of sensors and have the abilty to connect via Wi-Fi or Bluetooth. Each of these sensors are designed to serve a specific purpose (Figure 3) and they connect back to a hub, typically on the home network. These sensors are usually paired to the hub via Zigbee[1], Bluetooth[2] or WiFi. Some sensors may have the ablility to connect with an external network, so as to connect to a cloud-based application.

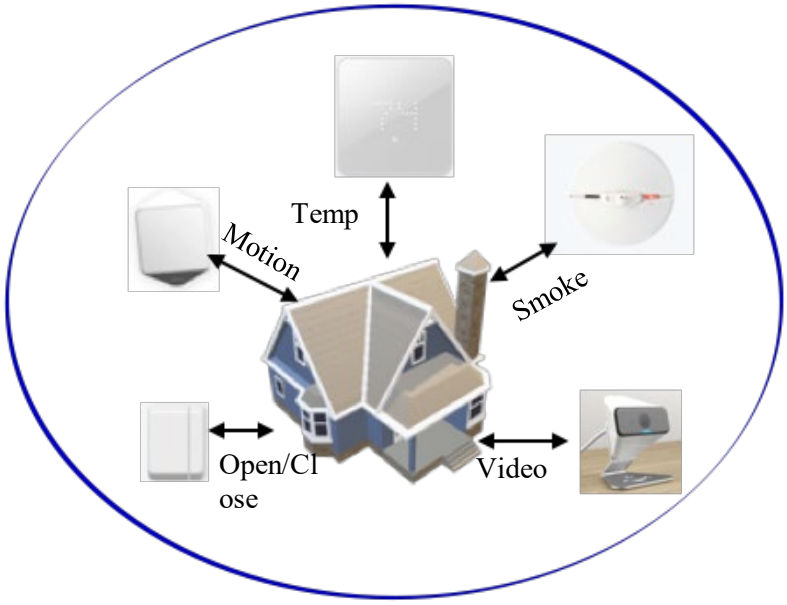

Figure 3 - Sensors in a Home Security Application

The example above is just one of many use cases that a typical IoT application would support. From a developer's perspective, this entails maintenance of all these components, on regular basis, so that the system functions without failure. Any update to one of the components has to be tested so that it doesn't impact the entire system. This includes updates to hardware and software components in the system.

[1] http://www.zigbee.org/
[2] http://www.bluetooth.com/

In any IoT network, multiple network protocols are involved, hence the need for a central gateway that can translate between protocols and forward packets for analysis. In the example above, the home gateway would be the IoT gateway, as it would have the necessary hardware and software to interact with devices which may use a different protocol. For example, there may be a rule set to turn on a light bulb upon detecting motion in the hallway. In this case, the motion detector could be a ZigBee-based device, and the light bulb could be based on BLE (Bluetooth Low Energy). In this case, the gateway would bridge the connection between the lightbulb and the motion sensor. Figure 4 shows a sample sequence diagram of an IoT application. In the following sections, we look at how newer sensing techniques and sensors could help bring in new features, improve efficiency, and ease system maintenance.

