Computer Networks 197 (2021) 108359

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A systematic methodology for continuous WLAN abundance and security analysis☆

Saku Lindroos *, Antti Hakkala, Seppo Virtanen

Department of Computing, University of Turku, 20014, Turku, Finland

ARTICLE INFO

Keywords:
IEEE 802.11
Internet of Things
IoT
Wardriving
Wireless LAN
Wireless security

ABSTRACT

In this paper, we present a systematic methodology for continuous surveying and analysis of 802.11 Wireless Local Area Network (WLAN) abundance and security, based on the passive wireless network scanning technique called wardriving. The objective is to provide an efficient, scalable, and easily accessible methodology for collecting, analysing and storing WLAN survey data. To adhere to these set requirements, the presented survey and analysis processes can be carried out with freely available open-source software and common off-the-shelf hardware. While extensive literature has been produced on wardriving and numerous WLAN survey studies have been documented in previous works, to our knowledge, no similar comprehensive methodology for systematic WLAN surveying and analysis has been previously presented. To further rationalise the need for surveying and analysing WLAN networks, an investigation on the related literature and the current state of the WLAN networking landscape has been conducted. Furthermore, as surveying WLAN networks via the wardriving technique undoubtedly raises legal and moral concerns, the legitimacy and ethics of wardriving have been examined. To test the effectiveness of the proposed methodology, a primary test and calibration WLAN survey was conducted in three separate locations within a middle-sized city located in Southwest Finland. Based on the survey results, WLAN security in Finland is in a relatively good state. During the test survey, we successfully collected and analysed data from 720 WLAN networks, proving the effectiveness of the proposed methodology. From the 720 detected WLAN networks, 6% used insecure encryption protocols, 12.8% were unencrypted and a clear majority of 81.3% used the WPA2 encryption protocol. Results also show that wireless network device owners in the surveyed areas are not inclined to alter the factory-set default settings of their wireless networks. It was noted that roughly 40% of the surveyed networks used easily identifiable factory-set SSIDs and only 5.4% of the networks had a cloaked SSID. Furthermore, the survey data shows that WLAN devices from 38 different manufacturers were detected. Three of the most popular manufacturers in the surveyed area were Cisco with 28.3%, Huawei with 15.7% and Ruckus Networks with 9.7%.

1. Introduction

Wireless Local Area Network (WLAN) technology, familiarly known by its marketing name Wi-Fi, is without a doubt one of the most popular and well-known wireless networking technologies. Since the ratification of the original IEEE 802.11 WLAN standard in 1997, having a wireless internet connection has become an everyday commodity and it is expected to be there wherever we go. The recent outpouring of affordable WLAN capable smart and Internet of Things (IoT) devices has further increased our reliance on WLAN technology. IoT technology has turned our everyday appliances, manufacturing processes and even entire cities into hotbeds of WLAN technology. It has been estimated that the current surge of WLAN capable smart home and IoT devices will drive the number of in-home WLAN devices up to 17 billion by the year 2030 from the estimated 5 billion in-home devices in 2019 [1]. Other estimates show that the number of IoT devices may reach 31 billion in 2020 [2]. In their 2019 study [3], Kumar et al. showed that in over 66% of the North American and in over 53% of the Western European home networks scanned for the study resided one or more WLAN capable IoT devices.

Wireless networking is a trade-off between security and convenience. It is undoubtedly much more cost-effective and convenient to connect devices wirelessly rather than run cumbersome wires between them. The price paid for the gained convenience is that the communicated information will be exposed to the possible eavesdropper within the communicating devices range. As the communicated information is propagated through the air in radio waves instead of being confined

☆ This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

* Corresponding author.
E-mail addresses: saplin@utu.fi (S. Lindroos), ajahak@utu.fi (A. Hakkala), seppo.virtanen@utu.fi (S. Virtanen).

https://doi.org/10.1016/j.comnet.2021.108359
Received 12 February 2021; Received in revised form 11 May 2021; Accepted 21 July 2021
Available online 27 July 2021

into wires, it is highly susceptible to interception and falsification attempts. The exposed communication can compromise the network user's privacy or, in the worst-case, compromise the security of the whole larger network infrastructure.

It should also be remembered that in addition to the communicated information, wireless networking often leaves the communicating devices exposed and vulnerable to manipulation. There is little use in securing the communicated information if security measures in the devices themselves are neglected. The increasing demand for affordable WLAN capable IoT devices can, for example, end up creating an incentive for device manufacturers to cut corners by providing only minimal or in other ways inadequate security measures for their devices. On the other hand, even if manufacturers do provide adequate security in their devices, the end-users might not have the needed knowledge to secure their devices properly [4]. These fears were confirmed during the Mirai malware incident of 2016. The malware scoured the internet for various network devices configured with either weak or hardcoded credentials. The infected devices were then used as part of Distributed Denial of Service (DDoS) attacks and cryptocurrency mining operations [5].

In addition to WLAN capable smart and IoT devices connecting household appliances and factories wirelessly to the larger network infrastructure, WLAN technology is shifting on to a new encryption protocol. The now out-dated Wi-Fi Protected Access 2 (WPA2) encryption protocol has been in use for almost two decades and is in the process of being replaced by the next generation of the WPA encryption protocol WPA3. WLAN technology is currently undergoing major changes and is at a watershed moment where masses of new devices are being introduced into WLAN networks, significantly increasing reliance on the security of these potentially insecure new devices. In order to stay on top and react to these changing circumstances accordingly, it is crucial to find new ways to study and raise awareness about WLAN security. Otherwise, we will end up paying a heavy price for our mistakes in the near future, and face more threats in the likes of Mirai.

In this paper, we are presenting a systematic methodology for continuous surveying and analysis of WLAN abundance and security. The objective has been to develop an accessible, efficient and scalable methodology for collecting, analysing and storing WLAN survey data. To our knowledge, no similar comprehensive methodology for systematic WLAN surveying and analysis has been presented in any previous works. By collecting and analysing WLAN data it is possible to create new knowledge about the insufficiencies and weaknesses in WLAN security. Actively collecting WLAN survey data on a longer time span makes it possible to follow the evolvement of WLAN abundance, security and usage as well as the adoption of new technologies and devices. The obtained knowledge can then be turned into concrete propositions and guidelines for increasing WLAN networking security and help predicting the future directions of WLAN networking.

In order to adhere to the set objectives, the proposed methodology has been formulated around freely available software and common off-the-shelf hardware. The presented WLAN survey and analysis processes have been founded on the passive wireless network scanning technique known as wardriving. Wardriving was popularised in the early 2000's, when Peter Shipley presented the results of his 18-month long wardriving survey during the hacker conference Def Con in 2001 [6]. Wardriving has since become a legitimate tool for information security experts and an active community of hobbyists has developed around the activity.

The rest of this paper has been structured as follows. In Section 2, we will discuss the past and current state of WLAN security and review the current literature related to surveying WLAN networks. Section 3 presents the hardware and software related to surveying WLAN networks. Furthermore, Section 4 introduces the reader to the concept of wardriving and presents the possible legal, regulatory and ethical boundaries of wardriving. Section 5 introduces the proposed WLAN survey methodology in its entirety. Section 6 discusses some of the observations and changes made to the survey and analysis processes after an initial calibration and test survey. The section also presents the results gained during the test survey as proof of the survey methodology's effectiveness. Lastly, Section 7 provides the conclusions and discussion about the results gained during the test survey and how the survey methodology will be developed and how it will be used in the possible future studies.

2. Related work and literature

2.1. The current state of WLAN security

WLAN security has its unique challenges compared to its wired counterpart. In typical wired Local Area Network (LAN), the only way for a new device to join the network is by physically connecting a cable into a network device. The use of a physical connection ensures that the communicated information is confined to the cables and communicating devices. In WLAN networking the process of joining into the network, and the following communication, is handled over the air in radio waves between the joining device and a wireless Access Point (AP), acting as a portal to the larger wired network infrastructure. Many of the inherent problems in WLAN networking security stem from this fundamental idea of being wireless. By its wireless nature, WLAN communication leaves the communicated information, as well as the communicating devices, vulnerable to eavesdropping and manipulation attempts. To deter and mitigate the effects of these inherent issues, various security mechanisms have been introduced into the IEEE 802.11 WLAN standard to bolster the security of WLAN networking.

The most notable security mechanisms presented in the 802.11 standard have been the cryptographic encryption protocols: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). The WEP protocol was defined in the original 1997 IEEE 802.11 WLAN standard to provide basic data encryption and authentication comparable to a wired LAN network. Unfortunately, the protocol was soon found to be inadequate, having several flaws and shortcomings in its implementation. The found weaknesses were so severe that the protocol had to be quickly replaced with the first generation of the WPA protocol known as WPA-TKIP. Standing for Temporal Key Integrity Protocol, the TKIP protocol used the same Rivest Cipher 4 (RC4) encryption algorithm as WEP, adding only a few extra layers of security on top of the broken WEP protocol. WPA-TKIP was intended only as a short-term fix that could be applied to the existing vulnerable WEP hardware via software updates. Fairly soon after its release, weaknesses in the WPA-TKIP protocol started to emerge and it too had to be replaced. Because of their irredeemable flaws, both WEP and TKIP protocols have been deprecated from the IEEE 802.11 WLAN standard and have been deemed unfit to be used in encrypting WLAN communication.

