The 5th IEEE International Symposium on Smart and Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems
17-18 September, 2020, Dortmund, Germany

Detecting Low-Level Attacks on Wireless OT Networks

Dr. Daniel Mahrenholz[1], Dr. Georg Lukas[2], Julius Paffrath[3], Prof. Dr. Kai-Oliver Detken[4]
[1,2,3] rt-solutions.de GmbH, Oberländer Ufer 190a, 50968 Köln,
{mahrenholz,lukas,paffrath}@rt-solutions.de, www.rt-solutions.de
[4] DECOIT® GmbH, Fahrenheitstraße 9, 28359 Bremen, detken@decoit.de, www.decoit.de

***Abstract*—Wireless networks are increasingly used in production environments but often cannot implement active security measures due to concerns about negative availability impacts. As these networks are increasingly targeted by adversaries, passive detection methods are required that supplement existing infrastructures. Therefore, the GLACIER research project [6] is developing a novel multidimensional analysis that combines anomaly detection with user feedback to avoid false positives as far as possible. For wireless OT networks, it uses low-cost distributed passive probes to observe low-level network properties that are aggregated in a central system to build a global view of the network, its nodes and their communication patterns, that is the baseline to detect anomalies or suspicious behavior.**

Keywords—Wi-Fi; OT Security; ICS; SIEM

I. Introduction

Digitization is one of the most important developments of the 21st century. In terms of the industrial business environment, digitization is currently considered a strong topic of discussion and research and has already been described as the fourth industrial revolution (Industry 4.0) [1]. The consistent networking of machines, processes, products and people lead to intelligent production environments and thus opens up numerous potentials for companies [2]. At the same time, companies face the great challenge of designing cost-effective processes. The field of industrial automation is undergoing a paradigm shift from rigid structures to dynamically growing plants. Traditionally, industrial automation relies on wired communication connections, which however, represent a high-cost factor. There is a need here to establish cost-effective communication through wireless connections [3].

However, there is a decisive difference between wireless and wired connections. Wireless based communications are available as exposed interfaces not only to authorized communication partners but also to malicious attackers [4]. It also shows, that the security of industrial plants has not been given sufficient consideration in recent years [5]. New types of research, for example by the search engine Shodan, illustrate the high risk that companies are facing if security is not taken into account from the outset. This shows the need for secure implementations of wireless communication in industrial environments.

An example attack scenario on wireless infrastructures in industrial environments are the use of rogue access points (AP). Here, an attacker installs a wireless AP that pretends to be a valid AP of an existing industrial infrastructure. By sending deauthentication packages, the attacker can bring the victims wireless clients, like PLCs, HMIs or SCADA systems, to connect to the rogue AP. The usage of a wireless attack scenario allows the attacker to operate from a much higher distance without the need for directly accessing the plant.

Defending wireless OT networks comes with several challenges. First, as availability and integrity are top security objectives, components can mostly not be changed to provide additional security monitoring functionalities. Thus, monitoring components must be added to the existing infrastructure and monitoring must be passive to not interfere with the designed functionality. Second, as OT components in a factory environment are usually distributed across a large geographical area, compared to the wireless transmission ranges, observing the whole network from a single point is impossible. Therefore, a number of geographically distributed probes are required which should be low-cost to be economically feasible.

II. Attack scenarios

This section discusses two major classes of low-level attacks on wireless OT networks, attacks that aim to disrupt communication and attacks that aim to eavesdrop on the communication or to gain access to a network using a wireless AP. Other attacks on the devices and services that run in the OT network are not considered.

A. Jamming

On the physical layer, communication can be disrupted by radio jamming, i.e. an adversary can flood the wireless spectrum using any kind of noise signal. This will lower the signal-to-noise (SNR) ratio for any wireless node in range of the adversary. Depending on the noise level, wireless nodes are forced to use a modulation scheme with lower bandwidth or communication is blocked completely. The same can be caused by interference of other non-Wi-Fi devices (e.g. Bluetooth, microwave oven).

