International Research Journal of Advanced Engineering and Science
ISSN: 2455-9024

Security Threats in Wi-Fi Networks

A. Masiukiewicz[1], V. Tarykin[2], V. Podvornyi[3]
[1, 2, 3]Vistula University, Faculty of Engineering, Warsaw, Poland, 02-787
Email address: [1]a.masiukiewicz@vistula.edu.pl

***Abstract*—*Wi-Fi networks are particularly vulnerable to the risks arising from the possibility of signal interception. Anyone who is within range of the access point has this capability. Of course, the use of encryption of WEP, WPA and WPA2 type significantly hinders the ability to take over a packets, you need to remember, however, that some information is a broadcast and goes to all users. An important aspect is the awareness of threats when using Wi-Fi. This is necessary to avoid the loss of privacy as a result of activities such as Evil Twin or Men in the Middle. The second threat often poorly identified by users of Wi-Fi is the area of location based services. Data obtained by the providers of such services can be used for different purposes and not always consistent with the interests of users.*

***Keywords*—** *Attacks against Wi-Fi networks, encryption, location-based services*

I. Introduction

Wi-Fi in addition to the GSM mobile networks, is most widely used solution in the area of wireless technologies [1], [2]. In the case of wireless networks there is one major threat to safety. Anyone who is within the signal range may try to break into such a network.

Not all wireless networks are subject to a variety of activities aimed at violation of their safety. It depends on a number of aspects such as applied technology, access to equipment, the price of equipment, software available, how to manage your network, security levels, frequency licenses. Taking into account the above factors can be assumed that breaking e.g. into the radio link is practically impossible for the average hacker. Frequencies used in radio-links are available only to licensed users, the equipment is expensive, and the technology makes it impossible acquisition of the signal. The situation is similar in the case of special communications systems, trunking and mobile telephony. These networks have frequency resources assigned to specific users, are administered, the devices are expensive and available only to operators and networks are protected by multi-level security. Hack into the system of CB radio probably does not make sense. What remains? Wi-Fi or WLAN is a very interesting and in many ways an easy target for hackers [3-6].

The frequencies on which networks work 802.11 have the character of ISM (Industrial, Scientific Medical) it means that they are accessible to all users. There is in this case any concept of frequency band protecting and each user can transmit and receive at frequencies assigned to the standard. The condition is the use of approved equipment and not to exceed the allowable power level. 802.11 technology is very often used to connect to the Internet, so users transmit using this technology relevant information. The transceivers are widely available and very cheap. Each user can configure his own point of transmission by assigning him any name, doubling the SSID or name of any AP (Access Point) point is carries no formal legal consequences. Many of 802.11 networks are home networks, the second way is to use hot spots that are generally accessible or available to selected users connection points to the Internet. This results in a relatively easy access to a signal generated by different users, as well as sending various messages to the users. In addition the log data in Wi-Fi networks are used by location service providers. The location may be associated with determining the position of a person or tracking the movements of the person over time. Data of this type have the nature of personal data, and if the service LBS does not have adequate security level can get into the wrong hands in breach of the privacy of users of the service [7-17]. The question to what extent the service provider LBS should process the location data, how to protect them against fraud, and what should be the law in this area appears as LBS has become ubiquitous, and tracking and determining the user's position especially in the case of instant messaging mobile occur several times a day [18-21]. The authors describe selected aspects of 802.11 common threats and security methods.

II. Wi-Fi Networks Basics

Standard Wi-Fi is one of the most popular wireless solution in the world. Unlicensed access to the resources of the electromagnetic spectrum and low prices of equipment have led to the widespread use of this technology [22]. Currently, most Wi-Fi network operates in 802.11b/g/n at a frequency of 2.4 GHz. 802.11n standard can operate in the 5 GHz band, however, because of the need for cooperation with 802.11b/g and very often he uses the 2.4 GHz frequency. Currently most of chipsets produced are compatible with 802.11n, and it is expected that in the coming years there will be 802.11ac [2] chipsets, nevertheless, still when it comes to the market structure of devices currently running a significant place have 802.11b/g chipsets. This structure of the market, forced most local area network to use the 2.4 GHz band not preferred due to the structure of the physical layer.