With the ratification of the 802.11i amendment as part of the 802.11 standard in 2004 came the second generation of the WPA protocol known familiarly as WPA2. The protocol fixed the many flaws of its predecessors and is based on the Advanced Encryption Standard (AES), providing significantly more robust security. WPA2 has now been in use for over 16 years and has started to show its age as several vulnerabilities have been found in its implementation over the years. The WPA2-personal protocol used in most consumer WLAN devices has been known to be vulnerable to brute-force password attacks since 2003 [7]. The situation has worsened over the years as computing power has increased and become gradually more affordable, making it possible to crack insufficient WPA2 passwords in a matter of hours [8].

The most recent critical vulnerability in WPA2 was unveiled in 2017 when Vanhoef and Piessens released their work on the Key Reinstallation Attack KRACK [9]. The attack forces a WPA2 protected device to reinstall an already used encryption key, making it possible for an attacker to decrypt and forge traffic between two devices without knowledge about the used encryption key. The latest bug in the WPA2 protocol's implementation was uncovered in early 2020 by the Slovakian security company ESET [10]. Researchers at ESET discovered that WLAN chips from certain manufacturers used encryption keys comprised out of zeros when encrypting the WLAN protocol frames left in the chip's transmit buffer after the clients had disassociated. A malicious actor could exploit this bug by forcefully disassociating clients repeatedly from the network and collect the protocol frames with weak encryption, possibly revealing sensitive information. Fortunately, the bug could be fixed by software updates from the device manufacturers.

In 2018 the WLAN device manufacturer advocacy group, the Wi-Fi Alliance, announced that the third generation of the WPA protocol would be replacing the now weakened WPA2 [11]. The first Wi-Fi Alliance certified WPA3 capable devices would reach the consumer market in late 2019. It has been announced that every device certified by the Wi-Fi Alliance after July 2020 must support the new encryption protocol [12].

Although many of the advancements made in the WPA3 protocol have been specifically targeted toward fixing the shortcomings of WPA2, recent research has shown weaknesses in the new protocol. In their work Vanhoef and Ronen [13] found multiple vulnerabilities in the early implementations of WPA3. The presented vulnerabilities make it possible, for example, to conduct brute-force dictionary attacks to recover the pre-shared network password and perform Denial of Service (DoS) attacks against WPA3 capable devices. However, it should be stated that many of the presented attacks are trivial and some could be again fixed with software updates.

2.2. Related literature

Much of the high-profile research done in the field of WLAN security has been concentrated toward the integrity of the encryption protocols used to secure wireless communication. This is, of course, understandable as the encryption protocols are perceived as the mainline of defence in WLAN communication. The problem of solely concentrating on the encryption protocols is that they are of little use if other security measures and protocols are neglected. This emphasis toward the encryption protocols has left a gaping hole in the field of WLAN security.

The rapid increase in the number of WLAN devices has highlighted some fundamental problems in the current state of WLAN security. The growing demand for affordable WLAN capable gadgets has brought forth devices lacking in proper up-to-date security protocols and features. The increase in the number of devices will also increase the likelihood of human error amongst the end-users. Even if the devices do have up-to-date security features, the chances are that average consumers lack the knowledge on how to secure devices, for example, by changing the factory-set default passwords.

These problems were highlighted during the 2016 Mirai malware epidemic [5] and more recently by Kumar et al. [3] and by Weidenbach and Dorp [14]. Kumar et al. used data collected from 15.5 million wireless home networks scanned with a free security tool provided by the security company Avast. The research data shows that out of the scanned WLAN capable IoT devices, 7.1% and out of home routers 14.6%, supported old FTP and Telnet protocols. 17.4% of these devices used well-known pre-set or otherwise weak FTP passwords and 2.1% had weak Telnet passwords. Similar problems in consumer routers were found by Weidenbach and Dorp who tested the firmware of 127 consumer routers from different manufacturers [14]. They note that 46 out of the 127 routers had not received any security updates within the last year, and even if they had been updated, many known vulnerabilities had not been fixed by the updates. In addition, 50 of the tested routers had hard-coded credentials and 16 used well-known weak credentials. Both Kumar and Weidenbach describe many of the same weaknesses Mirai had previously targeted in 2016.

As the number of WLAN capable IoT and smart devices grows, a significant increase in the number of attacks against IoT devices is to be expected. Signs about the increasing attacks against IoT have already been reported by the security companies F-Secure and Kaspersky. In their 2019 report, Kaspersky shows a 775% increase in the number of attacks against their decoy IoT services from 2018 to 2019 [15]. Similarly, F-Secure reports a 25% increase in attacks against their IoT decoys over the same period [16]. As IoT is gradually turning the surrounding environment into modern smart homes, cities and factories powered by small wirelessly connected devices and sensors, more cyber-attacks will be directed toward the surrounding smart infrastructure [17,18]. To effectively prevent such attacks from happening through WLAN capable IoT devices, it is crucial to devote more research on surveying the changes in the WLAN landscape.

One of the earliest WLAN survey studies was conducted in the early 2000s by Peter Shipley who presented the results of his 18-month long WLAN survey during the 2001 Def Con hacker conference [6]. In 2003 WLAN networks were surveyed in Australia by Webb [19] and Yek [20] and by Lin, Sathu and Joyce [21] in New Zealand. The results of these early surveys suggest that the use of encryption protocols was not yet self-evident among the common users. The results presented by Lin et al. show that only 40% of the surveyed WLAN networks had encryption enabled. In their work, both Webb and Yek showed that as the number of detected WLAN networks increased over time, the proportion of encrypted networks declined. These early results could be attributed to users' unfamiliarity with WLAN technology due to its novelty in the early 2000's consumer market. It should be recalled that the IEEE 802.11 WLAN standard had been ratified only a few years earlier in 1997 and that Apple had become the first manufacturer to offer built-in WLAN support for laptop computers in 1999 [22].

Results from more recent WLAN survey studies show positive development in WLAN security. Sarkar and Abdullah [23] study the evolvement of WLAN abundance and security in Auckland, New Zealand, based on surveys conducted in 2003, 2007 and 2010. Their results show a 406% overall growth in WLAN deployment from 2003 to 2010. Moreover, they show a 48% increase in encryption protocol use since 2003, with 88% of all detected networks in 2010 utilising some form of encryption.

Sarrafzadeh and Sathu [24] conducted their 2015 WLAN survey in the same area of Auckland as Sarkar and Abdullah. They report an overall 1600% increase in WLAN deployment from 236 to 4077 individual networks. Their results show that encryption protocol deployment has risen to 100% in 2015 from 40% in 2003. 71% of the surveyed networks used the strong WPA2 encryption.

Nisbet shows similar development in WLAN abundance and security in New Zealand [25,26]. He analysed the evolvement of WLAN security in four different locations within New Zealand based on surveys conducted in 2004, 2011 and 2013. Nisbet findings show that in one of the surveyed areas, WLAN deployment increased by 2600% from 2004 to 2011. In another surveyed area, WLAN deployment increased by over 700% during the same period. Encryption protocol use in 2013 varied from 77% to over 97% between the surveyed locations.

In Europe, the most recent WLAN survey studies have been conducted in the Balkan region. Dobrilovic et al. [27] compared differences in WLAN abundance and security between the cities of Budapest, Hungary and Belgrade, Serbia. In both cities, nearly 90% of the surveyed networks utilise some form of WPA encryption, leaving the number of unencrypted networks to under 10% and the number of networks utilising the weak WEP encryption to under 2%. Similar results are presented by Leca [28] and Valchanov, Edikyan and Aleksieva [29]. In his work, Leca collected data from a total of 100,000 wireless networks in various regions of Romania. From the 100,000 networks, 86% were WPA2 encrypted, 5% used WPA-TKIP encryption, 3% were WEP encrypted, leaving the remaining 6% unencrypted. Valchanov et al. surveyed over 11,000 WLAN networks in Varna, Bulgaria, showing almost identical numbers in encryption use as Leca.

While WLAN survey studies have been conducted since the early 2000s, no comprehensive methodology for WLAN survey and analysis has been defined in the related literature. None of the previously mentioned, nor any of the other related articles reviewed for this paper, offer a complete WLAN survey methodology. Although the survey and analysis processes are often presented, they are only superficially described. For instance, in their work Sajat, Hassan and Chit [30] do provide a cursory description of their WLAN survey process, but do not describe the data analysis process. Priya, Umar and Sirisha [31] thoroughly describe the hardware needed for wardriving, but do not present the WLAN survey process. Similarly, Eldaw, Akram and Sennan [32] and Kyaw, Tian and Cusak [33] describe small mobile wireless network scanners based on the Raspberry Pi single-board computer, but no description of the survey process is provided.

