Military Cyber Affairs

Volume 1 | Issue 1 Article 5

January 2016

Reliable Presence Detection through Passive IEEE 802.11 Management Frame Sniffing

Paul L. Jordan
Air Force Institute of Technology, paullj1@gmail.com

Andrew J. Sellers
United States Air Force Academy, Andrew.Sellers@usafa.edu

Reliable Presence Detection through Passive IEEE 802.11 Management Frame Sniffing[1]

PAUL JORDAN, Air Force Institute of Technology
ANDREW SELLERS, United States Air Force Academy

Modern automated control systems leverage significantly different and disparate data sets for modeling and decision-making. Yet, dynamic human presence detection and identification is not widely used in these systems despite the enriching effect such information would have. We behave in unpredictable ways and are not easily identifiable by computers. This paper outlines a method for reliably and passively detecting presence of a person and identifying that person by exploiting existing ubiquitous infrastructure: Wi-Fi networks and that persons Wi-Fi enabled smartphone without installing any additional software. We further enumerate several applications ranging from home security to energy efficiencies. We explore the security and moral implications of automated person tracking as well as suggest reasonable mitigation measures.

1. INTRODUCTION

Today, presence detection is done predominately with infrared motion sensors. Motion sensors are not as reliable or as effective as we would need them to be for many purposes. For example, if one needed to know the presence of a person in a room for a temperature control system, if that person were to sit still while reading a book or take a nap, the motion sensor may not detect any motion and therefore eventually determine that the room is empty. Our method depends on the presence of a device that is constantly beaconing information about itself in such a way that automating presence becomes trivial.

An equally troubling problem is accurately and reliably identifying people. Biometric equipment exists and continues to become more accurate and reliable, but it is still very expensive. In the home security domain, it is easy to determine when someone has entered a home if they trip a sensor while an alarm is armed, but it would be more useful to know the identity of a potential intruder to make decisions about that potential threat. Our method works by intercepting frames containing unique Media Access Control (MAC) addresses. Since people tend to be the only ones carrying their own cell phones, this method can reasonably be used to identify who is present.

As computers decrease in size and become cheaper to produce, consumers are beginning to carry these smaller computers with them wherever they go. The smartphone is the most prevalent of these devices today and the “wearable” category is only growing. In this paper, we outline our method of reliably determining the presence of these devices as well as their unique identity and prove its reliability. Since these devices are then associated with a person we can effectively deduce that the devices owner is also present.

It should be noted here that through extensive testing outlined in this paper, we have determined that the reason for the beaconing of this sensitive personally identifying information is due to the recent proliferation of “Location Services” in smart phones. One of the ways the location of the smart phone is determined is by sending a broadcasted probe request to learn the wireless access points in range. The access points that respond are then correlated with the OS manufacturers crowd-sourced database of BSSIDs and associated locations to determine if a location has already been assigned. If it has, then the phone can calculate where it is. If not, a location is assigned based on the current location of the device obtained through alternate means (GPS, other access points, or cell towers).

[1] The views expressed herein are solely those of the authors and do not reflect the official policy or position of the U.S. Air Force, the Department of Defense, or the U.S. Government.

The major smartphone OS manufacturers all claim that they do not use their customers location data ([1,5,8]), but we have observed that in order to obtain their crowd-sourced databases of wireless access points and associated locations, they depend on their users constantly mapping these access points consequently allowing anyone within about one hundred feet to detect the presence of said customers.

Finally, out of all concerned parties, the U.S. Military should be one of the most prominent. On both sides of the freshly-minted Cyber coin there are both benefits and risks of which the Government should be aware. We explore those risks and benefits to the Offensive Cyber and Defensive Cyber Operations. The risks include unwillingly giving up our locations as smartphones proliferate amongst our leaders and personnel, while this technology can also be leveraged by the emerging Cyber Mission Force to exploit controlled infrastructure in order to account for adversaries.