Are all types of Wi-Fi networks are just as vulnerable to different threats? Certainly not. In administered networks we usually have network administrator, who also takes care of security issues. Home networks are definitely vulnerable, but it depends on the location of the network. The houses, of spaced several hundred meters threat is decreasing due to the limited range of Wi-Fi signals, while in multi-dwelling buildings, the threat is growing. Special security considerations should be taken in unknown or random locations which have offered internet access.

III. Threats in Wi-Fi Networks

Threats to Wi-Fi networks to some extent are the same as in other networks. The primary source of threats are three elements: the Internet, e-mail and the ability to intercept communications session. What differentiates wireless networks from wired is the possibility of interception and interference by third parties into transmission sessions. Especially vulnerable to this type of threat are Wi-Fi networks. While, carrying out an attack on the LAN, the attacker needs to gain physical access to cable infrastructure, in case of a WLAN can operate unnoticed, found in the immediate area. And if he manages to break into a wireless network, can commit various abuses. For example, one can use the victim Internet link to perform actions contrary to the law. One may look around in the user local network and try to manipulate devices connected to it. And finally, can keep a passive attitude, recording all traffic, and then analyze the data acquired. In this way, attacker will find interesting information such as passwords. Despite the risk nobody is giving up Wi-Fi networks. Such is the fashion, Wi-Fi networks are easy to configure and use. Everybody should understand the risks so that it will be possible to avoid or minimize the effects of an emergency or its aftermath. Risks typical for Wi-Fi/WLAN are associated with the possibility of interception of on the communication session and packets capture [6], [23], [24]. Packets capture can be realized by using the Wi-Fi card that can work in supervised mode. The application of cards in supervised mode can be realized e.g. using the command *airmon-ng start* in Linux CLI. It is possible to realize such an option in the Kali Linux OS. In this way, network card becomes monitor of all packages that are within range, i.e. have signal power level that allows you to receive the package. The network card must be able to work in the so-called. Attended or supervisory mode. Practically Windows does not support this mode of Wi-Fi cards, although there are some exceptions. An example of the card which can operate in a supervised mode is TPLink WN722 Wi-Fi card [25].

The analysis of capture packets is possible through the use of packets analysis tools. There are available a variety of tools for analyzing packets such as the airodump-ng, tcpdump, Tshark, Ethereal, Wireshark. The most popular packet analyzer is now Wireshark, which replaced an earlier program Ethereal. Using Wireshark, we can through the card under supervised mode have the access to thousands of packets in case of open networks without encryption. When encryption is applied in Wi-Fi networks one can capture only the management, control and beacon frames because these frames are in plain text and not encrypted. Filtering packets in Wireshark using various expressions helps us to monitor the selected packets of users which we are interested. Anyone can read these packets and packet headers. It is also possible to modify these packages and re-send them, because there is no control of the integrity so it is very easy to do.

Adding own packages by the hacker (Packet Injection) is the second major threat to the Wi-Fi networks. The access to data concerning the addresses of the network is possible with the command aireplay-ng then it is possible to send own packets to different networks. A hacker card can inject some packets into the network even though the terminal is not connected to an access point for the network. Injecting the packets is possible, but only in one channel at the same time using one card. Sending Deauthentication packets force all eligible customers to disconnect and reconnect to the AP. This allows, among others, to obtain a selected set of information of different users including hidden station.

In the default mode configuration, all access points transmit their SSID in beacon frames. As a result, customers in the neighborhood can discover them easily. Hidden SSID is a configuration when the access point does not broadcast its SSID in the beacon frames. Thus, only clients who know the SSID of the access point can connect to it. Unfortunately, this measure does not provide comprehensive protection for networks, but some administrators hopes that it does.