The vulnerabilities and potential future threats presented in this section have significantly increased the importance of raising awareness about WLAN security. Although encryption protocol use has considerably improved over the years, WLAN networking is currently facing similar challenges as in the early 2000s. Large numbers of potentially vulnerable new WLAN devices are connected into WLAN networks by users lacking in the technical knowledge on how to secure their new devices. Because of these challenges and possible future threats facing WLAN networking, it is increasingly important to closely follow the changes in the WLAN landscape.

To our knowledge, previous work on the topic has not documented a systematic and comprehensive methodology for obtaining reproducible results to the extent made possible by the work presented in this paper. The methodology presented in this paper can be used to effectively collect and analyse WLAN survey data with freely available software and common off-the-shelf hardware. By collecting and analysing WLAN survey data, it is possible to acquire high-value information about the evolvement of WLAN abundance, security, and usage as well as the adoption of IoT devices and technologies. This information can then be turned into concrete propositions and guidelines on how to increase the security of WLAN networking in the changing environment and to predict the future direction of WLAN security.

3. Related hardware and software

3.1. Hardware

Very basic WLAN surveys can be undertaken with minimal and simple everyday hardware. One of the easiest ways for anyone to try wardriving is to use a smartphone or tablet computer coupled with a freely available application such as WiGLE Wi-Fi [34]. Smartphones with their built-in WLAN and Global Positioning System (GPS) capabilities make them a good starting point for anyone wanting to test wardriving without having to purchase new equipment. The downside of using smart devices for the wardriving process is that their built-in mobile WNICs are not as powerful as those designed for computers. This will negatively impact the results as the less powerful mobile WLAN interfaces have a more limited range compared to external WNICs designed for computers.

The typical hardware setup for surveying WLAN networks is the combination of a laptop computer coupled with a USB powered WNIC and GPS receiver. A more compact alternative for a laptop computer is to use a small single-board computer such as the Raspberry Pi as presented in [32,33]. While single board computers are more compact in size, their lacking computing power, input devices and adequate displays make them somewhat impractical for wardriving. They are better suited to be used as stand-alone devices for distributed WLAN detection and wireless intrusion detection.

When choosing a WNIC for wardriving, a few factors should be taken into consideration. The chosen WNIC should have an external high-gain antenna and dual-band capabilities. These features provide the wardriver with a longer range and the ability to survey devices operating in both 2.4 GHz and 5 GHz wireless bands. Another option is to have two separate WNICs, each dedicated to separate bands. Moreover, when choosing the WNIC, it is recommended to consult the WNIC manufacturer website to ensure that device drivers for Linux operating systems are provided and that the device driver allows the WNIC to be set into monitor mode. Lists of Linux compatible WNIC chipsets can be found in [35,36].

As for the GPS receiver, there are two options. The most straightforward option is to acquire a USB powered GPS receiver. Again, it is important to ensure that the device manufacturer provides device drivers for Linux operating systems. The second option is to use an Android smartphone as the GPS receiver. Using an Android smartphone as the GPS receiver calls for a few extra steps and prior experience with Linux operating systems. The process involves installing an application to the smartphone for sharing the GPS data with the chosen Linux operating system, enabling the developer options on the smartphone, and installing Android Debug Bridge (ADB) tools to the operating system. The smartphone can then be used to share GPS data via a USB connection. It should be stated that the GPS receiver is used only for the purpose of collecting location data and is not therefore mandatory for collecting WLAN data.

3.2. Software

Different Linux operating systems are commonly preferred for scanning wireless networks. Linux based operating systems are generally better suited for WLAN network scanning as they provide better support for setting WNICs into monitor mode, allowing passive WLAN scanning. For this reason, many of the most prominent wireless network scanning software have been designed for Linux operating systems. While it is possible to use the Microsoft Windows operating system for surveying WLAN networks, many of the software designed for Windows are either outdated or commercial and can only be used for active scanning as Windows lacks native support for setting WLAN interfaces into monitor mode.

One of the most commonly used Linux distributions used for wardriving is the Kali Linux distribution. Developed and maintained by the Offensive Security group, the Debian based Linux distribution is aimed toward security professionals to be used for penetration testing and security auditing [35,37]. Furthermore, Kali Linux has many of the tools needed for wardriving pre-installed, is well documented, and has good built-in support for many off-the-shelf WNICs [37]. For the more experienced user, almost any Linux distribution could be chosen.

It is also a common practice to run the chosen Linux operating system as a virtualised guest operating system on top of the host operating system. By using a virtual machine, it is possible to eliminate the need for installing a new operating system over the current operating system. Using a virtual machine also has many other benefits over installing a completely new operating system. For instance, virtual machines further increase the support for various device drivers and offer the possibility to save the virtual machine's state into snapshots. Snapshots make experimenting with the operating system easier for new users and make backing up the virtual machine easier.

Offensive Security also offers Kali Linux as ready to deploy virtual machine images. These images can be downloaded and deployed as is without the need for having any prior knowledge on how to create virtual machines or how to install a new operating system. Many of the hypervisor software needed to run virtual machines such as VMware Workstation Player and Oracle VirtualBox are freely available and can be used free of charge. It is also possible to run Kali Linux on top of Windows 10 operating system with the new Windows Subsystem for Linux (WSL) technology, but we would recommend this only for the more experienced users. Moreover, at present, WSL does not allow connecting USB devices to the guest operating system.

3.2.1. WLAN survey software

A plethora of different software for inspecting WLAN networks have been produced over the years for different operating systems, each having different purposes and features. One of the first freely available WLAN scanning software published for Windows operating systems was the Netstumbler software [6]. Two of the more recent WLAN scanning software developed for Windows operating systems are the updated version of Netstumbler dubbed as Vistumbler [38] and Acrylic Wi-Fi Home by Tarlogic Research [39]. The downside of using Windows-based software is that they are often outdated, commercial and only support active WLAN scanning [35]. Different versions of Netstumbler have also been released for the Apple OS X operating system under the names MacStumbler and iStumbler.

As already mentioned, the most prominent wireless network scanning software have been developed for Linux operating systems. One of the most preferred software for wardriving with Linux operating systems is the Kismet framework [40]. Kismet is an open-source wireless network detector and Intrusion Detection System (IDS) for Linux and Apple OS X operating systems. It is a versatile software with a simple user interface, built-in GPS support and can be configured to use multiple WNICs simultaneously [35]. It also has an active user base, good documentation and is frequently updated. Moreover, the software comes pre-installed with Kali Linux so new users unfamiliar with Linux operating systems do not have to install the software separately. The framework is comprised of two separate components, the Kismet client operated by the user, and the Kismet server which performs most of the work in the background [38]. When the user first starts Kismet, both the client and server components are launched. The user will then interact with the server through the client's user interface during the network scanning process.

3.2.2. GPS software

Another aspect of wardriving is charting the locations of the found WLAN networks. To be able to pinpoint the device locations, a GPS receiver must be used alongside the WNIC and survey software. When using Linux operating systems, the Global Positioning System Daemon (GPSD) is often used for processing GPS location data [41]. GPSD is a widely used Linux daemon that allows the use of GPS in various Unix based operating systems [6]. After a GPS receiver has been successfully configured and connected to the host system, GPSD processes the incoming data from the GPS receiver and makes it available at TCP port 2947 [38]. The GPS data can then be queried by the chosen WLAN survey software and tagged with the found WLAN devices.

If a smartphone is used as the GPS receiver, a separate application must be installed to transfer GPS data from the smartphone to the GPSD application. One example of such an application is Share GPS [42]. The application is available free of charge in the Google Play store. The application allows the GPS data to be transferred either via Bluetooth or USB connection. In the case of wardriving, we recommend using a USB connection as Bluetooth and WLAN operate on the same 2.4 GHz band, and using them closely together might cause interference during the survey process. Moreover, as already mentioned in Section 3.1, using a smartphone as a GPS receiver also requires enabling the developer options on the smartphone and installing the Android Debug Bridge tools to the operating system.

3.2.3. Data sampling and analysis software

Before the results of the WLAN survey can be analysed, the collected data must be processed into a more readable form. This process can be done in various ways depending on the used survey software. For instance, the WiGLE application does the sampling automatically on behalf of the user. If Kismet is used as the WLAN scanning software, the survey data must be extracted from the log files created by the software. By default, Kismet creates five different log files: .alert, .gpsxml, .nettxt, .netxml and .pcap files. The latest versions of Kismet combine these files into a single .kismet file by default.

Fig. 1. Surveyed WLAN network locations visualised on Google Earth.

The more experienced users often create their own applications for extracting data from the Kismet log files, but for the less experienced users, it is recommended to use pre-existing applications such as GISKismet [43]. The applications come pre-installed with Kali Linux and can be used to automatically parse data from the .netxml and .kimset log files into SQLite databases. Saving the collected data into SQLite databases makes it possible to pull wanted information from the database with simple SQL queries.

The SQLite database created by GISKismet contains two tables, one listing all the surveyed WLAN networks and another listing all the client devices connected to the networks. The table containing the scanned networks lists the following information: network SSID, MAC address, device manufacturer, used channel, SSID cloaking, used encryption, first and last time network was seen and variable GPS data.

