Wireless Network Security Status in Oulu: War-driving

University of Oulu
Faculty of Information Technology
and Electrical Engineering /
INTERACT research unit
Master's Thesis
Yurong Zhao
Date 16.06.2019

Abstract

Wireless networks have improvement not only in the timeliness, frequency, convenience and flexibility of connecting to the Internet, but also in economic cost and expansion of the number and location of access points that a user can connect to the internet. They have gained popularity especially after Wireless Local Area Network second evolvement about changing initial secure algorithm Wired Equivalent Privacy (WEP) to Wi-Fi Protected Access (WPA) and WPA2. WEP has been found to have vulnerabilities in cryptographic techniques and can't defend against brute force attacks for more than a few minutes and is considered broken nowadays. WPA, a stronger encryption algorithm than WEP, made Wi-Fi a reliable network connection method.

Wi-Fi security issues have been found probably since the first wireless network was deployed, but it is widely known by people because of Peter Shipley's wardriving experimentation and the statistic report which has been published in hacker conference in 2001. Several experiments have been carried out to reveal Wi-Fi security issues and to improve users' awareness of Wi-Fi security. Wardriving is not a new concept, but only lately wardriving was becoming easier for wardrivers because of continued evolution of technology. The updated software and hardware that are utilized in wardriving have given this activity more economic value and attracted interest from other researchers too. But this method has not yet been used in Oulu, at least in academic research. No studies have reported about wireless network security status with wardriving method by flying a drone to discover wireless APs and most of wardriving has been done by car, walking, or biking. Furthermore, Oulu, as a technology hub with many ICT companies and citywide panOULU public Wi-Fi infrastructure, makes it an ideal location for this experiment.

What is Wi-Fi performance and security status in Oulu? Author will scan wireless networks in Oulu center area with a tool kit setting up with Raspberry Pi, Wi-Fi adaptor, GPS receiver and drone using a method called wardriving. Wardriving is the act of discovering and mapping wireless networks in a certain area and restoring access points' data, such as an encryption standard, network name and location. The fundamental purpose is to find general information about Wi-Fi networks performance and security in Oulu center area and report the issues to raise the awareness of Wi-Fi security. Mobile devices do not need to be connected to wireless networks to be tracked. The Wi-Fi signal is transmitted continuously while a phone device tries to search for available networks. Whether discovered wireless devices quantification is indicative of local personnel density is another research question to be answered.

About 65.22% wireless APs have WPA-CCMP encryption standard and 4.2% Wi-Fi have unknown authentication in Oulu. The data showed that the majority of wireless networks in Oulu are secure. Less than 1% networks deployed WEP which has been found severe flaws in authentication method and 10% wireless access points had WPA-TKIP deployed which employed the same underlying mechanism as WEP, therefore it is vulnerable to similar attacks. The amount of insecure networks brings some concerns to the wireless network security state in Oulu.

Wardriving by drone turned out to be a more efficient method to discover wireless networks compared to wardriving on ground by walking or biking. The result also found that wireless device quantification is indicative of local personnel density, as almost everyone nowadays has a smartphone. This finding makes the Pi setup more practically usage, such as searching for lost people in forest. Thus, it becomes one future research direction, to build a real time indicator to show the direction and distance between the Pi setup and a specific wireless network device, based on the detected strength of signal.

Keywords
wardriving, Raspberry Pi, Kismet, Wi-Fi security encryption, wireless standards, IEEE 802.11, wireless network, WiGLE, GDPR

Supervisor
PhD, postdoctoral researcher Heidi Hartikainen

Secondary Supervisor
MSc Prateek Singh

Foreword

Wardriving is not a new concept. Wardriving with Raspberry Pi is not emerging topic either, but technology keeps updating and evolving, only lately the wardriving has become easier. This study has used the latest version of Raspberry Pi and Wi-Fi sniffing software Kismet. Several existing sources from internet write about how to wardrive with Raspberry Pi, I didn't create a brand-new method or come up with a new application. But no wardriving has been done in Oulu academically and it is a fun process to build a device which has multiple usages, like checking people's shopping behavior and movement behavior for companies that generate economic data or being used as neighborhood watch to check suspicious wireless activities in neighborhoods.

One of the achievements for me is getting to know Linux system and gain general knowledge about how to use terminal. Many procedures in the Appendix C were omitted, as the configuration is a troubleshooting and solution-finding process and it was a crooked road. I tried a way and found out it cannot work out, then I changed to another way. Though the process of Raspberry Pi configuration is hair pulling, but fortunately I made it work with the help of my friend Tomi.

The initial research idea was from supervisor Prateek. I got inspiration from him after a discussion with him. He also gave me advice on how to design the experiment.

Yurong Zhao

Oulu, May 26, 2019

Contents

1 Introduction and motivation

Wireless Local Area Network (WLAN)(see Appendix A for abbreviation) has become prevalent because it is convenient for a device, such as a laptop or mobile phone, gains access to internet without cable, which makes WLAN a cost effective and easy implemented network solution (Akram, Saeed, & Daud, 2018).

The IEEE 802.11 is a group of wireless specifications for managing wireless traffic. The latest standard IEEE 802 11ac is designed to reach very high data rates to sustain streaming video, voice, live gaming, and augmented reality applications running smoothly on mobile devices - maximum medium access control (MAC) throughput of at least 500 Mb/s for a single user, and 1 GB/s for multiple users. (Lutui, Tete'imoana, & Maeakafa, 2017) This amendment means that the maximum achievable rate is five times higher than the earlier amendments, IEEE 802 11n. This achievement made wireless communication catch attention and has been widely applied on mobile devices (Bejarano, Knightly, & Park, 2013; Lutui, Tete'imoana, & Maeakafa, 2017; Zou, Zhu, Wang, & Hanzo, 2016). Most of smart phones provide hotspot functions which turn a smartphone to a wireless access point and allow other Wi-Fi enabled devices to share the internet connection of the phone (U.S. Patent No. US9078137B1, 2015).

Although the wireless technology has growth at an exponential rate, the security risks are not nevertheless eliminated (Lawrence & Lawrence, 2004). As a result of open nature of broadcasting through electromagnetic waves, wireless networks are reported more vulnerable than wired networks (Lutui, Tete'imoana, & Maeakafa, 2017). The unit data transfers in data link layer of a wireless network called frame. The payload data in a frame is encrypted, but frame header is unencrypted and accessible to anyone within the radio range (Gancarz & Prole, 2012). The information in a frame header consists of protocol which encapsulates the payload data in a frame, MAC address of the destination device and source device, and so on. Wireless network sniffing software, such as Kismet, can capture information within wireless networks. The act of discovering and mapping wireless networks is called wardriving. The concept of driving around discovering vulnerable wireless networks has existed probably since the first deployment of wireless network and was widely known due to a computer security consultant named Peter Shipley and his automated wardriving experiment. Shipley conducted an 18 months survey of wireless networks in Berkeley, California in 2000. In the next year, the statistic report has been published in hacker conference to raise awareness of the insecurity of the wireless networks that were deployed at that time and laid the groundwork for the later wardrivers (Hurley, Rogers, Thornton, & Baker, 2007). Several studies have been carried out to reveal Wi-Fi security issues and improve user's awareness of the insecurity of wireless networks. In 2013, it was reported that less than 1% of analyzed networks still take WEP encryption as default setting in Leeds, UK (Schreuders & Bhat, 2013). In a statistical report of Wireless network security status in Auckland in 2015 and in Rabat, Morocco in 2016, it was found that among the discovered wireless networks, WEP encryption standard that deployed for networks accounted for 27.1% and 10% respectively in two different cities (Sarrafzadeh & Sathu, 2015; Sebbar, Boulahya, Mezzour & Boulmalf, 2016).

The consequences of having a vulnerable wireless network include data interception, modification, and theft for both individuals and organizations. The TJ Maxx parent company network invasion is the consequence of deploying WEP, which led to the theft of more than 90 million customer credit and debit cards numbers (Sagers, Hosack, Rowley, Twitchell, & Nagaraj, 2015). Thus, there is a necessity to know if the widely used wireless networks are secure. What encryption standards of wireless networks is utilized in general in Oulu area? Wardriving has been conducted by tremendous amount of researchers and wardriving aficionados to address their own purposes with a variety of tools. Wardriving is not new emerging concept, but only lately wardriving was becoming easier for wardrivers because of continued evolution of technology. The updated software and hardware that are utilized in wardriving are endued this activity more economic value and has attracted interest from other researchers too, but this method is not yet used in Oulu, at least in academic research.

The aim of this thesis is to collect information on wireless access points and find potential security issues in Oulu through the method called wardriving. This thesis is going to be done in Oulu, as author is studying in University of Oulu. Furthermore, being a technology hub with many ICT companies and citywide panOULU public Wi-Fi infrastructure, makes Oulu an ideal location for this experiment. The wireless network scanning tool that is built up for wardriving can also be adapted to collect data for commercial usage, for example, discovering people movement behaviors and shopping behaviors in a shopping center. Mobile devices do not need to be connected to wireless networks to be tracked. The Wi-Fi signal is transmitted continuously while a phone device tries to connect to a wireless network. The wireless network scanning sensor can pick up the Wi-Fi signal from a phone when it either connects to a wireless network or is searching for a wireless network(Baehring, 2019). In that case, can the wireless network scanning tool identify local personal density from discovering the number of wireless devices? To examine this, three hypotheses are made in the research method chapter to ensure the whole research process scientific and reliable. Raspberry Pi, Wi-Fi adapter, and a GPS receiver will be set up as wireless network scanning tool and be attached and flown on an unmanned aerial vehicle, widely known as drone, to scan and collect information of wireless access points in Oulu area. The experiment is carried out to address the following research questions:

1. What is the current state of wireless network security in Oulu center area?
2. Is the wireless device quantification indicative of local personnel density?
3. What is the difference in efficiency and amount of data collection between wardriving on ground or in air (by drone)?
4. What is the difference in efficiency and amount of data collection between wardriving by the Pi setup or WiGLE phone application?
5. How to design and implement the wardriving as a research method?

To answer the research questions, eight experiments will be carried out in 2 different days (on a weekday and on a weekend) in two places (University of Oulu and Oulu city center). On each day, experiments will be done in each place by drone and walk sequentially. Each experiment consists of three times run in the designed routes. The data collected from three runs will be averaged to increase data accuracy. The data that are analyzed to achieve this research purpose includes SSID (Network name), encryption type, BSSID (MAC address of Access Point), the AP manufacturer, the AP

location. The percentage of encryption type of discovered APs will be generated to see the general security state in Oulu.

The rest of the thesis will be structured in the following parts. Chapter two is theoretical knowledge relating to wireless networks and wardriving. Chapter three will discuss how to collect and analyze data, as well as the limitations of this study, chapter four is to report the findings of this study. Finally, chapter five will present discussion and conclusion of this study to compare this study to prior studies and summarize the main takeaway of this study.

2 Related work

The theoretical knowledge relating to Wireless networks and wardriving will be discussed in this chapter. Part one is about WLAN and mobile hotspot, part two talks about Wireless network security algorithms and IEEE Wireless standards, the following part will be Wi-Fi security concerns, the last part is about the definition of wardriving, wardriving ethics, legality and usage.

2.1 WLAN

WLAN is a broadcast technology that connects one or more devices with an access point by high-frequency radio waves. It is easy to set up and allow family members or employees to access the internet in a certain area without cable. because of its open nature and public broadcast, it is more fragile than conventional wired networks, anyone can intercept the signal within the radio range of a wireless network if the signal is not encrypted (Sagers, Hosack, Rowley, Twitchell, & Nagaraj, 2015). It also brings more risks and threats if the user doesn't have proper knowledge of security protocols and procedures. In 2002, the Australian law firm Deakins reported that few hundreds of wireless access points are encrypted by the factory default standard in Melbourne. Would-be wireless hackers could detect such insecure access points by using programs like NetStumbler (Lawrence & Lawrence, 2004). If a company didn't apply all security feature for its network, such as company doesn't change default administrator password on all equipment during setup process, it might leave a risk that an employee unintentionally sets up an insecure access point (Rogue AP) or a hacker made same access point maliciously without explicit authorization. The hacker could start criminal activities with consequence is taken by this company. (Lawrence & Lawrence, 2004)

Once a mobile phone is switched on the personal hotspot button in the setting, it converts mobile device to a Wi-Fi access point. This allows multiple devices nearby connect to mobile phone by using wireless broadcast technology via a WLAN. It acts like wireless access point with connecting to cellular networks provided by the internet service providers. (Keshav, Indukuri, & Venkataram, 2012.)

2.2 WEP, WPA and WPA2

Wi-Fi security evolved over three stages with transforming security algorithms from WEP to Wi-Fi Protected Access (WPA) and WPA2 throughout its development. WEP is designed to provide a secure communication over radio signals between end users in a WLAN and started to be applied in IEEE 802.11b standard in 1999 (Sebbar, Boulahya, Mezzour & Boulmalf, 2016). It is reported that Wi-Fi encrypted by WEP is vulnerable (Akram, Saeed, & Daud, 2018; Sebbar, Boulahya, Mezzour & Boulmalf, 2016) and can't survive with brute force attack (Berghel, 2004; Lutui, Tete'imoana, & Maeakafa, 2017), lately it is reported that WEP can't resist attack for a few minutes or even seconds (Lutui, Tete'imoana, & Maeakafa, 2017, Gaj, Bessis, & Liu, 2015).

Table 1. Various wireless encryption standards comparisons (Lutui, Tete'imoana, & Maeakafa, 2017; Akram, Saeed, & Daud, 2018)

	Full form	Encryption	Authentication	Key management
WEP	Wired Equivalent privacy	RC4 with 40 bits keys	Pre-shared keys	Manual key rotation
WAP	Wi-Fi Protected Access	Temporal Key Integrity Protocol (TKIP) with 128 bit key	802.1x with EAP and RADIUS	Per-packet key rotation
WAP2	Wi-Fi Protected Access V2	AES (Advanced Encryption Standard) and CCMP (Counter Mode CBC MAC Protocol)	802.1x with EAP and RADIUS	Per-packet key rotation

Therefore, WPAs were introduced to resolve the security vulnerabilities of WEP in 2003 and 2004, respectively (Berghel, 2004; Lutui, Tete'imoana, & Maeakafa, 2017). WPA has two generations – Personal and Enterprise. Personal WPA or WPA-PSK (Pre-Shared Key) was designed for home and small office and uses pre-shared key. Enterprise WPA employed RADIUS server and adopts 802.11i protocol and Extensible Authentication Protocol (EAP) for authentication which gives more effective control and security. (Lutui, Tete'imoana, & Maeakafa, 2017; Sebbar, Boulahya, Mezzour & Boulmalf, 2016). WPA employs a per-packet key by generating dynamically a new 128-bit key for two connected packets which make it a stronger security algorithm than WEP. WPA2 was utilized in 802.11i standard and improved WPA by employing Counter Mode CBC-MAC Protocol (CCMP) and AES (Advanced Encryption Standard)-based encryption mode which is a new and more secure encryption mode than Temporal Key Integrity Protocol (TKIP). AES is symmetric-key algorithm and encrypted and decrypted data from applying same key with a length of 28 bits, 192 bits or 256 bits (Sebbar, Boulahya, Mezzour & Boulmalf, 2016). Table 1 demonstrates the common wireless encryption standards among different network security protocols.

2.3 General Wi-Fi security concerns

Owing to the open nature of the wireless air interface, Wireless network is more vulnerable than wired network to malicious attacks. Wireless network architecture is comprised of application layer, transport layer, network layer, MAC layer and physical layer. Separate security techniques are implemented to address security threats and vulnerabilities from each layer to meet the security requirements with compromise of balanced implementation complexity and communication latency, for instance, security method cryptography asks for additional computational power and imposes latency. In the MAC layer, user's MAC address should be authenticated to prevent unauthorized access. MAC address filtering is used to allow only prefilled username to pass the authority. In the network layer, the WPA and WPA2 are widely used network-layer authentication protocols. (Zou, Zhu, Wang, & Hanzo, 2016.)

Table 2. Common threats to wireless LAN (Adapted from: Lutui, Tete'imoana, & Maeakafa, 2017).

Vulnerabilities & Threats	Description
Wi-Fi signal jamming	With a jamming device to be able to block off all communication in a WLAN
Misconfigured access point attack	With default network configuration
Rogue access point attack	Mislead user to a rogue access point to sniff all information from all traffics that connect to rogue access point
Eavesdropping	Intercept and disclose unencrypted or poorly encrypted information from all plain-text traffic from exploiting a wireless connection and getting into a computer network

There are risks existing in Wireless networks, those risks include vulnerabilities, threats (Table 2) and impacts. Vulnerabilities are security hole and caused by human failures that can be exploited (Lutui, Tete'imoana, & Maeakafa, 2017). Wi-Fi vulnerabilities and threats are mainly from the network deployment with insecure encryption method, for instance, revealing SSID and deployment of WEP (Gaj, Bessis, & Liu, 2015), and wrong configuration, such as, the unawareness of Wi-Fi security or Wireless network deployment with default configuration which provided by Internet Service Provider (ISP) (Schreuders & Bhat, 2013).

