Let Numbers Tell the Tale:
Measuring Security Trends in Wi-Fi Networks and Best Practices

Domien Schepers
Northeastern University
Boston, Massachusetts, USA
schepers.d@northeastern.edu

Aanjhan Ranganathan
Northeastern University
Boston, Massachusetts, USA
aanjhan@northeastern.edu

Mathy Vanhoef
New York University Abu Dhabi
Abu Dhabi, UAE
mathy.vanhoef@nyu.edu

ABSTRACT

Motivated by the recent push towards adopting new standards and the discovery of numerous vulnerabilities in both new and old protocols, this paper analyzes the security of Wi-Fi networks. Our analysis is based on publicly available datasets and our own survey covering 250,137 networks across four countries in three continents. We present several key insights, including the continued use of outdated security configurations and vulnerable protocols, the adoption rates of modern protocols, the increasing presence of mesh networks as part of smart city infrastructure, and the vast differences depending on the surveyed geographic region and frequency spectrum. Additionally, we identify and improve upon shortcomings in previous surveys, and recommend best practices for future surveying. In summary, our work provides a more fine-grained understanding on Wi-Fi network security in the real-world. Finally, we publish our tools used for extracting security statistics, and make all anonymized datasets available to other researchers.

CCS CONCEPTS

• **Networks → Mobile and wireless security**.

KEYWORDS

IEEE 802.11, Wi-Fi, Surveying, Measurements, Security

ACM Reference Format:
Domien Schepers, Aanjhan Ranganathan, and Mathy Vanhoef. 2021. Let Numbers Tell the Tale: Measuring Security Trends in Wi-Fi Networks and Best Practices. In *Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '21), June 28–July 2, 2021, Abu Dhabi, United Arab Emirates.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3448300.3468286

1 INTRODUCTION

The rapid deployment of wireless networks, combined with an increasing demand for performance and security, has resulted in significant evolution of the IEEE 802.11 standards. Today, Wi-Fi 6 (IEEE 802.11ax) is the most advanced standard and has the ability to achieve data rates over 10 Gbps. Similarly, the security of Wi-Fi networks have come a long way since the introduction of WEP. Recently, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2, which offers forward secrecy and mitigates security vulnerabilities caused due to poor choice of passwords. Nevertheless, the adoption of new standards and prompt deprecation of older and vulnerable protocols remains key to securing Wi-Fi networks. To encourage the adoption of new standards, devices now display a warning when outdated standards are being used (e.g., operating systems by Apple). Similarly, the Wi-Fi Alliance recommends user interface icons to indicate which standard a network supports [30].

In this paper, we analyze the state of Wi-Fi security using publicly available datasets as well as our own. We analyze datasets from Radiocells [16], a public mobile crowdsourced repository, and our own extensive survey collecting 250,137 networks. Cumulatively, these contain information on close to a million access points collected across three continents. We present statistics on security-related features, analyze trends over time, and discuss their practical relevance and ramifications. Based on the observed trends, we extract several key observations and insights on today's networks. First, we show how the geographic location of a survey plays a significant role in the resulting statistics. For example, we find the usage of WPA-TKIP as a group cipher ranges from 25.82% in Boston (US) to 45.06% in Hasselt (BE) in October 2020. Our case study in Belgium shows that Internet Service Providers (ISPs) have an overwhelming impact on the overall state of security, highlighting their role in phasing out deprecated protocols and adopting new and more secure standards. For example, our case study revealed that when one ISP phased out WPA-TKIP, its overall support in Belgium dropped from 45.06% to merely 7.30% of encrypted networks. Next, we show how statistics may be less representative over certain frequency spectra, which is further motivated by showing how networks are configured with notably different security features in the 5 GHz spectrum (e.g., using more secure encryption protocols). For example, we inspect the support for Wi-Fi Protected Setup (WPS) which is recommended to be replaced by the more secure Wi-Fi Easy Connect [2]. Additionally, we explore the type of wireless networks deployed by analyzing the amendments they support. For example, we observe worrisome trends of an ever-lasting support for vulnerable ciphers such as WPA-TKIP [19]. Despite the efforts to encourage the adoption of new standards, we observe a mere 1.03% support for IEEE 802.11ac Wave 2, 2.22% for IEEE 802.11w (released more than ten years ago) defining Protected Management Frames (PMF), and 1.08% for Simultaneous Authentication of Equals (SAE). We consider our work a starting point to track support of modern protocols such as PMF and SAE, since networks are now required to support them as part of WPA3. Finally, we discuss the increasing presence of hidden networks as part of smart city infrastructure.