Data in the database can be browsed and extracted either by using GISKismet, the sqlite3 command-line application or by using a more user-friendly software with a graphical user interface. An example of such software is the DB Browser for SQLite which can be downloaded free of charge for Windows, Linux and Apple operating systems [44]. The software allows users with no prior experience with databases to browse and extract data from SQLite databases. The wanted data from the database can be parsed into .csv files for further inspection and analysis. If GPS data was collected during the survey, GISKismet can be used to parse the locations of the found networks into .kml files which can then be opened in Google Maps or Google Earth software as seen in Fig. 1.

4. Legality and ethics of wardriving

Despite its intimidating name, wardriving is not by any means hacking, criminal or in any way harmful towards the surveyed wireless network devices, nor to the device owners. The name originates from the term *wardialing* inspired by the 1983 movie Wargames, in which the main character is seen using a computer to dial consecutive phone numbers to locate computers with networking capabilities [6]. In the early days of modern computer networking, devices communicated by modems connected to the landline phone network. This meant that it was possible to locate computers with modems attached to them simply by dialling consecutive numbers and waiting for a modem to answer.

Wardriving is based on the same concept as wardialing but updated to wireless networking and greater efficiency. Today wardriving has also been extended to other wireless communication technologies such as Bluetooth and ZigBee used by IoT and smart devices. In simple terms, wardriving is the act of charting wireless networks and network devices within a predetermined area. The gained results are often saved into databases to be further refined into statistics and maps visualising the locations of the surveyed devices.

Wireless network scanning can be done by using either active or passive methods, depending on the used tools and the purpose of the survey. The difference between the two methods is that with active scanning, the wireless network scanner must communicate with the scanned devices. This can be done for example by actively sending out probe request frames and then collecting the corresponding probe response frames sent by the surrounding WLAN devices. It is similar to the wardialing process in which the devices could be charted based on the responding phone numbers.

With passive scanning, the network scanner is listening for the wireless networking management frames broadcasted by the surrounding WLAN devices at regular intervals. WLAN capable devices broadcast various types of management frames such as beacon and probe request frames by default to announce their existence to other surrounding WLAN devices. These frames are, for the most part, sent unencrypted and can carry various information such as the wireless network identifier SSID, used encryption, used wireless channel, device MAC address and device manufacturer information.

When using passive wireless network scanning methods, the wardriver sets the Wireless Network Interface Controller (WNIC) into monitor mode and scans the whole WLAN wireless spectrum by hopping from channel to channel collecting data from the management frames broadcasted by the surrounding WLAN devices. This makes it possible for the wardriver to collect WLAN data without having to communicate with the scanned devices. The process could be compared to searching for the right channel on an FM radio. The WLAN survey methodology presented in this paper is based on the principles of passive wireless network scanning.

Maybe because of its misleading name, wardriving can easily be misinterpreted as something criminal and malign, namely hacking. To the contrary, wardriving is a well-recognised legitimate tool widely used by information security professionals, experts and hobbyist alike. The act of wardriving can potentially become illegal if it was to be used as a means for breaching the security of a wireless network. In practice this could mean surveying vulnerable WLAN networks with the sole intent of gaining unauthorised access to the network. Because of the misconceptions and potential of wardriving being used for nefarious intents, it is important to recognise the legal and regulatory constraints of wardriving.

The Finnish law's stance on the legality of wardriving is straightforward. According to the Finnish criminal law, it is perfectly legal for one to use any unsecured open WLAN network. This means that one can use any open WLAN network for activities like web surfing, video streaming and online gaming [45]. The use of an open WLAN network becomes criminal if the connection is used for accessing other devices or services residing on the network without the network owner's permission [46]. It is not therefore lawful, for instance, to log in to the wireless access point's web interface and make changes to the network settings or browse files on another device connected to the network. As connecting into an unknown secured WLAN network would require breaching the wireless network's security in one way or the other, these kinds of actions are naturally unlawful in the eyes of the Finnish criminal law.

In the United States, the laws considering wireless networks scanning are much more ambiguous, but ultimately take same position as the Finnish legislation. According to the Federal Bureau of Investigation (FBI), it is not illegal to scan wireless networks [6]. However if a theft of service, denial of service (DoS), or theft of information occurs as part of the scanning process, it becomes a federal crime through 18USC 1030 [6]. The Finnish and the U.S legislation differ in the case of connecting to a unsecured open WLAN network. There is no uniform federal law that explicitly allows or prohibits connecting on to or using an open WLAN network, but there seems to be some ambiguity on defining authorised and unauthorised access in the case of an open WLAN network [47,48]. Breaching the security of a wireless network is of course a criminal act according to the U.S legislation.

As we cannot present concrete up-to-date information about the differences in legislation between all possible countries, we would highly suggest the reader to refer to the local laws and regulations before surveying wireless networks. As a general rule of thumb, it can be said that passive wireless network scanning is legal as it is an integral part of WLAN networking and does not require any interaction with the scanned network.

4.1. The EU general data protection regulation

In addition to the local Finnish legislation, as a member of the European Union (EU), the possible regulations set by the EU must also be taken into consideration. The EU General Data Protection Regulation (GDPR) came into effect on May 25th of 2018 and is a set of rules and regulations set to control how different entities can collect and use one's personal information and data [49]. The regulation aims to give citizens more rights and power over their personal data and force transparency on how personal data is processed for example by governments and large online businesses such as Google or Facebook.

The GDPR documentation has very profound descriptions about the regulations considering the use and processing of personal data. Fully describing the GDPR documentation in detail would be out of the scope of this paper, so we are not going to provide an in-depth analysis of the documentation. Instead, the emphasis of the discussion will be on those portions of the documentation that affect collecting, processing and storing WLAN data. For a more detailed description of the regulation, we refer the reader to the GDPR documentation [49].

In the case of collecting and storing WLAN data in the context of scientific research, the first things to consider are the definition of personal data and how collecting and storing such data is regulated according to the GDPR. The documentation defines personal data as *"any information relating to an identified or identifiable natural person"* [49]. Furthermore, a natural person has been defined as someone who can be directly or indirectly identified by reference to an identifier such as a name, an identification number, location data or an online identifier [49]. In short, personal data is information related to an individual that can be used to either directly or indirectly identify an individual person.

As the proposed WLAN survey process can be used for collecting data which may constitute as *online identifiers*, namely device MAC addresses, network SSIDs and location data, the definition of online identifiers must be further explored. Recital 30 of the documentation identifies online identifiers as information provided by devices, applications, tools and protocols [49]. In practice, such information could include internet protocol (IP) addresses, MAC addresses, browser cookies and social media handles.

Based on these observations, it can be stated that MAC addresses, SSIDs and location data collected during WLAN surveys should be thought of as personal data. They can be seen as information that could either independently or in combination with other information, directly or indirectly, be used to identify the device owner. However, for instance, in the case of WLAN access points, there usually are several devices connected to a single AP, making it impractical to identify the true device owner. There are of course exceptions such as laptop computers, smartphones and IoT devices, but even in these cases, it is highly unlikely that the device owner could be identified solely based on the devices MAC address, network SSID and location data.

This is because even though the device MAC addresses are unique to a device, no one can ever truly tell the owner of the device since they are not connected to a person's name. Nor are there any databases which connect any other personal information to a specific device MAC address. Even by combining the device MAC address, SSID and location data, the probability that the information could be used to identify a single person is low. The scanned device's location data is only a rough estimate based on the device's signal strength and the network scanner's location. Moreover, many factors affect the signal strength and as wardriving is often conducted with a moving car, making accurate estimations about the devices true location based on the calculated location data is in most cases very implausible.

Nonetheless, because parts of the collected WLAN data are deemed personal according to the regulation, it must be ensured that the data is processed and stored in compliance with the GDPR. The regulation does give some specific guidelines and freedoms when personal data is processed and stored in the context of scientific research. In section *b* of *Article 5*, it is stated that personal data shall be collected for specified, explicit and legitimate purposes and can be further processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes [49]. Section *e* further permits storing personal data for scientific, historical and statistical purposes, in so far as it is done in accordance with the required appropriate technical and organisational measures [49]. Section *f* obligates that personal data shall be processed in a manner that ensures appropriate security and protection against unauthorised or unlawful processing and accidental loss [49].

Article 6 presents additional conditions based on which processing personal data shall be lawful. Sections *e* and *f* of *Article 6* state that processing personal data is lawful when it is done in the public interest, in the exercise of official authority or when it is necessary for the purposes of legitimate interests pursued by the controller [49]. *The controller*, as defined in the regulation, can be interpreted as a public authority, company, agency or legal person.

In conclusion, it can be stated that it is lawful (for a university) to collect and store WLAN data for the purposes of scientific research conducted in the greater public interest, given that appropriate confidentiality and integrity has been provided for the collected data at all stages. The data must be secured and stored in a manner that protects it from any unauthorised altering, loss or destruction.