2.4 Experiences of Wi-Fi security issues from other cities

In 2005, hacker Albert Gonzalez and his accomplices cracked the password of WEP network in a store owned by TJX companies, a major off-price retailer of apparel and home fashion (D'Amico, Verderosa, Horn, & Imhof, 2011; Sagers, Hosack, Rowley, Twitchell, & Nagaraj, 2015; Sadmin, 2018), soon they enter into the Massachusetts-based corporate network and planted a packet sniffer. This sniffer package successfully extracted 90 million customer credit and debit cards to a server in Ukraine. TJX probably already was aware of vulnerabilities in their network security, but they tended to believe that it was unlikely someone would notice (Sadmin, 2018). The break-in happened to TJX companies is not the first, and will not be the last, certainly similar intrusions have happened to business, individual, or government Wi-Fi networks but stayed unreported (D'Amico, Verderosa, Horn, & Imhof, 2011).

The study was carried out in Leeds, UK in 2013 (Schreuders & Bhat, 2013) found that there were still less than 1% of total studied networks were using WEP, it could be quite an unignorable amount when considering the whole network users and also pointed out that routers with Wi-Fi Protected Setup (WPS) feature are vulnerable to brute-force attacks. WPS was introduced by Wi-Fi Alliance in 2007 and aimed at simplifying network set up by allowing users who possess little knowledge of Wi-Fi configuration and security settings to automatically configure wireless network (Schreuders & Bhat, 2013; Gaj, Bessis, & Liu, 2015; Sagers, Hosack, Rowley, Twitchell, & Nagaraj, 2015). Viehböck (2011) revealed design and implementation flaw in WPS, it makes brute force attacks to a sufficiently configured wireless network

feasible. WPA supports few configuration methods, includes 1) Push-Button-Connect (PBC) that user clicks either real button or virtual one on both access point and new wireless device, the button will be active when the authentication has succeeded. 2) Internal registration, user has to go to router's administrator interface and enter PIN code from there, the PIN code is either printed on the label of router or software generated. 3) External registration, this way user enters access point's PIN code into a form on client device, for instance computer. External registration doesn't ask for any kind of authentication apart from entering a PIN, it is highly vulnerable to brute force attacks. PIN code consists of 8-digit numbers, since the last digit is the checksum of the previous digits, it makes PIN code $10^7 = 10{,}000{,}000$ possible combinations. Once the authentication fails, AP will send an EAP-NACK message to user. When user attempts to get authentication using PIN, AP will response the validity of the first and second Pin code separately, if attacker receives EAP-NACK message from sending the first 4 digits, he/she knows the correctness of the first part of PIN code. An attacker could crack the first part and second part of PIN code sequentially with validity message from an AP. It cuts down the combinations from $10^7 = 10{,}000{,}000$ to at most $10^4 + 10^3$ (=11.000) that needed to find the correct PIN. With enabling WPS on a router, user configures wireless network with an on request generated eight digital PIN code or a PIN code printed on the label of router which will ease the configuration of wireless network but with the consequence of eliminating any security advantages of using WPA2 (Sagers, Hosack, Rowley, Twitchell, & Nagaraj, 2015).

Two researchers reported the statistical report of wireless network security status in Auckland in 2015 and in Rabat, Morocco in 2016, and found that among the detected wireless networks in two different cities, WEP encryption standard that deployed for networks accounted for 27.1% (include open Wi-Fi 25,9% and WEP 1,2%) and 10% respectively. WPA-TKIP occupied 5.9% and WPA-CCMP had 67% in Auckland, and 77% for WPA/WPA2 in Morocco (Sarrafzadeh, 2015; Sebbar, Boulahya, Mezzour, & Boulmalf, 2016). Another research was done in 2017 in Tonga reported that WEP accounted for 1%, 7% for open Wi-Fi, 51% were still using WPA with PSK and WPA2 occupied 28% (Lutui, Tete'imoana, & Maeakafa, 2017).

Gaj et al. (2015) studied the networks deployment with different encryption standards, cipher authentication and WPS is enabled or not, and found out that Network utilizing WPA2 standard with AES-CCMP and Radius server for authentication is the most secure setup. This setup provides stronger encryption and key management, improved message integrity and authentication forging prevention. WPAs are not uncrackable, especially when encrypted with TKIP because it is deployed with the same underlying mechanisms as WEP.

2.5 Wardriving

Wardriving is an act of collecting information of wireless devices and networks for statistical purposes using a wireless network scanning tool kit that sweeps a specific area. The process of mapping the location of wireless devices and networks is carried by walking which known as warwalking, or driving which is referred as wardriving, bicycling, flying (Hurley, Rogers, Thornton, & Baker, 2007; U.S. Patent Application No. US20180063165A1, 2018), though with different methods, it can be generally called wardriving. The concept of wardriving spread out and get into public when Peter

Shipley, a computer security consultant, automated the experiment of discovering wireless networks in Berkeley, California (Berghel, 2004). The experiment lasted 18 months and the result was reported at the annual DefCon hacker conference in 2001 with the aim of raising awareness of the unsecured wireless networks that were deployed at that time.

Table 3. Stumbler Code of Ethics v0.2 (Adapted from: Renderman, 2019).

Ethic	Description
Do Not Connect	At no time should you ever connect to any AP's that are not your own. Disable client managers and TCP/IP stacks to be sure. Simply associating can be interpreted as computer trespass by law enforcement.
Obey traffic laws	It's your community too, the traffic laws are there for everyone's safety including your own. Doing doughnuts at 3am gets unwanted attention from the authorities anyways.
Obey private property and no-trespassing signs	Don't trespass in order to scan an area. That's what the directional antenna is for :) You wouldn't want people trespassing on your property would you?
Don't use your data for personal gain	Share the data with like-minded people, show it to people who can change things for the better, use it for education but don't try and make any money or status off your data. It's just wrong to expect these people to reward you for pointing out their own stupidity.
Be like the hiker motto of 'take only pictures, leave only footprints	Detecting SSID and moving on is legal, anything else is irresponsible to yourself and your community.
Speak intelligently to others	When telling others about wardriving and wireless security, don't get sensationalistic. Horror stories and FUD are not very helpful to the acceptance of wardrivers. Speak factually and carefully, point out problems, but also point out solutions, especially how we are not the problem because we don't connect.
If/When speaking to the media, remember you are representing the community	Your words reflect on our entire hobby and the rest of us. Do not do anything illegal no matter how much they ask. They may get pissed off, but at least you have demonstrated the integrity that this hobby requires.

In the early 2000s, Google also joined wardriving game and started collecting geotagged Wi-Fi data in their Google Street View initiative. It was led by engineer Marius Milner, the creator of NetStumbler, Google Street View cars started scanning Wi-Fi network around the world and created a directory of wireless networks tied to address and Google Maps imagery (Sadmin, 2018). NetStumbler is one of the earliest created and widely used Wi-Fi detection tools, which only was compatible with Windows XP and Windows 2000. NetStumbler has wide range of uses, for instance, mapping the coverage of wireless networks, detecting unauthorized rogue access points in a workplace, using for wardriving. (Saad, Amran, & Hasan, 2016.)

Speaking of wardriving, quite an amount of people are sensitive and cautious to this term, because they misunderstand wardriving with hacking. The statistics gathered from wardriving are mainly for raising the awareness of the security issues associated with

different types of networks, typically wireless. Those statistics include network names, the encryption status, GPS, security algorithms and so forth. (Hurley, Rogers, Thornton, & Baker, 2007; Akram, Saeed, & Daud, 2018.) Utilizing the data from detecting wireless access point or network without permission or authority from the owner is not part of the activities of wardriving (Hurley, Rogers, Thornton, & Baker, 2007).

Warchalking is activity derived from wardriving. Warchalking is the practice of marking down a series of symbols on the sidewalk or wall at the location of the accessible or vulnerable wireless networks to help other wireless user identifying nearby access points (Lawrence & Lawrence, 2004; Freeman, 2006). This idea was inspired by the practice of hobos during the Great Depression to indicate the location of the fraternity house. Warchalkers tried to prevent a legal fine for defacing public or private properties by drawing the temporarily chalk markings. (Lawrence & Lawrence, 2004.) Stumbler Code of Ethics v0.2 (in Table 3) was made by a wardriver with aims of keeping this activity safe and legal with enumerating a collection of suggestions for wardriving.

2.5.1 Wardriving applications

Wardriving can be applied to gather essential information of a target area, comprising a number of the clients of an access point, their MAC address and manufacturer's information. The data gives law enforcement agencies an additional insight of the targeted area and can be utilized to analyze criminals and terrorists' activities (Akram, Saeed, & Daud, 2018). Wardriving method can also be applied as an intrusion detection system or professional security analyst's toolkit, for instance, AirMagnet, Sniffer Wireless, AiroPeek and the Wireless Security Auditor. It monitors and captures all data packets within that WLAN and analyze data to find out if suspicious activities are happening, then storage the result and give a warning to the user in a proper way (Lawrence & Lawrence, 2004; Jian, Zhi-Feng, & Yong, 2012). Additionally, Marketing researcher could generate economic data on people's shopping behaviors and walking flow within certain areas. The data is from tracking phone's MAC address and location. (Baehring, 2019.)

2.5.2 The legality of wardriving

According to the regulation applied to U.S wardrivers, it is not illegal to scan the access points. However, it becomes federal violation once a theft of service, a denial of service (DoS), or a theft of information occurs (Hurley, Rogers, Thornton, & Baker, 2007). The distinction of scanning and identifying access points with utilizing the access points is the same as its of wardriving and theft, the former is legal and innocuous activities and can even be beneficial to society if bring out properly and ethically, and the latter one is against the law (Hurley, Rogers, Thornton, & Baker, 2007; Ryan, 2004).

Finnish mobile phone manufacturer Nokia claimed that sniffing bandwidth from the legitimate users and corporations without getting authorization from internet owner is theft, it compromises a company's online resource security (Kern, 2005; Lawrence & Lawrence, 2004), while the New York Times ethicist held a different opinion and declared that connecting to unencrypted wireless network creates value for individual and society through its expansion of accessibility of high speed wireless networks apart

from home or office (Kern, 2005). But Kern (2004) also pointed out that wardriving does not count as stealing, as it does not connect to the network, but just record the publicly broadcast information of a wireless access point, such as geo location and encryption standard, with a suitable receiver.

Table 4. Sample views on warchalking and wardriving (Lawrence & Lawrence, 2004).

	Opinion
Head of e-business for Confederation of British Industry (CBI)	*"The CBI condemns warchalking as an implicit incitement to irresponsible and illegal acts"*
IT infrastructure manager at the Institute of Directors, England	*"The idea that warchalking is helping companies to realise their security problems is wrong. IT directors have known for some time that wireless networks are targets for abuse. Simply, warchalking in public places is graffiti and may facilitate hacking which is an illegal act"*
Managing director of Secoda Risk Management	*"These people simply drive up to a building armed with their pornographic e-mail, log into the insecure wireless network, send the message to 10 million e-mail addresses and then just drive away. A drive-by spammer would send email by finding an unprotected SMTP (simple mail transfer protocol) port on a company's server and then sending email as if the person were a legitimate user of the company's network. The mail server wouldn't be able to tell otherwise"*
FBI advisory	*"Identifying the presence of a wireless network may not be a criminal violation, however, there may be criminal violations if the network is actually accessed including theft of services, interception of communications, misuse of computing resources, up to and including violations of the Federal Computer Fraud and Abuse Statute, Theft of Trade Secrets, and other federal violations"*

Different opinions towards wardriving have been emerging publicly. Wardriving aficionados believe that wardriving is not a crime, but a hobby of sporting challenge or even a community service. Industry and security pundits had an opposing view towards wardriving (Table 4) (Freeman, 2006; Lawrence & Lawrence, 2004). Researchers doubt the legality and ethics of wardriving, because they consider that part of wardrivers do it for fun and other part of wardrivers may have malicious intent. Though Stumbler Code of Ethics has been established to advocate an approach to the practice, but it is impossible to know if a wardriver has adopted these rules as a self-restrained approach to the activity. (Freeman, 2006)

No law states that wardriving is illegal or legal, though many countries have laws to forbid the unauthorized access to private networks and protect personal privacy. From a technical viewpoint, many wireless networks broadcast identifying data accessible to anyone who has a suitable receiver. Wardriving with programs like Kismet or KisMAC is passive and does not access or communicate with network. Active wardriving with program like NetStumbler make its legality less certain, it sends probe message and attempt to associate with network even no data is transferred. ("Wardriving", 2019.)

3 Research Methods and Implementation

This chapter first introduces the research process which used empirical research method that involves both qualitative and quantitative data. Secondly, description of the research setting and legality and ethics of research data. Thirdly, hardware setup and software setup of wireless network scanning tool, then demonstration of trial run and problems that has been found in trial run. Then followed by wardriving experiment design, and how to analysis data. Lastly, limitations of research, and what has been done and can be done to ensure reliability and validity of research data.

3.1 Research process

Quantitative research methods focus on numbers, nature sciences, phenomenon in general, statistical generalization and breadth of knowledge. It emphasizes objective measurements and the statistical, mathematical, or numerical analysis of data collected through polls, questionnaires, and surveys or by analyzing pre-existing statistical data using computational techniques. Quantitative research methods generalize data across groups of people or to explain a particular phenomenon. Qualitative research methods focus on text, social sciences, phenomenon in context, theory generalization and depth of knowledge. Qualitative research data collection can be done by interviews, participant observation and documents. Both of research methods should be rigorous and relevant. In many cases, researcher combines two or more data collection methods or even several research methods in one research study to increase the value of the research. (Lanamäki, 2016.)

This research has been addressed in two phases, first through studying literature review and prior researches' findings to understand evolvements of wireless network encryption standards, security issues associated with wireless networks and activities related to revealing wireless networks security status and propagating the consequences that bring from poor deployed wireless network or lack of security sense. Secondly, in the empirical research the researcher will carry out wardriving by setting up Raspberry Pi 3 model B+, Grove GPS, Wi-Fi antenna to map wireless network in Oulu center area and analyze the data that collects from scanning wireless networks.

The empirical research and will combine qualitative and quantitative method to better study research question and phenomenon. Empirical research uses empirical evidence to derive knowledge from actual experience rather than from theory or belief through the means of observation or experience. (Cahoy, 2019.) Most of the collected data in this research is qualitative data, for example, encryption type and the AP manufacturer, but it will be analyzed in a quantitative way, such as the percentage of each encryption type.

3.2 Research setting

Oulu city center is selected to scan wireless networks. It is the fifth most populous city in Finland and is called one of the "living labs" within Europe and residents are inclined to experiment with new technologies ("Oulu", 2019). Wardriving has been conducted by tremendous amount of researchers and wardriving aficionados to address their own purposes, it is not a new emerging subject and issue, but it has not reported any academic and ethical wardriving in Oulu, this is the main drive that takes the author to start this research. The fundamental purpose of this research is to answer the research question "what is the current state of wireless network security in Oulu center area? "

3.3 Ethical considerations concerning data collection

The EU General Data Protection Regulation (GDPR) is data privacy laws that are in effect from May 25th, 2018 onwards ("General data protection *regulation (GDPR)*", 2019). It is a uniform standard in all member states in the European Union regarding protecting personal data. It also simplifies the regulatory environment for international business within Europe ("General data protection regulation", 2019). According to gdpr-info.eu Art 6(1)("GDPR", 2019), there are six basis that processing data subject's personal data shall be lawful. These include

a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b. processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
c. processing is necessary for compliance with a legal obligation to which the controller is subject;
d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Not every basis can apply to the processing of MAC addresses and location data in wardriving. The basis of Art 6(1) under b, c and d cannot apply, because there is no legal obligation to track people via wardriving, no contract is made with random passers-by and it does not protect the vital interests of passers-by with wardriving. Art 6(1)a state that data subject has to give consent to process his/her personal data for different usage, which means the responsible party should ask prior consent from the party concerned, such consent is only valid if data subjects give freely and the consent includes specific information without any ambiguity. It is difficult to ask random people for permission to obtain their wireless device data. The performance of a task should be carried out in the public interest can almost only apply to administrative bodies when they have to make data-driven decision, so they have to obtain people's data. The

legitimate interests under the basis f is suitable for the organizations and companies who carry out a task to collect public data for their commercial purpose, but not all commercial purposes are legitimate interests. It is hard to say collecting personal data for research purposes has any of the basis under GDPR Art 6(1) for processing personal data. Kismet can view the following information of a specific wireless network:

1. SSID (Network name)
2. Device type
3. Capture Phy name
4. Encryption type
5. BSSID (MAC address of Access Point)
6. The AP manufacturer
7. Last seen signal
8. Last seen channel
9. Last seen time
10. Channel in use
11. Frequency
12. Signal strength
13. Noise
14. Last associated BSSID

Most of the information collected by Kismet are not identifiable data that can be used to target a person. However, MAC address is personal data that can be traced back to a person with a combination of other data, such as observed location data of the mobile phone (Baehring, 2019), but only phone company can provide approximate location data based on a phone's signal strength in relation to cell towers. In most situations, such identical information is not accessible. MAC address that assigned to wireless network devices cannot be associated with a person's name and other identical data, because MAC addresses are not registered in a central database with other identical data. The Website MAC Find (http://www.coffer.com/mac_find/) can look up MAC address to find its vendor information, but it does not have enough information to identify a person. ("Do you have a MAC address you need to trace", 2019.)