Another threat is to break MAC filtering. MAC filters are quite old techniques used for authentication and authorization, and have their roots in a wired technology. Unfortunately, they have not passed the exam in the wireless world. The basic premise of authentication is based on the MAC address of the client. Filter MAC is the identification code assigned to the network interface; the router can check the code and compare it to the list of approved MAC. This list of allowed MAC addresses is maintained by a network administrator and can be given to the access point. Unfortunately, it is easy to get around filters MAC.

When you turn on MAC filtering only allowed MAC addresses are able to successfully pass the authentication process with the access point. If you are trying to connect to an access point device that is not on the white list of MAC addresses, the connection fails. The access point sends error messages to authenticate the rejected clients. In order to break the MAC filter, you can use airodump-ng to find the MAC addresses of clients connected to the access point. Then, after changing the MAC address of the card thief is on the list of authorized MAC addresses.

One of the strongest attacks on the WLAN infrastructure is Evil Twin. The idea is to first of all introduce an additional access point in the vicinity of the user WLAN. This access point could has exactly the same SSID as the authorized WLAN.

Many wireless users may accidentally connect to the malicious access point, thinking that is part of a well-known AP. Once the connection is established, the attacker can perform attacks Man-In-The-Middle and is able to intercept all communications. In the real world, an attacker must be close to the authorized network, so you can get lost and accidentally connected to the network substituted by an attacker. Evil twin having the same MAC address as an authorized access point is even more difficult to detect and stop. Hacker can use the command airodump-ng to locate the access point BSSID and ESSID, which he would like to take advantage of the construction of the Evil Twin.

This new access point also shows up on the screen *airodump-ng*. It is important to note that it is necessary to run *airodump-ng* in a new window with the following command: *airodump-ng --channel 11 wlan0*. Then hacker send frame

Deauthentication frame to the client, so he hangs up and immediately tries to connect again. As a hacker is closer to the customer, his signal strength is higher, and the client connects to evil twin. It is possible also to fake BSSD and the MAC address of the access point using the following command: *airbase-ng -a <router mac> --essid "Wireless Lab "-c 11 mon0*. Now, if we look at the *airodump-ng*, it is almost impossible to distinguish between the two AP. Even *airodump-ng* is not able to see that there are actually two different access points on the same channel. It is the strongest form of the Evil Twin.

The result of packets intercept may be primarily the acquisition of confidential information including various types of passwords that can lead to financial losses, image and others. It is possible attack of the Man in the Middle. Attack of the Man-In-The-Middle occurs when coming out of your network packets do not reach the intended target system, but rather someone who acts as an intermediary in communication between the system, you and the recipient, pretending at the same time before you system, recipient and before your, recipient. This "man, located in the middle" may in this case be addressed to the recipient other than those sent. Also the response from the recipient reaches the man at the center who changes the message and sends it to you.

You should also remember that it is possible to break security from MAC filtering up to the WAP, WEP, WPA2 however WPA2 is unbreakable until one use to short or simple own password not generated by system.

A separate issue is very wide security of location data. This issue relates primarily to mobile users most of which are equipped with Wi-Fi interfaces. Location-Based Services (LBS) are experiencing dynamic development, in the last few years. The location may be associated with determining the position of a person or tracking the movements of the person over time. Data of this type have the nature of personal data, and if the service LBS does not have adequate level of security can get into the wrong hands in breach of the privacy of users of the service. The question to what extent the service provider LBS should process the location data, how to protect them against the fraud, and what should be the law regulation in this area appears as LBS has become ubiquitous, and tracking and determining the user's position especially in the case of instant messaging mobile occur several times a day [18-21], [26].