4.2. The ethics of wardriving

In the realm of information security, it is a well-known fact that in order to stay on top of their craft, information security professionals must master many of the same tools and techniques as their malicious counterparts. Security professionals are often hired by companies to run security audits and penetration tests on their information systems with the intent of finding and fixing possible vulnerabilities before malicious hackers can exploit them. As wardriving is a tool used by hackers and security professionals alike, it is important to examine its ethical and moral boundaries.

Extensive literature does exist on the topics of computer ethics, ethics of technology and ethics of information security, but very little has been written about the ethics of wardriving. The ethics of wardriving is at present a novel topic which would require a more in-depth conversation than can be offered in the confines of this paper for it to be examined in its full extent. Although offering an exhaustive examination about the ethics of wardriving is out of the scope of this paper, a brief commentary should nonetheless be offered.

To avoid a lengthy philosophical discussion of the ethics and morality of wardriving, the best course of action is to look at the subject from the stance of one specific ethical theory. For the purposes of this paper, classical consequentialist utilitarianism is a fitting choice as it is a well-known and explicit ethical theory. Utilitarianism tries to sort out the morally right actions by looking at the outcomes and consequences of one's actions [50]. The classical utilitarian way of thinking is centred on the *greatest happiness principle* [51]. The principle holds that the morality of an action is measured by the amount of happiness or "utility" the act produces for the greater community when compared with other possible actions that could be taken in the same situation. Therefore, we must first contemplate the possible consequences the act of wardriving might produce.

As acknowledged previously, wardriving in itself is a seemingly harmless act. It does not cause any disruption or harm to the surveyed wireless networks, network devices or device owners. In fact, the device owner and network users do not even know that their wireless network or network devices are being surveyed. The fact that the device owners do not know that their devices are being surveyed does raise questions about the device owners' consent on being scanned. Moreover, the device owners could see wardriving as an invasion of their privacy as the collected data can include personal information that could potentially be used to identify the device owner as discussed in Section 4.1. The issue of consent and privacy is quite problematic since it is not plausible to ask every device owner's consent on scanning their devices. Furthermore, it is impossible to know beforehand how many or whose devices reside in a specific area and which of those devices will be within the wardriver's range. Under these circumstances asking for consent would be an impossible task and would defer everyone from surveying wireless networks.

Deferring everyone from ever surveying wireless networks would mean that no one would have their insecure wireless network breached and have their privacy invaded. On the other hand, this would also defer security professionals and researchers from using wardriving in their work, hindering their ability to study and improve WLAN security on a larger scale. This kind of situation would surely cause much more distress than utility for every involved party. By conducting WLAN surveys according to laws and regulations and within reason, it is possible to serve a greater good by bringing up the possible issues and raising awareness about the state of WLAN security for the greater community.

It can be reasoned that when used as a tool in the context of information security work and legitimate research, wardriving will bring up more utility than harm to the greater community, making it an ethically and morally right act according to classical utilitarianism and the greatest happiness principle. The situation would be different if one would be acting solely for the sake of wardriving and going out of their way deliberately releasing private information to the public or handing out information about possibly vulnerable networks for malicious actors. Under these circumstances, the act of wardriving would be causing more harm than utility and would therefore be immoral in the eyes of utilitarianism.

5. WLAN survey methodology

As discussed in Section 2, the need for developing a systematic methodology for collecting and analysing WLAN data stems from the current changes in the WLAN networking landscape. The current surge of WLAN capable IoT devices and the shift to a newer encryption protocol have increased the necessity to study the current state and future directions of WLAN security. WLAN technology is at a watershed moment where masses of new devices are being introduced into WLAN networks, significantly increasing reliance on the security of these potentially insecure new devices. To stay on top and react to these changing circumstances accordingly, it is crucial to find new ways to study and raise awareness about WLAN security.

In this section, we will present the proposed systematic methodology for surveying and analysing WLAN abundance and security. The proposed WLAN survey methodology contains two components, the survey system and the survey process. The survey system contains the

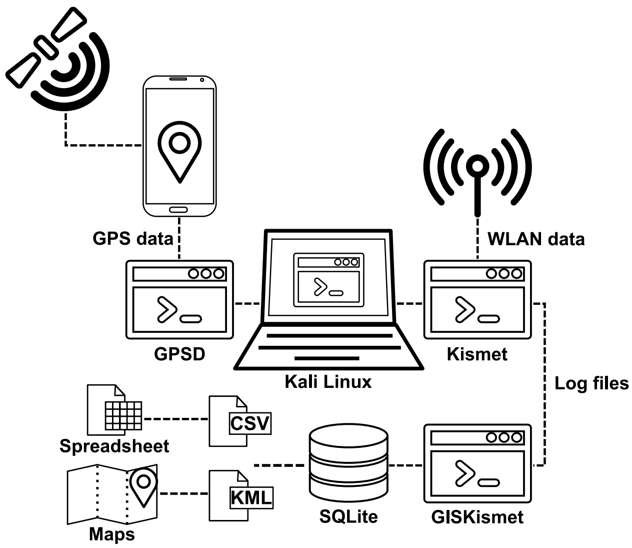

Fig. 2. Proposed WLAN survey system.

hardware and software needed for successfully carrying out WLAN surveys. The proposed WLAN survey process has been divided into three stages: the planning and preparation, data collection and data analysis stages. The premise has been to develop an effective, scalable, and accessible process for continuous mobile WLAN survey and analysis. To achieve these set objectives, the proposed survey system has been formed around open-source Linux operating system, freely available software, and common off-the-shelf hardware, while the survey process has been based on the principles of passive WLAN scanning and wardriving.

5.1. WLAN survey system

The proposed WLAN survey system (Fig. 2) consists of a laptop computer, a dual-band WNIC and a GPS receiver. While basic WLAN surveys could be conducted by using a mobile device as discussed in Section 3.1, a laptop computer was chosen as it has many benefits over a simple mobile device. The main benefit of using a laptop computer for WLAN surveys is the possibility to experiment with different kinds of WNICs and antennas. For the survey system to have the longest possible range, it is beneficial to use a more powerful WNIC with an external antenna over a less powerful mobile WNIC. To be able to map the locations of the detected WLAN networks, a GPS receiver is incorporated as part of the survey system. As we did not have a USB powered GPS receiver at hand while constructing the survey system, an Android smartphone is used as the GPS receiver. To share the GPS location data from the smartphone to the operating system, we have used the ShareGPS application described in Section 3.2.2.

As the WLAN survey platform, Kali Linux is deployed as a virtualised guest host on top of the laptop's Windows 10 operating system. While it would have been possible to use Windows 10 as the WLAN survey platform, we chose to use a Linux operating system as we want to be able to set our WNIC into monitor mode for passive WLAN scanning, which is not natively supported by Windows operating systems. Other common Linux operating systems such as Ubuntu and Parrot OS were also considered to be used as the WLAN survey platform. After experimenting with the different operating systems, Kali Linux was ultimately chosen as most of the needed software comes pre-installed with the operating system, making setting up the survey system simple and user friendly.

By deploying Kali Linux as a virtual guest operating system, it is possible to cut many corners in the process of choosing and installing the needed operating system and software. The main benefit of using virtual machines is that it eliminates the need to replace the current operating system. By using the ready to deploy virtual machine images provided by the Offensive Security group, Kali Linux can be deployed with very little preliminary knowledge about virtual machines. The virtualised guest hosts can also be easily backed up or copied on to a new host system. As the hypervisor software, we have used the VMware Workstation Player version 16. Oracle's VirtualBox hypervisor was also considered, but the software was found to be very unstable. The software also had compatibility issues with some of the tested WNICs.

For the WLAN scanning software, we chose to use the Kismet framework coupled with the GPSD daemon for processing GPS data. Other WLAN scanning and analysis software such as Acrylic Wi-Fi Home, NetStumbler and Vistumbler for Windows and Airodump-ng for Linux were also considered and tested while constructing the survey system. After experimenting with the different software, Kismet was chosen for its versatility, ease of use, good documentation and its native support for passive WLAN scanning and collecting GPS data. The software also comes pre-installed as part of the Kali Linux software library. None of the mentioned Windows software support passive WLAN scanning, and the log files created by Netstumber and Acrylic Wi-Fi Home were lacking for conducting proper WLAN surveys. We also found Netstumbler to be very much outdated. Airodump-ng is very similar to Kismet and shares many of the same features, including support for passive WLAN scanning and GPS, but its user interface makes it unpractical to be used for wardriving purposes.

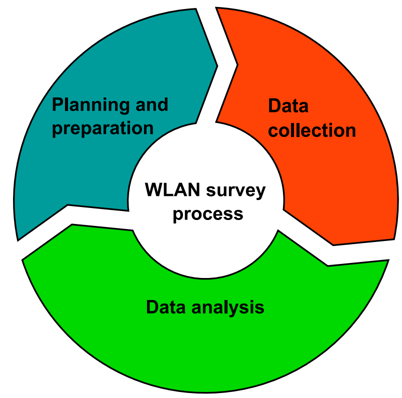

Fig. 3. WLAN survey process.