2. RELATED WORK

Much previous work has explored exploitation of the beaconing of IEEE 802.11 probe requests [4,6,7,11,12,13,14] but none of the existing approaches operated completely passively, were tested against handset operating systems covering a significant majority of the smartphone market, or explored the reliability of these probe requests in presence detection. Further, many of these approaches focused on positioning of the phone based on the beaconing of access points.

3. PROBLEM

Existing methods of detecting presence and identity requires investment in expensive infrastructure and community acceptance of presence disclosure. Of course the accuracy of the data obtained via this specialized equipment is much greater, but for many applications it may not be necessary to have pinpoint precision.

Presence is a highly useful data input to solving many real-world decision problems. Consider that presence informs work habits, consumer preferences, and traversal patterns. Privacy in the context of presence is a significant concern as we consider the implications of our experiments, as infrastructure owners can use the techniques we describe in a very straightforward way to uniquely track individuals by their mobile telephones with high fidelity with minimal additional investment.

4. CONCEPT

The IEEE 802.11 standard defines a protocol two for managing wireless networks. Within this protocol there exists a multi-purpose frame containing the unique MAC address of the device emitting it. This frame is called the Probe Request. The Probe Request is primarily used to identify the wireless access points in close proximity. This frame is typically sent to the broadcast MAC address to ensure all listening access points can receive it.

An IEEE 802.11 compliant device will continuously beacon broadcasted Probe Request frames for several reasons while the radio is turned on. An unassociated wireless Network Interface Card (NIC) is searching for networks that it knows and evaluating those that it does not. Any wireless NIC is capable of receiving these frames since they are sent to the broadcast address. Other reasons we found for broadcasting these requests are for access point roaming ([9]), and location services.

Through our testing, we had to ask ourselves why these devices were beaconing broadcasted probe requests so frequently. We conducted many tests to better understand what was happening and came

to the conclusion that these broadcasted requests were being sent in order to determine location. While we cannot scientifically prove that this is the case, it is a logical conclusion to draw based on the facts.

The major smartphone OS manufacturers (Apple, Google, and Microsoft) all admit to storing private "crowd-sourced" databases of wireless access points BSSIDs and their associated geographical locations ([1,5,8]). We believe this database is built and used by asking smartphones to report geographic location data simultaneously with the BSSIDs it can see. One way of determining which BSSIDs are present is to ask via a Probe Request. Once the database contains an entry for a BSSID and its location, it can pass that information to other devices.

Finally, these major mobile operating system manufacturers admit that they use these crowd- sourced databases to allow their devices to more quickly determine location. This method is much faster and more easily obtainable than depending solely on GPS data which can take minutes to obtain and can only be used when the device is within the line of sight of multiple GPS satellites.

Ensuring privacy means careful consideration of this cost of the convenience of location-based services in mobile apps: namely, the very real potential that this technology enables for surreptitious collection and aggregation of data that uniquely identifies people and their exact whereabouts.

5. DETAILS

While developing a home smart-thermostat we hypothesized that we could detect the presence of a users smartphone in an effort to select a more energy efficient set point while the user was away from his or her home. We developed this solution as an energy savings idea but quickly became aware of many other applications.

Initially, we thought the easiest solution would be to authenticate to the same network and then listen for traffic originating from the mobile device. At first, this method seemed unpredictable and we were not sure if there was sufficient traffic to be able to reliably determine presence. We next attempted to elicit an ICMP echo response from the device but quickly realized that mobile device OSs do not reliably transmit these packets. Further, we wanted our solution to work with minimal interference in the network and without any additional software installed on the device. This pursuit is what led us to uncover just how interesting this problem really is.

In the next few sections, we outline in chronological order the methods we developed and exactly how they work.

6. FIRST METHOD (BONJOUR)

The first method we developed involved sniffing a layer-three protocol used to advertise services and hostnames. Used predominantly in Apple products to advertise local area network services like AirPlay and file sharing, this protocol is widely known and accepted. Since we wanted to be able to detect presence without installing any additional software, this solution worked very well for Apple products.

