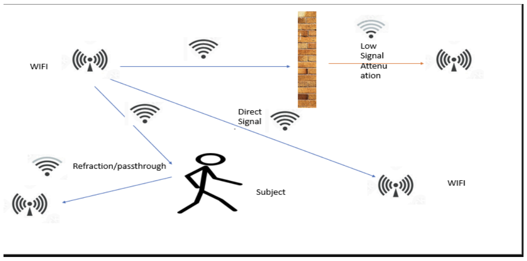
What WiFi signals technical that can be used in Gun Detection

Kieran Scanlon, Delray Frierson, Felipe Trinidad Pilier

I. Problem Background

WiFi (Wireless Fidelity) has become one of the most useful technologies in the Internet of Things. Becoming an ubiquitous term that anyone, even the layperson can recognise. These high frequency radio signals have been providing a service since IEEE introduced the 802.11 standard. Making the world an interconnected network. One service that is being developed and researched is how it can aid in the use of object detection. Or more specifically in the case of firearms. Firearms are a large security risk and are a hot topic in the realm of security. Having a detection method more than the standard metal detector that can be unobtrusive would be a boon to the security landscape. The crux of this issue is the signal which sends back the data that a firearm is in the vicinity. There are many signals which may be useful for the job. However there are also factors that hinder the reliability of a wifi signal. Propagation and attenuation can be a deciding factor in the technology.



In detection of a high risk object, reliability and accuracy is everything.In this paper we will provide an in-depth analysis of each of the signals that WiFi provides in the IEEE 802.11 protocol. How each aids in the detection of a firearm. As well as the implementation of those signals and using channel state information (CSI) to use this data.

II. Potential Solutions

The most promising adaptation in the field of detection is the method of recording the changes in CSI amplitude. Researchers in the university of China were able to leverage this tech to detect movement as particular as fall detection by using a combination of CSI techniques, using a signal preprocessing model , a signal segmentation module and a fall detection module. What we are most interested in is the signal preprocessing and segmentation. These detection techniques can accurately detect disturbances in the CSI phase creating fluctuations in the signal of detection.

Unfortunately this only tells us that this is possible but in a non-obtrusive environment. Further details show that there is significant delay in signal to transmitter. This research goes in depth about the difference of 802.11 signals in target detection in a low clutter environment and a high clutter environment. This is where our aforementioned signal processing model comes into play since this can reduce the errors that can occur in attenuation. This specific model was simulated using a OFDM (orthogonal frequency division multiplexing). A concept we will see throughout this paper. Data was also differentiated by the way that the experiment was conducted. Transmitter and receiver positioning is important; both in high density and low density environments. In combination with a Chebyshev filter. Noise and interference was cut down to minimize the error in the signal data. Their signal was processed using the

Kaiser-Bessel window which is a filter used for signal processing. That data is useless if garbage data is used in place of the useful data therefore, an algorithm was used to determine the number of false alarms that the system generated. The “CLEAN” algorithm adapts and determines the limit of power a receiver can feasibly handle. Their data showed that the signal accuracy can be improved by the number of transmitters that were placed in addition to the time for data collection integration. This however leads back to the Concept of CSI based technologies for signal propagation, which [2] also details a methodology in which the Received Signal Strength (RSS) can be used to concentrate the position of an object. Which is much more useful for our purposes in firearm detection. It uses the detection based on the power of the reflected signal. Coincidentally, this signal is untenable at longer ranges and suffers from a lack of accuracy. The research proposes a solution to this in the form of Channel Impulse Response (CIR). By using CSI and CIR we can more accurately use multipath propagation to parse the signal information. Using the frequency signal from IEEE 802.11 a/g/n we can estimate the OFDM signals to more accurately determine the characteristics of the object in question, in this case a firearm.

CSI and (IEEE 802.11 a/g/n) seems to be the most robust signal to effectively detect metal that is concealed. [3] proposes that the changes in amplitude from a metal object can aid in detection. Like [2] the method uses (OFDM) with hardware modifications that allows the devices to carry a data transmission signal over a 20MHz bandwidth. The findings were that the target while stationary was able to find a noticeable variance, enough to make a distinction between the metal and non metal signal reflection. Metal surfaces happen to be a reflector for radio signals.