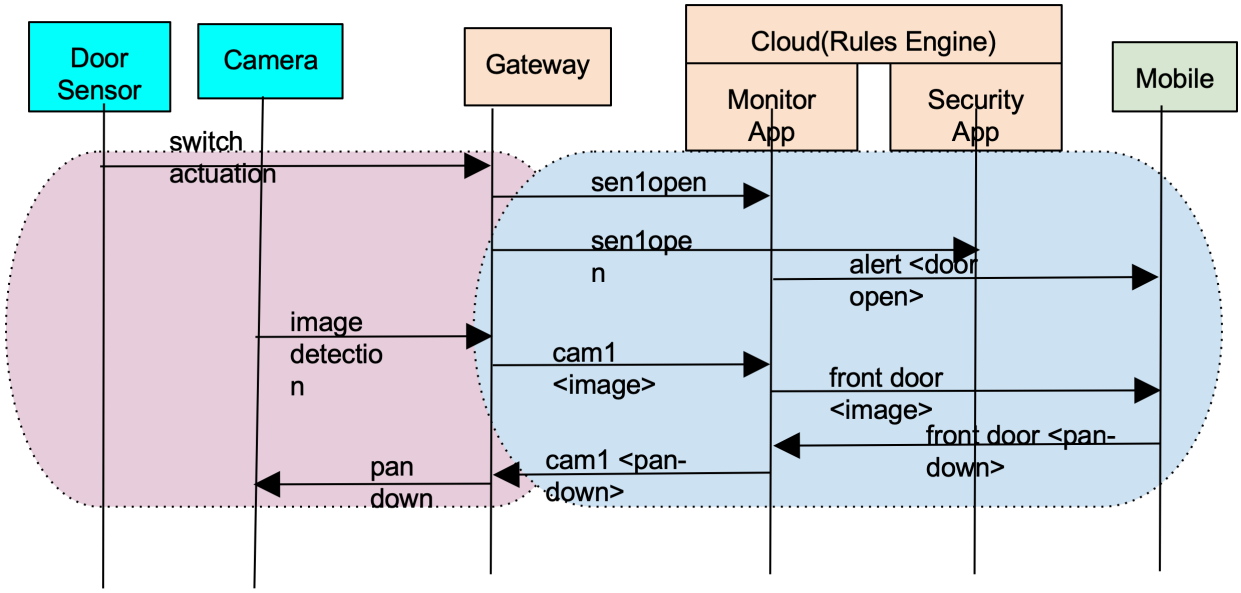

Figure 4 - Example Sequence Diagram of an IoT application

New Sensing Techniques

The current family of sensors have been operationally effective for a long period of time. As a result, any changes to those sensing techniques involves a lot of research and require ample confidence in the technology in order for them to be adopted. This section lists some technologies that show a lot of promise, are not a "heavy lift", in terms of adoption, and could work with the existing systems. The communication mechanism of these newer sensors with the rest of the system is compatible with the sensors and gateways already in the market (WiFi/Zigbee/Bluetooth.)

1. RF Sensing for IoT Applications

RF sensors have been around in the scientific community for decades, and are prevalent in avionics and military applications; they also hold great promise for residential IoT applications. We have been watching this space closely and have observed significant advancements, in terms of algorithms and sensors.

As mentioned, most IoT networks employ passive infrared/PIR-based motion sensors and cameras for surveillance applications. While these sensors work well and provide the desired results, there are some challenges. These are line-of-sight sensors, for starters, and thus cannot detect motion through a wall. Cameras are used mostly for outdoor surveillance, and are often perceived as being intrusive for indoor tracking (and, notably, activity monitoring in eldercare environments). These challenges could be easily overcome by instead using RADAR (Radio Detection and Ranging)-based sensing. RADAR has been historically dominant in aviation and military applications, but is increasingly applicable to residential and commercial applications. RADARs can detect presence and motion through walls, while providing good coverage, without cameras.

RF(Radio Frequency) devices that are compact, accurate, reliable, and inexpensive are currently commercially available. Over the past few years, attempts to apply such devices to biomedical measurements has increased. Although some studies applied these devices to medicine and health care, such research is still in its infancy. Nonetheless, radio-frequency sensing techniques -- originally developed for military applications, and later applied to search and rescue operations, such as locating earthquake survivors buried under rubble -- all carry plausible applicability for health care and home monitoring use cases, like aging in place and smart homes.

Doppler RADARs can be used to implement motion classification, which can be used for applications like activity monitoring, fall detection and Personal Emergency Response Systems/PERS. Traditionally, fall detection applications employ a wearable or push button device that needs to be activated after a fall occurs. The intent is to help the patient trigger emergency assistance. Using RADARs for fall detection is non-intrusive and does not need require manual intervention (pushing the button) to trigger an alarm. This matters because in many cases, people lose consciousness after falling, which obviates the applicability of such "push to enable" help calls. A RADAR, by contrast, monitors activities and can both auto-detect a fall, and raise an alarm. With machine learning capabilities, RADAR-based devices can also learn over time, to then more accurately detect falls.

Another form of activity monitoring enabled by RADAR is biometric, or the application of statistical analysis to biological data. Specifically, RADAR can provide effective, non-invasive and non-restrictive sensing techniques to acquire vital signs. For instance, RADAR could be used to monitor characteristics including body surface vibrations, mental state, and sleep apnea. For instance, RADARs can detect minute vibrations on the body surface, such as those induced by heartbeat and respiration. Simple equipment can

be used to self-monitor certain medical parameters or conditions, as well as to acquire related data required for senior living homes as well as medical facilities.

RADARs provide two specific attributes that provide accurate details about a person's locations and movement. FMCW (frequency-modulated continuous wave) RADARs provide range[3] and microdoppler[4] as the primary attributes. These parameters help an application to know the location of a target, and also effectively track movement of the target. Hence presence detection and motion detection are made possible, with a much higher resolution, to provide details on specific motion artifacts of the target (walking, sitting) including anomaly detection like fall detection. Doplar RADAR signatures are illustrated in Figure 5 (and the author wishes he had a nickel for every time he had to train the model to learn the "falling" artifact!)