In order to determine reliability we conducted a few tests. For the first test, we used tcpdump with a kernel filter to only report layer-three packets with a source address matching that of an iPhone on

the network that was utilized as usual for the duration of the test. The phone entered and left the network as I did and was often left idle overnight. We then used grep to filter out only the bonjour packets based on some of the clear text inside the packet. We allowed tcpdump to run for seven days and exported the results to an Excel spreadsheet.

The second test we conducted was the same as the first except instead of an iPhone used normally, the IP address of an iPad that sat idle for the duration of the test was the target.

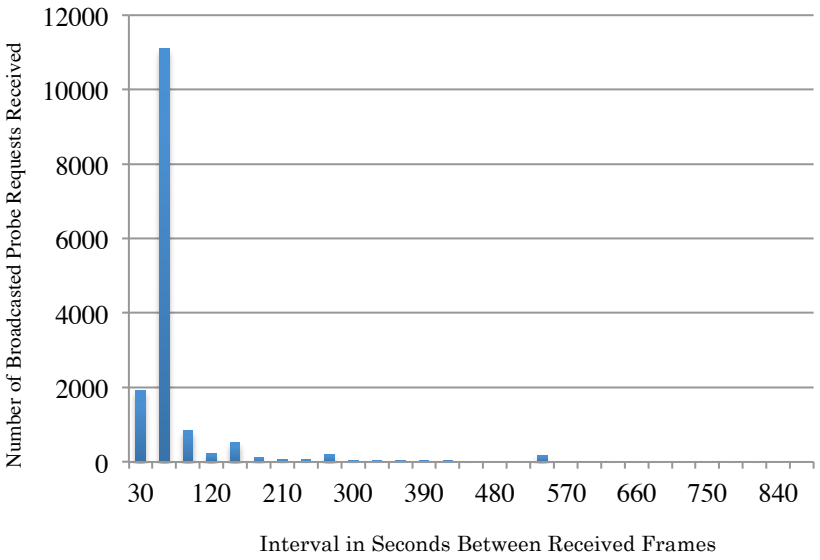
After conducting the above described tests, we determined that Bonjour packets were sent by an iOS device on average every twenty minutes but ranged between two and forty minutes. Unfortunately, this was not reliable enough for our purpose. Additionally, this solution only worked for a short period of time because just after developing the solution, Apple patched iOS and it no longer beaconed these packets for us. Finally, since Bonjour is a layer-three protocol we had to make sure the device always received the same IP address to ensure detection. We decided to pursue an alternate method.

7. SECOND METHOD (IEEE 802.11 PROBE REQUEST)

Our second more successful solution was to place an unauthenticated wireless network interface card in monitor mode and listen for layer-two broadcast frames emitted by our target devices. The IEEE 802.11 standard defines a layer-two management protocol for network management features like association, de-authorization, and roaming, etc. We found use of a multi-purpose broadcast frame called the Probe Request to be highly effective. A device with an IEEE 802.11 compliant implementation will beacon out probe requests for many reasons. Pre-association, access points and end points communicate their features using the Probe Request. An end point will regularly send them out containing all of the devices supported features, then each access point that receives the Probe Request will respond with a list of their own supported features. This is actually the first step in association but also serves to allow the device to keep a list of available access points. Post-association, the device sends Probe Requests in an effort to identify other access points in case the current one goes down or it must roam to a different access point on the same network.

We found this method of detecting presence to be based on a more standard protocol and therefore be more reliable as these frames are sent at more regular intervals. Further, this approach leveraged a widely- used open standard, and is thus a vendor-agnostic presence detection technique. In addition, since it is a layer-two protocol it also serves as a more effective device identification technique through use of the hardware defined unique MAC address.

Figure 1. Time Between Received Broadcast Frames



To determine the reliability of this method we conducted a few tests very similar to the aforementioned tcpdump tests for the bonjour protocol. We already had the thermostat running which updated a MySQL database each time it received a probe request, so instead of a separate instance of tcpdump we enabled logging on the database. After twenty days of normal use, we exported the data to a spreadsheet for analysis. We received 15,653 broadcasted layer-two probe requests from two devices that were in and out of range several times throughout the test period. We observed that on average these frames were sent every sixty seconds and ranged between two seconds and twenty minutes. While this was a much wider range than the Bonjour packets, it was much more reliable (Fig. 1).