Another solution to detecting guns using WiFi signals is a WiFi based sensing system called IntuWition. IntuWition’s main function is to send out a WiFi signal from a drone and scan the returning scattered polarized waves sent out from the drone. The reason why the returning waves are different from when they were first sent out is because they have been reflected off another service. Each service the WiFi signal reflects off of changes the signal slightly by either scattering it or changing the signal's polarity. Due to this change we actually tell what object the signal reflects off from, and what that material is made out of.

IntuWition is able to detect all of this because it can send and receive these signals all without additional wireless infrastructure. IntuWition is able to function on the already pre existing WiFi radio waves found on a drone without compromising the drone capabilities. 4 antennas are equipped to the drone, one set up vertically to transmit the signals and 3 set up horizontally and perpendicular to each other to receive the reflected signals. Each antenna is connected to an Intel 5300 AGN card that runs the Linux 802.11n CSI tools to get the information.

In practice IntuWition would send out a drone equipped with the antennas to transmit and receive the wifi signals to determine what is around the drone and its environment. The drone is then able to interpret that data IntuWition gives it, in order to know what the objects around it are made from. This environmental interpretation extends to people, copper, aluminum, plywood, birch, and more. However while IntuWition has made some great strides in developing this wifi based sensing tool it does have its limitations.

IntuWition is still a very new tool and naturally has some downsides to it. For starters IntuWition can have difficulties determining the material of a weak reflector signal. This can be because of the distance the signal has to travel or the size of the material. Another major problem for IntuWition is that it has difficulties separating objects from one another. IntuWition might think a human could actually be a part of a wall simply because they were leaning on it slightly. Lastly the biggest flaw with IntuWition is that it does not deal with multi-bounce reflections well as each reflection reduces the power of the receiver. This can not only lead to miss classification of material but could also be wrong entirely due to inaccurate data.

While IntuWition has many upsides to its sensing based system, it would need much further development and testing to be used as a viable option to detect guns. IntuWition is able to base through walls and work without preexisting wifi infrastructure since it's set up on top of a drone. However the flaw with materials blending into each other would need to be resolved in order for IntuWition to be able to find specific materials.

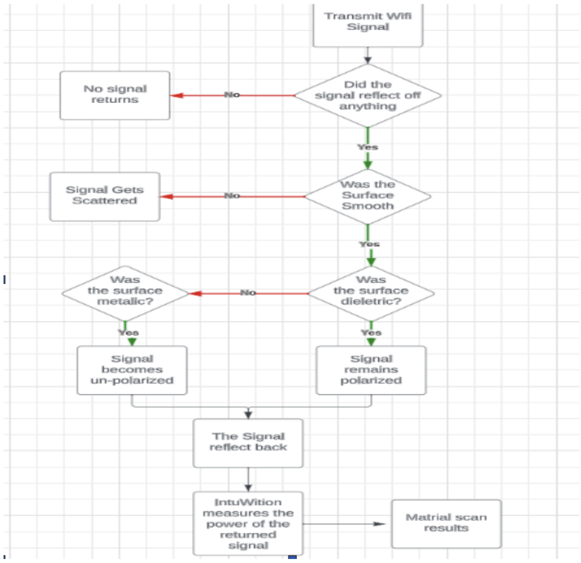


Fig.1 IntuWition logic flowchart

Many studies require the person of interest to be stationary and can easily create an inconvenient bottleneck in the facility's access point(s). One solution to this stems from the current emergence of machine learning and artificial intelligence. Evolv Technology has recently gained traction with its innovative take on security protocols that detect metallic and non-metallic weapons. According to Peter George, the CEO of Evolv Technology, they use advanced sensors, cameras, and artificial intelligence to find threats by picking up material composition, shape, and density. On the user side, they do not have to go through the stride-breaking experience of being stationary and exposing themselves to harmful X-ray scans.

Evolv primarily operates in settings that suffer heavily from the inconvenience of long lines such as schools, convention venues, concerts, and sports events. Because privacy becomes an issue of ethics, metadata from users is only taken with the user's consent. The data then gets sent to their Amazon Web Services cloud and is fed into the artificial intelligence. This allows the scanners to increase the accuracy of detected threats. In the year 2020, COVID-19 weaponized people, giving them the potential to spread the virus. Thanks to machine learning, Evolv scanners were able to recognize elevated body temperatures and raise and alert security if such a danger gets picked up.