In the H2020 ethics self-assessment test (Năstase, 2017), it will be a concern if this data is not anonymized. Only having the MAC address does not arise any ethics concern. The data collection method inherently forms an anonymous dataset. However, due to the uncertainty of whether collecting MAC address violate GDPR and whether legitimate interests can be applied to this study, after data analysis, the collected data will be deleted from all devices.

3.4 Hardware setup

The simplest way to conduct wardriving is to download an application called WiGLE Wi-Fi Wardriving. It is a tool to observe, visualize, and catalog networks and only supported on Android phone so far. The detected access points can be uploaded to the Wigle.net website (WiGLE: Wireless network mapping, 2019), it is a collective searchable database that has stored all discovered networks by participated wardrivers since 2001. Over 537,98 million networks have been detected and mapped to date from all over the world. The data within a network that can be detected by WiGLE contains GPS, SSID, MAC address, and the encryption method. WiGLE Wi-Fi Wardriving

application utilizes few measurements to target APs, those measurements include precise GPS and signal strength measurements to calculate the position of an AP, very often down to few meters. From WiGLE Statistics, it shows WEP encryption has decreased in a stable speed since 2010, it only accounts for 5.66% of total discovered networks until 2019. ("WiGLE", 2019.)

Most wardrivers combine Raspberry Pi, GPS receiver and Wi-Fi antenna as a wireless network scanning tool and map the wireless network by car. Wardrivers place wireless network scanning tool in the car and put antenna outside of car to make sure it is in open air to get GPS data. It is slightly more time consuming to setup and configure hardware and software with Raspberry Pi than downloading the WiGLE application, but it has more selections to customize one's own wireless network scanning tool with Raspberry Pi. Technically, a laptop can be used to wardrive with a wardriving software installed, ideally, wardriving tool should be small, portable, light-weighted and not catch attention by passersby. Raspberry Pi is selected for this study, because it is a small, lightweight and powerful single motherboard computer that is suitable to be developed as wardriving tool. Even though Raspberry has small size and can fit in a pocket, it can be configured to run Linux and most applications. Wireless detection tool made from Raspberry Pi is used not only for wardriving, but also for threat management, for example, scanning unauthorized or misconfigured access points within a corporate environment, identifying unaffiliated Access Points (AP) and prevent access to unauthorized networks, monitoring wireless access point connections to verify clients within organization network. (Saad, Amran, & Hasan, 2016.)

Table 5. Hardware requirements

Hardware
1. Raspberry Pi 3 model B+ 2. Grove GPS (connect to Pi with Female to Female Pin Connector) 3. Alfa Wi-Fi antenna (compatible with IEEE 802.11 b/g/n wireless standards, 5dBi) 4. Power bank 5. Drone - fly the above listed tools to discover wireless networks

Table 5 demonstrates the hardware used in this experiment. Most of the hardware are purchased using own budget, except the Grove GPS was borrow from University of Oulu. In order to get geolocation coordinates for wireless devices, Kismet needs to integrate with GPS device. Grove GPS was borrowed is used as a GPS receiver. The wireless network scanning tool was designed to be light and small, so that Drone could carry it while flying. Grove GPS has very small size, thus it is suitable for this experiment.

3.5 Software Setup

A selection of Linux operating systems that can be installed on Raspberry Pi, such as Raspbian, Ubuntu, Kali Linux, CentOS etc., Raspbian was installed for this experiment, simply because it is community recommended and with New Out Of Box Software (NOOBS), an operating system installation manager which contains Raspbian and LibreELEC, NOOBS can be downloaded from its official site raspberrypi.org ("Downloads - software for the raspberry pi", 2019). It is good for beginners to use. For

alternative operating systems, it can be directly downloaded operating system's image file and save to SD card of Pi. Once installation is done, there are two ways to install software for Pi - connecting mouse, keyboard and monitor to Pi or accessing to Pi from another computer via SSH. For this experiment, the installation process of Raspbian was done with connected monitor, keyboard and mouse. After installation, the rest of configuration was done via SSH.

Table 6 illustrates the software that is installed in Pi in this experiment. All the software in this study is free. Kismet is one of the main software which has to be installed for this study. It is a passive wireless networks detector, sniffer, wardriving tool and wireless intrusion detection framework. It cycles through Wi-Fi channels listening to information that is publicly broadcast by networks and records the details information of wireless networks from packets. Unlike NetStumbler, an active detection software trying to connect and communicate with wireless network, Kismet is a passive detection tool. It is designed to not log traffic content in a network, but to record high-level details of wireless networks, such as SSID and security encryption, which are publicly broadcasted. (Schreuders & Bhat, 2013.) Basically, Kismet can discover all the wireless packets within the available Wi-Fi channels - including automated beacon frames, such as a wireless access point keeps sending signal periodically to announce the presence of a wireless LAN, the frequency is up to multiple times per second, or probe frames that is sent by a device that is looking for a wireless access point to connect to, or data packets exchanged from associated devices. Kismet installation went pretty well, the latest version of Kismet from GitHub was cloned and installed successfully with required dependencies.

Table 6. Software requirements.

Software
1. Raspbian - official supported operating system. It can be installed with NOOBS or download the image 2. Kismet - main wireless network detecting tool, used to log the details of wireless networks 3. GPSD - receive data from GPS receiver and send data to Kismet 4. Screen - able to create separate "screen" sessions that can switch back to, or even disconnect and reconnect to later

To be able to capture location of Raspberry Pi, GPSD, a service daemon, needs to be installed to monitor GPS receiver that attaches on Raspberry Pi through serial or USB ports. It makes all data on the location/course/velocity of the GPS sensor available for query on TCP port 2947 of Raspberry Pi, so Kismet could locate an AP from its geolocation data with other information of that AP tagged with. For more information regarding how to set up a wireless network scanning tool, see Appendix B.

3.6 Trial run

The purpose of trial run is to test if all setting is proper for wardriving on the field. This test run will not wardrive with drones, but with bikes. The route is to run a circle around the Valkea building. Figure 1 displays all the hardware used for this trial run.

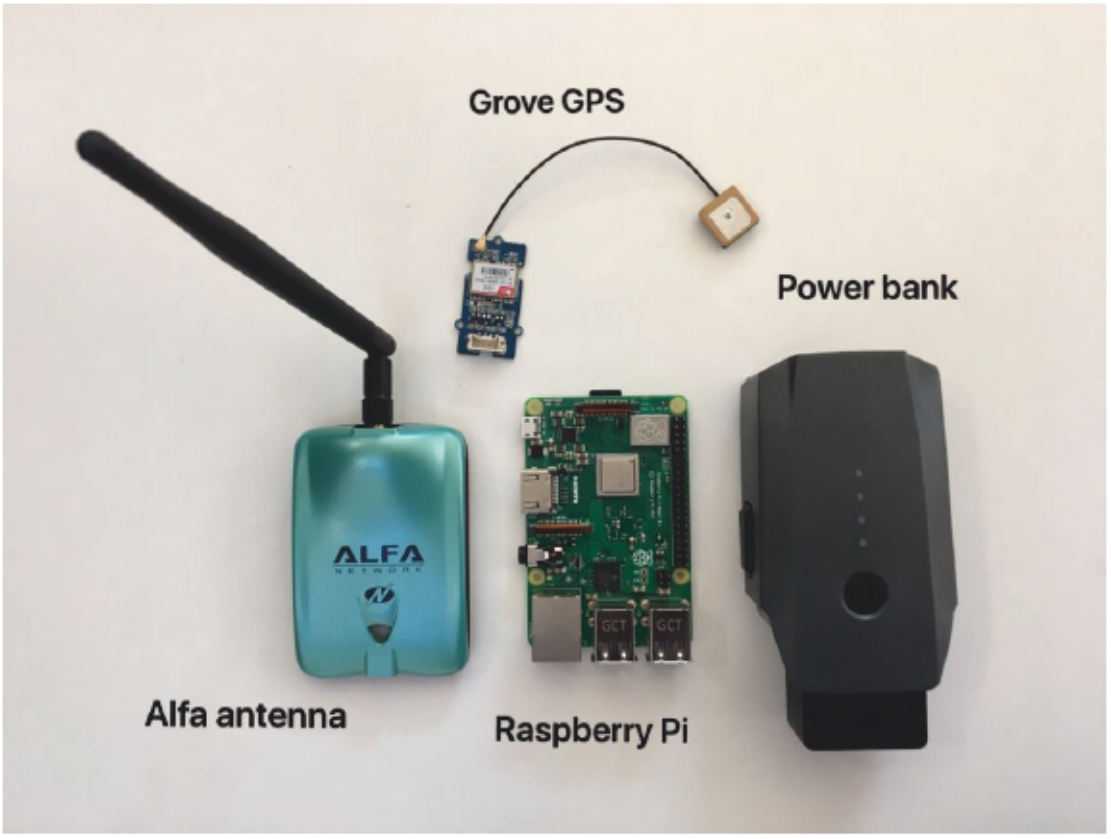

Figure 1. Hardware requirements for trial run.

According to Kismet site (Kismet, 2019), Kismet is the primary log format used by Kismet, the log file contains all the data Kismet can capture during wardriving, it includes packets, device records, alerts, system messages, GPS location, non-packet received data etc. The log file in Kismet format can be converted to csv format which can be read by Google Map. To achieve that, execute `kismetdb_to_wiglecsv --in original-log-file-name.kismet --out output-file-name.csv`. To copy log file from Pi to computer, type `rsync -avh pi@raspberrypi.local:/home/pi/file-name.csv ~/file-name.csv` in terminal, the log file will be copied to computer home folder with the command. Then import the csv file to Google map to locate the all scanned devices on map (Figure 2).

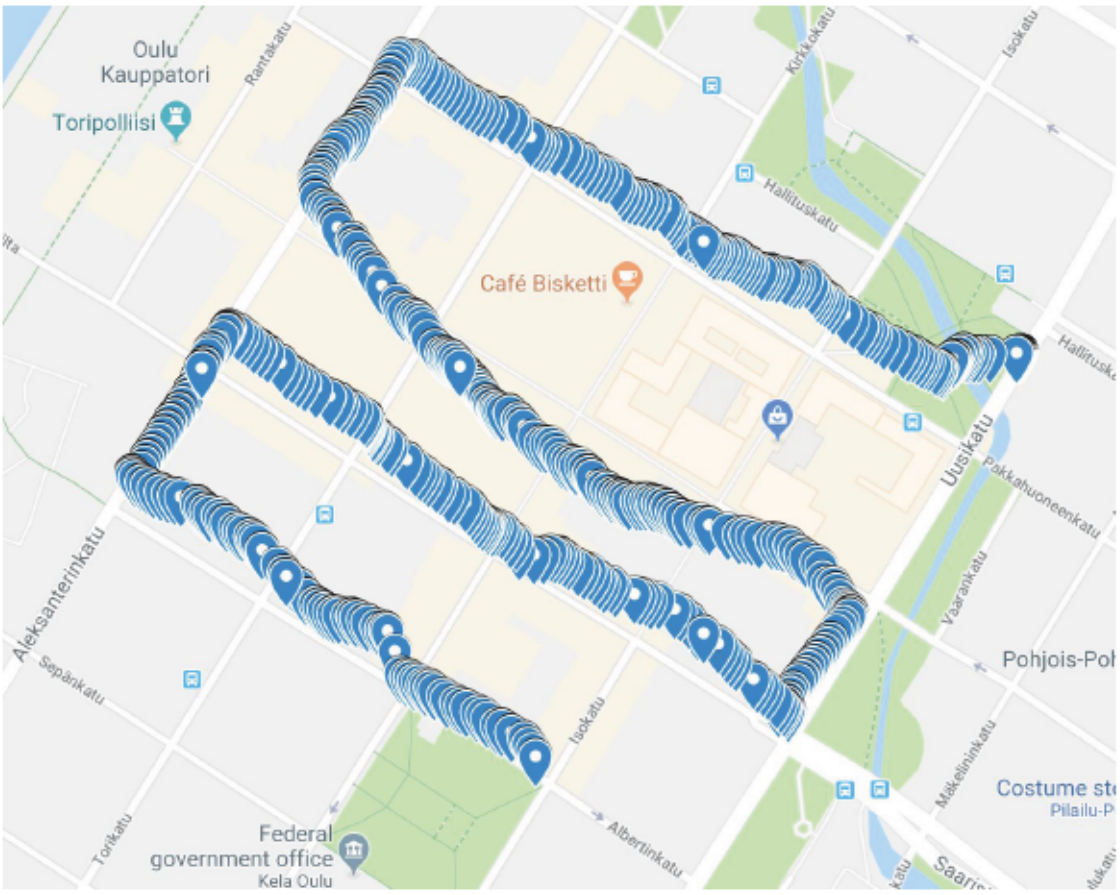

Figure 2. Scanned devices from trial run.

The trial run was successful as it captured all the data needed for this study. However, it lacks practicality - Pi needs to connect to another computer to start GPS and Kismet. It will be convenient to start GPS and Kismet automatically when the power of Pi turns on. This is especially beneficial when wardriving by bike or by drone, as it is not practical to connect computer with Pi outside to start GPS and Kismet on every run. Appendix C(1) demonstrates how to automate the startup of wardriving.

3.7 Wardriving experiment design

The research is going to answer the research questions in the following lists. To answer questions 2, the hypotheses are made to ensure the whole research process scientific and reliable. This research design was guided by supervisor Prateek. The presentation Shuchman (2014) was given in **DefCon hacker conference in 2005 has inspired the design methodology of this study**.

1. **What is the current state of wireless network security in Oulu center area?**
2. **Is the wireless access point quantification indicative of local personnel density?**
    - **Hypothesis 1 (H_1): Higher people density in Oulu city center on weekends than on weekdays, and higher people density in University of Oulu on weekdays than weekends.**
3. **What is the difference in efficiency and amount of data collection between wardriving on ground or in air (by drone)?**

- Hypothesis 2 (H_1): Wardriving by drone has higher efficiency than its on ground.

4. What is the difference in efficiency and amount of data collection between wardriving by the Pi setup or WiGLE phone application?
    - Hypothesis 3 (H_1): Wardriving with the Pi setup has higher efficiency than its with WiGLE phone application.
5. How to design and implement the wardriving as a research method?

Four wardriving experiments will be carried out to answer the research questions and examine hypotheses.

Design 1

Wardriving with Pi setup and WiGLE phone application in University of Oulu by walk in weekdays. The Pi setup and WiGLE phone application should start scanning wireless network devices at the same time in each experiment. It takes 45 seconds to boot Pi. In this experiment, Starting WiGLE application is 45 seconds late than starting the Pi setup. The route is from entrance 2T to entrance ABC across Cafe Hub (Figure 3).

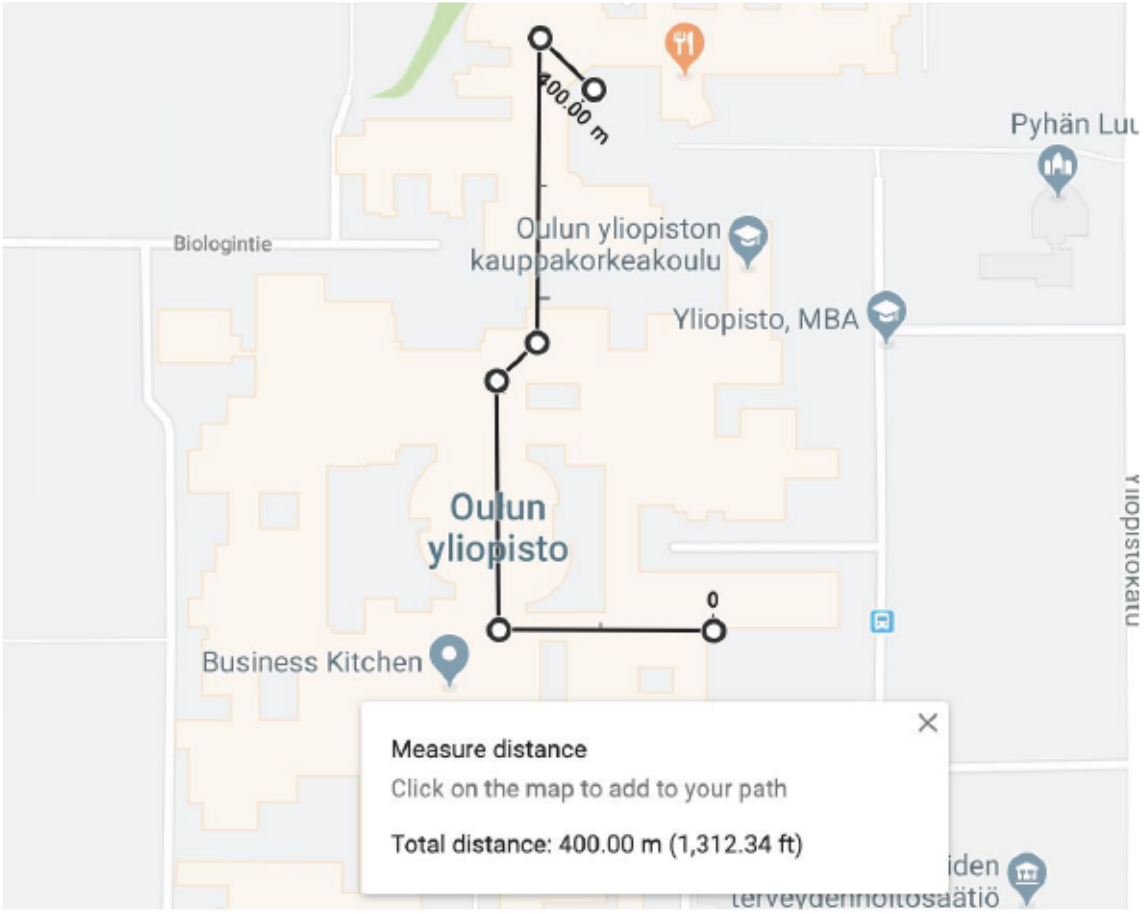

Figure 3. The wardriving route in University of Oulu.