The localization process often but not always related to the determination of the position of the person. We can identify two basic forms of this service: tracking the object/ person or to determine the position at a given point in time. LBS services are associated with different areas of user activity. The most important of these include: health, safety, entertainment or work. Many of the services of a localization can be used for military purposes or by different public services. The essence of the service may be the location of the user or also the location of various objects and services linked to the location of the user, e.g. The nearest gas station, restaurant, roadside assistance etc. [9]. Not all of the currently available services are ordered by the user, and what more is accepted. Location-based services LBS are increasingly used for marketing and sales, and thus gained a significant financial dimension. LBS services market in the US is valued at hundreds of billions of dollars and is constantly expanding. In large galleries and stores you can be located through a variety of wireless systems and consequently, we cease to be anonymous. The issue of privacy is important and is reflected in the regulatory framework, both in the US and the European Union. Not all information is processed in a manner that corresponds to the users. Tracking the movement of the car can afford to establish the fact [8], [16] that we spent a few hours an parking lot belonging to the pub. What might be the consequences? Control of sobriety behind the nearest corner, and even if you did not drink a drop of alcohol is that information can get to our insurance company, which will change our status to a higher risk, and at the earliest opportunity we will raise the rate for insurance. What happens if some of the data in the right hands? People using the Web sites offering LBS services do not always understand the fact that provide their location. If the location data and the changes gets into the wrong hands whether intentionally or due to lack of sufficient safeguards to protect the data we can put yourself in danger.

IV. Tools and Methods for Wi-Fi Networks Security Analysis

In the case of Wi-Fi networks, we have to deal with the many threats the same as for the wired network. There is a safety issue related to the fact that use of the wireless carrier. Many of the programs are described as a tool to analyze the security of wireless networks. Meanwhile, we have a number of software used for network traffic analysis, analysis of the distribution of the access points, analysis packages, management of network elements that can be used in various networks. Many programs are universal and can analyze both Wi-Fi and wired networks. The greatest risk in both cases is formed at the interface with the global network or the Internet. Some programs, however, are dedicated to the analysis of the physical layer PHY of Wi-Fi network. Tools can be classified according to the following criteria: pay, trial, free, open source, depending on the operation system Linux, Windows, functionality, wired and or wireless.

Figure 1 shows the classification of programs for the analysis of network security from the point of view of their functionality.

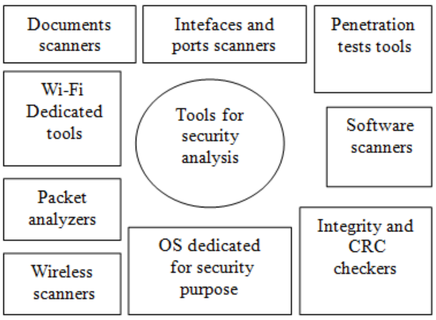
Documents scanners
Intefaces and ports scanners
Penetration tests tools
Wi-Fi Dedicated tools
Tools for security analysis
Software scanners
Packet analyzers
Integrity and CRC checkers
Wireless scanners
OS dedicated for security purpose

Fig. 1. Classification of tools to analyze network security

The majority of free tools that are used to detect the gaps and shortcomings in security to applications running in a Linux environment. Only for this operating system modified WLAN controllers allow you to switch the network adapter to supervision mode. There are several solutions of complex nature. These include dedicated operating systems in which there is the whole set of tools for network analysis. Typically, these solutions based on the Linux operating system. Table I includes most common Linux distributions dedicated to the analysis of network security.

TABLE I. Linux distributions dedicated to security analysis

Linux distribution	Webpage	Description
deftlinux	www.deftlinux.net	Set of several tools for security testing
Back Track / Kali Linux	www.kali.org	Set of several tools for security testing
caine-live	www.caine-live.net	Set of several tools for security testing
SELinux-Security Enhaced Linux	www.selinux.pl	Set of Linux kernel modifications and tools for assigning resources to the applications

Most distributions include a similar range of diagnostic tools. The operating system can be installed on a flash drive and run as an independent operating system using the wizard to create multiboot flash drive, which can be downloaded from the http://www.sarducd.it/. Among the various types of scanners are many programs that we call anti-virus. They usually have a number of functions such as scanning, monitoring, vaccination, quarantine. Due to the similar functionality it is difficult to differentiate between different types of scanners. Table II summarizes some of the tools.