B. Saturation of the wireless medium

Concurrent wireless networks can cause saturation of the wireless medium to reduce the available bandwidth. The same can happen due to careless setup of multiple wireless networks, bad coverage planning or other nearby legitimate users. Usually, if a wireless node in an IEEE 802.11 Wi-Fi detects a collision during transmission, it will perform a random backoff before it will try the transmission again. An adversary can ignore this behavior (cheating on backoff rules [7]) and use a small, fixed backoff that will effectively block other clients from sending.

C. Low-level protocol attacks

An adversary can also exploit other properties of the IEEE 802.11 protocol family [8]. Wireless APs can be attacked by authentication/association flooding. In this scenario, an adversary simulates a huge number of clients by sending authentication requests with random MAC addresses, followed by respective association requests. This behavior consumes memory and processing resources that are limited on the AP device, thus denying service to legitimate clients. The adversary can also perform a deauthentication attack, i.e. send spoofed deauthentication requests with the MAC address of a legitimate client to the AP that will then disconnect the client. To prevent the client from reconnecting, the adversary can repeat sending deauthentication requests in short intervals (deauthentication flooding). These attacks are possible, because management frames such as the deauthentication message are usually not authenticated and therefore can easily be forged. The IEEE 802.11w introduces protection for management frames but is not widely adopted, especially in OT environments.

D. Traffic flow manipulations

Another denial-of-service (DoS) attack is a so-called Evil Twin with black-hole routing. Here, the adversary installs a rogue AP that mimics a legitimate AP (i.e. uses the same SSID) and uses a higher signal strength. This way clients are tricked to connect to the rogue AP but communication is not forwarded to the intended network. Evil twins are often combined with deauthentication attacks to disconnect clients from legitimate APs.

An adversary that targets the confidentiality needs to perform either a man-in-the-middle (MiTM) attack or must perform passive sniffing and offline decryption. For a MiTM attack, the evil twin scenario can be used, but the adversary now needs to provide routing to the target nodes. This can be either by a direct connection to a backbone LAN or by connecting to a legitimate AP which requires valid credentials. For WEP and WPA2 a pre-shared key (PSK) can be retrieved using brute-force methods on previously captured association/authentication frames. We do not consider these attacks in our analysis as they do not generate usable traces.

Another dangerous attack on Wi-Fi networks is ARP spoofing. An attacker forwards spoofed ARP packets to clients, which overwrite their ARP cache and cause them to use a different gateway other than the default one for data transmission. The traffic then continues to pass through the Wi-Fi AP, which decrypts the received packets and forwards them to the attacker's gateway with its Pairwise Temporal Keys (PTK) re-encrypted before sending them. This key is temporarily generated for data transmission after a user's master key. According to the IEEE specification, the base station and Wi-Fi client can also detect via the PTK whether sender and receiver addresses were falsified during data transmission. Since the attacker acts as a proxy during ARP spoofing, all data can now be read on the simulated gateway.

E. Principle challenges

A general problem in OT environments is that Wi-Fi devices are significantly older than in typical office/enterprise environments. This is partly due to the location of their installation, e.g. in a logistics warehouse the Wi-Fi APs are distributed on a ceiling at a great height, or they are certified as part of the whole machinery by its supplier and cannot be replaced individually. Besides, the end devices are often designed for robustness and availability rather than for current operating systems. For this reason, it is often not possible to use the latest security technologies (e.g. only WEP for handheld scanners). Due to the poor physical access to the Wi-Fi APs and the often-necessary overall replacement of the end devices, a renewal is therefore considered in much larger cycles.

III. Attack Detection Techniques

Attacks on wireless network can be detected by different principal methods:

a. direct detection of interfering signals or manipulated data packets,
b. indirect detection by analyzing the effects on individual Wi-Fi nodes,
c. correlation and anomaly detection using data from different sources.