Design 2

Wardriving with the Pi setup by drone and by staying on ground separately and sequentially in University of Oulu in weekend. The Pi setup will be attached on the drone and flown 70 meters high from top of Napa restaurant at a fixed point (Figure 4) for 5 minutes. The sensor range of Alfa wireless card is 90 meters, the drone flying height should be no less than 50 meters high from the building according to aviation regulations, so the compromised height is 70 meters. Drone's battery only supports approximately 25 minutes flying. It consumes energy especially when taking off drone. To be able to run three rounds without charging battery and taking off drone three times, a loop script (Appendix C (2)) was made to turn on and off Kismet every five minutes. The ground experiment will stay at the same point on map as flying experiment for same scan duration. The ground experiment will be done right after the flying experiment to decrease the difference of people density in each experiment duration, in order to compare the efficiency of wardriving by drone or on ground. Another experiment with the Pi setup will be taken within the design route as in Figure 3 to compare data on weekday and weekend.

Figure 4. The static point to discover wireless network devices in University of Oulu.

Design 3

Wardriving with Pi setup and WiGLE phone application by bike in Oulu city center on weekdays. The Pi setup and WiGLE phone application should start scanning wireless network devices at the same time. The route is back and forth path across Oulu city center (Figure 5).

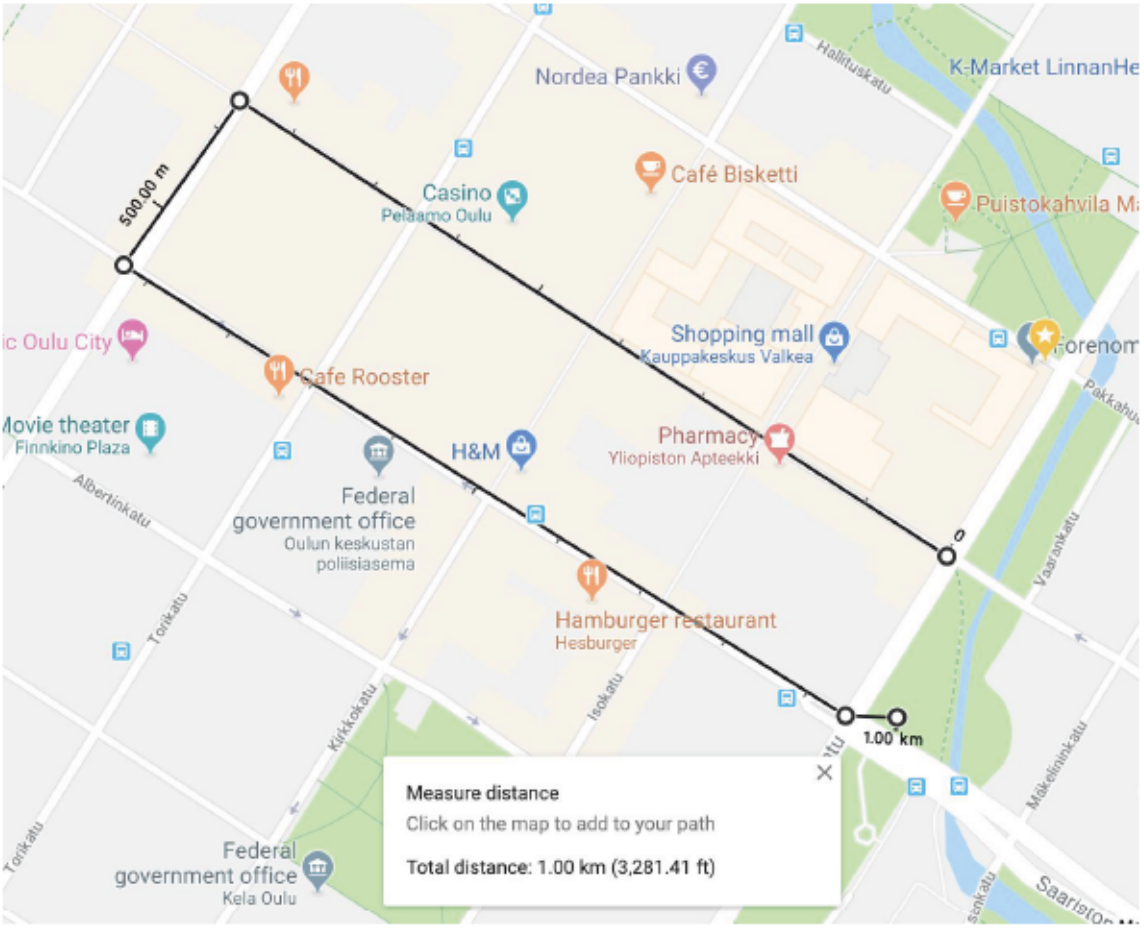

Figure 5. The wardriving route in Oulu city center.

Design 4

Wardriving with the Pi setup by drone and by foot separately and sequentially in Oulu city center in weekend. The Pi setup will be attached on the drone and flown above a fixed point (Figure 6) with the same script that was ran in Design 2. The ground experiment will stay at the same point as flying experiment for the same scan duration. The ground experiment will be done right after the flying experiment to decrease the difference of people density in each experiment duration, in order to compare the efficiency of wardriving by drone or staying on the ground. Another experiment with the Pi setup will be taken within the design route as in Figure 4 to compare data on weekday and weekend

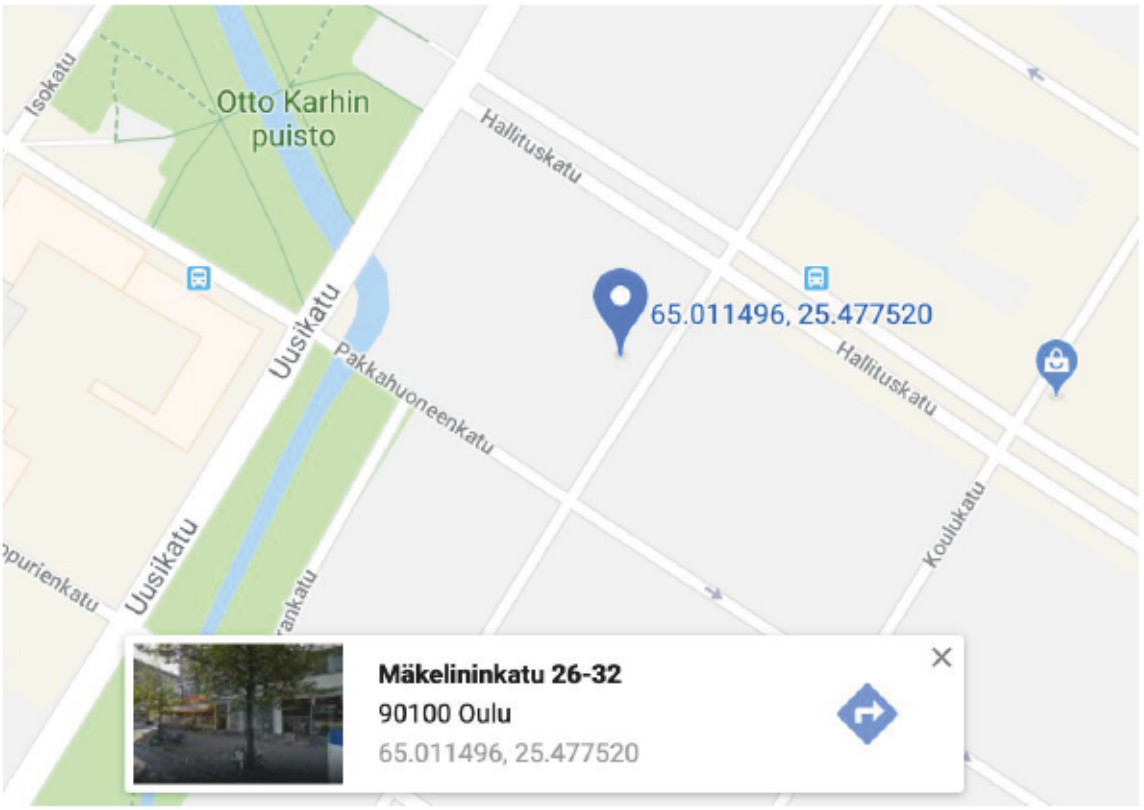

Figure 6. The static point to discover wireless network devices in Oulu city center.

Each experiment includes three times run with the same route which makes the whole experiment 12 times runs. The data from three runs will be averaged to increase data accuracy for each experiment. Figure 7 shows the final setup for this research.

Figure 7. The Pi setup attached on drone.

3.8 Data analysis

"Data analysis is the process of systematically applying statistical and/or logical techniques to describe and illustrate, condense and recap, and evaluate data". The accurate and appropriate analysis of research data is an essential component of ensuring data integrity. ("Responsible conduct in data management", 2019.) Data analysis procedures consist of data collection, data processing (organize and process data into format such as table for further analysis), data cleaning (prevent and clean data errors, like incomplete or duplicated data), data analysis, modeling and algorithms and finally data visualization (report data to reader in visualized format) ("Data analysis", 2019). In this study, the findings will be discussed in the light of what has been known in chapter 2 literature review.

Kismet can capture more than ten information of a wireless device or an access point as mentioned in the chapter 3.3, but only SSID (Network name), encryption type, BSSID (MAC address of Access Point), the AP manufacturer, the device type and the AP location are analyzed to answer the research questions. For trial experiment, the logs from three runs were converted to csv format and imported to Google Sheet to filter unique wireless devices. Kismet stores same devices multiple times if they are within the range of sensor. Removing the duplicated data gets the data only from the unique wireless devices to be analyzed. MAC address is unique identification of a device. Filtering unique MAC addresses will get the unique wireless devices. For the actual data analysis, the csv file that was converted from Kismet log by the ready-made script does not include part of data that are needed for this study, such as device type and device manufacturer. Since Kismet log file is saved in SQLite database, it is better to gain the needed data directly from database. A customized bash script (Appendix D) was made to make this process semi automatically.

To compare local personal density in weekday and weekend in University of Oulu and Oulu city center(H1), data from wardriving with the Pi setup will be taken to analysis (Table 7). Design 2 and Design 4 are two groups of data to compare the efficiency of wardriving by drone or by walk (ground). Design 1 and Design 3 aims to examine H3 which is the comparison of wardriving efficiency with the Pi setup and with WiGLE phone application.

Table 7. Experiment designs in different day and different location.

	Uni	**City center**	**Examined Hypothesis**
Weekday	Pi, WiGLE by walk (Design 1)	Pi, WiGLE by bike (Design 3)	H3
weekend	1) by drone, on the ground at fixed point 2) by walk within designed route with the Pi set up (Design 2)	1) by drone, on the ground at fixed point 2)By bike within designed route with the Pi setup (Design 4)	H2
Examined Hypothesis	H1 (Pi's data by walk in route)	H1(Pi's data by bike in route)	

To get the general wireless network security state in Oulu, all the unique data collected in Oulu city center and University of Oulu will be summed up separately and frequency table of encryption type will be generated to get percentage of each encryption method. Kismet collects all wireless devices, such as Wi-Fi AP, Wi-Fi Client, Wi-Fi Device, Wi-Fi Bridged. In order to have general idea of wireless network security status in Oulu area, stationary wireless AP, like wireless routers, need to be analyzed. Filtering wireless device type to Wi-Fi AP answers the research questions.

3.9 Limitations of the research

The limitations of the research are "characteristics of design or methodology that impacted or influenced the interpretation of the findings". They are restraints that result from the initial design of the study is chosen, the methodology was taken to establish the reliability and validity and the result of unexpected challenges that emerged during the study. The limitation in research is a way to show the reader that the author has critically thought about research problem, studied the previous relevant published literature, correctly assessed the research method, and to what extent, the limitations impact the research results and conclusions. (Labaree, 2019.)

In this study, wardriving by drone or on ground are arranged in the same day and run one after another. The ideal situation will be having two sets of wardriving devices to scan wireless devices by drone and on ground at the same time to eliminate the difference of available devices within that area. However, with the limited budget and tight schedule, another new Raspberry Pi and the necessary accessories can't be received and configured in time.

Another trial run has been done by bike in Oulu city center within the designed route. It took approximately 12 minutes to complete each run. Once the three times run was completed, data was checked in the log file in Pi and found that there was significant difference in the size of each log that generated by each run. An idea almost was formed in the mind that the amount of APs discovered by Kismet at each run has a high standard deviation. But after filtered unique data and imported to Google Map, it did not show any AP in the latter part of route. It turned out that the battery plug was getting loose while biking on the bumpy road, this also got confirmed by checking the summary of log statistic, it showed the starting time and ending time of each run. It is vital to know if Pi has power on constantly and Kismet is working properly within each wardriving duration. The ideal situation would be having a small monitor connects to Pi via SSH to display the Kismet interface to make sure Kismet keeps running within the designed route and be able to know any interfering or errors happen to Kismet to stop scanning wireless network devices.

As mentioned in Appendix C, Pi does not have a real time clock (RTC), it will get time updated once connecting to internet or retrieving time from `gpsd`. `Gpsd` can't be ran successfully in the systemd service to get date and time updated once the Pi boots. Furthermore, it takes approximately two minutes for the system to update to current time, but once Pi boots, Kismet will start in 45 seconds, so the log file will be named with not updated date, and it will also interfere the log event that saved with time if time suddenly jumps after two minutes. The workaround is to increase the frequency of updating the fake-hwclock to every minute. Each of experiments will last more than one

minute, so overwriting log file will not happen. But still need to manually update Pi's date before starting an experiment in order to be sure date in log file name is written with current date. To automatically update date, more research needs to be done. It is not a must-have feature, but a nice-to-have feature.

3.10 Reliability and validity

Reliability and validity are two scientific criteria to establish the presence and severity of measurement errors (Rajanen, 2015). Reliability concerns to which extent the experiments or any measuring procedures bring out the same result on repeated trials. Validity examines the degree to which a study accurately reflects the specific concept that a researcher is aiming to measure. Reliability is concerned with the accuracy of the measuring procedures; validity is to measure the success of study at measuring what research set out to measure. (Carminies & Zeller, 1979, Rajanen, 2015.)

If not monitor a specific AP, it is not necessary to disable channel hopping. Channel hopping enables channel sources to hop channels to cover the entire spectrum. Enabling channel hopping indicates that Kismet radios can only tune to a single channel at a time. (Kismet, 2019) In configuration file kismet.conf, `channel_hop=true | false` determines that datasource enables channel hopping or not. `channel_hop_speed=channels/sec | channels/min` controls the speed the datasource hops from one channel to another. For this study, the purpose is to monitor all available wireless networks devices as much as possible, the channel list is automatically created from the channels supported by the driver. Wireless card monitors dynamic channels to discover available wireless networks devices. Therefore, it is likely that Kismet is scanning one channel, devices in other channels are missed, even though the default hopping speed is five channels per second. This is the reason why each experiment was designed to be run three times within same route. Additionally, this is a way to verify the standard deviation of the amount of discovered wireless devices at each run.

For the purpose of data reliability, the experiments are taken in Oulu city center and University of Oulu to double confirm that finding does not happen occasionally. Each designed experiment also was conducted in a weekday or a weekend to compare the difference in people density to examine the hypotheses.

4 Empirical Results

This chapter first presents the results of the wardriving experiment concerning the amount of wireless devices discovered in different research designs. Next, results concerning whether the wireless access points quantification is indicative of local personnel density is analyzed and finally the percentage of encryption standards deployed by wireless APs and the distribution of wireless devices manufacturers are presented.

4.1 Amount of wireless devices discovered in the experiments

This chapter presents the quantitative data discovered in four design settings. Starting from the amount of wireless devices discovered in University of Oulu, then the same data discovered in Oulu city center, ending with amount of wireless devices discovered on weekday/weekend by Pi setup.

4.1.1 Amount of wireless devices discovered in University of Oulu

In Figure 8, the three bars in different colors represent the total amount of discovered wireless devices discovered by the Pi setup (blue bar), the amount of wireless AP that was filtered from all of the discovered devices by Pi setup (red bar), and the total amount of devices discovered by WiGLE application (yellow bar). Kismet can discover not only wireless AP, but wireless devices like mobile phones and wireless bridged devices. From the bar length of the total number of discovered wireless by the Pi setup and by WiGLE application, the length of the total discovered wireless devices by the Pi setup are few times taller than its by WiGLE application. The amount of Wireless AP discovered by the Pi setup is almost equivalent to the whole amount of wireless devices discovered by WiGLE application in the experiment that was taken in University of Oulu. The error bars are the standard deviation of each group of data, the error bar in blue columns are the standard deviation (SD) of the total amount of discovered wireless devices which is 107. It is relatively small comparing to Mean (M = 909) of the total amount of wireless devices discovered by the Pi setup. Red columns are the standard deviation (SD = 47) of the amount of discovered wireless AP by the Pi setup, the yellows (SD = 5.5) are its of discovered by WiGLE application.