TABLE II. Selected tools

Documents scanners	Malwarebytes Anti Malware, ClamAV, Virus Total, RootkitRevealer, ArcaVir, Panda, AVAST, AVG Anti Virus, Kaspersky, Norton Symantec, Eset Nod32 Antivirus, Avira Antivir, BitDefender, Comodo AntiVirus, Immune Protect, Microsoft Security Essentials,
Anti Virus and similar software	
Intrusion Detection Software	Snort, Ossec Hids, Ossim, Squil, ArcSight,
Integrity and CRC checkers	tripwire, AIDE, md5sum, cmp, sha512sum,
OS monitors	TripWire, AIDE, DumpSec, Highjack This, Canvas, Core Impact, Metasploit,
Packet analysers	Whireshark /Ethereal, Cain and Abel, tcpdump, Kismet, EtterCap, NetStumbler, dsniff, Ntop, Ngrep, EtherApe, NetworkMiner, P0f, inSSIDer, KisMAC,
Web scaners	Netsparker, BeEF, WebGoat, w3af,
Ports and network scanners	Nmap, Nessus, Ntop, SolarWings, Whireshark, Argus,

A number of tools are dedicated to the analysis of the Wi-Fi network. The first group are programs that analyze the physical layer of the network. These programs [27] are generally available on the Internet, and their level of sophistication allows them to use by a average user. These programs are based on the measurement capabilities of the card implemented in a desktop computer, laptop or other mobile device running the Windows operating system. List of measured parameters may include:

- SSID network name,
- signal level measured in dBm,
- standard version 802.11a, b, g, n,
- encryption type WEP/WPA/WPA2,
- the physical address of the device,
- channel number on which a network is transmitting,
- used band in GHz,
- channel width in MHz,
- maximum network throughput in Mb/s,
- spectral density of the noise power in dBm,
- the ratio of signal power to noise ratio in dB,
- the coordinates of geographical location.

Some of the parameters are analyzed by all programs, and some are optional. Geographical location coordinates are given only in the case where the card used for measuring supports 802.11v ensuring distribution of information on the location of the workstation [28]. The most important parameters necessary for the proper selection of channels are: signal level network of own and other networks, 802.11, channel numbers which give all network and used band (2.4 or 5 GHz).We tested seven programs that allow you to analyze the environment from the point of view of the number of Wi-Fi 802.11 and define the basic parameters of the network. Table III presented the information about the tested programs.

TABLE III. Selected information about tested programs for 802.11 network analysis

Name	Version	Webpage	OS
Xirrus Wi-Fi Inspector	1.2.1.2	xirrus.com	Windows: XP, Vista, 7, 8
inSSIDer Home	3.1.2.1	programosy.pl	Windows: XP, Vista, 7, 8
WirelessNetView	1.55	nirsoft.net	Windows: XP, Vista, 7, 8
Ekahau HeatMapper	1.1.4.39795	ekahau.com	Windows: XP, Vista, 7, 8
Common View for Wi-Fi[1]	7.0	tamos.com	Windows: XP, Vista, 7, 8
Wi-Fi Hopper[2]	1.2	pobieralnia.pl	Windows: XP, Vista, 7, 8
Network Stumbler	0.4.0	netstumbler.com	Windows: XP

1 / version of the time, performs the analysis in time for the 5 min from the start
2 / trial version

One way to test the network are penetration tests. To determine the level of security for your network, you can try to break it. Such action is possible with the use of Linux systems Kali and Deft. For reasons of formal and legal in this type of action is needed awareness of the consequences of such activities. You can lead them to their own networks and / or to order the administrator/owner of the network.