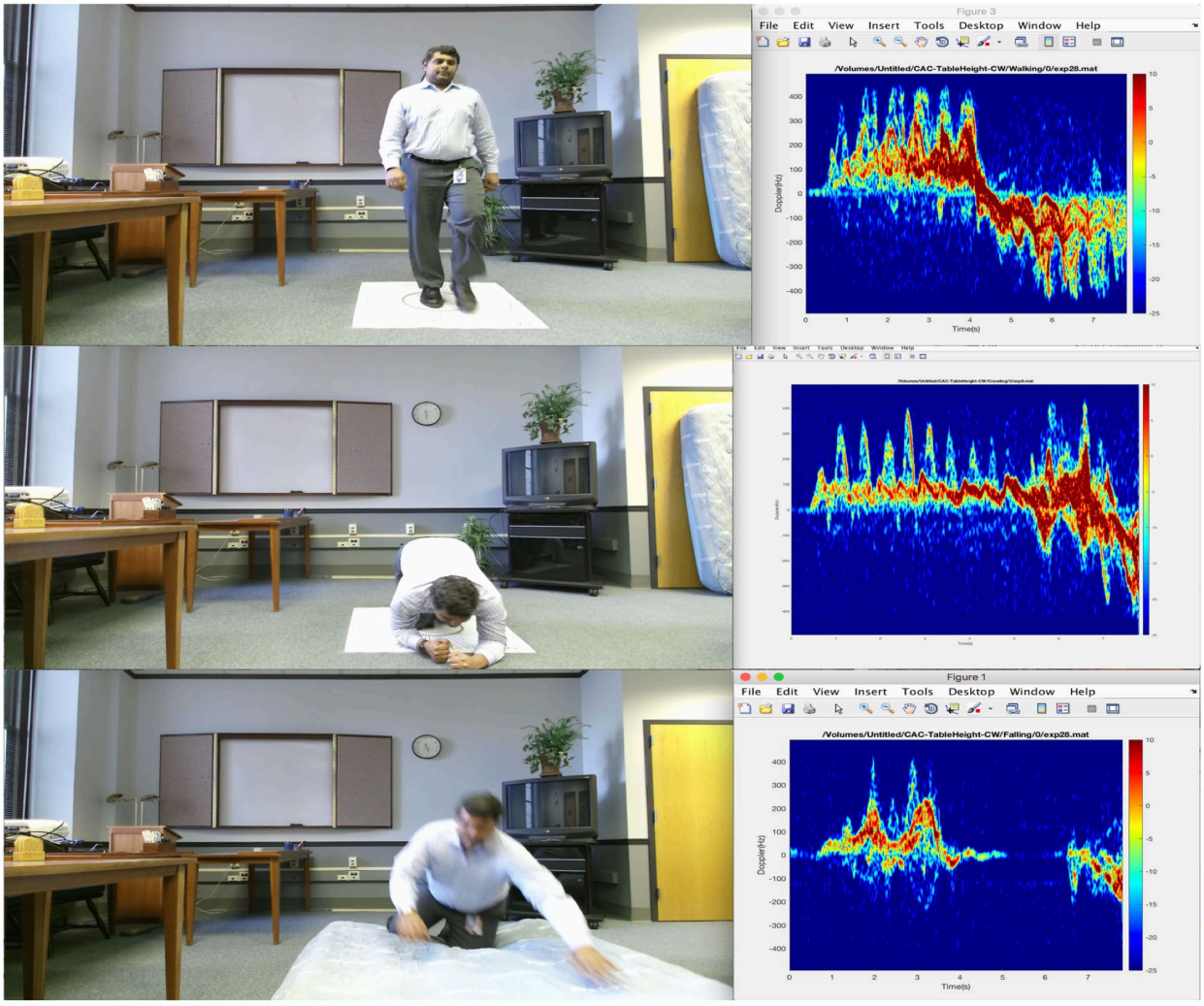

Figure 5 - Doppler Signatures for different motions

[3] http://www.radartutorial.eu/01.basics/Distance-determination.en.html

[4] http://www.radartutorial.eu/02.basics/Continuous%20Wave%20Radar.en.html

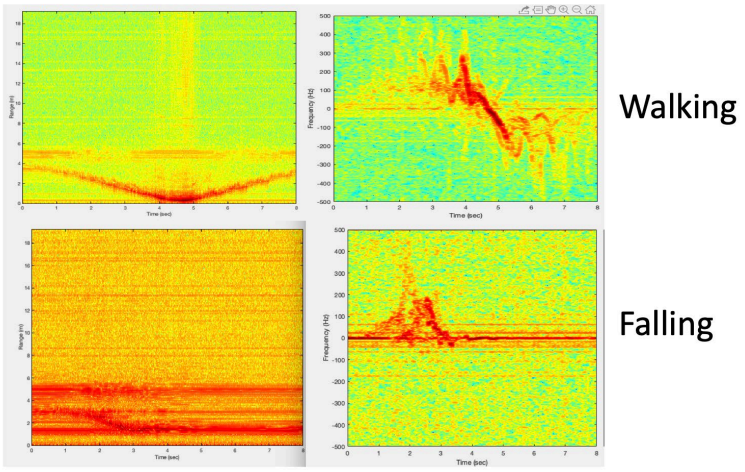

Figure 6 - Range Data for Walking and Falling using RADAR

6 shows the ability of a RADAR to detect motion artifacts, which could be used in many of IoT-based applications like healthcare and home security. 7 shows the ability of the RADAR to measure the distance from the AP (Access Point) and the target. This is helpful in detecting presence and location inside the home. The sensors would provide accurate position information, at the same time detecting postures. Perimeter protection is also possible with this technology. Since RF waves can penetrate walls, there is not a requirement for one sensor per room, which carries potential economic incentives that are beyond the scope of this paper but nonetheless worth acknowledging.

RADARs have already been used in cars to provide features like collision warning and prevention systems, as well as parking assistance and blind spot warnings. Extensive research has been done to ensure human safety while using RADAR systems, which have been proven to be safe. RADARs are thus a favorable sensing technology that IoT systems could use to enhance range and performance.

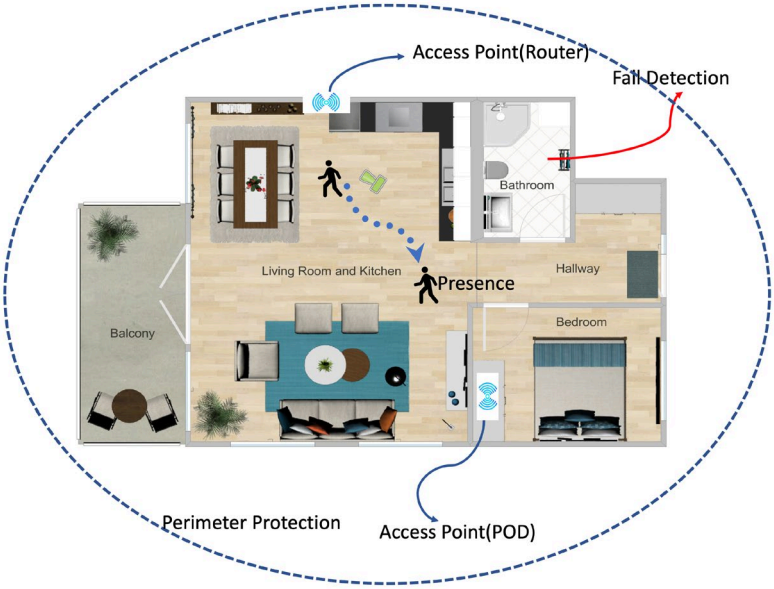

Figure 7 - Home Security/Automation using RF Sensing

2. WiFi as RF sensor?