A. Direct detection techniques

A jamming attack can be detected by monitoring the wireless spectrum (2.4GHz for 802.11bg and 5GHz for 802.11a) with a spectrum analyzer. There exist dedicated commercial spectrum analyzers optimized for the two Wi-Fi frequency bands that emit noise level statistics based on short measurement intervals (multiple measurements per second). These devices can be used to detect changes in the noise level even when no actual data transmissions take place, and can also provide hints at other users of the Industrial, Scientific, and Medical (ISM) frequency ranges, like microwave ovens or short-range frequency-hopping technologies like ZigBee or Bluetooth. However, as these devices cannot receive actual Wi-Fi packets, they are unable to differentiate legitimate traffic sent by the industrial devices from malicious traffic or jamming. Using an estimation of the background noise level, a spectrum analyzer can also distinguish between times a wireless channel is idle or in use and so can detect saturation of the wireless medium. The ability to detect devices using frequency-hopping technologies highly depends on the timely resolution of the spectrum analyzer, i.e. the number of measurements performed per frequency per second, to display the signals accurately, quickly and seamlessly in real-time. Only in this way short, unwanted signals can be examined in detail.

A passive Wi-Fi scanner can be used to listen for wireless packets and to analyze them. As any other Wi-Fi client, the passive scanner can see changes in the perceived noise level from the packets it receives and so can detect jamming if it is below a certain threshold that still allows for successful communication. From the number of packets received over time, the passive scanner can calculate the utilization of the wireless channel and thus detect saturation attacks.

If the passive scanner is configured with the list of allowed ESSIDs (network names) and BSSIDs (access point MAC addresses), it is possible to monitor for disallowed networks, i.e. serving a different network name (like personal smartphone hotspots) or serving a network name associated with the production site, but with a different BSSID (rogue access points). Furthermore, it is possible to detect deauthentication frames (which are sent by attackers to force a station out of the Wi-Fi network) and malicious RTS/CTS packets that can be used to artificially block the wireless channel.

To perform this kind of monitoring, it is not sufficient to monitor the channel(s) that the legitimate network operates on. Instead, the scanner needs to either monitor all channels simultaneously or to perform channel hopping to ensure that all Wi-Fi channels are covered.

B. Indirect detection techniques

Jamming attacks can be principally detected by multiple methods. If the noise is too weak to impact actual transmissions, then a wireless device will still be able to transmit data, albeit with a higher packet error rate, thus leading to the selection of more robust (and thus slower) transmission rates. The wireless card's Medium Access Control (MAC) implementation keeps track of these sender transmission statistics. Some drivers can be queried to obtain them, allowing to derive the typical transmission rates and to detect spontaneous changes. Transmission rates and numbers of retransmissions can also be monitored by a passive receiver tuned to the same channel.

If the jamming signal exceeds a certain signal strength, it is observed as a carrier signal, thus preventing a normal device from sending legitimate traffic. The same effect can be achieved by an attacker sending valid wireless frames back-to-back without the protocol-advised back-off times. When new data is generated by the legitimate sender without the ability to transmit it on the medium, the packets will be queued in the network stack transmission queue for a certain time, eventually causing a queue overrun, which can be detected at the OS level. A recipient or a passive monitoring station will be able to detect the absence of periodic data packets, and use that as a sign of a busy medium. Such a monitoring system should be calibrated for the expected rate of data packets to detect deviations. Every wireless Access Point is sending periodic Beacon frames, typically at a rate of 10/s. A monitoring system should measure the rate of Beacons as well. However, as each station intending to send data determines the noise level individually, APs may operate normally, while actual stations are blocked because they are closer to the jammer. Therefore, monitoring should include all known periodic packet sources. A passive monitoring station can furthermore detect such cheating using sequential analysis [7].

When the industrial application is not sending data permanently (i.e. because some processes only run at a certain time of the day), it is still important to monitor the medium for potential issues at all times. This can be accomplished by active probes. Such probes consist of a pair of sender and receiver. The sender generates synthetic traffic with a predefined pattern and timing, and send it to the receiver over the wireless infrastructure. The receiver then measures the packet loss rate, latency and jitter of the transmissions. Such a pre-defined stream is also useful in combination with passive Wi-Fi probes that can augment the measurement with the data rate and retransmission rate on the wireless medium, which cannot be directly seen by the receiver.

