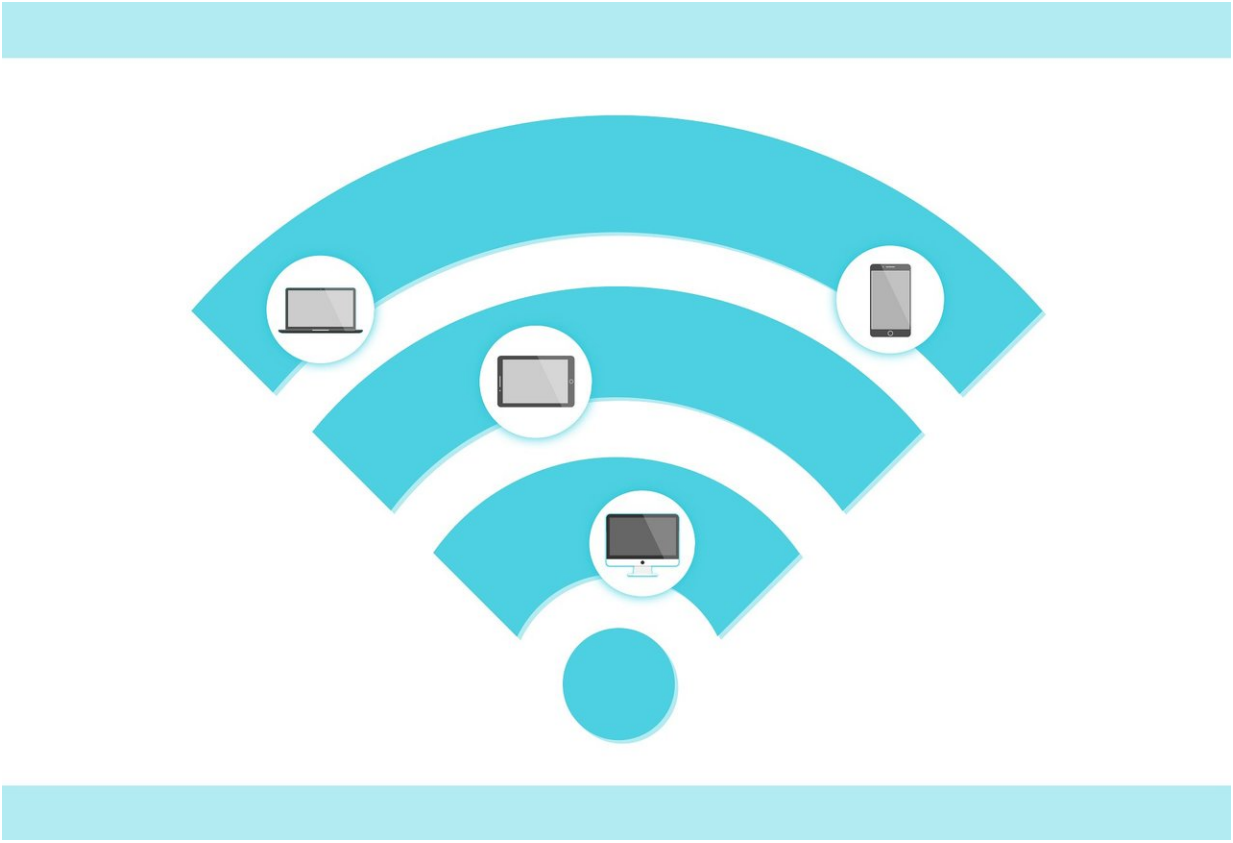
How your WiFi can protect against intruders

April 2 2018, by John Aasted Sørensen



Credit: CC0 Public Domain

The applications of wireless networks go far beyond logging onto the free Airport WiFi while you wait to board your flight, or binge watching the latest Netflix series on a rainy Sunday afternoon.

WiFi is routinely used for such applications, connecting people and allowing information to be transferred from one person to another (file sharing), between a person and a computer (streaming and Internet use), or between two or more machines (cooperating robots).

But very different applications are under development at the Technical University of Denmark (DTU) and the IT University of Copenhagen (ITU) in Denmark, (here and here), which use WiFi Internet for very different purposes: To identify and track the movement of people within a building covered by a wireless network. It's a high tech surveillance system that not even The Night Fox of Ocean's Twelve could capoeira his way out of without triggering the alarm.

A new generation of security monitoring

These applications could lead to a new generation of security or monitoring systems for detecting physical intrusion by humans in your home or workplace, using only the radio frequency (RF) signals of your wireless network.

In some cases, this could avoid the cost of physically mounting traditional burglar alarm systems, such as the widely used Passive InfraRed (PIR) sensors, ultra-sound sensors, door contacts, motion detectors, or glass break detectors.

Most of these devices already communicate wirelessly, so what I'm suggesting is a rather small adjustment that might just change the way we think about security.

A simple security system

Consider a classic PIR based surveillance system, where the PIR unit is

divided into two parts: An infrared sensor and a wireless communication part.

The PIR is physically mounted in a room and communicates, typically via WiFi, with the main alarm system elsewhere in the house.

When an intruder enters the room, the PIR sensor measures the heat radiation from that person and converts these measurements to a digital signal, which is then communicated through the wireless network to the main alarm unit. If the changes in heat radiation are sufficient then the alarm is sounded.

This system can be rearranged simply by removing the infrared sensor and retaining only the wireless communication units.

In this new configuration, the intruder is identified by changes in radio frequency signals exchanged between the two communication units. No need for an infrared sensor or fancy dancing laser beams!

Discarded data could spot a burglar

Existing setups already detect how radio waves change, or ripple, as they move around objects between the two units.

Typically, the wireless network transfers this information using many, closely spaced, discrete frequencies. The system identifies how the physical environment, such as the couch in the sitting room or your coat hanging by the front door, influenced the radio waves at each of these frequencies, corrects for it, and then deletes the data.

This allows the greatest throughput of data between the units.

But it is this discarded "environmental" data (the position of your sofa or

coat) that could also identify any changes in the physical environment, such as an intruder moving through the hallway. So all we just need to do is capture and analyse these data to spot the intruder.

An alarm system that can see through walls

Such a radio frequency surveillance unit could be much cheaper, since removing the need for a traditional sensor would reduce the overall cost. In addition, the simpler system could be more reliable as there would be fewer components that could go wrong.

There's also the possibility of being able to "see" through walls. Certain radio frequency waves propagate through walls, allowing the detection of intruders in the next room or upstairs from one single unit.

Although this might not be as useful as it first sounds: In the middle of a building it might be great to be able to "see" through walls, but placed along the outer walls of a building this might be a weakness if you're constantly woken up by the next door neighbour coming home in the middle of the night!

An example on such a system, targeting family homes or apartments is already available in Canada. While here in Denmark we are working on the next steps of research in this area and so that you will one day, in the near future, be able to install a similar system in your own home.

Looking ahead, we expect many more new applications to arise from existing wireless networks, far removed from their original intended purpose.

This story is republished courtesy of ScienceNordic*, the trusted source for English-language science news from the Nordic countries. Read the original story* here.

Provided by ScienceNordic