Improvements in Wi-Fi technologies have made it possible to add more signal processing capabilities in the Wi-Fi chips, to function as RADAR. Specifically, a portion of the antenna could be apportioned to act as a RADAR, which would enable all the features supported by the RADAR previously discussed.

Newer Wi-Fi chips support elastic MIMO (multiple-input and multiple-output), which would give application developers the flexibility to dynamically choose the antenna pairs for multiple purposes. The system could use two antenna for RADAR applications, for instance, and the remainder of the antenna for Wi-Fi communications purposes. When there is no demand for communications traffic, more antennae could be in RADAR mode, for higher resolution imaging and better overall coverage. Figure 8 shows an example of an elastic MIMO configuration. Figure 9 shows the hardware and software components of such a sensing system. Using Wi-Fi is advantageous in that it makes use of existing hardware, and as such simplifies system maintanence.

The data colleted from an 802.11 AX [5] system shows that the Doppler signatures are similar to a traditional RADAR. Also, Wi-Fi pods help in expanding coverage and provide multiple data points to improve efficiency. Figure 10 shows Doppler signatures derived from a Wi-Fi system (top) and from a traditional 24Ghz RADAR system (bottom). These two look similar and hence algorithms that are developed and trained using traditional RADAR system could be easily ported across to a Wi-Fi system.