Based on our analysis, we find limitations in public datasets such as CRAWDAD [13], WiGLE [33], and Radiocells [16], since they may be outdated and provide limited raw measurement data. For example, Radiocells provides several million records of networks containing the BSSID, ESSID, network capabilities, and channel number.

WiSec '21, June 28–July 2, 2021, Abu Dhabi, United Arab Emirates

However, more fine-grained information of a beacon frame (e.g., an extended capabilities information field) is often necessary. As a result, researchers resort to performing their own survey in order to contextualize or motivate research projects. For example, surveys were used to show widespread usage of insecure protocols [19] or to understand the adoption rate of security features [14, 20, 24]. However, the methodologies used to collect and present these datasets vary significantly, leading to inconsistencies affecting the interpretation of their results. Therefore, we recommend best practices based on our observations and insights. Future surveys can take these practices into account, such that their results are interpreted, and compared to each other, in a more rigorous and accurate manner.

2 DATASETS

In this section, we present the datasets used in our analysis, and discuss the data collection methodology and available information. We use publicly available datasets and data captured by performing our own extensive survey. In total, we analysed 728,306 unique networks from Radiocells and 250,137 from our own survey efforts.

Best Practices. Throughout this paper, we present best practices on how to capture, analyze, and present Wi-Fi datasets. Although we focus on Wi-Fi, these best practices can apply to any wireless protocol. Future surveys should take these best practices into account, such that their results can be interpreted, and compared to each other, in a more rigorous and accurate manner. This is especially important because popular public datasets have notable limitations, often forcing researchers to perform their own surveys.

2.1 Public Datasets

Public repositories such as CRAWDAD [13], WiGLE [33], and Radiocells [16] crowdsource data collection on Wi-Fi networks and publish a subset of information online. For example, Radiocells is a community project providing a free and open Wi-Fi and cellular database, where its data is crowdsourced through an Android application named RadioBeacon [16]. The project has several use cases, e.g., geolocation through Wi-Fi and cell tower location data eliminating the need for GPS. For each Wi-Fi network, Radiocells provides the BSSID, ESSID, encryption capabilities, signal strength and frequency. We retrieved data from 2011 to 2019, and specifically for 2019, the data covered 728,306 unique networks across nineteen countries, with 75% of its unique networks collected within Europe.

Limitations. Public datasets often crowdsource their data in part from Android (e.g., Radiocells and WiGLE). Unfortunately, Android does not make fine-grained information accessible to its users, and therefore these datasets have their limitations. For example, to check if protected management frames are required or supported, one needs to inspect the robust secure network capabilities information field (e.g., from a beacon or probe response), and this information may not be available in public datasets. Additionally, public datasets can be outdated: Radiocells has no new data, and CRAWDAD has seen few new datasets in 2020. These limitations cause researchers to perform new surveys, highlighting the importance of our best practices to assure the resulting data are sound and representative.

Table 1: Number of unique networks in our various surveys, listed per their respective date, region, and frequency band.

Date	CC	Region	2.4 GHz	5 GHz	Total
2019/10	US	Boston (Back Bay)	25,405	13,404	38,809
2019/10	US	Boston (Fenway)	9,992	6,579	16,571
2019/10	US	Providence	7,425	3,255	10,680
2019/10	AE	Abu Dhabi	16,503	7,584	24,087
2019/10	BE	Limburg	4,051	1,328	5,379
2020/10	US	Boston (Back Bay)	18,892	21,637	40,529
2020/10	AE	Abu Dhabi	20,447	11,867	32,314
2020/10	BE	Limburg (Hasselt)	19,267	12,099	31,366
2020/10	CH	Zürich	10,775	11,721	22,496
2021/05	BE	Limburg (Hasselt)	17,647	10,259	27,906

2.2 Our Own Wi-Fi Survey

We performed an extensive survey in October 2019, October 2020, and May 2021. We passively captured all access points by channel-hopping non-overlapping channels on the 2.4 and 5 GHz spectrum. While doing so, we captured beacon frames and probe responses of access points. The beacon frame is a management frame transmitted periodically by the access point announcing the presence of a network and contains all of its configuration information. Similarly, a probe response sends this information to a client following a probe request. Clients may send a probe request either as a broadcast frame, or targeted towards known access points. We then define the uniqueness of networks based on their MAC address. As such, it increases the weight of networks that are deployed over a large region (e.g., ISP hotspots), and reveals how many deployed devices support a certain feature (e.g., indicating an attack's real-world impact). Our survey was performed by walking around in predominantly residential areas. If applicable, we present a dataset per neighborhood (e.g., we split Boston in the Back Bay and Fenway neighborhood). We used a laptop or single-board computer (e.g., a Raspberry Pi) with dedicated Wi-Fi dongles per frequency band, together with Kismet [12] or tcpdump [10] to passively capture, and store, the resulting network captures. In Table 1, we present the number of unique networks per geographic region, date, and frequency spectrum. In total, we collected 95,526 unique networks in October 2019, 126,705 in October 2020, and 27,906 in May 2021, adding up to 250,137 networks of which 215,836 are unique (i.e., due to surveying a certain region each year). These networks span a total of four countries in three continents. Understanding how we perform a survey is needed to accurately interpret our results, and is important in any survey, highlighting our first best practice:

