# IoT Emergency Detection Devices

ISAAC TRESENWRITER, University of Cincinnati, United States
MO DANIEL, University of Cincinnati, United States
NATHAN ELROD, University of Cincinnati, United States

**ABSTRACT** In a world where technology continues to vastly grow and improve, IoT devices have increasingly become more and more a part of people's everyday lives. Although that is the case there is a need to understand how to better use these devices for threat detection. This paper presents early work to understand gaps in this regard using a review of previously used techniques to identify known threats to households. Through the use of smart home device clusters we seek to effectively reduce the amount of false alarms and create a more reliable resource for home residents.

**ACM Reference Format:**
Isaac Tresenwriter, Mo Daniel, and Nathan Elrod. 2020. IoT Emergency Detection Devices. In *IT Research Symposium '20: School of Information Technology IT Research Symposium, April 14, 2020, Cincinnati, OH*.https://scholar.uc.edu/

## 1 INTRODUCTION

The past decade has seen a marked increase in natural disasters. "Extreme weather events, wildfires, earthquakes, tsunamis, and slow-onset disasters like droughts and polar vortexes have left many American homes in peril." Pioneering[4] Alabama's recent tornado outbreak and 2018's record-setting wildfires in California are quickly becoming the new normal, and with river flooding in cities worldwide, there has emerged an immense challenge to urban resilience. Kasler[2] These disasters have destroyed numerous homes and caused incredible losses. Smart home devices have created opportunities to identify threats to smart homes, unfortunately, there are few connections between data rich smart homes and the emergency response services. One reason for this is that current Internet of Things (IoT) devices in smart homes are noisy–producing false alarms that emergency response services do not have the capacity to validate. Frustrating individual and government efforts to address these types of threats, has lead to the inadequacy of many devices to accurately detect them. Our smart solution seeks to improve threat detection and make for a more accurate deferential determination, when it comes to natural disasters negatively effecting the home. With succession this would ultimately cut down the rate of false alarms, save money and cut down on the home loss or damages due to natural disasters.

## 2 PROBLEM BACKGROUND

The Internet of Things (IoT) refers to a paradigm where physical devices (e.g., home appliances, environmental sensors and actuators, vehicles) are interconnected using a communication network that allows for real-time data exchange and control. Kyung[3] The is a means over which internet devices communicate and share information about their environment.

It has been well demonstrated that many devices, smart or otherwise, are unreliable at threat detection on their own. A false alarm, also called a nuisance alarm, is the deceptive or erroneous


*IT Research Symposium '20, April 14, 2020, Cincinnati, OH*

report of an emergency, causing unnecessary panic and/or bringing resources (such as emergency services) to a place where they are not needed. Farlex[1] Smoke alarms, for instance, may be triggered by only a small amount of smoke; high humidity might also falsely trigger the device. Vivint[6] In 2011, between 94 percent and 98 percent of all burglar alarm activation's in the US were falsely triggered. Sampson[5] Programs such as those implemented by the city of Seattle, Washington have been able to effectively reduce this number, and we believe that our approach will make an dynamic impact as well.

## 3 RESEARCH QUESTION

RQ1: How can combinations of IoT devices be used to improve the detection of threats in smart homes?

## 4 METHODOLOGY

We examined a number of common threats a smart home might potentially face, and assembled a list of IoT devices, for which may aid in emergency threat detection. We also have considered devices which we would use to detect threats such as a fire, flood or robbery in smart homes. By connecting multiple of these IoT devices we plan to use the different threat detection analysis methods within each device, to more accurately determine what is a true emergency threat versus a false alarm. Anytime a potential threat is detected, a notification will be sent to the owner and his/her designated family member, with the objective being to minimize or prevent damage to the home/building.

## 5 CONCLUSION AND FUTURE WORK

Our goal is to use IoT devices to create solutions to security issues, prevent loss and inform individuals before damage is done to their homes.We have identified possible device clusters that we feel will more accurately report threats, versus a single device alone. By connecting multiple IoT devices within these devices clusters, we plan to combine the different threat detection analysis methods, to more accurately differentiate what is a true emergency threat versus a false alarm.

Our main objectives for the future work is to create a test simulation environment with a number of different scenarios. Each of these scenarios would consist of gathering a number of different suites containing helpful devices and test groups. Within these tests groups we will compare these different devices in collaboration with one another, through device group testing and single testing.

## REFERENCES

[1] Farlex. [n.d.]. Nuisance Alarm. Retrieved March 2, 2020 from https://www.thefreedictionary.com/Nuisance+alarm
[2] D. Kasler. 2018. Worst wildfire year since when More California acres have burned in 2018 than the past decade. Retrieved March 2, 2020 from https://www.sacbee.com/latest-news/article221788220.html
[3] Lee H. and Lee, K.C. 2004. Network-based fire-detection system via controller area network for smart home automation. *IEEE Transactions on Consumer Electronics* 50, 4 (2004), 1093–1100. https://ieeexplore.ieee.org/abstract/document/1362504
[4] Pioneering Minds. 2019. Using IoT To Protect Our Homes And Cities From Climate Change. https://www.pioneeringminds.com/iot-protect-homes-cities-climate-change/
[5] Sampson R. 2011. *False Burglar Alarms 2nd Edition* (2nd ed.). https://cops.usdoj.gov/RIC/Publications/cops-p014-pub.pdf
[6] Vivint. 2019. Combination of techniques could improve security for IoT devices. https://www.vivint.com/resources/article/smoke-detector-sensitivity

| Threat | Devices | Reliability |
|---|---|---|
| Flood/n | • wireless sensor networks eg<br>• water leak detectors placed near appliances, such as washing machines, dishwashers, or water heaters, or they can be mounted in basements, kitchens, bathrooms, toilets, or garages to prevent burst pipe disasters.<br>• Water Alarms<br>• Humidity sensors | • sound<br>• pollution levels<br>• humidity |
| Fire | • Smart Smoke Detectors<br>• Network work-based fire detection<br>• Thermostats<br>• Humidity sensors | • Smoke<br>• heat<br>• Gas<br>• Carbon Monoxide |
| Robbery | • Video doorbell(This device allows you to see who is at your door from your smartphone).<br>• Passive Infrared (Detects body heat (infrared energy))<br>• MicroWave (passive infrared (PIR) plus Microwave (MW) – an active sensor, to monitor an area)<br>• Dual Technology Motion Sensors(passive infrared (PIR) plus Microwave (MW) – an active sensor, to monitor an area) | • Movement detection<br>• Breaking objects like doors. |

Table 1. IoT Threat Detection Methods