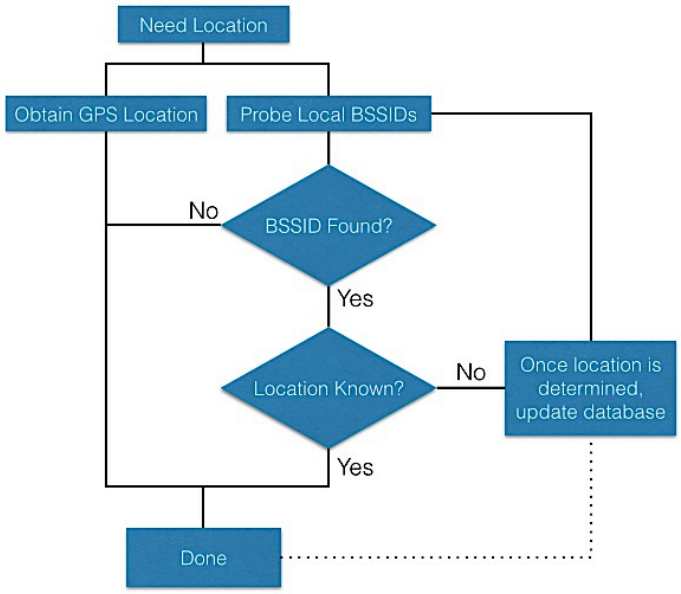
We then conducted a second test using an Android device. During this second test, we opted for an extra tcpdump instance and monitored the frequency of probe requests received from the device. The results of this test were not great. After twenty- four hours of monitoring, we had not received any Probe Requests. This was troubling, but we attributed it to the fact that it was an older version of the Android OS (2.2) and we obtained a newer device running Android OS version 4.4. This device with location services enabled was sending IEEE 802.11 QoS frames at a surprising rate of approximately 350 per second. Further, it was broadcasting Probe Requests at a rate which supported the data obtained from the iPhone in the first test.

The results of this second test beg the question: why are these devices beaconing Probe Requests? Further, the surprising transmission of these requests for the newer Android device warranted further investigation. We first attempted to imitate the access point and send an IEEE 802.11 "Deauth" frame in an attempt to get the end device to re-authenticate and thus leak its presence. This attempt was futile due to the fact that modern access points and IEEE 802.11 implementations support a secure management frame protocol called IEEE 802.11w Protected Management Frames [10]. This standard classifies the management frames into three groups. Only the frames sent in group one are allowed to be sent unauthenticated and therefore, our unauthenticated Deauth frames were ignored. Further, when devices did accept the Deauth frames we were able to confidently assert their presence, but it was no longer passive.

We then tried to do an authenticated ARP request that was successful and will certainly provide a useful way of determining presence of a smart phone when authenticated network access is available. As mentioned previously, in an attempt to preserve battery life we have observed that mobile devices often ignore certain packets like the ICMP echo request. These devices sometimes do respond, but not often enough to be reliable. The ARP request however, was reliably countered with a response by the mobile devices tested. Unfortunately, this required authenticated network access and was not passive.

After another test of a more modern Android device, we realized the reason these Probe Requests were being sent was because the devices being tested were or were not attempting to determine their location via wireless access points. In this last test, we observed that a more modern implementation of the Android OS with location services enabled was beaconing Probe Requests at a comparable rate to the iOS devices. Further, with this specific device it was broadcasting IEEE 802.11 QoS packets at a staggering rate of almost 300 per second. With this kind of beaconing, a device could potentially be tracked in real time.