5.2. WLAN survey process

The proposed WLAN survey process can be divided into three stages: planning and preparation, data collection and data analysis (Fig. 3). The planning and preparation stage includes verifying the lawfulness of collecting WLAN data, defining the survey scope, acquiring, and preparing the needed hardware and software. Because laws and regulations can vary between countries, the lawfulness of wardriving should be ensured as discussed in Section 4. Next, the scope of the WLAN survey should be defined. The survey location, mode of transportation and the hardware and software should be chosen according to the survey's purpose. If the purpose is simply to test out wardriving, then using a smartphone and walking around any populated area can suffice. If the aim is to collect accurate data from a wider area, then a faster mode of transportation and more advanced hardware are needed. A good method for scouting suitable areas and planning routes for wardriving is to consult satellite map images as those often have accurate depictions of buildings and road networks.

After determining the survey purpose and scope, the needed software and hardware must be prepared. The hardware should be chosen according to the survey scope as having the right hardware can have a significant impact on the survey results. If, for example, the aim is only to collect data from WLAN devices operating on the 2.4 GHz band, and not to visualise the found networks on to a map, then almost any WNIC will suffice, and no GPS receiver is needed. If, on the other hand, the aim is to gain as much WLAN data as possible from the surveyed area, and chart the found networks, then a dual-band high-gain antenna and GPS receiver are needed. However, it could be argued that using a high-gain antenna around tall apartment buildings is not beneficial as those often have a wider horizontal range instead of a taller vertical range. At this stage, it is also important to make sure that the hardware supports Linux operating systems and can be set into monitor mode. Carefully refining the entire process at this stage makes it effective, scalable, and accessible for future surveys.

After the preliminary planning has been completed and all the needed hardware and software have been acquired and set up, the data collection stage can begin. As already stated, the surveys can be conducted with varying software and modes of transportation, depending on the wanted results and scope of the survey. Depending on the survey environment and mode of transportation, some factors should be taken into consideration. When surveying a densely populated city environment, it should be remembered that the collected data is propagated in radio waves which can be obstructed by buildings and other natural obstacles. Therefore, it is recommended to plan the survey routes in a manner that allows a thorough systematic survey of the area. When moving by car, it is important not to use excessive speed as it will decrease the quality and accuracy of the collected data. We would recommend using speeds under 60 km/h and surveying the chosen area multiple times consecutively for the best results.

When the planned area has been thoroughly surveyed and enough data has been collected, the data must be further arranged before it can be analysed. The data sampling and analysis stage can be accomplished by various means depending on the sought information and results. When Kismet has been used as the primary survey software, data from the .netxml and .kismet log files can be imported into an SQLite database by using the GISKismet application. There are many similar open-source scripts and software available, but we are recommending GISKismet as it comes pre-installed in Kali Linux and offers other useful features than just simply importing data into an SQLite database. GISKismet also allows the user to pull the collected data from the database into a .csv file which can then be opened in spreadsheet software for further analysis. Moreover, the application can be used to convert the collected data into .kml file format for visualising the located networks in Google Maps or Google Earth. When the wanted data has been pulled from the database and converted into a more readable form, it can then be further studied and refined into statistics and graphs.

6. Survey methodology calibration and test survey results

After constructing the WLAN survey system and process, an initial test survey was conducted to see how the chosen software and hardware would fare in real-world scenarios and if they meet the requirements set for the survey methodology. It was also important to see if the results collected during the test survey would suffice in terms of the possible future WLAN survey studies. Based on the observations made during these initial tests, it was possible to calibrate the survey process and see if any piece of hardware or software needed to be replaced or upgraded. The test survey was conducted in three separate locations within a medium-sized city located in Southwest Finland. The chosen areas represent three typical locations for WLAN usage: the industrial district, the densely populated city centre, and the suburb. Each area was surveyed three consecutive times to ensure the best possible results.

To ensure that the survey methodology would coincide with the set requirements of efficiency and accessibility, no proprietary software or hardware were used. The test survey was conducted by using the common off-the-shelf hardware, open-source operating system, and freely available software as described Section 5.1. The used hardware consisted of a laptop computer along with the Asus N-13 dual-band USB WNIC and a Huawei Android smartphone used as a GPS receiver. Alongside the laptop survey setup, an Android tablet computer equipped with the WiGLE Wi-Fi wardriving application was used to compare the performance between the two setups.

The results gained during the test survey were promising. After sampling and analysing the collected WLAN data, it can be stated that the survey methodology performed as intended. Still, even though the test survey was successful, a few observations were made, leaving room for future improvements. Firstly, the WNIC used during the test survey did not have an external antenna, meaning we could only collect data on a limited range. For future surveys, it was decided that the WNIC would be upgraded to one with an external antenna. The current WNIC model we are using is the TP-Link AC600 Archer T2UH with the MediaTek MT7610U chipset.

Secondly, we did not have a separate GPS receiver at the time of the test survey and therefore opted to use a smartphone as a substitute. For this reason, we could not compare the two solutions during the test survey. After receiving a USB powered GPS receiver sometime after the first test run, it was noted that the smartphone application gave more accurate results than the USB GPS receiver. The GPS receiver model tested is the GlobalSat G-Start IV BU-353S4. It would seem that there is a trade-off between convenience and accuracy between the GPS receiver and the smartphone solution.

Some of the more minor observations made during the testing considered making small adjustments to the Kismet framework's configuration file and testing various scripts and software during the data sampling and analysis process. It was also noted that the location chosen to represent the suburb would not be sufficient for future studies due to poor traffic and road conditions in the area, which made it challenging to effectively survey the area. When comparing the results obtained with the laptop and tablet configurations, it was noted that the tablet lacked in effective scanning range. Additionally, the WiGLE Wi-Fi Wardriving application drained the device battery at a much faster rate compared to the laptop setup. Still, it should be said that using WiGLE streamlines the data sampling process when compared to Kismet. WiGLE automatically creates a database for the survey results and the data can be pulled from the database as .csv and .kml files with a push of a button.

6.1. Test survey results

After importing the gained survey data into SQLite databases and sorting the wanted information into spreadsheets, we concluded that we had collected data from 720 WLAN networks. From the collected data we can derive the network SSID's, the wireless access points MAC address, manufacturer, used channel, used encryption protocol, and the estimated location of the network. Based on the collected information, it is possible to make observations about the state of WLAN security in the surveyed area. This can be done, for example, by observing encryption protocol use and the prevalence of other security practices such as cloaking or altering the network SSID.

Devices from altogether 38 different manufacturers were located during the survey. Three of the most popular device manufacturers were Cisco 28.3%, Huawei 15.7% and Ruckus Networks 9.7% as seen in Fig. 4. Out of all the device manufacturers, devices from Inteno Broadband were the most poorly secured. From the 22 located Inteno Broadband devices, 21 used the outdated WPA-TKIP encryption.

Further inspection of encryption protocol deployment in the surveyed areas shows that from the 720 located networks, 92 (12.8%) were unencrypted, 7 (1%) used WEP encryption, 36 (5%) used WPA-TKIP encryption and a clear majority of 585 (81.3%) used some form

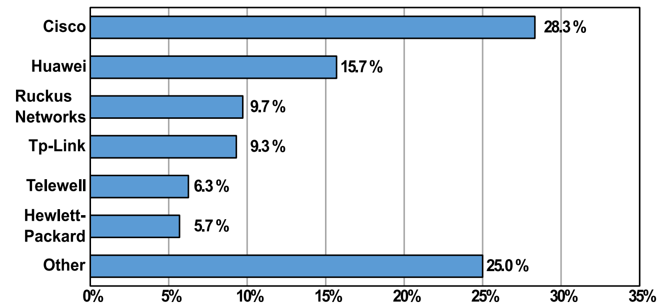

Fig. 4. Device manufacturer popularity in the surveyed areas.

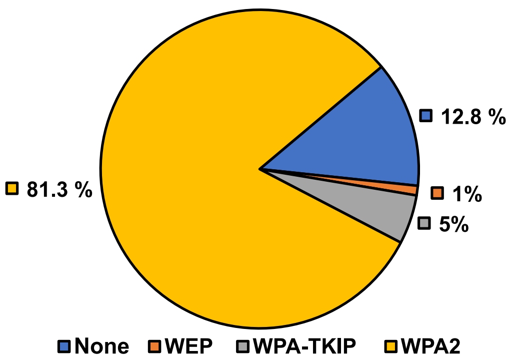

Fig. 5. Encryption deployment by percentage.

Table 1
Encryption protocol deployment in the three surveyed areas.

Encryption	None	WEP	WPA-TKIP	WPA2	All
Industrial district	13	5	9	118	145
City centre	49	2	8	313	372
Suburb	30	0	19	154	203
Sum	92	7	36	585	720

of WPA2 encryption, as seen in Fig. 5. From the 585 WPA2 enabled networks, 106 (18%) were configured to use the less secure WPA2/WPA-TKIP mixed mode. The relatively large number of open unencrypted networks can be partially explained by the open guest networks offered by various businesses, schools and administrative buildings residing in the surveyed areas. Table 1 presents encryption protocol deployment in the three surveyed areas.