According to Art. 267 of the Criminal Code (Official Gazette 1997 No. 88, item. 553) [29] to access the telecommunications network without authorization is an offense against the protection of information, the offender shall be liable to a fine, restriction of liberty or imprisonment of up to two years. Paragraph 1 of mentioned above article provides that unauthorized persons are not allowed to access to information, which are not intended for them, or avoid or overcome this for protection. In accordance with paragraph 3 are not allowed to use to the listening purposes any devices or software.

The aim of the various methods of ensuring privacy when using LBS services is to reduce the risk of fraud. There is currently no integrated security, each of the existing methods is considered independently, although in the aspects in the often share similar features. Methods Privacy is currently the subject of several studies and projects [13], [30-36]. Currently, there are three basic methods such as providing false data, anonymization and blurring accuracy.

Providing false information is to provide the service provider false data on the user, rather than the actual data. Entering false information may relate to the user name (ID) and location data for example. We can give the name of the parallel street or a place which is situated near the actual location. In addition, the data indicated when we visit several times the same place we can change [37], [38]. This method can be easily implemented by a user. Instead of the actual ID we give any name and also change the coordinates of the location.

K-anonymization is used e.g. in relational databases and enables users to distinguish the base [39]. The method was used to protect the privacy of users of LBS. We developed a number of versions of this method: strong, diversity, closeness, sensitivity, historical [40-44]. This method provides both user anonymity and the anonymity of the question. Ensuring privacy queries to the database associated with the location by some scientists it is treated as a separate issue.

Method dilution of precision is to change the location accuracy. Instead of the point specified by the coordinates of a potential burglar receives information about the area. This causes the other hand, the deterioration of the accuracy of position. Two solutions have been proposed in the literature. The first point is given instead of a [7]. The second algorithm is used instead of the graph given point [45]. Another aspect is the protection of information about the user's location in time (Trajectory). Developed several solutions that allow for the protection of information on the movement of the user (user trajectories [46-49].

V. CONCLUSIONS

Wi-Fi networks are exposed to a much greater extent on third party intervention in the communication session. Can we block this vulnerability Wi-Fi network to the threat? The answer is no. We have a range of tools such as hiding the SSID, MAC address filtering, encryption, authentication using WEP, WAP, WAP2, tools for monitoring network environment. All available security, however, are prone to breaking or bypassing. Can we prohibit the use of Wi-Fi devices in our neighborhood - answer is no. What can we do?

We can of course use all available tools. But keep in mind that these tools are available to hackers and they can freely test its software and its ability to violate or circumvent security. It seems that in the current situation is very important awareness of the user's network via Wi-Fi technology and the need to give up the connection in a given situation. If you use an unknown Hotspots is let's not go to the site of our bank and not let us list our data. It seems to raise awareness of Internet users can significantly improve various aspects of their safety.

REFERENCES

[1] I. Dolińska and A. Masiukiewicz, “Wireless technologies and application,” *AFiBV Publishing* (in Polish), 2013.

[2] *Aruba White Paper*, “802.11ac technology, Chapter I: Introduction and technology overview,” Aruba Networks Inc. 2012

[3] P. Rutkowski, “Cibersecurity common responsibility,” *Computerworld*, no 25, (in Polish) 2013.

[4] A. Steliński, “Enterprises under pressure: 5 most dangerous threats,” *Computerworld*, no 25 (in Polish), 2013.

[5] P. Kowalski, “Crafty attacks. Efficient defense,” *Computerworld*, no 25 (in Polish), 2013.

[6] V. C. Buchanan, *Kali Linux Wireless Penetration Testing*, Packt Publishing 2nd Edition, 2015

[7] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. Di Vimercati, P.Samarati, “Location privacy protection through obfuscation-based technique,” *Data and Applications Security XXI*, Springer, pp. 47-60, 2007.