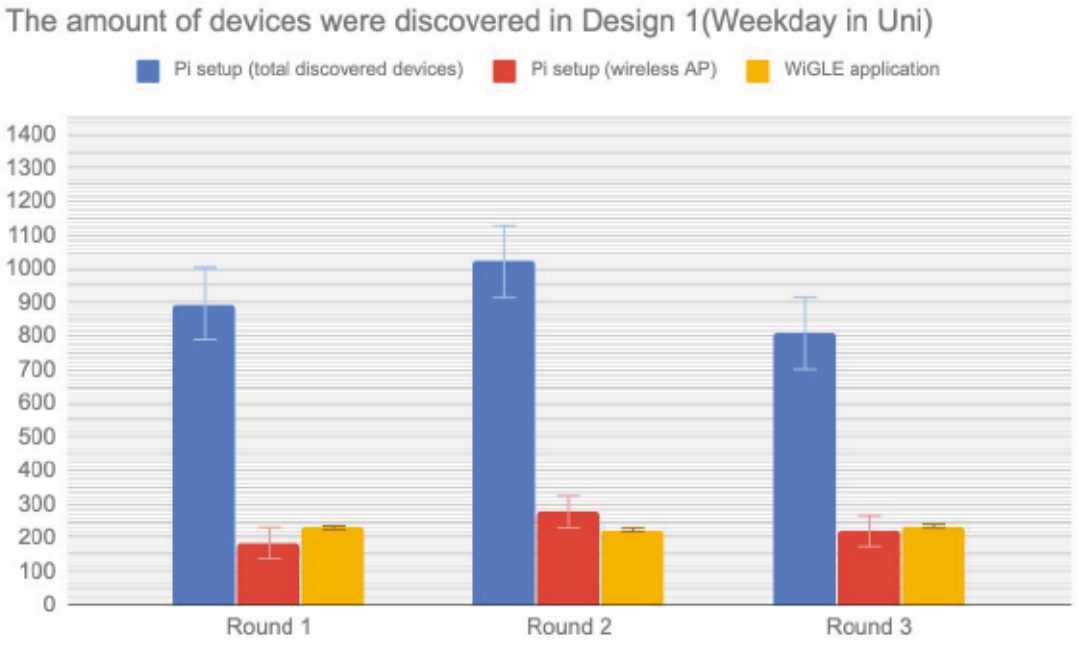

Figure 8. The amount of devices were discovered in Design 1 (Weekday in Uni).

In Figure 9, the total amount of discovered devices by Pi setup that was flown by drone in three rounds has Mean = 203,7 and SD = 16.3 as shown in error bars. The total amount of discovered devices by the Pi setup that was placed on the ground in three rounds are slightly less than the total amount of devices that were discovered by drone. It has Mean = 168 and SD = 9. The stationary wireless devices (AP) were discovered with both means (drone and on ground) have small standard deviation - by drone (SD = 6,1) and on ground (SD = 0.6). Those are small standard deviations compared to the mean of wireless AP discovered by both methods, by drone (M = 105) and on ground (M = 7).

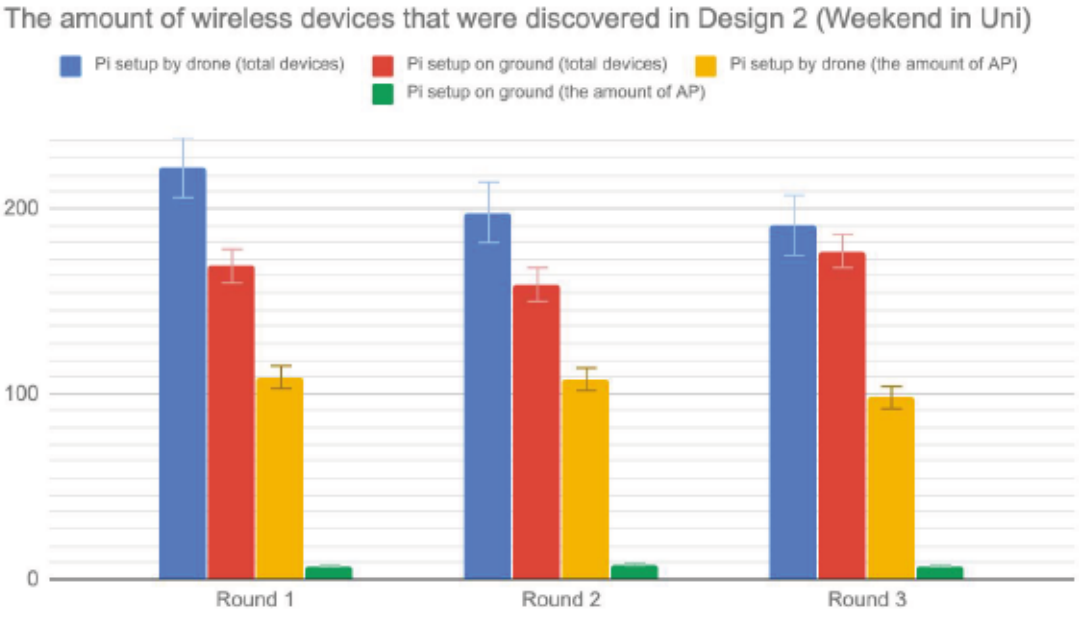

Figure 9. The amount of devices were discovered in Design 2 (Weekend in Uni).

4.1.2 Amount of wireless devices discovered in Oulu city center

In Figure 10, the mean of the whole amount of discovered wireless devices discovered by the Pi setup in three runs is 2336, and SD = 88.5. For the WiGLE application, the mean of the total amount of discovered devices in three runs is 724 with a relatively large standard deviation (SD = 279). The stationary wireless devices were discovered by the Pi setup are stable in three runs (M = 1193, SD = 45).

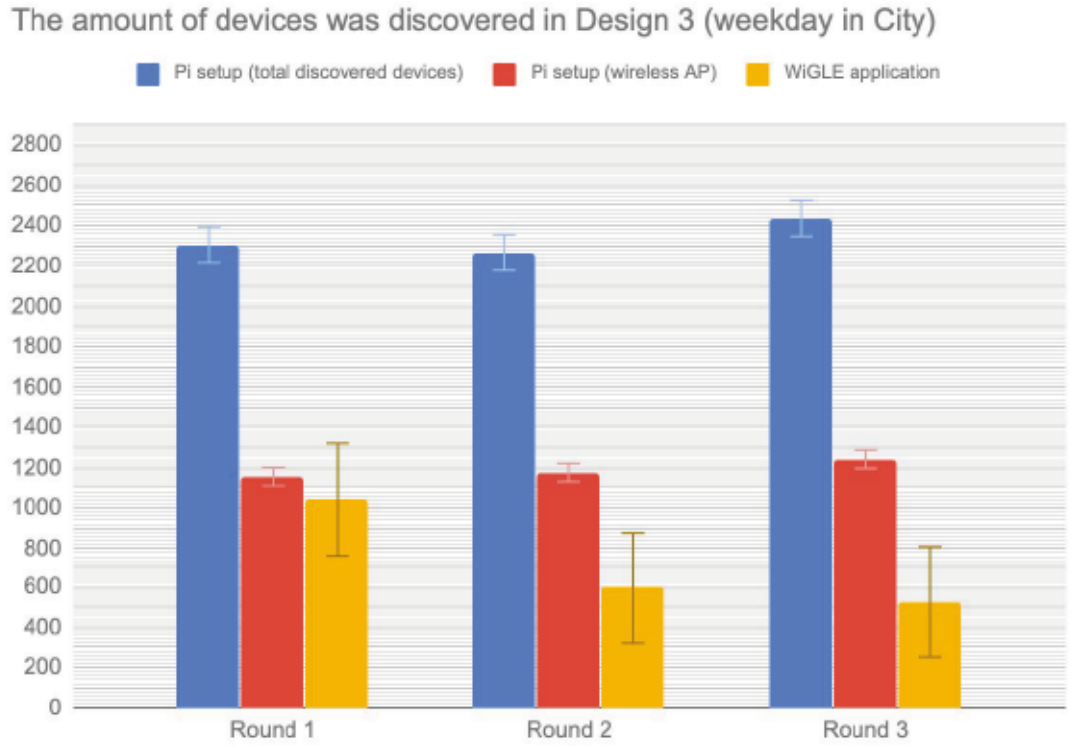

Figure 10. The amount of devices were discovered in Design 3 (Weekday in City).

As shown in Figure 11, the four groups of data in three runs is exceedingly stable with small standard deviations. It is the total amount of devices discovered by the Pi setup by being flown with drone and being placing on ground at a fixed point in Oulu city center. The total amount of wireless devices discovered by the Pi setup (M=759, SD=15) in sky is one time larger than the amount detected (M = 387, SD = 13) on the ground.

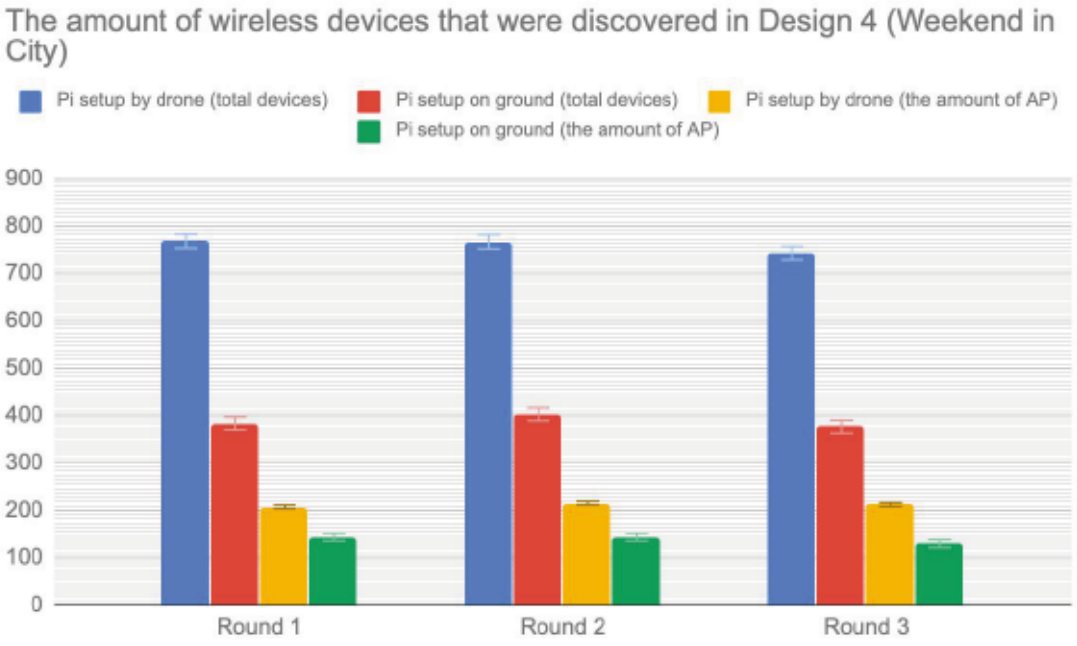

Figure 11. The amount of devices were discovered in Design 4 (Weekend in City).

4.1.3 Amount of wireless devices discovered on weekday/end by Pi setup

In Figure 12, the total amount of discovered wireless devices has significant difference between weekdays and weekends. On weekdays the mean of the total amount of discovered wireless devices in three runs is 1276. On the weekend the amount is 511 which is less than half compared to weekdays. The mean of the amount of wireless AP in three runs in both weekday and weekend has no significant difference, on weekdays it is 210 (SD = 27), 235 (SD = 42) on weekends.

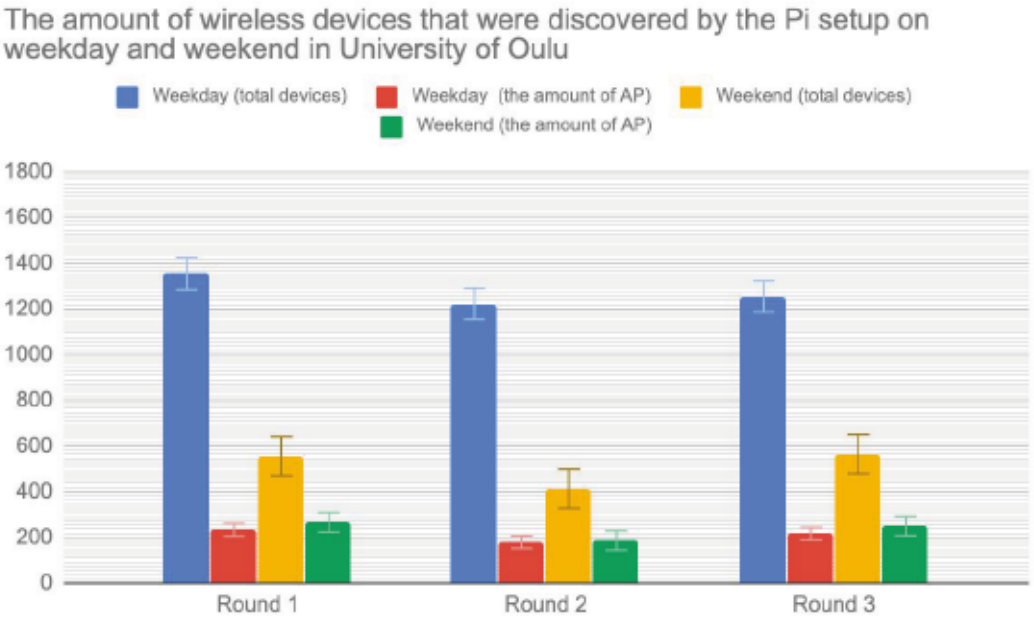

Figure 12. The amount of devices were discovered by the Pi setup on weekday and weekend in University of Oulu.

Figure 13 demonstrates the difference in the amount of devices that were discovered by the Pi setup in Oulu city center on weekdays and on weekends. The total amount of discovered wireless devices on weekdays and on weekends in three runs formed a small curve that firstly went up and then dropped down. The mean of the total amount of wireless devices that were discovered by the Pi setup on weekdays is 2336 (SD = 88), the mean of wireless devices discovered in three runs on weekdays is 2378 (SD = 152). For the wireless AP on weekday and weekend, the mean of the former is 1193 (SD = 45), the mean of the latter is 1088 (SD = 24).

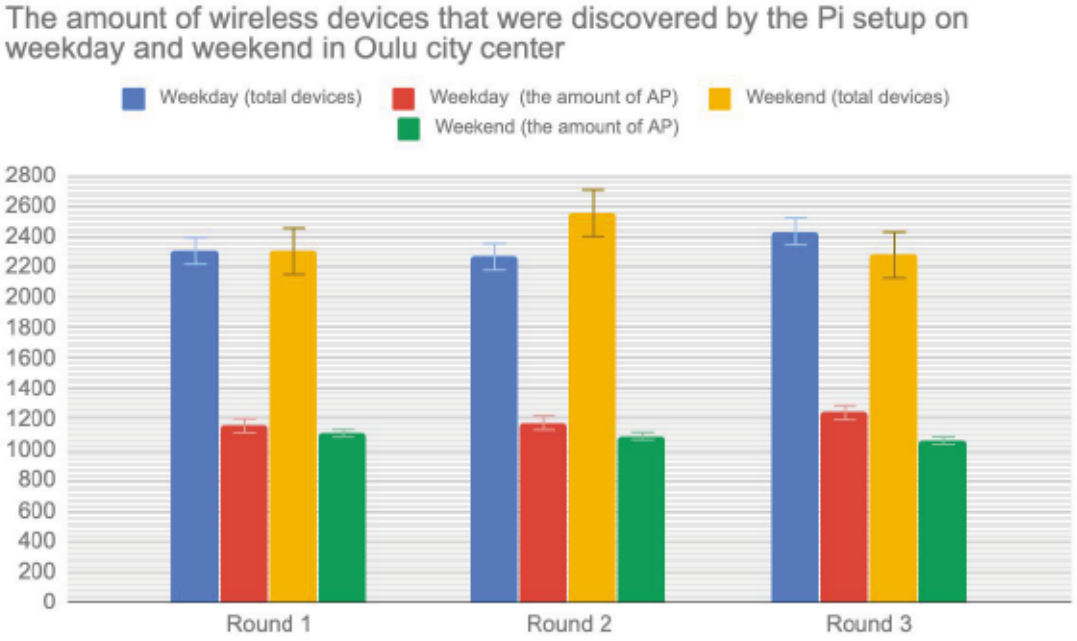

Figure 13. The amount of devices were discovered by the Pi setup on weekday and weekend in Oulu city center.

4.2 Comparing amount of wireless devices discovered on weekend and weekday

Hypothesis 1 (H_1): Higher people density in Oulu city center on weekends than on weekdays, and higher people density in University of Oulu on weekdays than weekends. Hypothesis 1 (H_0): No difference in people density in Oulu city center on weekends than on weekdays, and no difference in people density in University of Oulu on weekdays than weekends.