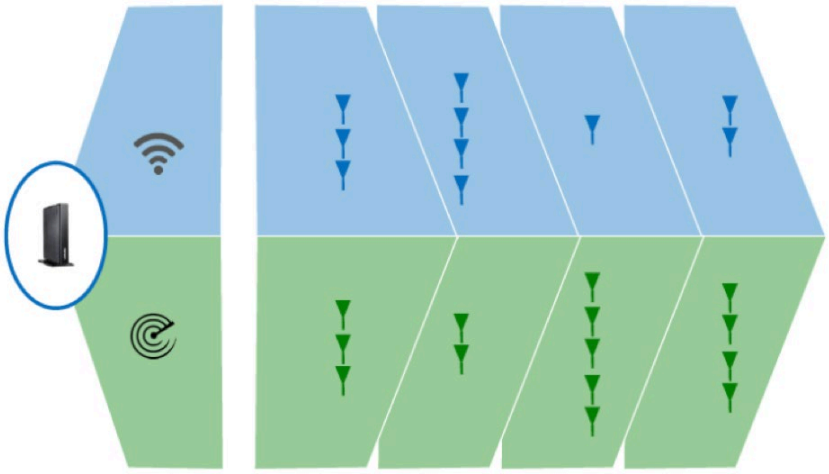

Figure 8 - Example MIMO system and WiFi RADAR Hardware and Software

[5] https://en.wikipedia.org/wiki/IEEE_802.11ax

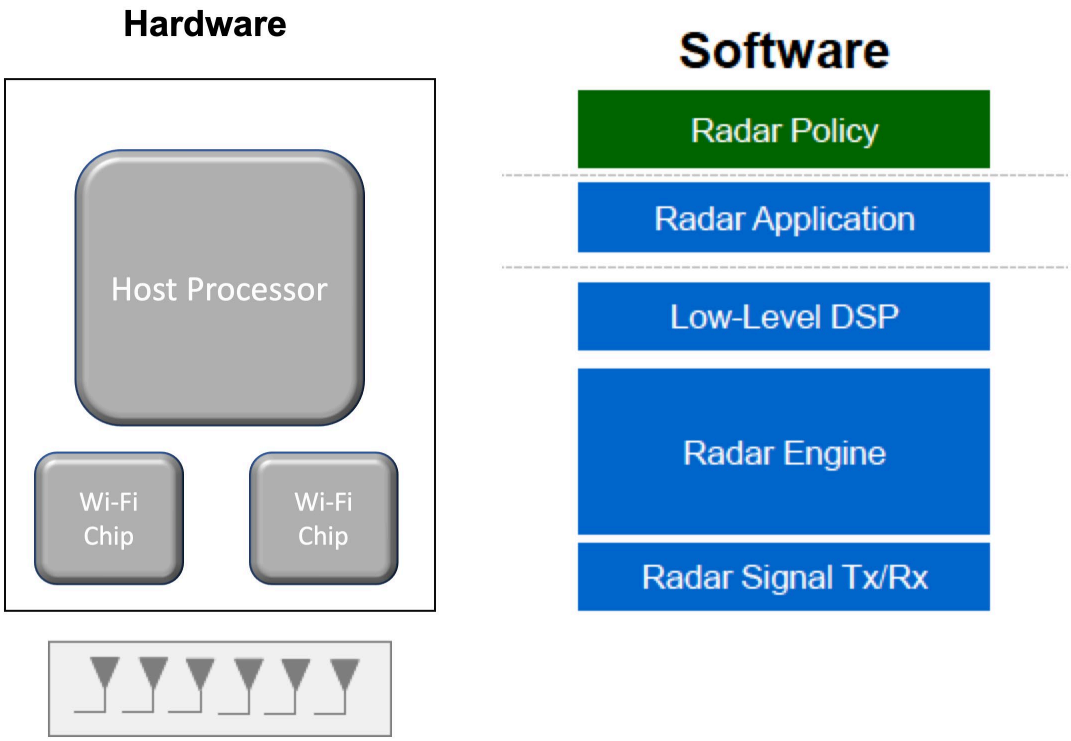

Figure 9 - Components of a Wi-Fi RADAR system

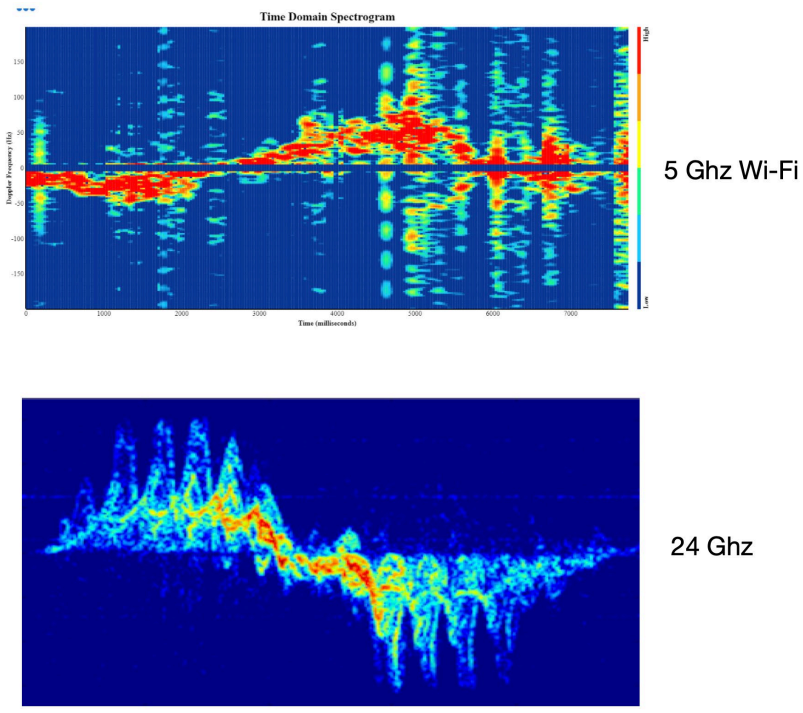

Figure 10 - Dopper Signatures of Wi-Fi and traditioal RADAR system

3. Audio-based Sensing

Acoustics analysis solutions can work when vision may be impaired, when obstacles are blocking the RADAR, and when sensors may not apply. Beyond the obvious solutions of using voice recognition, acoustic analysis applications can apply specific behaviors to the acoustic signature. Based on samples from an audio library, a list of events could be developed to track specific events. Using deep learning algorithms, sounds such as "door closing" or "water running" could be classified for correlation with daily activities.

Algorithms could be trained to detect anomalies like glass breaking, garage door opening, fire alarms and even calls for help. Figure 11 shows an example of a "confusion matrix" with a variety of sounds.

The diagonal represents correctly detected sound samples. Apart from the diagonal, the higher the number, the higher the chance of sounds getting confused with one another, which represents a high correlation.

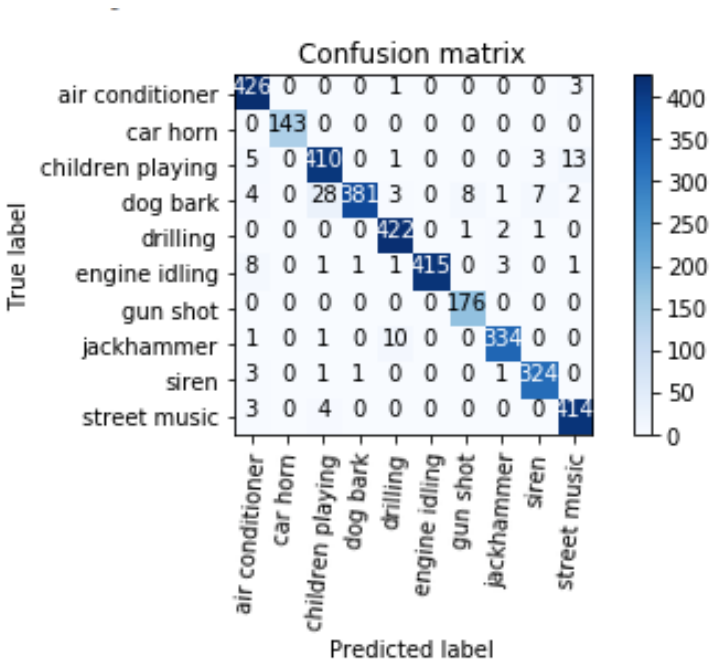

Figure 11 - Confusion Matrix for various sounds

Ambient noise can be widespread in the home environment, and as such must be accounted for. Any acoustic monitoring technology must use a machine learning algorithm, to distinguish the targeted sounds correctly. Audio attenuation can aid in echo location, but can create challenges for acoustic analysis. Another challenge is that some sounds are quite similar and are therefore difficult to distinguish, even with machine learning.

Examples of highly correlated sounds:

- Children playing outside vs street music
- TV vs. conversation within a house
- Gunshot vs dog bark
- Engine idling vs. air conditioning

There are currently no commercially available products for IoT applications which use acoustic analytics. While the use of deep learning algorithms in acoustic analysis is a fairly common practice, their use requires the development of individual modules for detecting sounds applicable to IoT applications. The technology itself is quite nascent.

Microphones capture dialog in addition to the environmental noises. Microphone use can also raise privacy concerns. Similar to the concerns around video analytics, as the technology evolves, there will be opportunities to abstract certain acoustic content, and secure it, so that privacy concerns are minimized.

Microphones for audio capture are often much less noticeable and intrusive than other monitoring technologies. Many devices are being added into the home which capture and process voice commands today. Amazon Echo™, Google Now™ and Apple Siri™ are examples of common voice capture solutions in use today.