[8] K. Kuebler, D. Palm, and A. Slavec, “The ethics of personal privacy and location- based services,” *Editors Laurie Burkhart Jake Friedberg Trevor Martin Kavitha Sharma Morgan Ship, Confronting Information Ethics in the New Millennium*, http://www.ethicapublishing.com/confronting_information.pdf access 16.07.2015

[9] J. Pan, Z. Zuo, Z. Xu, and Q. Jin, “Privacy Protection for LBS in Mobile Environments: Progresses, Issues and Challenges,” *International Journal of Security and Its Applications*, vol. 9, no. 1, pp. 249-258, 2015.

[10] M. L. Damiani, “Third party geolocation services in LBS: privacy requirements and research issue,” *Transactions on Data Privacy*, vol. 4, no. 2, pp. 55-72, 2011.

[11] M. L. Damiani and M. Galbiati, “Handling user-defined private contexts for location privacy in LBS,” *Proceedings of the 20th International Conference on Advances in Geographic Information Systems*, pp. 574-577, 2012.

[12] M. L. Damiani and C. Cuijpers, “Privacy challenges in third-party location services,” *IEEE 14th International Conference on Mobile Data Management (MDM)*, pp. 63-66, 2013.

[13] J. Krumm, “A survey of computational location privacy,” *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391-399, 2009.

[14] A. Solanas, J. Domingo-Ferrer, and A. Martínez-Ballesté, “Location privacy in location-based services: Beyond TTP-based schemes,” *Proceedings of the 1st International Workshop on Privacy in Location-Based Applications (PILBA)*, 2008, pp. 12-23.

[15] T. Wang and L. Liu, “From data privacy to location privacy,” *Machine Learning in Cyber Trust*, Springer, pp. 217-246, 2009.

[16] *FCC Report, “*Location-based services an overview of opportunities and other considerations,” Federal Communications Commission 445 12th Street, SW Washington, DC 20554, Wireless Telecommunications Bureau, 2012.

[17] Shreetha, and S. Girish, “Survey on privacy-preserving by a trajectory for participatory sensing in wireless sensor networks,” *International Journal of Engineering Research & Technology (IJERT)*, vol. 4, issue 03, 2015

[18] J. Figueiras, and S. Frattasi, *Mobile Positioning and Tracking From Conventional to Cooperative Techniques*, John Wiley and Sons, Ltd 2010.

[19] H. A. Karimi, *Advanced Location-Based Technologies and Services*, CRC Press, 2013.

[20] S. Goswami, “Indoor location technologies,” *Springer*, 2013.

[21] I. G. Petrovski, *GPS, GLONASS, Galileo, and BeiDou for Mobile Devices*, Cambridge University Press, 2014

[22] R. Hiertz Guido, D. Dee, S. P. Lothar, Y. Zang, and C. X. Pérea, Walke Bernhard, “The IEEE 802.11 universe,” *IEEE Communications Magazine*, 2010.

[23] W. L. Pritchett and D. De Smet, *Kali Linux Cookbook*, Packt Publishing, 2013.

[24] R. W. Beggs, *Mastery Kali Linux for Advanced Penetration Testing*, Packt Publishing, 2014.

[25] *TP Link User Guide*, "TL WN722N Wireless N USB Adapter" Rev. 3.0.0TP Link Technologies CO., Ltd. 2012.

[26] I. Dolińska, M. Jakubowski, and A. Masiukiewicz, "Location ability of 802.11 access point," *IEEE sponsored IDT Conference*, Żylina 2015.

[27] A. Masiukiewicz and P. Szaleniec, "Wi-Fi networks measurements," *VU Scientific Papers*, no 38 (in Polish), 2014.

[28] *Standard* IEEE 802.11v, 2011

[29] *Official Gazette (Dziennik Ustaw)*, no. 88, item. 553 Polish Parliament (in Polish), 1997.

[30] M. F. Mokbel, "Privacy in location-based services: State-of-the-art and research directions," *International Conference on Mobile Data Management*, pp. 228-228, 2007.