Best Practice 1 (Address the Methodology). *In order to understand and interpret survey results, one must discuss the methodology and provide context for the performed survey. Specifically, one must clarify when and how data is collected (e.g., the frequency bands, location, passive or active data collection) in addition to any assumptions made during processing (e.g., how unique networks are defined).*

Depending on the survey purpose, it may not be required to, for example, collect data on both the 2.4 and 5 GHz spectrum. Nevertheless, it is important to discuss this in the survey methodology as it is necessary to properly contextualize the resulting statistics, e.g., supported standards, availability on commercial products, etc.

2.3 Preserving Privacy in Dataset Publication

Ideally, survey data is shared with other researchers in order to enable further research, and to allow results to be reproduced and verified for correctness. There are two common options for sharing Wi-Fi survey data: submitting to a repository like CRAWDAD [13], or publishing data through a crowdsourcing tool like WiGLE [33] or Radiocells [16]. Data published using tools like Radiocells typically require an application installed on a smartphone. The uploaded data is rather specific, e.g., data may be limited to certain fields of a beacon frame rather than the entire frame itself. However, the publication of datasets raises the concern of privacy. For example, CRAWDAD's data license agreement [5] states that one is not allowed to deanonymize any person whose data is in the dataset. It is up to the contributors to sanitize the data, leaving the risk and liability of sanitization to the data publishers. The risks of an ineffectively sanitized dataset are high. It might become possible to expose sensitive client information, e.g., allowing to track someone's location at a coarse-grained level if they frequently use a personal hotspot. As another example, smart sensors may include sensor readings in beacon frames, which can pose more privacy risks [26]. Furthermore, these risks are not just limited to beacon frames; researchers identified several privacy concerns within probe requests [3, 6, 17], and showed that well-established location privacy defenses are ineffective for mobile crowdsourcing tools [4], raising concerns on the provided privacy level. Therefore, it is essential to adequately sanitize the dataset before publishing.

Best Practice 2 (Preserve Privacy in Published Datasets). *Prior to publication, one should consider the privacy risks in publishing the dataset (e.g., which user-identifiable data is included). The publisher can describe which privacy-sensitive information it aims to protect (e.g., MAC addresses, SSIDs, sensor readings) and explain the actions taken to sanitize the dataset properly.*

In our datasets, we anonymize any user-specific information that would allow them to be tracked or located. We remove the three least significant bytes of each MAC address to sanitize the data, thereby keeping its vendor-assigned bytes. As such, future analysis remains possible on vendor-related properties while preserving user privacy [15, 17]. Next, we map every SSID to a pseudonym "SSID-N" where N is an incremental number. This preserves privacy while still revealing how many APs broadcast a specific anonymized SSID. Additionally, we removed the frame's destination MAC address for probe responses as it identifies client stations. Finally, we release only a single beacon or probe response frame per network, thereby limiting the potential leakage of sensitive sensor data [26].

2.4 Releasing our Datasets, Tools, and Results

In order to enable and stimulate further research we make all anonymized datasets available to other researchers upon request [1]. Additionally, we release tools to anonymize datasets and extract security statistics, and present fine-grained results for each survey.

3 KEY OBSERVATIONS AND INSIGHTS

In this section, we inspect the security configuration of all networks, and identify key security trends, observations, and insights. Unless noted otherwise, all statistics are based on our October 2020 survey.

3.1 Impact of Wi-Fi Survey Methodology

In any wireless survey the methodology (e.g., region, frequency) directly impacts the results, and Wi-Fi networks are no exception.