There are several ways that acoustic analysis can be achieved, such as detecting sounds by running the raw audio input through a Fourier Transform. This calculates the frequencies per given unit of time, which can be displayed in a spectrogram. Once audio has been converted to a spectrogram, visual analytics engines, such as ConvNet, can be utilized for audio classification. Figure 12 shows an example of an acoustic event displayed as a spectrogram. Studies have shown that this technology could be applied to detect age, gender and also voice recognition, which would help to personalize the experience for the customer.

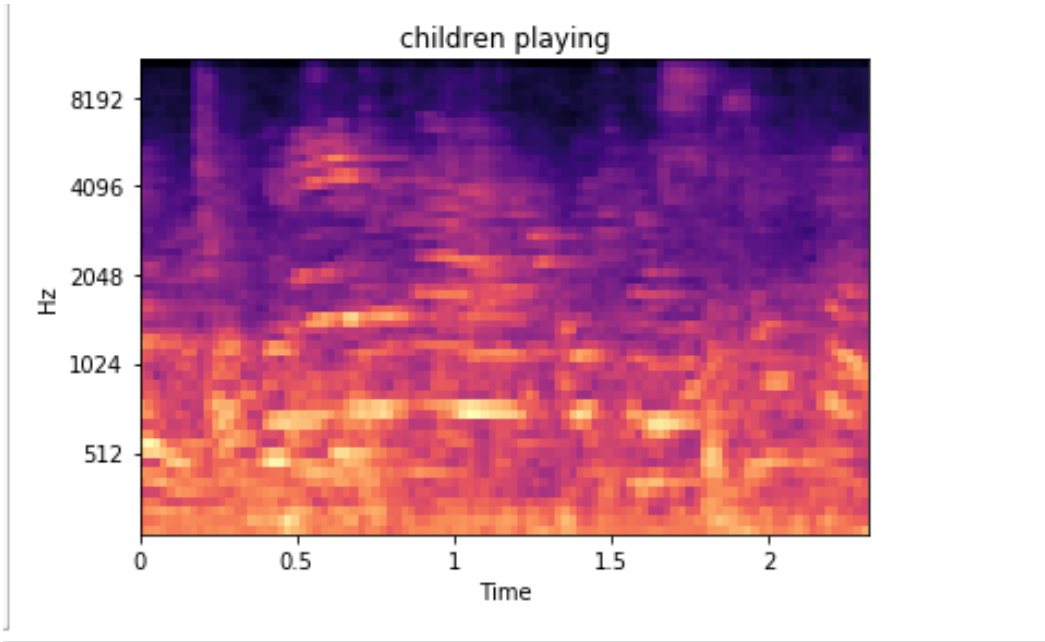

Figure 12 - Example Spectrogram of an Audio Signal

4. Predictive Analysis using Advanced Machine Learning

Significant progress is being made to adapt AI and ML techniques to IoT applications. These algorithms have played a significant role in offering new features and improving the efficiency of IoT applications. Algorithms exist, for example, to protect the customer's network and devices. That matters because the increase in IoT applications has led to an increase of attacks, such as bots that exist to compromise the home network – and also the entire network, if there are unknown network vulnerabilities.

Network security is an important aspect of providing peace of mind to customers. Many applications offer network security as a service, in order to protect a customer's data, network and devices. There has been significant research about how customer data could provide detailed insights and hence offer some of these features without using any sensors. It must be noted that such techniques carry huge implications for privacy, and as such need to be dealt with great care to ensure that no privacy-critical data is being used without proper consent from the customer.

Edge compute is another topic of interest, because newer chips can provide some of the advanced compute to the network edge and hence improve latency. An Edge compute system, shown in Figure 13, would also provide an enhanced environment of privacy – the data is being processed on-premise, and never leaves the home network. This would enable using sensors like cameras and applied computer vision technology. With this the model could be trained in the cloud and the model could be deployed at the edge.

Computer Vision-based applications could also be applied to anomaly detection and advanced features like facial recognition and object detection. (Facial recognition techniques are outside of the scope of this paper.)