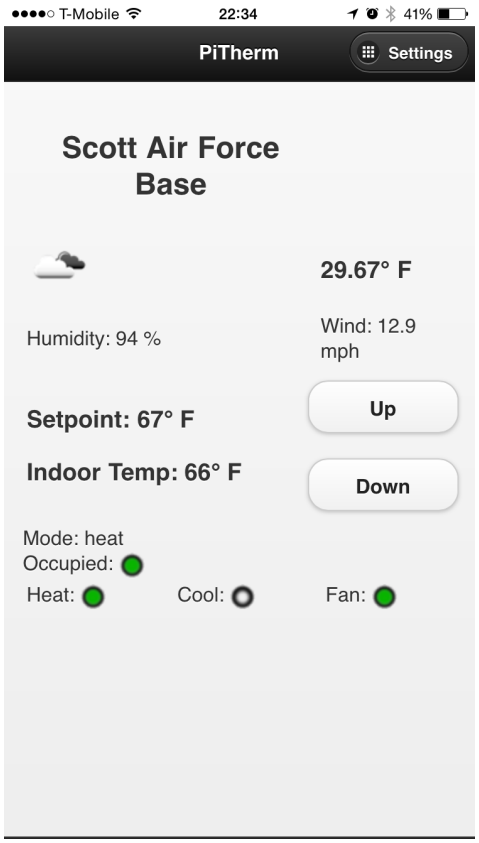
Figure 2. Location Services Flowchart

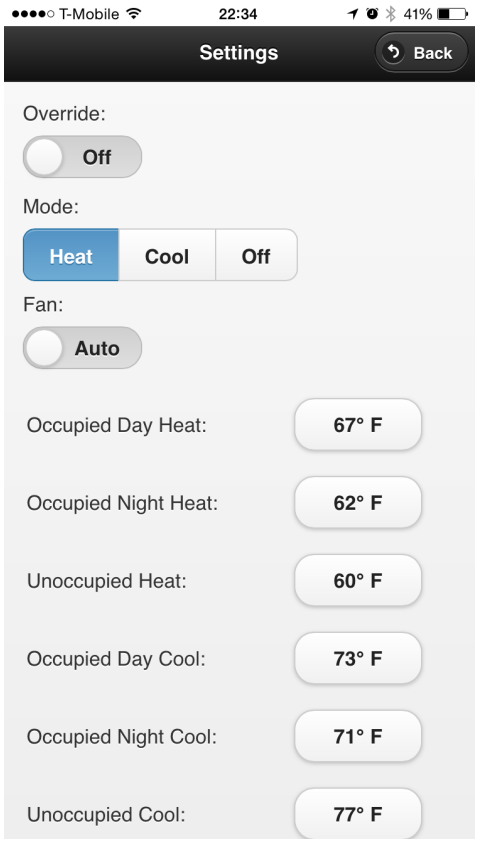


All of the above mentioned tests and observations led us to believe the reason our method of presence detection works is because of the devices attempting to learn which access points are available in an effort to determine their location. GPS can take a long time to determine physical location but probing wireless access points can be nearly instantaneous and when correlated with a crowd sourced database of unique BSSIDs can provide accurate location data. If a new BSSID is introduced into the system, its location can be easily sent to the device manufacturers database (Fig. 2). The use of this information has been identified in Apple, Google, and Microsoft's mobile operating system privacy policies ([1,5,8]).

This method of detecting presence has been successfully applied to our home smart-thermostat application built using a Raspberry Pi computer, three solid-state relays, and a digital temperature sensor. The project is called PiTherm and has been released as open source at

http://www.github.com/paullj1/pitherm. The application consists of a front-end web-interface and a middleman PHP MySQL interface to the backend python daemon that actually controls the relays. The application allows users to manually set the thermostat or define six conditions based on heat/cool, night/day, and occupied/unoccupied. This simple application has saved a noticeable amount of energy in a home environment. Further, this project implements an API that can allow other projects to expose presence detection as a modular extension.





8. ASSUMPTIONS AND TRADEOFFS

During the course of developing this solution we have identified a few tradeoffs and assumptions that must be made. We have organized these into two groups as this method provides two solutions: presence detection, and identification.