3.1.1 *Impact of Survey Region.*

We find that statistics can change *significantly* based on the surveyed region. For example, in our survey, on average 32.89% of encrypted networks use WPA-TKIP as their group cipher, a deprecated protocol demonstrated to have security vulnerabilities [19, 22, 27, 28]. However, we find notable differences when we inspect each distinct region; for example, in Boston its support rate is 25.82%, in Abu Dhabi 27.17%, in Limburg 45.06%, and in Zürich 34.79%. Variations can even be observed within a single city [18, 19]. For example, dividing our 2019 Boston survey in the Back Bay and Fenway neighborhoods, we observe they have a WPA-TKIP usage rate of 36.57% and 29.96%, respectively. These observations are also seen in the Radiocells dataset. For example, in 2019, we find an average 35.13% of networks use WPA-TKIP as the pairwise cipher, while this percentage is as low as 17.99% in Lithuania and as high as 54.32% in Austria. Similarly, even among neighboring countries we find a support rate of 21.27% in Italy and 48.21% in France. The observed geographic differences are not restricted to the usage of WPA-TKIP, and can also be found within other security features. For example, in the Radiocells dataset we find the networks observed in 2019 in Taiwan have a WPS support rate of 29.94%, while for Mexico 68.12% of networks support WPS. These findings deviate significantly from the worldwide average of 55.20%. All combined, these findings lead to our third best practice:

Best Practice 3 (Survey Distinct Regions). *Survey results can be impacted by the region in which they are conducted. Therefore one must specify where the survey took place (e.g., city, residential or commercial neighborhood). To the extent possible, sufficient distinct regions must be surveyed to avoid any regional bias in the survey results (e.g., regions in a different country or different ISP landscape).*

3.1.2 *Impact of Frequency Spectrum.*

The frequency spectrum on which a survey is performed has a significant impact on the derived statistics. As an example, consider IEEE 802.11ac, a standard that specifies physical-layer improvements for operations within the 5 GHz spectrum. Naturally, it makes sense to only consider its adoption rate over the networks collected within the 5 GHz spectrum. In other words, it would be misleading to measure the adoption of IEEE 802.11ac while also including networks in the 2.4 GHz spectrum. Therefore, as a general rule, it is recommended to present survey results for each frequency spectrum, and thereby these observations lead to our fourth best practice:

Best Practice 4 (Survey Appropriate Frequency Spectra). *Based on a survey's goals, one must consider the appropriate frequency spectra on which to collect data. Survey results can then be presented for each spectrum, together with the amount of (unique) networks.*

[1] Available at https://github.com/domienschepers/wifi-surveying.

Furthermore, we note that when configuring the hardware setup for a survey, it is possible that no equal time is spent listening on each frequency band or channel. Therefore, one must be aware that certain frequency bands or channels may be over-represented in a survey. The challenge of surveying multiple frequency bands is further exacerbated since 5 GHz networks are harder to detect as the range in this frequency band is lower than in the 2.4 GHz band, and there are more 5 GHz channels to perform channel-hopping on. As a result, it may lead to the collection of more 2.4 GHz networks. Therefore the impact of 5 GHz networks on the combined statistics can be significantly reduced, further illustrating the importance of reporting statistics for each frequency band separately.

Comparing the Security Configuration of 2.4 and 5 GHz Networks. We observe Wi-Fi networks in the 5 GHz spectrum are configured with notably different security features than networks in the 2.4 GHz spectrum. In our survey, 5 GHz networks have an average WPA-TKIP group cipher support rate of 30.47%, in contrast to 34.87% for networks in the 2.4 GHz spectrum. When analyzing the 2019 Radiocells dataset, we obtain similar observations, where 29.09% of networks in the 5 GHz spectrum use WPA-TKIP as the group cipher, while as many as 36.85% networks use it in the 2.4 GHz spectrum. As another example, enterprise authentication mechanisms based on IEEE 802.1X have a support rate of 21.02% in 5 GHz and 16.38% in 2.4 GHz networks. As another example, 5 GHz networks are slightly more likely to be a hidden network with 24.52% in contrast to 20.29% in 2.4 GHz; a topic we explore further in Section 3.4. Furthermore, in order to investigate where these differences stem from, we analyzed networks broadcasted by the same hardware on opposing frequency bands. That is, we matched the five most significant bytes of the BSSID and two-byte SSID prefix within a restricted time window. We found that the presence of less secure network configurations in 2.4 GHz is mainly caused by APs that only advertise a network in the 2.4 GHz band. We conjecture that these APs are older and therefore have less secure (default) settings.

3.2 Impact of Internet Service Providers

From Section 3.1.1, we learned a survey's geographical region has a significant impact on the resulting statistics. After inspection, we find an important factor differentiating these regions are their respective Internet Service Providers (ISPs). In order to understand the practical impact of an ISP on the overall statistics, we perform a case study tracking their default security configurations over time.

3.2.1 *Case Study: Tracking Wi-Fi Configurations of ISPs in Belgium.*

We track the default security configuration of ISPs in Belgium over a total of three years. Belgium serves as a good reference example to illustrate potential impact, since it has shown to have a large number of insecure networks. For example, it has the most substantial support rate for WPA-TKIP, a deprecated protocol that has been widely demonstrated to have security vulnerabilities [19, 22, 27, 28].