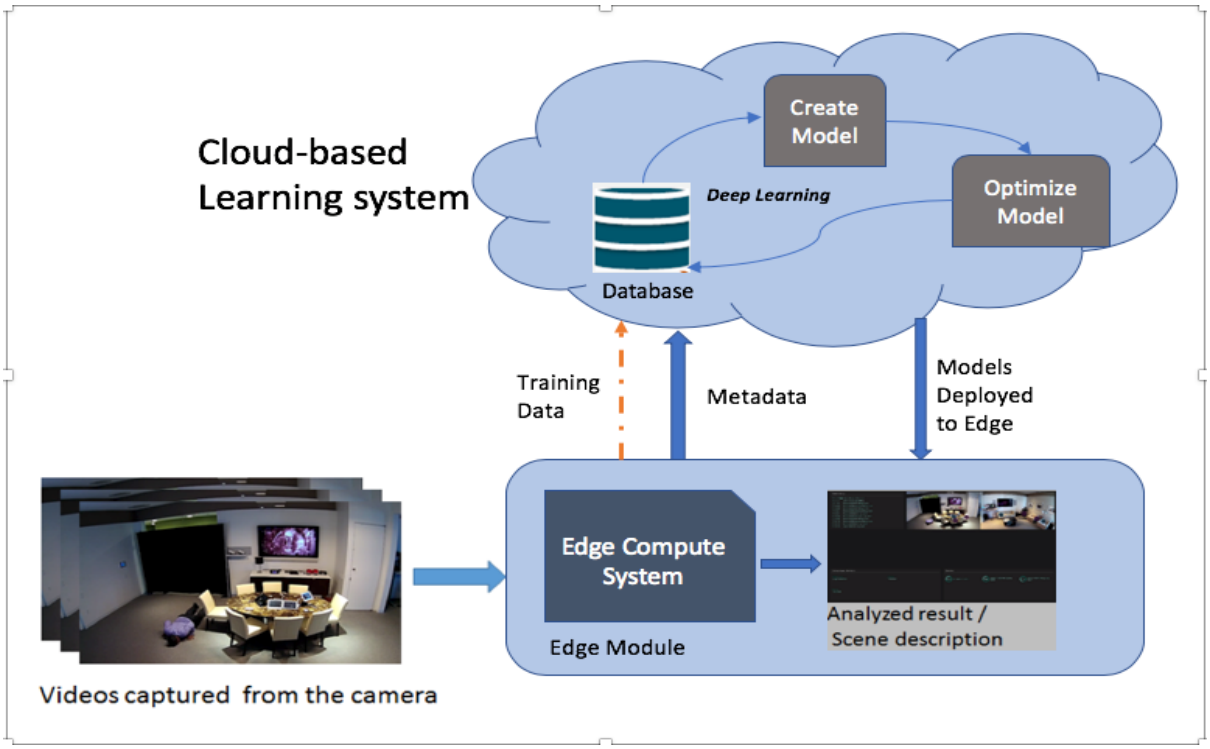

Figure 13 - Edge Compute System

Conclusion

Multiple potential use cases and technological viability indicate that IoT technologies can definitively provide peace of mind to consumers. There are innumerable examples that can address the peace of mind factor in a consumer's life – whether it involves tracking a child, to ensure that he/she left school and reached home, or being able to check on elderly parents to ensure that they're doing ok, and, most importantly, to be alerted when they need help.

In this paper we examined the current state of sensors in an IoT applications, and then examined the potential of a variety of new sensing techniques. These new sensors are of interest because they provide advanced features while improving efficiency.

A wide variety of solutions, ranging from simple beacons using Wi-Fi, to elaborate, cutting edge solutions based on military technology, are edging to the forefront of the technologically-relevant in the IoT. The non-invasive nature and improved accuracy of RADAR, for instance, yields strong potential for IoT applications.

RADAR can track and monitor postures (activities) with reasonable accuracy. Some activities, like talking and reading, cannot be suitably monitored using RADAR, because RADAR's sensing capabilities do not cover acoustics or visual analytics.

The ability to use Wi-Fi signals to detect presence and to provide perimeter protection makes it easier to maintain, as it is a complete and widely deployed software solution that is easier to scale.

Acoustic analysis is very helpful in cases where visibility or RF penetration is low, and enables specific aspects in terms of security.

The paper also looked at the shift of critical data processing to the edge, which would reduce latency and also improve privacy, in that the data doesn't leave the home network. This would allow the application of Computer Vision- based techniques to a variety of applications.

Another important aspect that is under development is "Sensor Fusion". This involves employing different types of sensors and analyzing their data in unison to provide enhanced features – for example, combining RADAR,audio and/or video analysis. Such combinations would add another dimension to the sensor and provide greater overall detail.

Finally, we looked at predictive analysis, which, while interesting, carries considerable privacy implications which would have to be considered carefully and applied to very specific cases.

Abbreviations

AI	Artificial Intelligence
AP	Access Point
BLE	Bluetooth Low Energy
FMCW	Frequency Modulated Continuous Wave
Hz	hertz
ISBE	International Society of Broadband Experts
MIMO	Multiple Input Multiple Output
ML	Machine Learning
PERS	Personal Emergency Response System
RADAR	Radio Detection and Ranging
SCTE	Society of Cable Telecommunications Engineers