This method of detecting presence depends on the fact that people must carry their phones or some other IEEE 802.11-enabled device on them at all times. We believe that with the expansion of the wearable category of devices as well as the proliferation of the Internet of Things (IoT), this may not be a problem for much longer.

Our method of determining identity cannot stand-alone for legal purposes. While it is not easy for the common user to do, it is possible for a device to send IEEE 802.11 management frames containing

incorrect information in an attempt to mask its true identity. We suggest that if this method of identification is used in home security systems that it only be used as supporting evidence and given appropriate consideration. For example, if an alarm is tripped a log of all unique MAC addresses should be taken for future correlation (see "Other Applications").

9. OTHER APPLICATIONS

Upon developing this method, we identified many potential applications. The following list provides an assessment of other applications.

The most obvious application of this technology is in energy savings. From climate control to lighting, the impact a technology like this could have on energy savings is significant. With three sensors in a home, one could accurately detect presence in three dimensions enabling a connected home automation system to turn lights on and off, turn televisions and home audio systems on or off, or even certain appliances could be set to shutdown when their users leave their immediate vicinity. These applications will continue to grow as wearable technology permeates into our daily lives.

Physical security is often overlooked in the information security realm. Our method of detecting presence could be correlated with alarm systems both at home and in business settings. A security system could keep a record of unique MAC addresses it sees regularly. If an alarm is tripped, it could take a snapshot of all present devices. While this snapshot cannot stand on its own in a court of law, it could be used in conjunction with other evidence to corroborate a legal defense or prosecution. In a business setting, this application might help to identify insider threats. The limitation here is that MAC addresses can be spoofed so this information could not be used independently of other evidence.

Another potential application would be in personnel accountability. Employees spend far too much time logging time when they are at work. Further, the reliability of this data can at times come into question. An automated system applying our approach to passively detecting presence could easily be employed to serve as a timekeeping system tracking when employees were in the office. This application would serve two major purposes, increased productivity, and reduced risk of fraudulent accountability.

Our system could also be used during emergency situations when accountability must be obtained quickly like in the event of a building fire. Emergency responders could assess the situation with increased confidence based on the number of people still inside the building. Further, if multiple sensors were employed, responders could locate individuals in a three-dimensional space reducing risk to themselves while reaching these individuals in need faster.

Retailers can also take advantage of our method of passively determining presence by tracking visits to their stores and correlating sales data. With the right analytic, the recognition of a device present when certain transactions occur could enable targeted real-time in-store advertisements. For example, if one can determine that an individual device is present when milk, eggs, and bread are purchased every week at a specific time one can target the holder of that device for promotions upon entering the store. This is just a simple example, more sophisticated analytics could of course be easily developed.

Finally, presence detection could be used for telecommunication purposes. Presence could be associated with which device receives phone calls or text messages. For example, when an individual is away from home or work, his or her cell phone would receive all phone calls and notifications. When

the individual returns home or goes to work, phone calls could be routed to his home or business phone respectively.

We have shown that there are many applications for a passive, cost-efficient, and reliable method of detecting a person's presence. As previously stated, the above list is not inclusive and we are confident that as the technology matures there will be many more applications.

10. SECURITY AND SOCIAL IMPLICATIONS

It is unsettling to think of the implications posed by the ability to cheaply detect presence and identification of an unsuspecting individual. As demonstrated in [2], individual users when notified are already uncomfortable with how often their apps ask for their location. Users technically have to permit apps to know their location but our method does not require any such permission. In the hands of a private citizen, it could be used for a severe invasion of individual privacy. An attacker could sniff the MAC address of a victims smartphone without any specialized equipment from up to 100 feet away and then set sensors in places which would alert him or her of the victim's presence in real-time. Further, significant existing work describes the use of triangulation with multiple access points to calculate location with high fidelity (within a few feet) as in [13].