Attributing WPA-TKIP Networks. From our October 2020 survey in Belgium, we find 45.06% of encrypted networks use WPA-TKIP as their group cipher. Surprisingly, 84.82% of these networks can be attributed to a single ISP. Out of all WPA-TKIP networks we find that 50.82% have the SSID "TelenetWiFree", a hotspot provided by ISP Telenet. The remaining 34% have an SSID that can be attributed to home routers whom by default have an SSID starting with "Telenet". Given that ISP Telenet accounts for a total of 84.82% of WPA-TKIP enabled Wi-Fi networks, they have an overwhelming influence on the state of Wi-Fi security in Belgium. Similarly, in our 2019 survey, the ISP accounted for 83.46%. We obtain similar results with Radiocells: 38.46% of encrypted networks support WPA-TKIP, out of which 69.72% can be attributed to ISP Telenet (34.91% with SSID "TelenetWiFree" and 34.81% attributed to home routers). It is worth noting the majority of Radiocells networks are located in the region of Brussels, which has a more competitive ISP market compared to our survey in the Flemish province of Limburg. As a result, we find that Telenet's competitor ISP Proximus accounts for an additional 6.81% of networks with its public hotspot "Proximus Smart Wi-Fi".

Table 2: Overview of supported standards and amendments. Rows with a (*) are measured over encrypted networks only.

Version	2019		2020	
	2.4 GHz	5 GHz	2.4 GHz	5 GHz
IEEE 802.11e	97.77 %	97.17 %	98.66 %	98.00 %
IEEE 802.11n	96.64 %	97.88 %	97.43 %	98.64 %
IEEE 802.11w*	2.77 %	6.06 %	2.01 %	2.48 %
IEEE 802.11ac Wave 1	9.80 %	87.52 %	12.98 %	87.19 %
IEEE 802.11ac Wave 2	0.01 %	0.99 %	0.00 %	1.03 %
IEEE 802.11ax	0.04 %	0.14 %	2.13 %	3.26 %

Improved Default Security Configurations. At the time of writing, ISP Telenet still recommends WPA-TKIP as a secure protocol [21] and has WPA/WPA2 listed as the default for home routers provided to their customers. As such, it comes as no surprise that insecure protocols remain adopted in practice. However, recently we found ISP Telenet adjusted the configuration of its hotspots to enforce enterprise authentication, supporting CCMP-encryption only. As a result, we performed a new survey in May 2021 and found support for WPA-TKIP in Belgium dropped to merely 7.30% of encrypted networks, a decrease of 37.76% and the lowest adoption rate we observed in any survey. Since ISPs can phase out deprecated protocols within their public hotspots, and potentially remotely update customers' home routers, it becomes clear they play a major role in the overall security landscape of their respective regions.

3.2.2 *Discussion.*

Our case study has shown that ISPs can have an overwhelming impact on the overall state of Wi-Fi security, highlighting the role of ISPs in phasing out deprecated protocols and adopting new and more secure standards. Insights like these highlight the importance of our observations on a survey region, illustrating that a survey in a single region can yield biased results.

3.3 Support for Modern Standards

It is well-known that new standards take time to be adopted in practice, as observed in Section 3.2. For instance, it took several years for WPA2 to replace the broken WEP protocol [32]. However, recently significant efforts have been made to promote the adoption of new standards. For example, the Wi-Fi Alliance made Protected Management Frames (PMF) part of new certification programs [31], and Apple devices now display the warning *"legacy access point"* when connected to an AP that only supports the old IEEE 802.11b physical-layer standard. Additionally, the Wi-Fi Alliance released WPA3 in 2018, along with a new naming convention that includes a set of recommended user interface icons to inform users regarding a device's supported physical-layer protocols [30]. In Table 2, we present an overview of supported standards and amendments. The three major standards are IEEE 802.11n, 802.11ac, and 802.11ax which the Wi-Fi Alliance refers to as Wi-Fi 4, 5, and 6 respectively. With the recent push towards adopting new standards, it becomes valuable to investigate its impact and determine whether the efforts are (or will be) successful in increasing adoption rates in practice.

3.3.1 Supported Standards and Amendments. We find 88.22% of 5 GHz networks support (a subset of) IEEE 802.11ac. IEEE 802.11ac Wave 2 (e.g., supporting 160 MHz bandwidth channels), has an adoption rate of merely 1.03% despite being released in 2016. Interestingly, IEEE 802.11ax, released in 2019, has been adopted by 3.26% of 5 GHz networks, a notable increase compared to 0.14% in 2019. These findings suggest networks are adopting Wi-Fi 6 over IEEE 802.11ac Wave 2. In addition to major standards, it is worthwhile to inspect the usage of encryption protocols. We find WPA-TKIP remains supported as a group cipher in 32.89% of protected Wi-Fi networks, even though the more secure CCMP protocol was ratified in 2004. With the exception of Belgium, usage of WPA-TKIP has not seen a noticeable decrease since our 2019 survey result of 33.18%.