[31] A. Solanas, J. Domingo-Ferrer, and A. Martínez-Ballesté, "Location privacy in location-based services: Beyond TTP-based schemes," *Proceedings of the 1st International Workshop on Privacy in Location-Based Applications (PILBA)*, pp. 12-23, 2008.

[32] A. Solanas, F. Sebé, and J. Domingo-Ferrer, "Micro-aggregation-based heuristics for p-sensitive k-anonymity: one step beyond," *Proceedings of the International Workshop on Privacy and Anonymity in Information Society*, pp. 61-69, 2008.

[33] M. L. Damiani, "Privacy enhancing techniques for the protection of mobility patterns in LBS: Research issues and trends," *European Data Protection: Coming of Age*: Springer, pp. 223-239, 2013.

[34] D. P. Suresh, and C. A. Dhote, "A Framework for detecting and avoiding location based queries to preserve content and user privacy in databases: A review," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 4, issue 1, 2015.

[35] R. Shokri, G. Theodorakopoulos, P. P.apadimitratos, E. Kazemi, and J.-P. Hubaux, "Hiding in the mobile crowd: Location privacy through collaboration," *IEEE Transactions on Dependable and Secure Computing, Special ISSUE on Security and Privacy in Mobile Platforms*, 2014.

[36] Shreetha and S. Girish, "Survey on privacy-preserving by a trajectory for participatory sensing in wireless sensor networks," *International Journal of Engineering Research & Technology (IJERT)*, vol. 4, issue 03, 2015

[37] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," *Proceedings, International Conference on Pervasive Services, ICPS'05*, pp. 88-97, 2005.

[38] P. Shankar, V. Ganapathy, and L. Iftode, "Privately querying location-based services with sybilquery," *Proceedings of the 11th international conference on Ubiquitous computing*, pp. 31-40, 2009.

[39] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557-570, 2002.

[40] C. Zhang and Y. Huang, "Cloaking locations for anonymous location based services: a hybrid approach," *GeoInformatica*, vol. 13, no. 2, pp. 159-182, 2009.

[41] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with privacy grid," *Proceedings of the 17th international conference on World Wide Web*, pp. 237-246, 2008.

[42] N. Li, T. Li, S. Venkatasubramanian, and T. Closeness, "Privacy beyond k-anonymity and l-diversity," *ICDE*, pp. 106-115, 2007.

[43] A. Solanas, F. Sebé, and J. Domingo-Ferrer, "Micro-aggregation-based heuristics for p-sensitive k-anonymity: one step beyond," *Proceedings of the 2008 International Workshop on Privacy and Anonymity in Information Society*, pp. 61-69, 2008.

[44] S. Mascetti, C. Bettini, X. S. Wang, D. Freni, and S. Jajodia, "Providenthider: An algorithm to preserve historical k-anonymity in lbs," *Tenth International Conference on Mobile Data Management: Systems, Services and Middleware, MDM'09*, pp. 172-181, 2009.

[45] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, "Preserving user location privacy in mobile data management infrastructure," *Privacy Enhancing Technologies*, pp. 393-412, 2006.

[46] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," *Proceedings of the 1st international conference on Mobile Systems, Applications and Services*, pp. 31-42, 2003.

[47] G. Ghinita, M. L. Damiani, C. Silvestri, and E. Bertino, "Preventing velocity-based linkage attacks in location-aware applications," *Proceedings of the 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pp. 246-255, 2009.

[48] J.-G.Lee, J. Han, and K.-Y.Whang, "Trajectory clustering: a partition-and-group framework," *Proceedings of the 2007 ACM SIGMOD international conference on Management of data*, pp. 593-604, 2007.

[49] G. Mumtaj Muthu, B. Akthar, and P. Babu, "Privacy preserving for participatory sensing using trajectory mix-zone model," *International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)*, vol. 1, issue 3, pp. 8-14, 2014.