The Government has been under intense scrutiny over the past few years for its bulk data collection practices, especially phone call metadata that notably contains geo- locality. This technology could be used to enhance their tracking systems for both legal and illegal purposes. The recent fervor of the public debate surrounding these programs, along with their modification under the Freedom Act, suggests a lack of public tolerance for such efforts. Yet, modern wireless technology is built to support information transport even in the presence of other networks and can be configured to not broadcast its SSID. Coupling this reality with the observation that "war driving" or other similar cataloging of existing wireless infrastructure is exceedingly rare among property owners, a malicious actor could likely create a significant corpus of personnel movement data without the permission or knowledge of the legitimate facility manager.

On the opposite end of the spectrum, this capability could be leveraged for significant societal benefit. For example, a home security system with multiple sensors could alert a homeowner of the presence of a potential attacker or home invader before the attacker can get close enough to cause any harm, though this system can be easily countered by attackers simply turning their phones off before participating in criminal activity. Another positive use is specific personnel location for recovery during national catastrophes. Yet, these examples are highly specific. In general, strong public consensus and legal precedent compel location-based querying of mobile users should only be allowed when informed users have consented to location-based monitoring.

Given this analysis, this technology has specific application to U.S. military as detailed in the following section.

11. MILITARY CONSIDERATIONS

With the rapid increase in cyber threats and advancement of technology, the U.S. Military has begun preparing itself to fight a cyber war. Our method of presence detection presents many risks and benefits in military operations.

A major potential risk is the detection of presence of our senior military leaders. The proliferation of smartphones has not stopped at private industry. Each day our senior leaders become more connected and the devices they carry are not specialized in any way. Our leaders carrying these devices enable more accurate targeting and increased awareness of our operations by our enemies. It is important to be aware of these risks as we begin to fight in an increasingly connected environment.

This risk does not stop with our military leaders though. If every troop is carrying a smartphone, it becomes much easier to determine how big a force is. If the enemy places a few sensors as they evacuate a location, they can easily get an idea of how many people are in that location based on how many smart devices are present. Further, since these sensors could be completely passive, they would be virtually undetectable and extremely easy to conceal.

A few potential mitigation techniques might be to rotate devices or develop a device that beacons false data to deceive an enemy into thinking there are a great number more troops present. Devices could also randomize their MAC addresses to confuse an enemy or force them to abandon this technique. This leads into potential benefits of this type of presence detection. If these techniques can be used against us, then nothing prevents us from using them against our enemies.

12. FUTURE WORK AND RECOMMENDATIONS

Smart phones today emit other signals with unique IDs. As software defined radios become cheaper, it may be possible to even more reliably determine identity and presence of a smart phone by the GSM, Bluetooth, or near field communication (NFC) signals it emits.

We believe Bluetooth would be more reliable, but the range would be greatly reduced. Bluetooth systems seem to have a more active pairing process due to the short range. For example, when entering a vehicle smartphones often automatically pair with the vehicle's Bluetooth audio system if present. This type of active pairing indicates at least one of the devices is beaconing. We would like to point out that it is possible that the same passive pairing occurs on the device side as it does with the IEEE 802.11 protocol. Further investigation would have to be done.

Out of the four (Wi-Fi, Bluetooth, NFC, and cellular), we believe that cellular would be the most reliable and accurate method of presence detection. It is widely known that cellular devices use a beaconing function to find towers. This method of presence detection is already being used by law enforcement and emergency services. If they have the capability of determining location using this protocol then so does anyone capable of receiving those beacons.

It is important to realize that this information is being publicly broadcasted to anyone in the immediate vicinity. If a user does not wish to have his or her information broadcasted there are steps that user can take to prevent this broadcast. First, devices placed in airplane mode with the Wi-Fi and Bluetooth radios turned off will not broadcast anything. However, having all radios turned off will render the device mostly useless. It is possible to turn Bluetooth and Wi-Fi off when not being used but unfortunately, this still leaves cellular.