3.3.2 Wi-Fi Protected Access 3. In 2018, the Wi-Fi Alliance announced WPA3. It requires support for Protected Management Frames (PMF), as defined in IEEE 802.11w. The standard provides protection mechanisms for management frames, e.g., it prevents deauthentication attacks where an adversary forcibly disconnects clients from a network. Additionally, WPA3 requires support for the Dragonfly handshake, named Simultaneous Authentication of Equals (SAE) by the IEEE. We find networks have little support for PMF (2.22%) and SAE (1.08%), only 0.06% supports WPA3 in transition mode (a network supports SAE and is PMF capable, yet does not mandate its usage), and zero networks support WPA3-only. Similarly, WiGLE reports close-to none WPA3 networks. These findings are surprising, since IEEE 802.11w was released more than ten years ago, has a certification program to test interoperability between implementations, and is mandated to be supported in security protocols such as WPA2 and WPA3 [31]. Even more so, WPA2 security flaws such as KRACK have been identified since 2017 [29].

3.3.3 Discussion. Despite the IEEE efforts through deprecating old standards and amendments and researchers and the community highlighting weaknesses in insecure protocols, we find the adoption rate of new and more secure standards remains low in practice. As a result, and most worrisome, vulnerable protocols remain supported in today's Wi-Fi networks. As observed in Section 3.2.2, ISPs will play a major role in increasing adoption rates. We consider it interesting future work to keep monitoring the adoption rates of modern standards (e.g., IEEE 802.11ax, SAE), and our survey can serve as a baseline and aid in monitoring security trends over time.

3.4 Prevalence of Hidden Networks

In several regions, more than a quarter of all networks do not broadcast their SSID. In other words, a large percentage of Wi-Fi networks are hidden (i.e., its SSID either has a length of zero or starts with a zero byte). This is surprising because most routers by default do not use hidden networks. Even when one uses hidden networks out of privacy concerns, it remains possible for an adversary to recover the SSID of the network [1]. Furthermore, hiding the SSID in fact lowers the privacy of all users of such networks [9]. This is because users that previously connected to a hidden network constantly transmit probe requests that contain the SSID of the network, and this makes it easier for adversaries to track users. As a result, for home users it is now recommended not to use hidden networks, and in certain regions we indeed find a low usage of hidden networks. For example, in Limburg 6% of networks are hidden, a remarkable contrast to Boston where over 44% is hidden.

3.4.1 Mesh Networks and Smart City Infrastructure. We find an increasing number of hidden networks to be part of mesh networks and smart city infrastructure, and conjecture these are not meant for ordinary users. From our survey, 0.93% of all networks are part of a mesh network, and all of these are hidden. For instance, in Abu Dhabi a significant fraction of hidden Wi-Fi networks had a MAC address belonging to Tropos Networks of ABB Group, a company providing mesh networks for smart city infrastructure. Ordinary users would be unable to use such networks, and therefore not broadcasting the SSID of these (private) networks is a logical choice since it prevents them from being displayed in user interfaces. Similarly, semi-professional products such as Ubiquity APs use hidden networks for wireless uplinks between APs. We consider it interesting future work to further study this type of networks in detail, and devise techniques to determine their exact purpose.

3.4.2 Security of Hidden Networks. We find hidden networks are configured with significantly different security features than their non-hidden counterparts. For example, if we inspect a region with a high number of hidden networks, such as Boston, we find that 39.42% of hidden networks support WPA-TKIP as its group cipher, and merely 12.57% for non-hidden networks. Across all networks in our 2020 dataset, we find 6.63% of hidden networks support SAE, and 0.15% for non-hidden networks. In fact, 96.47% of networks supporting SAE are hidden networks. Over 94% of all mesh networks are surveyed in Boston, which is the main reason why its support for SAE is comparatively high. Similarly, 2.38% of hidden networks support WPS, whereas 53.35% for non-hidden networks.