Based on the survey results, it seems that altering the network SSID is a fairly uncommon practice in the surveyed area. Roughly 40% of the surveyed networks used factory-set easily identifiable SSIDs containing the device manufacturer name, device model or the internet service providers name coupled with a series of numbers and letters. Furthermore, only 5.4% of the located networks had a cloaked SSID.

A look into the wireless channel use unsurprisingly reveals that a clear majority of 80% of the surveyed networks operated on the 2.4 GHz band. Most of the networks operating on the 2.4 GHz band were configured to use the non-overlapping channels 1, 6 and 11 as seen in Fig. 6. Fig. 7 shows that on the 5 GHz band, most of the networks are configured to operate on channel 36. One noticeable finding is that two of the located devices operating on the 2.4 GHz are configured on channel 14, which is not allowed in Europe and is instead only allowed in Japan.

7. Conclusion and future work

In this paper, we have presented a systematic methodology for continuous surveying and analysis of WLAN abundance and security,

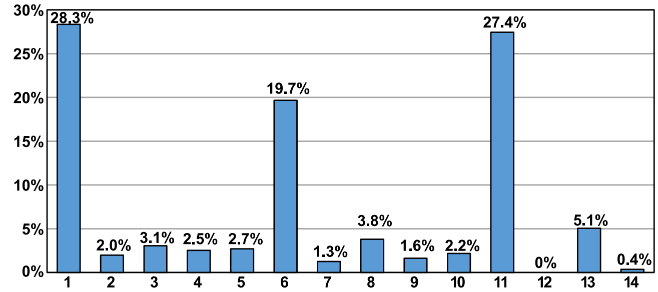

Fig. 6. Wireless channel popularity on the 2.4 GHz band.

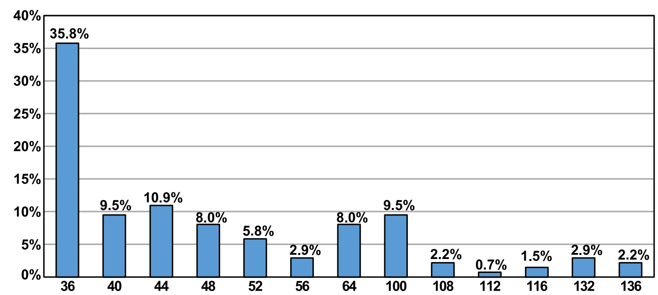

Fig. 7. Wireless channel popularity on the 5 GHz band.

based on the principles of passive WLAN scanning and wardriving. In addition, a specification for the hardware and software needed in the WLAN survey and analysis processes has also been given. The objective has been to develop an accessible, efficient and scalable methodology for collecting, analysing and storing WLAN survey data. To our knowledge, no similar comprehensive methodology for systematic WLAN surveying and analysis has been presented in previous works on the topic. By collecting and analysing WLAN survey data, it is possible to acquire high-value information about the evolvement of WLAN abundance, security, and usage. This information can then be used to construct concrete propositions and guidelines on how to increase the security of WLAN networking in the changing environment and to predict the future direction of WLAN security.

Moreover, we have presented the possible legal and ethical limitations of surveying WLAN networks. Although there are some legal and regulatory boundaries set for collecting WLAN data, according to the Finnish and U.S criminal laws and the EU general data protection regulation, it is indeed legal for one to passively survey and collect WLAN network data in the context of scientific research. Furthermore, although surveying WLAN networks does raise moral and ethical questions about the network device owners' consent and privacy, we concluded that collecting WLAN network data is morally right from the consequentialist utilitarian perspective. When done in the context of information security and scientific research, conducting WLAN surveys will undoubtedly generate more utility for the greater community than banning WLAN surveys would.

To prove the effectiveness of the proposed methodology, an initial WLAN survey was conducted. The survey was carried out in a typical middle-sized city located in Southwest Finland. During the test survey, three separate locations within the city were surveyed by using freely available open-source software and common off-the-shelf hardware. After the successful test survey and survey data analysis, it can be concluded that the proposed methodology met the set requirements and that the methodology can indeed be used to effectively collect and analyse WLAN survey data even with very basic hardware and freely available software.

Based on the survey results, WLAN security in Finland is in a relatively good state when considering encryption protocol use. From the collected survey data it could be concluded that the use of insecure encryption protocols is relatively low in the surveyed areas. From the 720 detected networks, 7 (1%) used WEP encryption, 36 (5%) used WPA-TKIP encryption, 92 (12.8%) were unencrypted, and a clear majority of 585 (81.3%) used some form of the more secure WPA2 encryption. Although the number of unencrypted networks is relatively high, it should be remembered that most of them are open guest networks offered by businesses, schools, and public administration. From the 38 device manufacturers identified during the survey, devices manufactured by Inteno Broadband had the most issues with insecure encryption protocol use.

A further look into the survey results shows that wireless network device owners in the surveyed areas are not inclined to alter the factory-set default settings of their wireless networks. It was noted that roughly 40% of the surveyed networks used easily identifiable factory-set SSIDs and only 5.4% of the networks had a cloaked SSID. Moreover, a clear majority of 80% of the surveyed networks operated on the more congested 2.4 GHz band and over 75% of the networks were configured to operate on channels 1, 6 and 11.

It is recommended to alter the wireless access points factory-set default settings including a default SSID, channel, and passwords. A known weak default password together with a pre-configured network SSID that reveals the device model and manufacturer can give an attacker all the needed information to launch an attack against the wireless network. While the benefits of altering the network SSID can be circumvented with wireless network scanners, these simple measures can help keep the casual eavesdroppers at bay and add an extra layer of privacy and security to the wireless network.

To carry out more comprehensive studies on the evolvement of the WLAN landscape, the presented methodology will be further developed and used for conducting continuous long-term WLAN network surveys. The used hardware will be further enhanced for increased survey result accuracy by experimenting with newer WNICs and different types of antennas. The data analysis process must also be improved as the amount of collected WLAN data will increase over time, calling for more effective data storing and sampling practices. In addition to conducting studies on the evolvement of the larger WLAN networking landscape, a more comprehensive study on the ethics of wardriving will be presented in the future.

CRediT authorship contribution statement

Saku Lindroos: Conducted the WLAN survey, Conducted the survey data analysis, Writing – original draft, Writing - review & editing. **Antti Hakkala:** Supervision, Writing - review & editing. **Seppo Virtanen:** Conducted the WLAN survey, Conceived and formulated the research problem and objectives, Supervision, Writing - review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Businesswire.com, Smart home will drive third wave in wireless home evolution strategy analytics, 2019, https://www.businesswire.com/news/home/20190807005530/en/Smart-Home-Drive-Wave-Wireless-Home-Evolution. (Accessed 1 September 2020).

[2] I. Tanseer, N. Kanwal, M.N. Asghar, A. Iqbal, F. Tanseer, M. Fleury, Real-time, content-based communication load reduction in the internet of multimedia things, Appl. Sci. 10 (3) (2020) 1152.

[3] D. Kumar, K. Shen, B. Case, D. Garg, G. Alperovich, D. Kuznetsov, R. Gupta, Z. Durumeric, All things considered: An analysis of IoT devices on home networks, in: Proceedings of the 28th USENIX Conference on Security Symposium, USENIX Association, Santa Clara, CA, USA, 2019, pp. 1169–1185.

[4] R.O. Andrade, S.G. Yoo, L. Tello-Oquendo, I. Ortiz-Garcés, A comprehensive study of the IoT cybersecurity in smart cities, IEEE Access 8 (2020) 228922–228941.

[5] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J.A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, Y. Zhou, Understanding the mirai botnet, in: 26th USENIX Security Symposium (USENIX Security 17), USENIX Association, Vancouver, BC, Canada, 2017, pp. 1093–1110.

[6] C. Hurley, R. Rogers, F. Thornton, D. Connelly, B. Baker, WarDriving and Wireless Penetration Testing, first ed., Syngress Publishing Inc, Rockland, MA, USA, 2007.

[7] R. Moskowitz, Weakness in passphrase choice in WPA interface, 2003, https://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html. (Accessed 2 September 2020).

[8] T. Roth, Breaking encryptions using GPU accelerated cloud instances, in: Black Hat Technical Security Conference, Las Vegas, NV, USA, pp. 1–9.

[9] M. Vanhoef, F. Piessens, Key reinstallation attacks: Forcing nonce reuse in WPA2, in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS '17, ACM, New York, NY, USA, 2017, pp. 1313–1328.

[10] M. Čermák, M. Svorenčík, R. Lipovský, O. Kubovič, KR00K - Serious Vulnerability Deep Inside Your Wi-Fi Encryption, Tech. rep., ESET, 2020.

[11] Wi-Fi Alliance, Wi-Fi Alliance introduces Wi-Fi 6, 2018, https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-6. (Accessed 20 October 2020).