Specifically for Wi-Fi, we pointed out that older devices without location services were less susceptible to this type of presence beaconing. They only performed IEEE 802.11 probe requests when the user was actively trying to select a new wireless network to join. We have observed that with location services turned off for all devices, the phone is asked to determine its own location less often leading

to fewer broadcasted probe requests. Further, we observed that if a device is left idle with location services disabled it does not broadcast probe requests at all.

It should be noted that if the major mobile OS developers did not rely so heavily on active scanning for wireless access points, this type of detection would be much harder. By default most access points beacon out to allow for passive detection of access by devices. The only fidelity in location that is gained by actively scanning is by being able to locate access points that do not broadcast their location. We believe that changing the way smartphones determine their location to be more passive would drastically reduce how often a device beacons its presence and would not sacrifice much accuracy in location.

Ultimately, unless the IEEE changes these protocols to be more passive on the user side, this type of presence detection is very difficult to avoid. This type of change is extremely unlikely though considering how widely these protocols are used and accepted. A change of this magnitude would be met with resistance similar to that of the IPv6 migration in effect today.

13. CONCLUSION

In this work, we considered the potential societal cost of location-based services in mobile technology: the ability of infrastructure owners to passively track users uniquely through time in order to collect meaningful personal data. We executed three experiments around this concept after exploring this problem while developing a sensor environment for residential climate control. Our work led to an investigation of the impact of this technology and we suggested several possibility mitigation strategies from protocol changes to personal choices.

This work should serve as a call to mobile manufacturers and authors of telecommunications standards to work toward a technical framework that protects users from invasive tracking, or at least better educate users about the potential risk that location- based services exposes to third-party presence awareness. While most users are aware that they share their data with their respective smartphone OS developer, even technically sophisticated consumers may not be aware of the exposure to third party sensors or even that they are sharing the location of their own access points. We hope that this is only the first step toward an increased sense of awareness and level of privacy.

REFERENCES

[1] "About Privacy and Location Services Using IOS 8 on IPhone, IPad, and IPod Touch." Apple Support. March 6, 2015. Accessed June 17, 2015.

[2] Almuhimedi, Hazim, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Cranor, and Yuvraj Agarwal. "Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging." *CHI 2015* CMU-ISR-14-116 (2014): 1,21. Accessed June 17, 2015.

[3] "Apple Q&A on Location Data." Apple Press Info. April 27, 2011. Accessed June 17, 2015.

[4] Paramvir Bahl and Venkata N. Padmanabhan. Radar: an in-building rf-based user location and tracking system. pages 775–784, 2000.

[5] "Enable Android Location Access." Google Support. Accessed June 17, 2015.

[6] Frédéric Evennou and Franc ̧ois Marx. Advanced integration of wifi and inertial navigation systems for indoor mobile positioning. EURASIP J. Appl. Signal Process., 2006:164–164, January 2006.

[7] Yanying Gu, A. Lo, and I. Niemegeers. A survey of indoor positioning systems for wireless personal networks. Communications Surveys Tutorials, IEEE, 11(1):13–32, First 2009.

[8] "Location and My Privacy FAQ." Windows Phone, How-To, Browsing Maps. September 1, 2012. Accessed June 17, 2015.

[9] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. New York, New York: Institute of Electrical and Electronics Engineers, 2012. 53, 87, 429-433, 978-980.

[10] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz. New York, New York: Institute of Electrical and Electronics Engineers, 2013. 1,111.
[11] G. Retscher, E. Moser, D. Vredeveld, D. Heberling, and J. Pamp. Performance and accuracy test of a WiFi indoor positioning system. Journal of Applied Geodesy, 1:103–110, September 2007.
[12] C. Roeding and A.T. Emigh. Method and system for detecting presence using a Wi-Fi network probe detector, February 3 2011. US Patent App. 12/764,522.
[13] Sánchez, David, Sergio Afonso, Elsa Macías, and Ávaro Suárez. "Devices Location in 802.11 Infrastructure Networks Using Triangulation." 2006. Accessed June 17, 2015.
[14] Z. Xiang and et al. A wireless lan-based indoor positioning technology, 2004.