4 RELATED WORK

Few works systematically analyze the security trends of Wi-Fi networks, and those that do have their limitations. As some works lack important methodological information, it is challenging if not impossible to correctly interpret their survey results. For example, works like [11, 14, 18, 19] perform a survey over several distinct geographic regions, unlike field studies [20, 24] which limit the scope of their study to one geographical region. That is, the empirical field study in [20] is conducted in Rabat, Morocco. Similarly, the study in [24] takes place in Varna, Bulgaria. As a counter-example, the authors of [18] discuss the wireless spreading of Wi-Fi AP infections using WPS flaws, and do so in several distinct neighborhoods within Boston, US, contextualizing results by describing the kind of residents living within them. Similarly, in [19] several regions in different countries are surveyed to identify the support rate for WPA-TKIP. Although it shows different results per geographical region, the authors do not discuss or investigate what may cause them. In our paper, we performed a survey across three continents, demonstrated the impact of the survey region, and identified the impact of ISPs on the respective geographic regions they operate in. Additionally, in our paper we demonstrated significant differences in the 2.4 and 5 GHz frequency spectrum, and as such performed our survey over both spectra. Investigating related works within the last five years, we find several [7, 14, 24, 25] that do not specify on which frequency spectrum their respective surveys were conducted. Works like [18–20] which do state this methodological information, are limited to the 2.4 GHz spectrum. Though it may be justifiable for a survey to limit its scope, it often goes without clarification on why it may or may not be so for the goals of their respective surveys. To the best of our knowledge, only one recent prior work [8], making an analysis on urban Wi-Fi characterization, performs a survey on both frequency spectra. Finally, several older works like [11, 23, 34] perform Wi-Fi surveys as well, some even up to five million networks [11]. Since these are older works in a time where the wireless security landscape was different, for example, 5 GHz networks were not as prevalent, we excluded them from analysis in our paper. Analyzing these related works stressed the need for a well-described methodology, with special attention to the impact of the survey region and frequency spectrum. In our work, we addressed limitations and recommended best practices, which can serve as a helpful guideline for future surveys. Our work is a first step towards a fine-grained understanding of modern Wi-Fi network security in the real-world, and monitoring the effects of the recent push towards adopting new and more secure standards.

5 CONCLUSION

In this paper, we inspected the security configurations of Wi-Fi networks using publicly available datasets and our own survey. Our analysis identified several key security trends such as the slow adoption rate of new standards, widespread support of deprecated and vulnerable standards, and the increasing presence of hidden networks as part of mesh networks and smart city infrastructure. In practice, we found ISPs can drive the adoption of new standards, and therefore are encouraged to phase out deprecated protocols. Finally, we recommended a set of best practices to perform and present a survey, and released all our tools and anonymized datasets.

ACKNOWLEDGMENTS

We would like to thank our shepherd Martin Henze and reviewers for their valuable feedback. This work was partially supported by NSF grant 1850264 and the Center for Cyber Security at New York University Abu Dhabi (NYUAD). Mathy Vanhoef holds a Postdoctoral fellowship from the Research Foundation Flanders (FWO).

REFERENCES

[1] Acrylic. 2017. Hidden Wi-Fi Network: How to know the name of a wireless network with no SSID. Retrieved 26 July 2018 from www.acrylicwifi.com/en/blog/hidden-ssid-wifi-how-to-know-name-of-network-without-ssid/.

[2] Wi-Fi Alliance. 2021. Wi-Fi Easy Connect. Retrieved 25 May 2021 from https://www.wi-fi.org/discover-wi-fi/wi-fi-easy-connect.

[3] Bram Bonné, Peter Quax, and Wim Lamotte. 2014. Your Mobile Phone is a Traitor!–Raising Awareness on Ubiquitous Privacy Issues with SASQUATCH. *International Journal on Information Technologies & Security* (2014).

[4] Spyros Boukoros, Mathias Humbert, Stefan Katzenbeisser, and Carmela Troncoso. 2019. On (the lack of) location privacy in crowdsourcing applications. In *USENIX Security*.

[5] CRAWDAD. 2020. CRAWDAD Data License. Retrieved 23 March 2020 from https://crawdad.org/data-license-agreement.html.

[6] Mathieu Cunche, Mohamed-Ali Kaafar, and Roksana Boreli. 2014. Linking wireless devices using information contained in Wi-Fi probe requests. *Pervasive and Mobile Computing* 11 (2014), 56–69.

[7] Dalibor Dobrilovic, Borislav Odadzic, Zeljko Stojanov, and Zlatko Covic. 2015. Approach in IEEE 802.11 security analytics and its integration in university curricula. In *Proceedings of the Mechatronics Conference and Workshop*.

[8] Arsham Farshad, Mahesh K Marina, and Francisco Garcia. 2014. Urban WiFi characterization via mobile crowdsensing. In *2014 IEEE Network Operations and Management Symposium (NOMS)*. IEEE, 1–9.

[9] Julien Freudiger. 2015. How talkative is your mobile device? An experimental study of Wi-Fi probe requests. In *WiSec*.