In Figure 13, the amount of wireless devices that were discovered by the Pi setup on weekday and weekend in Oulu city center has no significant difference. The average amount of wireless AP that was discovered in both days are similar, this amount slightly decreased from 2336 to 2378 from weekday to weekend. The total amount of wireless device was discovered in weekday and weekend in Oulu city center didn't show significant inclination towards going up or going down. Part of hypothesis 1(H_0) which states it has no difference in people density in Oulu city center on weekend than weekday can't be rejected. The total amount on both days in three rounds form small curve which might indicates that the crowd flow changes all the time in Oulu center area. In Figure 12, the average amount of devices discovered on weekdays has

significant difference compared to the amount discovered on weekend. This difference is from 1276 to 511. But the average amount of discovered wireless AP on weekday and weekend has small difference, from 210 to 235. This indicates that the stationary wireless AP stay with similar amount on weekday or weekend. The amount of other wireless devices, such as wireless mobile phone, laptop, have drop down from weekday to weekend. This change shows that more portable wireless devices in University of Oulu on weekday than weekend. Hypothesis 1 (H_0): no difference in people density in University of Oulu on weekday than weekend is rejected.

4.3 Comparing wardriving efficiency in air and on ground

Hypothesis 2 (H_1): Wardriving by drone has higher efficiency than its on ground.
Hypothesis 2 (H_0): Wardriving by drone has the same efficiency as its on ground.

From Figure 9 and Figure 11, the total amount of devices and amount of wireless AP consistently indicate that flying the Pi setup by drone could discover more wireless network devices than keeping the Pi setup on ground in both location Oulu city center and University of Oulu. Therefore, Hypothesis 2 (H_0) is rejected and alternative hypothesis 2 is accepted.

4.4 Comparing wardriving efficiency by Pi setup and by WiGLE phone application

Hypothesis 3 (H_1): Wardriving with the Pi setup has higher efficiency than its with WiGLE phone application.
Hypothesis 3 (H_0): Wardriving with the Pi setup has the same efficiency as its with WiGLE phone application.

As shown in Figure 8 and Figure 10, the total amount of wireless devices discovered by the Pi setup few times outweigh its discovered by WiGLE application. The amount of wireless AP that was discovered by the Pi setup is greater than its discovered by WiGLE application. The Pi setup has outstanding advantage of discovering wireless devices than WiGLE application. Therefore, Hypothesis 3 (H_0) is rejected and the alternative hypothesis is accepted.

4.5 Encryption standard deployed by wireless APs

The majority of deployed encryption method among wireless networks has been discovered in Oulu city center and University of Oulu is WPA-CCMP, which accounts for 59.33% (Figure 14) in total amount of wireless AP in University of Oulu, and 71.11% (Figure 15) in total amount of wireless AP in Oulu city center. WEP has less than 1% in both University and Oulu city center. The percentage of WPA-TKIP deployment are 9.44% in University of Oulu and 10.60% in Oulu city center. The wireless APs that deployed without encryption constitute a noticeable proportion (25.17%) of the whole discovered wireless AP in University of Oulu.

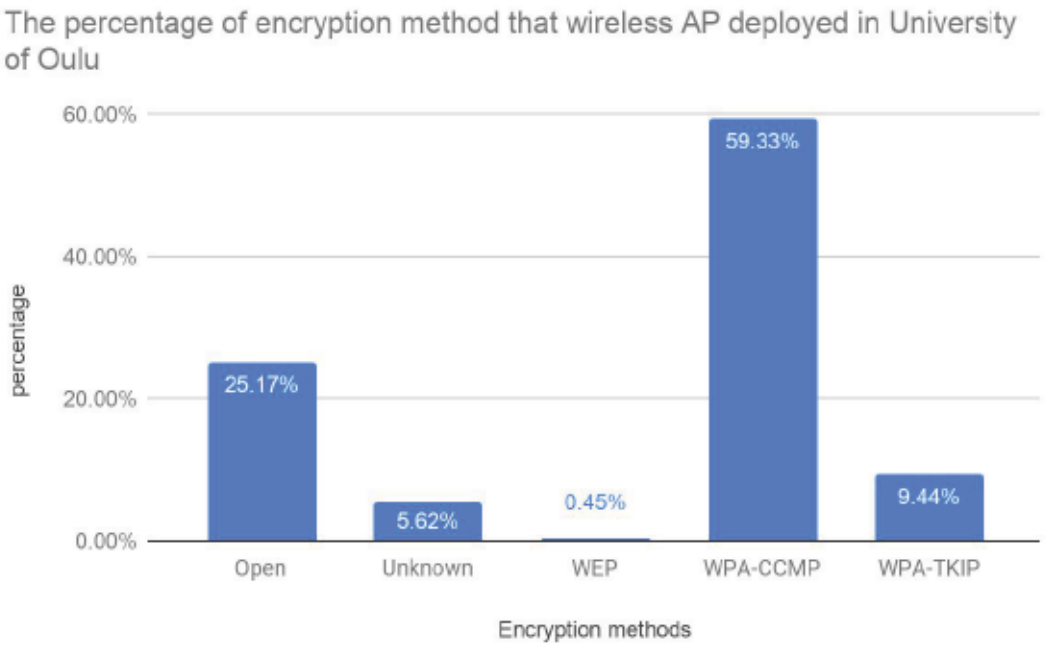

Figure 14. The percentage of encryption method that wireless AP deployed in University of Oulu.

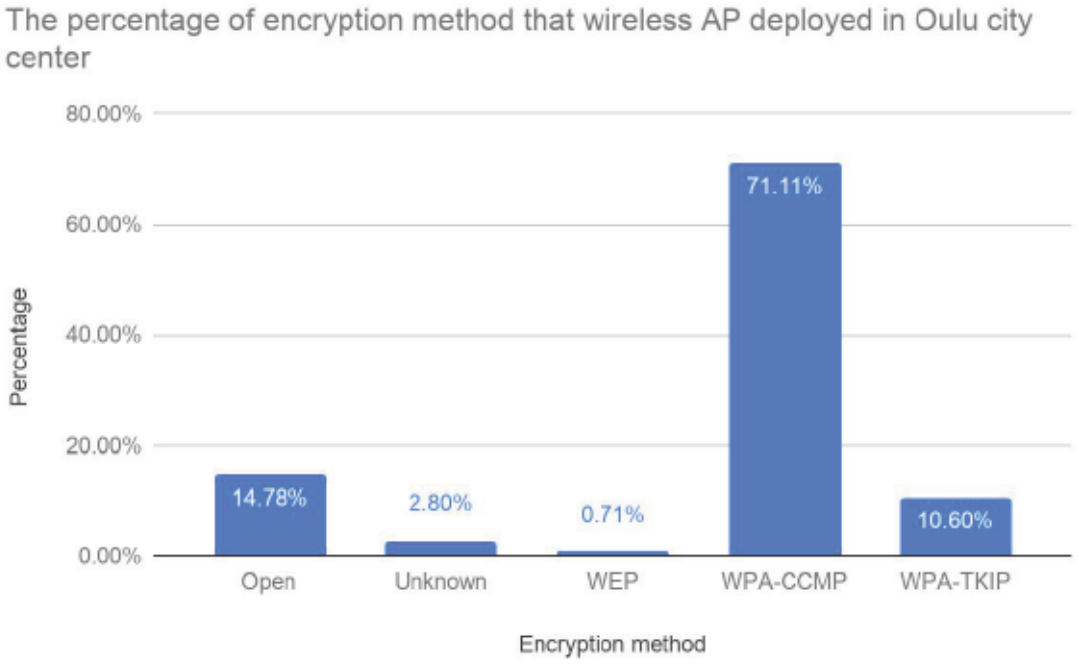

Figure 15. The percentage of encryption method that wireless AP deployed in Oulu city center.

As shown in the pie chart (Figure 17), the four largest proportion of wireless device manufacturers are Unknown, Cisco Systems Inc, Huawei Technologies Co. Ltd, Ruckus Wireless. The ones that have second largest proportion are ZyZEL, ASUSTek Computer, Sagemcom, Strix Systems and TP-Link in Oulu center area.

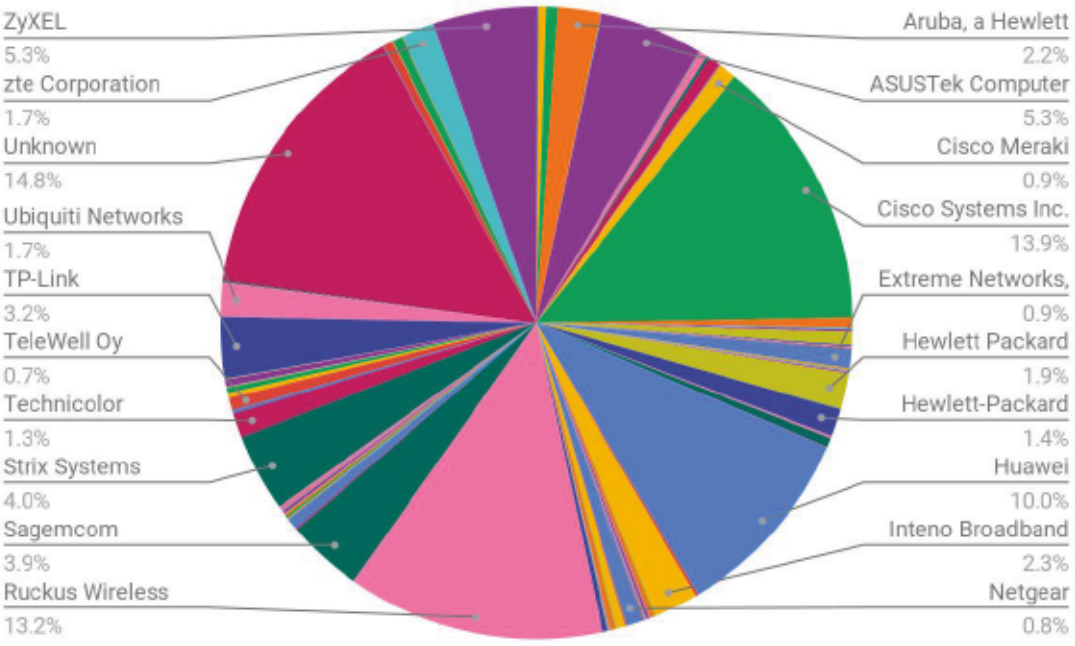

Figure 17. The percentage of manufacturers among the whole discovered wireless devices in Oulu city center and University of Oulu.

5 Discussion

In this chapter I will first present the current state of wireless network security in Oulu center area, then continue by analyzing whether wireless access point quantification is indicative of local personnel density, finally answering research question: how to design and implement the wardriving as a research method.

5.1 RQ1: The current state of wireless network security in Oulu center area

According to the data in chapter 4, the wireless AP that deployed with WEP accounts for 0,71% in Oulu city center and 0,45% in University of Oulu, which has slightly less amount of WEP deployment than the two researches that have been done in Auckland (1,2%) in 2015 (Sarrafzadeh, A., & Sathu, H., 2015), and in Tonga (1%) in 2017 (Lutui, Tete'imoana, & Maeakafa, 2017). Another two researches reported higher amount of WEP deployment in 2013 in Leeds, UK (5%) (Schreuders & Bhat, 2013), and in Morocco (10%) in 2016 (Sebbar, A., Boulahya, S. E., Mezzour, G., & Boulmalf, M., 2016). In Oulu one of 165 wireless APs has deployed with WEP, it is not a big amount, but a disturbing number when considering the whole Wi-Fi users in Oulu area, unless Wi-Fi users deployed this way by purpose, otherwise it is necessary to let people know the high risk of cracking WEP encryption standard.

About 65.22% wireless APs have WPA-CCMP encryption standard in Oulu. This number was reported 67% in Auckland (Sarrafzadeh, A., & Sathu, H., 2015) and 51% in Tonga (Lutui, Tete'imoana, & Maeakafa, 2017). In Oulu, 10% networks encrypted with WPA-TKIP, which is considered less secure encryption standard than WPA-CCMP (Gaj, Bessis, & Liu, 2015). This number is slightly higher than in Auckland (6%) (Sarrafzadeh, A., & Sathu, H., 2015) and much less than research was conducted in Tonga (51%) (Lutui, Tete'imoana, & Maeakafa, 2017).

The security status in Oulu is very close to the finding was reported in Auckland in 2015. They have similar percentages of WEP and WPA/WPA2, except 14,8% hidden authentication in Auckland (Sarrafzadeh, A., & Sathu, H., 2015), but 4,21% in Oulu. Open wireless network has the second largest proportion in Oulu city center (14,78%) and University of Oulu (25,17%). This number was reported 25,9% in Auckland (Sarrafzadeh, A., & Sathu, H., 2015), 7% in Tonga (Lutui, Tete'imoana, & Maeakafa, 2017) and 13% in Morocco (Sebbar, A., Boulahya, S. E., Mezzour, G., & Boulmalf, M., 2016). Having an open Wi-Fi in a city conveniences those people who cannot have cellular data network available, especially travelers. But the security issue should be concerned when connecting to open Wi-Fi, particularly when one has to access to bank account or work environment. It is possible the hacker can sniff all data transmitted within that open Wi-Fi.

5.2 RQ2: Wireless access point quantification and local personnel density

With the fast updating speed of technology, most people have their own smartphone. Kismet can discover the signals a wireless device sends out when it is connected to a Wi-Fi or it is trying to connect to Wi-Fi. Discovering the amount of wireless devices is a way to know the amount of people in a certain area. Through this data, companies can analyze people movement flow and shopping behaviors in a certain area, such as shopping malls.

Based on the results (see Figure 12 and 13), a conclusion can be drawn that the Pi setup can distinguish the personal density by detecting the number of wireless devices, especially from the data is collected from University of Oulu on weekdays and on weekends. It explicitly showed that the amount of people in University of Oulu on weekend is less than on weekdays, but stationary wireless devices have the same amount of numbers in both days.

5.3 RQ3: The efficiency of wardriving on ground or in air (by drone)

Drone has been used in different projects for different purposes, as it has fast movement and can access to hostile environment where factors such as wind, height, radiation that can result in accidents or health issues. In this study, drone is assumed to be more efficient tool to do wardriving than car/bike/walk (on ground) does. In Figure 8 and Figure 10, two experiments had been done to examine the efficiency of wardriving with drone or staying on ground. The collected data showed that drone has higher efficiency in discovery wireless network devices than staying on ground does. This is because the radiation pattern of Alfa antenna is theoretically a sphere centered on the Pi setup with a radius of Alfa antenna sensor distance. When staying on ground, half of the sphere has no wireless networks signals access to, while wardriving with drone, the space Alfa antenna can reach is almost a sphere. The valid radiation area of the Pi setup is almost twice larger when flying with drone than placing on ground. This laid the groundwork to the future application like rescuing a lost person in forest by flying drone with wireless network detection tool.

5.4 RQ4: The efficiency of wardriving by the Pi setup or WiGLE phone application

WiGLE Android application is easy to use and there is no configuration or other devices needed besides a phone. But it also reveals the fact that a sensor of a typical phone will not be as powerful and precise as the specialized wireless network card and location targeting devices. The Pi setup has specialized wireless network card which has 90 meters sensor range making it more efficient in discovering wireless devices than WiGLE application does. Furthermore, the packets, interfaces, devices, and other data that are captured in a Kismet session will be stored in Kismet database. That data can be used for further analyses. The SD of total amount of wireless devices discovered by the Pi setup in each experiment is relatively small compared to the total amount, which evidences the Pi setup behaves stably.

5.5 RQ5: Design and implement the wardriving as a research method

A wide range of selection of hardware and software is available to conduct wardriving for different research purpose. One research was done in Tonga in 2017 was with an Android phone with G-MoN application installed (Lutui, Tete'imoana, & Maeakafa, 2017); In Morocco in 2016 the research was conducted by installing a wireless network scanner called inSSIDer on a laptop and drove around to discover networks (Sebbar, A., Boulahya, S. E., Mezzour, G., & Boulmalf, M., 2016); In Auckland, the researcher conducted wardriving with purchased wireless network monitor software Acrylic Pro and WiGLE Android application (Sarrafzadeh, A., & Sathu, H., 2015); The research was done in UK had similar software and hardware setting as this research, except this research has flown drone with the Pi setup to discover networks, but research in UK was with car. Not many researches have used Raspberry Pi as computer to run software neither. For this research the scanning tool needed to be as light as possible because of flying with drone and that's the reason Raspberry Pi was chosen. Raspberry Pi and Kismet need configurations, and it is time-consuming, that's why some researchers choose Android application like G-MoN and WiGLE to get research data. For this research, the goal was to explore the possibilities of a configurable detection system built from specific components. Such a system will also function as a platform for further development like adding real time indicator to show the direction and distance between the Pi setup and a specific wireless network device.

6 Conclusion and future work

The wireless network security status in Oulu city area is promising. The majority of wireless AP in Oulu center area has deployed WPA-CCMP standard. 10% has WPA-TKIP standard deployed which is considered less secure than WPA-CCMP. Less than 1% wireless networks deployed with WEP standard. It can be a large number when considering the whole amount of people who has wireless network devices in Oulu area.