However, one major drawback of using machine learning is that it simply does not have enough knowledge of concealed weaponry at the moment. According to a report by Blair Sabol on Live5news, a field test in Ohio in 2021 showed that Evolv detectors did not catch concealed knives forty-two percent of the time and missed micro-compact guns. As knives are the most common concealed weapon, this poses a great danger to the sense of security that the user is entitled to.

Experiments on WiFi signals are currently experiencing similar difficulties to those of Evolv Technology. Along with the likelihood of false positives, it is not at the point where it can accurately produce an image of concealed objects. With artificial intelligence being the talk of modern media, we utilize its inherent learning capabilities to rectify such risks. The only solution to this is to continue to feed the artificial intelligence information for it to learn. AI systems “learn” by identifying patterns and relationships in data that allow them to make predictions and decisions. With repeated testing, AI-incorporated systems can pick up on composition and shape and will eventually be recognized through WiFi signals’ reflections.

As mentioned before, IntuWition is a currently emerging tool that provides a safe way of metal detection. The current problems with it revolve around its inability to distinguish different weapons. By collecting data through the access points of schools, performance venues, and offices, the system can learn metallic items that the average citizen carries on their person. Combining the IntuWition drones with the data they need will provide results with much higher accuracy. It will also provide a safe alternative to typical X-ray and infrared scanners.

References

[1] Bahache, Mohamed, et al. “An inclusive survey of contactless wireless sensing: A technology used for remotely monitoring vital signs has the potential to combating COVID-19.” *RS Open Journal on Innovative Communication Technologies*, 2020, https://doi.org/10.46470/03d8ffbd.5b3676f3.

[2] Gorla, Praveen, and Teerapat Sanguankotvhakorn. *Object Detection Using Wireless Signals*, 2019, https://doi.org/10.35543/osf.io/ug9xk.

[3] Hanif, Asif, et al. “Non-obtrusive detection of concealed metallic objects using commodity WIFI Radios.” *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, https://doi.org/10.1109/glocom.2018.8647871.

[4] Khan, Faiza, et al. “Wi-Fi signal analysis for heartbeat and metal detection: A comparative study of reliable contactless systems.” *2019 6th International Conference on Dependable Systems and Their Applications (DSA)*, 2020, https://doi.org/10.1109/dsa.2019.00018.

[5] N, Mahiban Lindsay, et al. “Real-time object detection with tensorflow model using edge computing architecture.” *2022 8th International Conference on Smart Structures and Systems (ICSSS)*, 2022, https://doi.org/10.1109/icsss54381.2022.9782169.

[6] Sabol, Blair. “Report Shows A.I. Weapons Detectors Used in Schools Are Not Always Effective.” *Https://Www.Live5news.Com*, 22 June 2023, www.live5news.com/2023/06/22/report-shows-ai-weapons-detectors-used-schools-are-not-always-effective/.

[7] Sabol, Blair. “Report Shows A.I. Weapons Detectors Used in Schools Are Not Always Effective.” *Https://Www.Live5news.Com*, 22 June 2023, www.live5news.com/2023/06/22/report-shows-ai-weapons-detectors-used-schools-are-not-always-effective/.

[8] University, Diana Zhang Carnegie Mellon, et al. “On the Feasibility of Wi-Fi Based Material Sensing: The 25th Annual International Conference on Mobile Computing and Networking.” *ACM Conferences*, 1 Aug. 2019, dl.acm.org/doi/10.1145/3300061.3345442.

[9] Wang, Chen, et al. “Towards in-baggage suspicious object detection using commodity WIFI.” *2018 IEEE Conference on Communications and Network Security (CNS)*, 2018, https://doi.org/10.1109/cns.2018.8433142.

[10] Wu, Kaishun. “Wi-metal: Detecting metal by using Wireless Networks.” *2016 IEEE International Conference on Communications (ICC)*, 2016, https://doi.org/10.1109/icc.2016.7511472.

[11] Zhang, Daqing, et al. “Anti-fall: A non-intrusive and real-time fall detector leveraging CSI from commodity WIFI devices.” *Inclusive Smart Cities and E-Health*, 2015, pp. 181–193, https://doi.org/10.1007/978-3-319-19312-0_15.

Kaushik, Shailandra. “An overview of Technical aspect for WiFi Networks

Technology .” *International Journal of Electronics and Computer Science Engineering*.

Bandyopadhyay, Prof. Samir K, et al. “Identifications of concealed weapon in a Human Body.” *Department of Computer Science and Engineer, University of Calcutta*.