[12] M. Alleven, Wi-Fi Alliance makes WPA3 mandatory for device certification, 2020, https://www.fiercewireless.com/tech/wi-fi-alliance-makes-wpa3-mandatory-for-device-certification. (Accessed 1 November 2020).

[13] M. Vanhoef, E. Ronen, Dragonblood: Analyzing the dragonfly handshake of WPA3 and EAP-pwd, in: 2020 IEEE Symposium on Security and Privacy (SP), IEEE, San Francisco, CA, USA, 2020, pp. 517–533.

[14] P. Weidenbach, J. Vom Dorp, Home Router Security Report 2020, Tech. Rep., Fraunhofer Institute for Communication, Information Processing and Ergonomics, 2020.

[15] D. Demeter, M. Preuss, Y. Shmelev, IoT: a malware story, in: Securelist.Com, 2019, https://securelist.com/iot-a-malware-story/94451/. (Accessed 25 January 2021).

[16] M. Michael, Attack landscape H1 2019: Iot, SMB traffic abound, 2019, https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/. (Accessed 25 January 2021).

[17] Z.A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, N. Syed, M. Peacock, Future challenges for smart cities: Cyber-security and Digital Forensics, Digit. Investig. 22 (2017) 3–13.

[18] J. Lee, J. Kim, J. Seo, Cyber attack scenarios on smart city and their ripple effects, in: 2019 International Conference on Platform Technology and Service (PlatCon), IEEE, Jeju, South Korea, 2019, pp. 1–5.

[19] S. Webb, Growth in the deployment and security of 802.11 b wireless local area networks in Perth, Western Australia, in: Australian Computer, Network & Information Forensics Conference, Perth, Western Australia, 2004, pp. 48–56.

[20] S. Yek, Wily attackers seek wireless networks in Perth, Western Australia for easy targets, in: European Conference on Computer Network Defence, London, United Kingdom, 2006, pp. 125–136.

[21] C. Lin, H. Sathu, D. Joyce, Network security of wireless LANs in Auckland's central business district, WSEAS Trans. Commun. 3 (2004) 511–516.

[22] W. Lemstra, V. Hayes, J. Groenewegen, the Innovation Journey of Wi-Fi: The Road to Global Success, first ed., Cambridge University Press, Cambridge, United Kingdom, 2011.

[23] N.I. Sarkar, A.H. Abdullah, Exploring wireless network security in Auckland city through warwalking field trials, in: 13th International Conference on Advanced Communication Technology (ICACT2011), IEEE, Gangwon-Do, South Korea, 2011, pp. 685–689.

[24] A. Sarrafzadeh, H. Sathu, Wireless LAN security status changes in auckland CBD: A case study, in: 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), IEEE, Madurai, India, 2015, pp. 1–6.

[25] A. Nisbet, A tale of four cities: Wireless security & growth in New Zealand, in: 2012 International Conference on Computing, Networking and Communications (ICNC), IEEE, Maui, Hi, USA, 2012, pp. 1167–1171.

[26] A. Nisbet, A 2013 study of wireless network security in New Zealand: Are we there yet?, in: Proceedings of the 11th Australian Information Security Management Conference, ISM 2013, SRI Security Research Institute, Perth, Western Australia, 2013, pp. 75–82.

[27] D. Dobrilovic, Z. Stojanov, S. Jäger, Z. Rajnai, A method for comparing and analyzing wireless security situations in two capital cities, Acta Polytech. Hung. 13 (2016) 67–86.

[28] C. Leca, Overview of Romania 802.11 wireless security & statistics, EAI Endorsed Trans. Secur. Saf. 4 (12) (2017) e5.

[29] H. Valchanov, J. Edikyan, V. Aleksieva, A study of Wi-Fi security in city environment, IOP Conf. Ser.: Mater. Sci. Eng. 618 (2019) 012031.

[30] M.S. Sajat, S. Hassan, S.C. Chit, An analysis of Wi-Fi security vulnerabilities in Malaysia: A survey in Golden Triangle Kuala Lumpur, in: 2006 International Conference on Computing & Informatics, Kuala Lumpur, Malaysia, pp. 1–6.
[31] C.S. Priya, S. Umar, T. Sirisha, The impact of wardriving on wireless networks, Int. J. Sci. Eng. Comput. Technol. 3 (6) (2013) 230–235.
[32] E. Eldaw, A.M. Zeki, S. Senan, Analysis of wardriving activity and Wi-Fi access points, in: International Conference on Wireless Sensor Networks for Developing Countries, WSN4DC, Jamshoro, Pakistan, 2013, pp. 51–59.
[33] A. Kyaw, P. Agrawal, B. Cusack, Wi-Pi: A study of WLAN security in Auckland CBD, in: Proceedings of the Australasian Computer Science Week Multiconference, ACSW '16, Canberra, Australia, 2016, pp. 1–9.
[34] Bobzilla, Arkasha, Uhtu, WiGLE.net, 2020, https://wigle.net/index. Accessed 1 November 2020).
[35] B. Sak, R. Jilumudi Raghu, Mastering Kali Linux Wireless Pentesting, first ed., Packt Publishing, Birmingham, United Kingdom, 2016.
[36] Sadmin, Buy the best wireless network adapter for Wi-Fi hacking in 2019, 2019, https://null-byte.wonderhowto.com/how-to/buy-best-wireless-network-adapter-for-wi-fi-hacking-2019-0178550/. (Accessed 25 April 2021).
[37] Offensive Security, What is kali linux? Kali linux documentation, 2020, https://www.kali.org/docs/introduction/what-is-kali-linux/. (Accessed 3 October 2020).
[38] J. Cache, J. Wright, V. Liu, Hacking Exposed Wireless, Second Edition: Wireless Security Secrets and Solutions, second ed., McGraw-Hill, New York, NY, USA, 2010.
[39] Tarlogic Research, Acrylicwifi.com, 2020, https://www.acrylicwifi.com/en/wlan-wifi-wireless-network-software-tools/wlan-scanner-acrylic-wifi-free/. (Accessed 28 October 2020).
[40] Kismet Wireless, Kismet, 2021, https://www.kismetwireless.net/. (Accessed 1 April 2021).
[41] GPSD, Global positioning system daemon, 2021, https://gpsd.gitlab.io/gpsd/. (Accessed 1 April 2021).
[42] Jillybunch, Share GPS, 2015, http://jillybunch.com/sharegps/. (Accessed 24 April 2021).
[43] J.D. Abraham, GISKismet, 2016, https://github.com/xtr4nge/giskismet. (Accessed 24 April 2021).
[44] DB Browser for SQLite, 2020, https://sqlitebrowser.org/. (Accessed 4 October 2020).
[45] Edita Publishing Oy, Finlex - Laki rikoslain 28 luvun 7 §:n muuttamisesta 190/2011, 2020, https://www.finlex.fi/fi/laki/alkup/2011/20110190. (Accessed 21 October 2020).
[46] Edita Publishing Oy, Finlex - Rikoslaki 39/1889, 2020, https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L28. (Accessed 21 October 2020).
[47] P.S. Ryan, War, peace, or stalemate: Wargames, wardialing, wardriving, and the emerging market for hacker ethics, Virginia J. Law Technol. 9 (2004) 3–57.
[48] B.D. Kern, Whacking, joyriding and war-driving: Roaming use of Wi-Fi and the law, Santa Clara High Technol. Law J. 21 (2004) 101–162.
[49] European Parliament and the Council of the European Union, Regulation EU 2016/679 of the European parliament and of the council of 27 April 2016 (general data protection regulation), Off. J. Eur. Commun. 59 (119/1) (2016) 1–88.
[50] F. Feldman, Introductory Ethics, first ed., Prentice-Hall, Englewood Cliffs, NJ, USA, 1978.
[51] M.J. Quinn, Ethics for the Information Age, seventh ed., Pearson Education Inc, Boston, MA, USA, 2017.

Saku Lindroos received his BBA degree in business communication and information security from the Turku University of Applied Sciences, Turku, Finland, in 2014 and his M.Sc. (Tech) degree in networked systems security from the University of Turku, Finland, in 2020. He is pursuing the D.Sc. (Tech) degree in communication engineering at the University of Turku, Department of Computing, where he is currently working as a project researcher. His research interests include wireless network security, security and privacy in communication systems, ethical hacking and computer ethics.

Dr. Antti Hakkala is a University Teacher in Communication Systems and Cyber Security at Department of Computing, University of Turku, Finland. He received his D.Sc.(Tech.) degree in Communication Systems in 2017 from the University of Turku. He has over 10 years experience in teaching engineering students on cyber security and communication systems engineering, and has supervised over 100 Bachelor's and Master's theses on cyber security topics. His current research interests include wireless network security, cyber security in autonomous systems, and security and privacy in networked information society.

Seppo Virtanen received his D.Sc.(Tech.) degree in communication systems from the University of Turku, Finland, in 2004. He is currently Associate Professor of Cyber Security Engineering with the University of Turku, Department of Computing, where he also is the Vice Head of the department. His research currently focuses on information security issues in communication and network technology, especially for smart environments.