[10] Van Jacobson, Craig Leres, and S McCanne. 1989. The tcpdump manual page. *Lawrence Berkeley Laboratory, Berkeley, CA* 143 (1989), 117.

[11] Kipp Jones and Ling Liu. 2007. What where wi: An analysis of millions of wi-fi access points. In *2007 IEEE International Conference on Portable Information Devices*. IEEE, 1–4.

[12] M Kershaw. 2005. *Kismet: 802.11 Layer 2 Wireless Network Sniffer*. https://www.kismetwireless.net/

[13] David Kotz and Tristan Henderson. 2005. Crawdad: A community resource for archiving wireless data at dartmouth. *IEEE Pervasive Computing* (2005).

[14] Cristian L Leca. 2017. Overview of Romania 802.11 wireless networks security. In *International Conference on Electronics, Computers and Artificial Intelligence*.

[15] Jeremy Martin, Erik Rye, and Robert Beverly. 2016. Decomposition of MAC address structure for granular device inference. In *ACSAC*. 78–88.

[16] Radiocells. 2020. Radiocells.org. Retrieved 22 February 2020 from https://radiocells.org.

[17] Pieter Robyns, Bram Bonné, Peter Quax, and Wim Lamotte. 2017. Noncooperative 802.11 mac layer fingerprinting and tracking of mobile devices. *Security and Communication Networks* 2017 (2017).

[18] Amirali Sanatinia, Sashank Narain, and Guevara Noubir. 2013. Wireless spreading of WiFi APs infections using WPS flaws: An epidemiological and experimental study. In *Conference on Communications and Network Security (CNS)*. IEEE.

[19] Domien Schepers, Aanjhan Ranganathan, and Mathy Vanhoef. 2019. Practical Side-Channel Attacks against WPA-TKIP. In *AsiaCCS*. 415–426.

[20] A Sebbar, SE Boulahya, G Mezzour, and M Boulmalf. 2016. An empirical study of wifi security and performance in morocco-wardriving in rabat. In *2016 International Conference on Electrical and Information Technologies (ICEIT)*.

[21] Telenet. 2021. Hoe Telenet-hoofdstation (modem) instellen en aanpassen? Retrieved 24 May 2021 from https://telenet.be/nl/business/klantenservice/wireless-modem-instellen/.

[22] Erik Tews and Martin Beck. 2009. Practical attacks against WEP and WPA. In *Proceedings of the second ACM conference on Wireless network security*. ACM.

[23] Guillaume Valadon, Florian Le Goff, and Christophe Berger. 2009. A practical characterization of 802.11 access points in Paris. In *2009 Fifth Advanced International Conference on Telecommunications*. IEEE, 220–225.

[24] Hristo Valchanov, Jan Edikyan, and Veneta Aleksieva. 2019. An Empirical Study of Wireless Security in City Environment. In *Proceedings of the 9th Balkan Conference on Informatics*. ACM, 11.

[25] Mathy Vanhoef. 2016. *A Security Analysis of the WPA-TKIP and TLS Security Protocols*. Ph.D. Dissertation.

[26] Mathy Vanhoef, Prasant Adhikari, and Christina Pöpper. 2020. Protecting wi-fi beacons from outsider forgeries. In *WiSec*. 155–160.

[27] Mathy Vanhoef and Frank Piessens. 2013. Practical verification of WPA-TKIP vulnerabilities. In *AsiaCCS*. 427–436.

[28] Mathy Vanhoef and Frank Piessens. 2015. All Your Biases Belong to Us: Breaking RC4 in WPA-TKIP and TLS. In *USENIX Security*. 97–112.

[29] Mathy Vanhoef and Frank Piessens. 2017. Key reinstallation attacks: Forcing nonce reuse in WPA2. In *CCS*. ACM.

[30] Wi-Fi Alliance. 2018. Generational Wi-Fi User Guide. Retrieved 30 May 2020 from https://www.wi-fi.org/file/generational-wi-fi-user-guide.

[31] Wi-Fi Alliance. 2018. *Wi-Fi Alliance introduces security enhancements*. Retrieved 30 May 2020 from https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements

[32] WiGLE. 2020. WiGLE: WiFi Encryption Over Time. Retrieved 30 May 2020 from https://wigle.net/enc-large.html.

[33] WiGLE. 2020. WiGLE: Wireless Network Mapping. Retrieved 22 February 2020 from https://wigle.net/.

[34] Suen Yek and Chris Bolan. 2004. An analysis of security in 802.11 b and 802.11 g wireless networks in Perth, WA.. In *Australian Computer, Network & Information Forensics Conference*. 117–124.