C. Correlation and anomaly detection

The state of the wireless network depends on the position of the observer, i.e. all observers perceive the state differently. For instance, a signal source interfering with the reception on a wireless client located in the opposite direction from an AP may not be detectable for the AP. Even deciding on normal communication behavior is a distributed task for moving clients that roam between different APs. Wi-Fi controller that manages several APs can provide a solution for the communication aspect as they have visibility into all connected APs.

As a general solution, the BMBF project GLACIER [6] comes into play. As a SIEM (Security Information and Event Management) system it provides the ability to normalize and correlate data from different data sources into a single view. It performs automated intrusion detection by multidimensional analysis as well as the use of anomaly detection algorithms in combination with user-provided feedback to minimize false-positives events.

The GLACIER prototype will be able to alert on pre-processed events delivered by individual sources and anomalies detected by its own analysis engine. For rogue AP detection it builds a consolidated inventory of legitimate clients and APs across the infrastructure and alerts on any unknown (rogue) nodes or legitimate nodes used in unusual network segments. From the traffic flow statistics reported by different passive monitoring stations it creates a consolidated model of the nodes' communication and movement (in terms of AP associations) behavior over time to alert on any deviations. It finally correlates such low-level events with data from higher layers (e.g. IDS events, vulnerability assessments, system logs) to provide visibility into the adversaries activities after an initial intrusion (e.g. to detect lateral movement or network reconnaissance).

IV. Implementation Details

A. *Overall Architecture*

The implementation consists of three layers: sensor, pre-processing, and SIEM (s. Fig. 1). The sensor layer gathers the raw data which the pre-processing layer then analyzes to produce aperiodic event data or condensed periodic statistics data suitable for processing in the SIEM system.

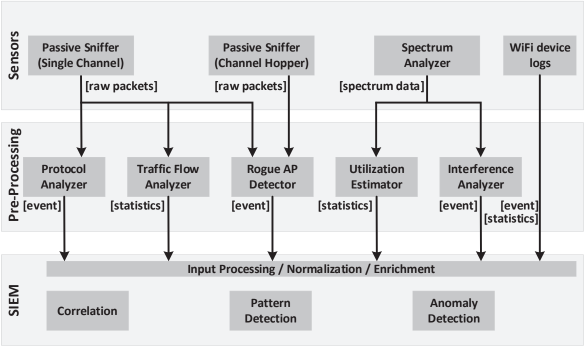

Figure 1. Architecture Overview

The SIEM system developed within the GLACIER project is designed to handle arbitrary security and operational data. For the wireless OT network scenario, the sensors listed in Table 1 are used to gather spectrum samples, raw Wi-Fi data frames, and log data from Wi-Fi device. The Wi-Fi device log data (list of available APs for clients and associations and (de-)authentication events for APs) can be directly processed by the SIEM layer, i.e. do not require any pre-processing.

TABLE I. Current Sensors and data streams

Sensor	Pre-processed Data
Spectrum Analyzer	Event: interfering pattern detected Periodic: channel utilization (%)
Passive Sniffer	Event: rogue AP detected Event: protocol violation detected (e.g. backoff cheating) Periodic: data flows (pos, src, dest, count, size) Periodic: channel utilization (%)
Access Point	Event: client association and client (de-) authentication
Client	Periodic: list of available APs (with signal strength)

Sensor and pre-processing components are logically separated and can be placed on the same or different physical devices. Different implementations of each sensor type are supported, e.g. a passive sniffer comes in two versions - a sniffer that is bound to a single Wi-Fi channel and monitors all packets, and a channel-hopper that periodically switches between different channels and delivers only a sample of all packets. This separation has been designed to allow to trade accuracy against implementation costs. While a channel-hopper is sufficient for rogue AP detection (a scan across all available channels takes several seconds) it cannot reliably report channel utilization and thus detect saturation attacks. Sensors on all relevant channels, in turn, result in significantly higher costs.