The purpose of the second research question is to find out whether the quantification of wireless access points is indicative of local personnel density. Based on the data collected in University of Oulu and Oulu city center, this research question was proven from data was discovered by the Pi setup in University of Oulu - less amount of wireless network devices on weekends than on weekdays. Furthermore, comparing amount of discovered devices by drone and on ground shows that the Pi setup with drone has higher efficiency than on ground. This finding indicates that the Pi setup flying with drone is an efficient tool kit to discover wireless networks in a certain area, this can be utilized as a tool to rescue people who gets lost in the forest or discover people movement in a designated area. Comparing the amount of discovered devices by the Pi setup and WiGLE android application found out that the Pi setup was more efficient and stable wardriving tool.

Developing a real time indicator to show the direction and distance between the Pi setup and a specific wireless network device, based on the detected strength of signal could be the future research direction.

References

Akram, Z., Saeed, M. A., & Daud, M. (2018). Wardriving and its application in combating terrorism. Paper presented at the *1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, 2018,* pp. 1-5. doi:10.1109/CAIS.2018.8442035

Baehring, J. (2019) *What does the GDPR say about WiFi tracking?* (2019). Retrieved from https://www.privacycompany.eu/en/what-does-the-gdpr-say-about-wifi-tracking/

Bejarano, O., Knightly, E. W., & Park, M. (2013). IEEE 802.11ac: From channelization to multi-user MIMO. *IEEE Communications Magazine, 51*(10), pp. 84-90. doi:10.1109/MCOM.2013.6619570

Cahoy, E. *Library guides: Empirical research in the social sciences and education: What is empirical research?* Retrieved from guides.libraries.psu.edu/emp/whatis

Chechani, P., Chandra, S. S. G. (2015). U.S. Patent No. US9078137B1. Retrieved from https://patents.google.com/patent/US9078137B1/en

D'Amico, A., Verderosa, C., Horn, C., & Imhof, T. (2011). Integrating physical and cyber security resources to detect wireless threats to critical infrastructure. Paper presented at the *2011 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, 2011,* pp. 494-500. doi:10.1109/THS.2011.6107918

Do you have a MAC address you need to trace?. (2019). Retrieved from https://www.lifewire.com/tracing-mac-address-stolen-computer-3971329

Carminies, E.G and Zeller, R.A. (1979). *Reliability and validity assessment* (Vol. 17). Sage publications.

Fahmy, S., Nasir, A., & Shamsuddin, N. (2012). Wireless network attack: Raising the awareness of kampung WiFi residents. Paper presented at the *2012 International Conference on Computer & Information Science (ICCIS)*, Kuala Lumpur, 2012, pp. 736-740. doi:10.1109/ICCISci.2012.6297124

Freeman, E. H. (2006). Wardriving: Unauthorized access to wi-fi networks. *Information Security Journal, 16*(1), 11.

Gaj, M., Bessis, N., & Liu, L. (2015). Introducing auto generated certificates to rank wireless home network security. Paper presented at the *10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, Krakow, 2015, pp. 591-596. doi:10.1109/3PGCIC.2015.17

Gancarz, K., & Prole, K. (2012). Visual techniques for analyzing wireless communication patterns. Paper presented at the *012 IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, MA, 2012, pp. 341-347. doi: 10.1109/THS.2012.6459872

General data protection regulation (GDPR). (2019). Retrieved from https://gdpr-info.eu/

Berghel, H. (2004). Wireless infidelity I: War driving. *Communications of the ACM, 47*(9), pp 26-29. doi: 10.1145/1015864.1015879

Hurley, C., Rogers, R., Thornton, F., & Baker, B. (2007). *WarDriving and wireless penetration testing*. Rockland, MA: Syngress Publishing, Inc.

Jian, W., Zhi-Feng, F., & Yong, C. (2012). Design and implementation of lightweight wireless lan intrusion detection system. Paper presented at the *Fourth International Conference on Multimedia Information Networking and Security*, Nanjing, 2012, pp. 75-78. doi:10.1109/MINES.2012.96

Juniper networks. (2015) *Understanding the network terms SSID, BSSID, and ESSID - technical documentation - support - juniper networks.* (2015). Retrieved from https://www.juniper.net/documentation/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-ssid-bssid-essid.html

Kern, B. D. (2005). Whacking, joyriding and war-driving: Roaming use of wi-fi and the law. *Santa Clara Computer & High Technology Law Journal, 21(1)*, 101. Retrieved from: https://digitalcommons.law.scu.edu/chtlj/vol21/iss1/3

Keshav, K., Indukuri, V. R., & Venkataram, P. (2012). Energy efficient scheduling in 4G smart phones for mobile hotspot application. Paper presented at the *National Conference on Communications (NCC)*, Kharagpur, 2012, pp. 1-5. doi:10.1109/NCC.2012.6176904

Kismet. (2019) Data sources. Retrieved from https://www.kismetwireless.net/docs/readme/datasources/

Kismet. (2019) Logging. Retrieved from https://www.kismetwireless.net//docs/readme/logging/

Lanamäki, A. (2016). Qualitative Research overview & research design [PowerPoint slides]. Oulu, Finland: Department of Information Technology and Electrical Engineering, University of Oulu.

Lawrence, E., & Lawrence, J. (2004). Threats to the mobile enterprise: Jurisprudence analysis of wardriving and warchalking. Paper presented at the *International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004.*, Las Vegas, NV, USA, 2004, pp. 268-273 Vol.2. doi: 10.1109/ITCC.2004.1286645

Labaree, R. V. (2019). Research guides: Organizing your social sciences research paper: Limitations of the study. Retrieved from //libguides.usc.edu/writingguide/limitations

Lutui, P. R., Tete'imoana, O., & Maeakafa, G. (2017). An analysis of personal wireless network security in tonga: A study of nuku'alofa. Paper presented at the *27th International Telecommunication Networks and Applications Conference (ITNAC)*, Melbourne, VIC, 2017, pp. 1-4.doi:10.1109/ATNAC.2017.8215409

Mankovskii, S., Greenspan, S. L., & Rojas, M. C. V. (2018). U.S. Patent Application No. US20180063165A1. Retrieved from https://patents.google.com/patent/US20180063165A1/en

Martin, J., Mayberry, T., Donahue, C., Foppe, L., Brown, L., Riggins, C., et al. (2017). A study of MAC address randomization in mobile devices and when it fails. *Proceedings on Privacy Enhancing Technologies,* 2017(4) pp. 365-383. doi:10.1515/popets-2017-0054

Năstase, A. (2017). *Public ethics at the european commission*. London; New York: Routledge.

Rajanen, D. (2015). Validity and Reliability, Sampling, Data Analysis - Inferential Statistics [PowerPoint slides]. Oulu, Finland: Department of Information Technology and Electrical Engineering, University of Oulu.

Raspberry pi (2019). Downloads - software for the raspberry pi. Retrieved from https://www.raspberrypi.org/downloads/

Responsible conduct in data management. (2019). Retrieved from https://ori.hhs.gov/education/products/n_illinois_u/datamanagement/datopic.html

Renderman. *Stumbler code of ethics v0.2.* (2019). Retrieved from https://www.renderlab.net/projects/wardrive/ethics.html

Ryan, P. S. (2004). War, peace, or stalemate: Wargames, wardialing, wardriving, and the emerging market for hacker ethics. *Virginia Journal of Law & Technology, 9*1).

Saad, A., Amran, A. R., & Hasan, M. N. A. (2016). WarBox: Portable wardriving over raspberry PI. Paper presented at the *International Conference on Information and Communication Technology (ICICTM)*, Kuala Lumpur, 2016, pp. 227-235. doi:10.1109/ICICTM.2016.7890806

Sadmin. (2018). *How to wardrive on an android phone to map vulnerable networks.* Retrieved from https://null-byte.wonderhowto.com/how-to/wardrive-android-phone-map-vulnerable-networks-0176136/

Sagers, G., Hosack, B., Rowley, R. J., Twitchell, D., & Nagaraj, R. (2015). Where's the security in WiFi? an argument for industry awareness. Paper presented at the *48th Hawaii International Conference on System Sciences*, Kauai, HI, 2015, pp. 5453-5461. doi:10.1109/HICSS.2015.641

Sarrafzadeh, A., & Sathu, H. (2015). Wireless LAN security status changes in auckland CBD: A case study. Paper presented at the *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Madurai, 2015, pp. 1-6. doi:10.1109/ICCIC.2015.7435676

Schreuders, Z. C., & Bhat, A. M. (2013). Not all ISPs equally secure home users: An empirical study comparing wi-fi security provided by UK ISPs. Paper presented at the *International Conference on Security and Cryptography (SECRYPT)*, Reykjavik, Iceland, 2013, pp. 1-6.

Sebbar, A., Boulahya, S., Mezzour, G., & Boulmalf, M. (2016). An empirical study of WIFI security and performance in morocco - wardriving in rabat. Paper presented at the *International Conference on Electrical and Information Technologies (ICEIT)*, Tangiers, 2016, pp. 362-367.doi:10.1109/EITech.2016.7519621

Shuchman, M. L. (2014). *Building WarDriving Hardware Workshop* [Video file]. Retrieved from https://www.youtube.com/watch?time_continue=138&v=TOBX-xRBNjw

Techopedia. (n.d) What is a brute force attack? Retrieved from https://www.techopedia.com/definition/18091/brute-force-attack

WiGLE: Wireless network mapping. (2019). Retrieved from https://wigle.net/

Wikipedia. (2019). *Data analysis*. Retrieved from https://en.wikipedia.org/wiki/Data_analysis

Wikipedia. (2019). *General data protection regulation*. Retrieved from https://en.wikipedia.org/w/index.php?title=General_Data_Protection_Regulation&oldid=891790437

Wikipedia. (2019). *Oulu*. Retrieved from https://en.wikipedia.org/w/index.php?title=Oulu&oldid=890278150

Wikipedia. (2018) *Wardriving*. Retrieved from https://en.wikipedia.org/w/index.php?title=Wardriving&oldid=869467261

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE, 104*(9), pp. 1727-1765. doi:10.1109/JPROC.2016.2558521

Appendix A. Terms and definitions

WLAN: The abbreviation of wireless local area network, it is a broadcast technology that connects one or more devices with an access point by high-frequency radio waves (Sagers, Hosack, Rowley, Twitchell, & Nagaraj, 2015).

Wi-Fi: Short for wireless fidelity. It is a term for certain types of WLANs that defined by the specifications in the 802.11wireless protocol family (Fahmy, Nasir, & Shamsuddin, 2012).

WEP: Short for wired equivalent privacy (Sebbar, Boulahya, Mezzour & Boulmalf, 2016). It is the earliest wireless security algorithms which is considered vulnerable and can be cracked in a few seconds. It utilizes shared key authentication and data can be intercepted and decrypted easily. (Lutui, Tete'imoana, & Maeakafa, 2017, Gaj, Bessis, & Liu, 2015.)

WPA, WPA2: Short for Wi-Fi protected access and Wi-Fi protected access v2. They were introduced to resolve the security vulnerabilities of WEP in 2003 and 2004 (Berghel, 2004; Lutui, Tete'imoana, & Maeakafa, 2017). WPAs employ a per-packet key by generating dynamically a new 128-bit key for two connected packets which makes it a stronger security algorithm than WEP (Sebbar, Boulahya, Mezzour & Boulmalf, 2016).

WPA-TKIP: Temporal Key Integrity Protocol(TKIP) is new wireless network security protocol which was implemented with new features, such as per-packet key hashing, broadcast key rotation, to address the security issues WEP encountered. It employed the same underlying mechanism as WEP, therefore it is vulnerable to similar attacks. (Gaj, Bessis, & Liu, 2015.) It was officially deprecated in the 2012 revision of the 802.11 standard.

WPA-CCMP: Counter Mode CBC MAC Protocol(CCMP). It utilized an Advanced Encryption Standard(AES)-based encryption mode and can was considered a robust solution than TKIP. (Sebbar, Boulahya, Mezzour & Boulmalf, 2016.)

SSID: "Service Set Identifier (SSID) is a 32-alphanumeric character unique identifier that attached to the header of every packet that transmit over a wireless LAN. The SSID acts as a password when a mobile device tries to connect to the basic service set (BSS) -- a component of the IEEE 802.11 WLAN architecture." (Paula R. L., Osai T., George M., 2017). SSID is the identification name for the WLAN(Zou, Y., Zhu, J., Wang, X., & Hanzo, L., 2016), for instance the name of wireless networks lists show on phone or laptop when the wireless icon was clicked (Juniper networks, 2015).

MAC address: Globally unique network addresses, bound to a hardware device instance or other object that requires unique identification. (IEEE Standards

Association, 2019; Martin et al., 2017). It is conventionally used as ID of basic service set (BSSID)(Juniper networks, 2015).

Mobile hotspot: A portable device that taps into cellular networks provides wireless internet access for multiple devices, like mobile phone, laptop, tablet.

Wardriving: Wardriving is the act of scanning wireless access points in a specific area, and storing access points' data, for instance SSID, MAC address and geographical location and reporting them for raising awareness of the security issues (Hurley, Rogers, Thornton, & Baker, 2007).

Brute force attack: It is a trial-and-error method to get information such as username and password. Automated software is used in a brute force attack to try various combinations of username and password until get the value of desired data. (Techopedia, 2019)

WiGLE: Short for WiGLE Wi-Fi Wardriving. It is a tool to observe, visualize, and catalog networks and only supported on Android phone so far. (WiGLE: Wireless network mapping, 2019.)

Kismet: A passive wireless network detector, sniffer, wardriving tool and wireless intrusion detection framework (Schreuders & Bhat, 2013).

Raspberry Pi: A single motherboard computer based on Linux operating system (Saad, Amran, & Hasan, 2016).

Appendix B. Procedures of Setting up Wireless network scanning tool

1 Install Raspbian to Pi SD card

Connecting the SD card to computer with SD card reader, download NOOBS from raspberrypi.org, unzip the file and copy all files to SD card. It is noted SD card should be empty, if not, it has to be formatted before moving NOOBS files into it. After downloading operating system installer NOOBS, put the SD card to Pi and connecting mouse, keyboard, monitor and power supply to Pi, follow the instructions on the Monitor to download Raspbian and do the general settings for system too. Several alternative methods to install Raspbian, and it is easy to find from the internet, here only describe the simplest way for beginner. The default username is pi and password is raspberry. It is highly recommended to change the password, to do that, open terminal and give command `passwd`, it will reset the Pi's default password. Update the system by running command `apt-get update` and `apt-get upgrade`.

2 Enable SSH

The default SSH is easy to be cracked, the default SSH key need to be removed and a new key should be generated. First, go to the SSH keys folder and reconfigure the server from giving following commands in the terminal

```
cd /etc/ssh/
dpkg-reconfigure openssh-server
```

Then create new SSH key and configure it to enable runlevels for SSH and allow to start service at boot so it is possible to log in to Pi remotely.

```
update-rc.d -f ssh remove
update-rc.d -f ssh defaults
nano /etc/ssh/sshd_config
```

In the configuration file of SSH key, make sure that "PermitRootLogin" is uncommented and change its value to yes (Figure 1). Press Ctrl + O to save file and Ctrl + X to exit.

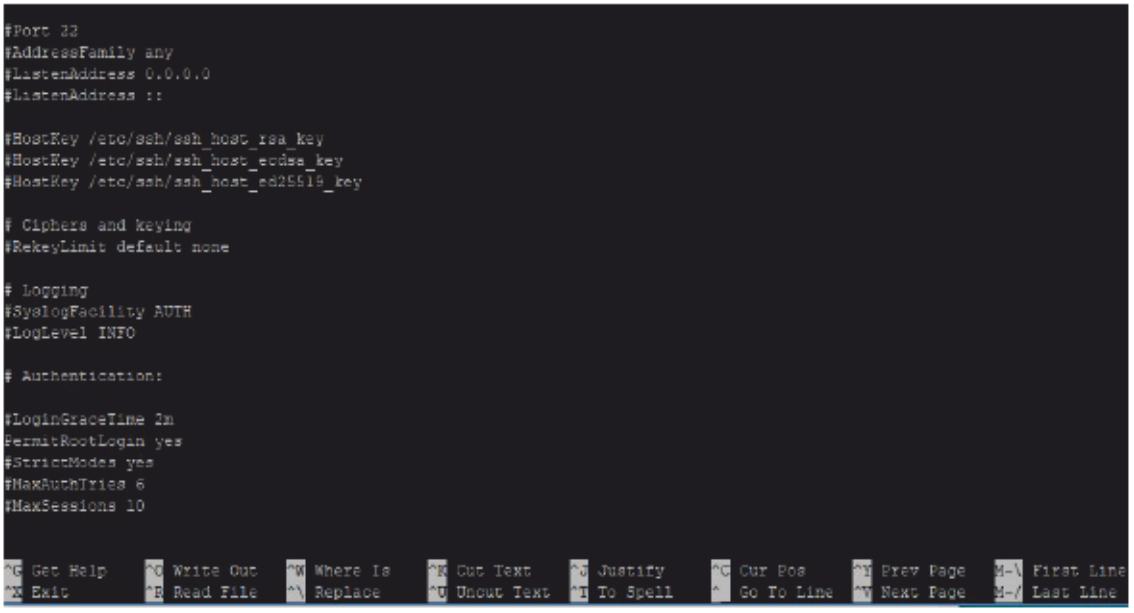

Figure 1. SSH key configuration file.

Next, restart SSH key to apply these changes and enable SSH at boot with the settings that is applied with following commands

```
sudo service ssh restart
update-rc.d -f ssh enable 2 3 4 5
```

Until here, the new SSH key is ready, shut down the Pi and unplug mouse, keyboard and monitor. To restart the Pi, just unplug the power and plug back again. Now the Pi connected to the same wireless network as computer or laptop, so only need to know the IP address of Pi. To know Pi's IP address, it either opens router's control panel to find the list of devices on this network or uses command ip addr show in terminal to find out. Then open the terminal on the Macbook and add server to known host from command

```
ssh-keygen -R 192.168.1.102
```

Adding server to host just needs to be done once. Next, connect to server by command `ssh pi@192.168.1.102` or `ssh pi@raspberrypi.local`

3 Install Kismet

To download the latest version of Kismet, it is better to download from its GitHub repository, this is easy to follow from Kismet quick start https://www.kismetwireless.net/docs/readme/quickstart/ , the following commands are how Kismet is installed for this study, only place need to pay attention to is that The new version requires a lot of dependencies to install. If a problem occurs because of the lack of a dependency, just use `sudo apt-get install dependency name` as a workaround.

```
git clone https://www.kismetwireless.net/git/kismet.git
sudo apt install build-essential git libmicrohttpd-dev pkg-config
zlib1g-dev libnl-3-dev libnl-genl-3-dev libcap-dev libpcap-dev libnm-dev
```

```
libdw-dev      libsqlite3-dev      libprotobuf-dev      libprotobuf-c-dev
protobuf-compiler   protobuf-c-compiler   libsensors4-dev   screen   gpsd
ncurses-dev tcpdump libmicrohttpd-dev flex byacc libusb-1.0-0-dev

cd libpcap

./configure

make

sudo make install

cd ..

cd kismet

./configure

make

sudo make suidinstall
```

4 Install GPSD

The above step already installed GPSD in Pi. GPS receiver was attached on Pi by female to female pin connector through HW UART instead of USB port, it needs extra configuration for Raspberry Pi to disable Serial console and enable UART. This can be done by running sudo raspi-config and follow instructions to go to Interface Options and Serial, then select No on enabling the login shell and select Yes to enable serial port. Additionally, in the GPSD configuration file, DEVICES value needs to change to /dev/serial0.

The first time to run GPS by giving command cgps -s without enabling UART port, it gave no GPS fix, because the gps receiver connected to Pi from QART, but QART is not enabled. When QART is enabled, open GPSD again, service daemon did not get information updated, so even after enabled UART, it still gave errors and showed no gps fix. To disconnect the service daemon,

```
sudo systemctl stop gpsd.socket
sudo systemctl disable gpsd.socket
```

need to be run. Then to reset GPS by executing following commands, after this a fixed GPS should be shown (See in Figure 2).

```
sudo killall gpsd
sudo gpsd /dev/serial0
cgps
```

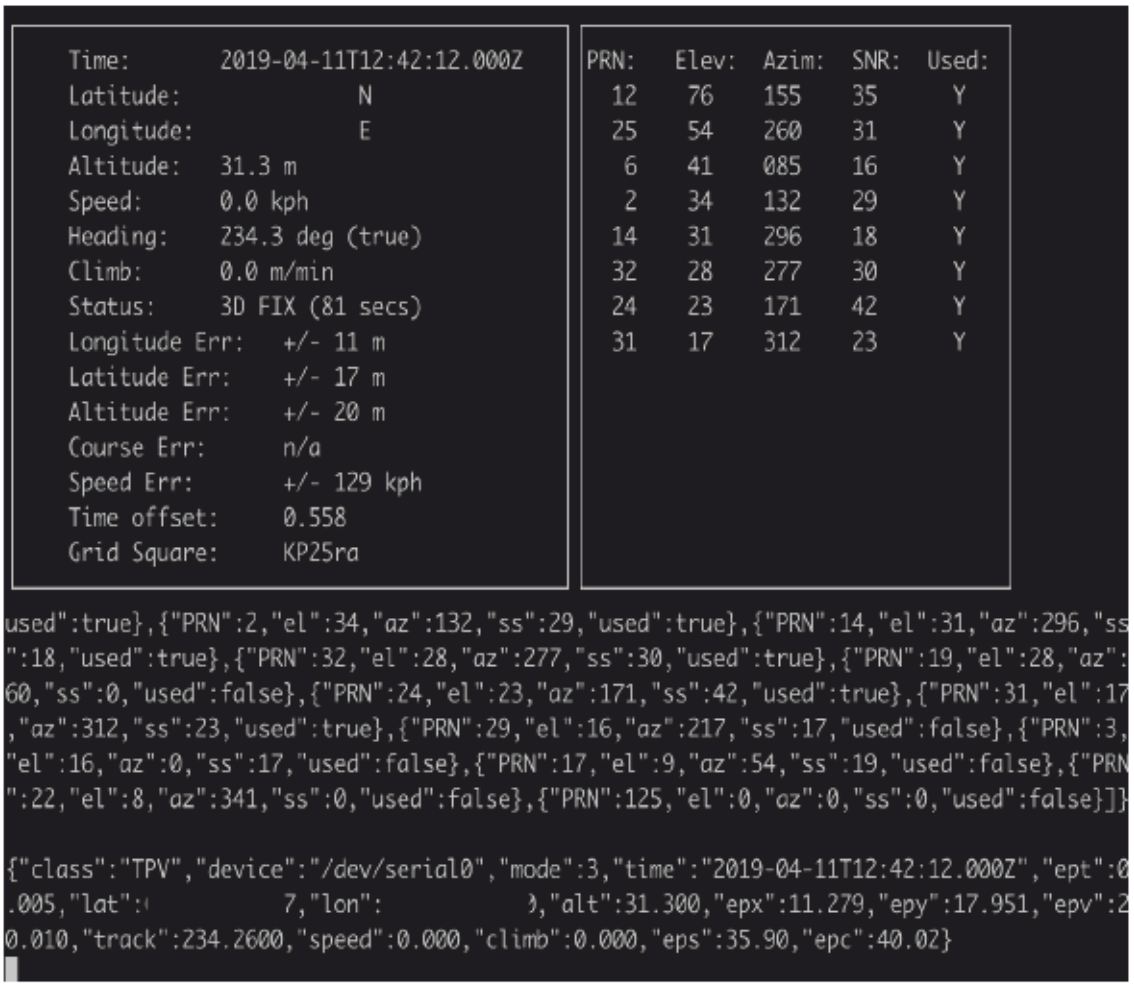

Figure 2. GPS fix.

5 Run in the field

Now accessing Pi via SSH is feasible as Pi and Macbook share the same network, when wardriving outside of house, this connection gets lost. Then an Ethernet cable is used to connect Pi and Macbook and you can get access to Pi with ssh pi@raspberrypi.local. If ethernet connection is not active, the ethernet service should be restarted. To do that, go to System Preferences → Network → Select USB 10/100/1000 LAN → select Make Service Inactive from the setting menu and then reactivate it again. (see Figure 3 below)

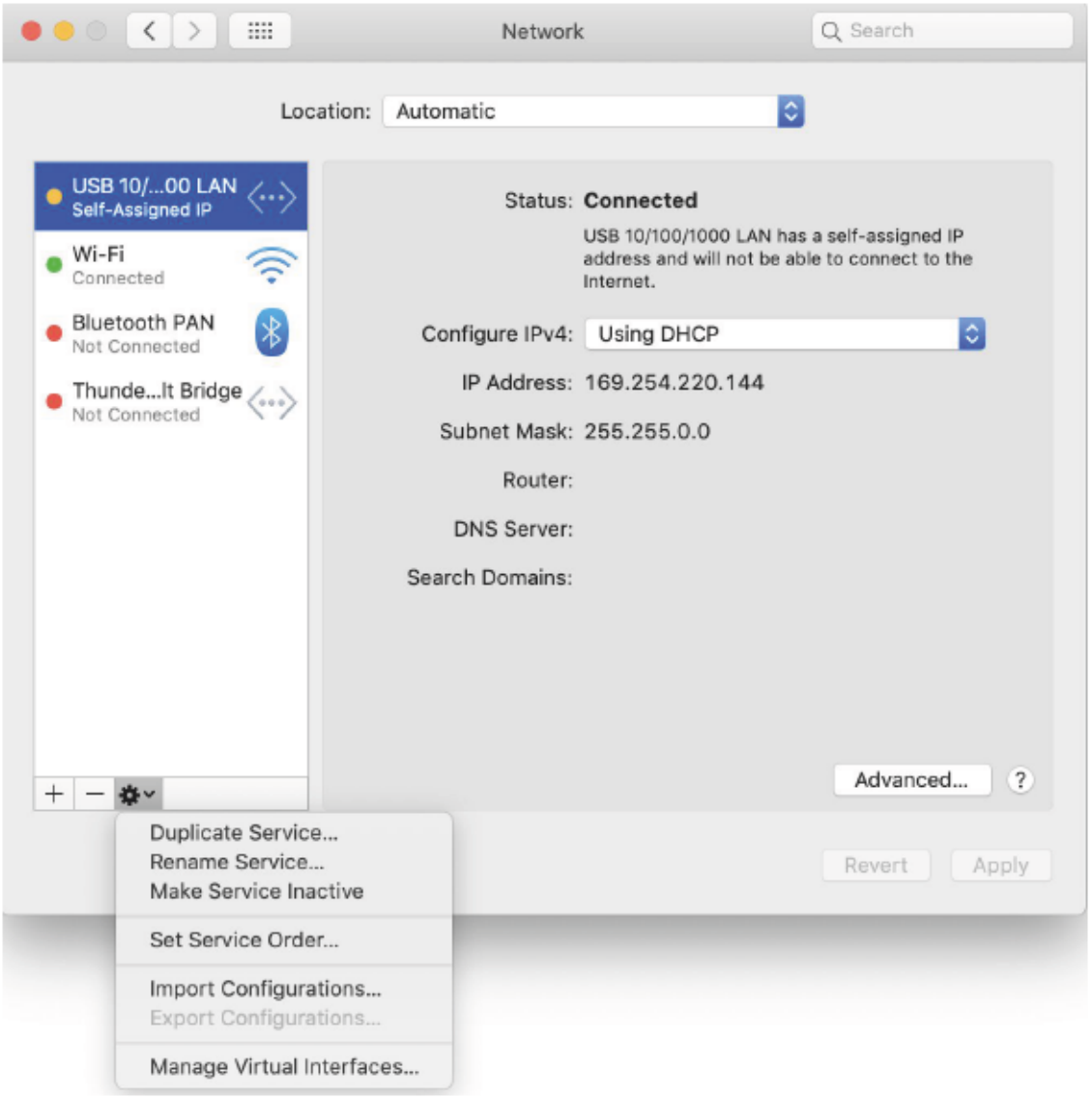

Figure 3. Network setting of MacOS.

When wireless network scanning tool is attached on Drone, the Ethernet should be disconnected, but the connection to Pi will lose again and Kismet will be killed. To solve this issue, Screen is downloaded. To install screen, execute following command in the terminal.

```
apt-get install screen
```

When open screen and run Kismet and GPSD, then disconnect screen, GPSD and Kismet still will be run in the background and can be reconnected again. So, when disconnect screen, the ethernet cable can be removed and put Pi to the Drone and do scanning. Once scanning is done, reconnect to screen and close Kismet and exit screen. The following steps demonstrate how to use screen:

1. Start screen, GPSD and Kismet

```
screen
gpsd /dev/serial0
kismet
```

2. Disconnect screen

```
Ctrl A, then d
```

3. Reconnect to screen

```
screen -r
```

4. Shut down Kismet

```
Ctrl C
```

5. Exit screen

```
exit
```

To collect AP data with Kismet, the important step is to have a Wireless card. Pi have internal build-in wireless card that is commanding control Wi-Fi, one can login in to Pi with this Wi-Fi and configure Pi. Internal wireless card doesn't have the right chip for Kismet to scan AP. To manage this, Alfa Network AWUS036NHA is chosen as wireless card. It is bought from Amazon, and cost about 30 euros. It connects to Pi from USB.

One more step to do before testing Kismet is the Alfa wireless card need to be put in monitor mode. To do this, airmon-ng need to be installed, then run sudo airmon-ng start wlan1 in terminal to enable monitor mode for Alfa wireless card, it will add a suffix "mon" to Alfa wireless card name wlan1, the default wireless card is wlan0. To check wireless card name, use the command ifconfig, all the network connected to Pi will be displayed (Figure 4). Eth0 is the ethernet cable that connects Macbook and Pi.

```
pi@raspberrypi:~ $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 169.254.62.192  netmask 255.255.0.0  broadcast 169.254.255.255
        inet6 fe80::db78:29e8:caa4:37e5  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:60:a6:9e  txqueuelen 1000  (Ethernet)
        RX packets 806  bytes 145792 (142.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 471  bytes 91050 (88.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 82  bytes 15179 (14.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 82  bytes 15179 (14.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.104  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 2001:14ba:14fa:e100::4  prefixlen 128  scopeid 0x0<global>
        inet6 2001:14ba:14fa:e100:8720:7e0d:5e06:a804  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::5b4a:e9e0:9298:8640  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:35:f3:cb  txqueuelen 1000  (Ethernet)
        RX packets 328  bytes 55133 (53.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 111  bytes 17587 (17.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan1mon: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        unspec 00-C0-CA-97-B7-5C-30-30-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 42634  bytes 10065466 (9.5 MiB)
        RX errors 0  dropped 41658  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

pi@raspberrypi:~ $
```

Figure 4. Network names of Pi

6 After reboot Pi

Basically, after reboot Pi or just start Pi, the following commands need to run GPS and Kismet to scan AP:

1. To open Alfa wireless card monitor mode - `sudo airmon-ng start wlan1`
2. Run screen session - `screen`
3. Open GPSD and run Kismet - `gpsd /dev/serial0 && kismet`

Appendix C. Procedures of Setting up Auto Start Wardriving

1 Auto-wardriving

Several ways can start a program on Raspberry Pi at its startup. Systemd is chosen for this experiment. Systemd provides standard process for controlling starting a program when a Linux system boots up. Firstly, go to Systemd folder to make a service file, in the service file to give the order to Pi to start the GPS and Kismet when every time Pi reboot.

```
sudo nano /lib/systemd/system/wardrive.service

[Unit]
Description=Wardriving auto start
After=multi-user.target

[Service]
Type=forking
ExecStart=/home/pi/kismetautostart.sh

[Install]
WantedBy=multi-user.target
```

Next, kismetautostart.sh need to be created to give command to turn Alfa wireless card to monitor mode and start GPS and Kismet.

```
#!/bin/bash

#turn off Wi-Fi
sudo ifconfig wlan0 down

#turn antenna on to monitor mode
#sudo airmon-ng start wlan1
sudo ifconfig wlan1 down
sudo iwconfig wlan1 mode monitor
sudo ifconfig wlan1 up

#run gpsd
gpsd /dev/serial0

#start screen in detached mode and run gpsd and kismet inside screen
sudo -iu pi screen -dm bash -c "kismet --no-ncurses"
```

With above configuration, it worked perfectly, only when three rounds wardriving were done, it returned one log instead of three. It turns out that Raspberry Pi is not implemented with real time clock (RTC) module, time on Pi will be updated to real time once connected to the internet, however when reboot Pi, it takes time from Pi fake-hwclock, time is saved to fake-hwclock will be updated periodically. When Pi is power off, the time will stop. The built-in wireless card is turned off when automotive

wardriving script starts, Pi can't update to real time from internet, each of the three round experiments took about five minutes, it is not long enough for fake-hwclock to renew time either, so Pi was rebooted with same time in the three experiments. Kismet log is named with date and time of Pi, it always overwrite the previous log. To avoid this situation, fake-hwclock need to be updated every minute, as each of the experiments will be over one minute, it is a workaround for this experiment. To ask fake-hwclock updates every minute, go to cron with command `crontab -e` and add `*/1 * * * * sudo fake-hwclock save` to the end of the file.

When ending a wardriving run, the power is switched off. This way, Kismet is shut down abnormally. The rest of the data will be saved in a ...-journal file. Then execute `sqlite3 Kismet-file-name.kismet 'VACUUM;'` to move the data in journal file to the main log.

2 Loop Kismet

```
[Unit]
Description=Wardriving auto start
After=multi-user.target
StartLimitBurst=3
StartLimitInterval=300

[Service]
Type=forking
ExecStart=/home/pi/kismetautostart.sh
Restart=always
RuntimeMaxSec=300

[Install]
WantedBy=multi-user.target
```

Appendix D. Procedure of retrieving data from sqlite database

First got to /home/pi/ folder and make a new bash script by executing `sudo nano kismettocsv.sh` and paste the following code in the bash file and save it. To convert a kismet file to a csv file with the selected seven fields (MAC address, type of device, the average latitude and longitude, SSID, manufacturer, encryption type) from devices table, execute `./kismettocvs.sh input-file-name.kismet output-file-name.csv`.

```
#!/bin/bash
sqlite3 -header -csv $1 "SELECT
  \"devmac\",
  \"type\",
  \"avg_lat\",
  \"avg_lon\",
   json_extract(devices.device, '$.\"kismet.device.base.commonname\"') AS
"SSID",
     json_extract(devices.device,   '$.\"kismet.device.base.manuf\"')   AS
"Manuf",
     json_extract(devices.device,   '$.\"kismet.device.base.crypt\"')   AS
"Encryption" from devices;" > $2;
```