A sensor module can feed its data to multiple pre-processing modules. Data from a spectrum analyzer, for instance, is fed to the Utilization Estimator (estimates utilization of a wireless channel over time) and the Interference Analyzer (detects non-Wi-Fi devices). Again, this is designed to allow to trade accuracy against costs. A spectrum analyzer with sufficient resolution to detect non-Wi-Fi devices costs significantly more than one sufficient to analyze channel utilization. Furthermore, the interference analysis requires very fast signal processing power and therefore cannot be implemented on low-power embedded devices or can run on the AP itself. Similar, a passive sniffer feeds the raw packet data to multiple modules to detect various protocol violations and to calculate the periodic traffic flow statistics.

All pre-processed data is then fed into the SIEM system that can perform attack and anomaly detection from a global perspective.

B. *Spectrum Analyzers*

There are a number of commercial spectrum analyzers available that provide precise detection of non-Wi-Fi devices out-of-the-box. All of them come with a high price tag that makes them unsuitable for use as distributed long-term sensors.

Two low-cost solutions have been used within the project. First, RF Explorer [9], a small portable device that allows to perform periodic scans across a configurable frequency band, and second, the spectral scan feature supported by various Atheros Wi-Fi cards.

The RF Explorer provides a frequency resolution of 1 kHz and a time resolution of about 3ms, i.e. delivers about 350 raw data samples per second for further analysis. This is sufficient to estimate the channel utilization on a single Wi-Fi channel with high and across multiple channels with moderate accuracy. But it is insufficient to identify non-Wi-Fi devices directly. By correlating channel utilization with data flow information from passive sniffers it is at least possible to detect that Wi-Fi transmission is impeded by noise or non-Wi-Fi devices.

With the Atheros Wi-Fi card spectral scan feature it is possible to detect non-Wi-Fi devices directly. An implementation of this detection is provided by the proprietary AirShark software [10].

C. *Passive Sniffer*

Passive sniffing is supported by a wide range of Wi-Fi cards on any major operating system. Within the GLACIER project, a Python-based solution using the Scapy packet manipulation framework [11] has been implemented that can be run on embedded Linux devices such as the Raspberry Pi. It supports traffic flow analysis, rogue AP detection and protocol analysis for Wi-Fi management frames.

For rogue AP detection and traffic flow analysis, a second sensor has been implemented on an ESP8266 micro controller. It is very cheap but limited to the 2.4GHz band and not suited to perform advanced analysis.

D. *Clients and Access Points*

For Linux or Windows-based clients, the list of visible APs with their respective signal strength is periodically gathered using build-in mechanism of the different operating systems. No custom software or system modifications is required which makes adoption in industrial environments easier.

E. *SIEM and Anomaly Detection*

For the GLACIER SIEM system, only the functions relevant for the detection of low-level wireless attacks will be discussed here.

First, the SIEM systems maintains an inventory of legitimate devices, i.e. devices that are detected from various log data and approved by a SIEM operator to belong to the monitored infrastructure. The existence of a device is assumed if it is the source of log data, the source or destination of a data flow or listed in some statistics data. From this inventory, the SIEM system can then identify and alert any new and potentially malicious devices or devices that are inactive for a certain time.

Second, the SIEM system can correlate events from different log sources by normalizing them onto a common set of well-defined fields that have the same semantic independent of the log source. As the SIEM system uses ElasticSearch as its primary log storage and search engine, events are normalized using the Elastic Common Schema [13]. The normalized events can then be analyzed for pre-defined patterns to detect suspicious activities.

Third and most important, the SIEM system is able to determine and describe in a human-readable way the typical behavior, more specifically the values of parameter combinations that describe the behavior of individual system components and typical communication patterns between them. From this baseline, it will detect deviations and alert suspicious activities that can be investigated by humans or mitigated automatically. For this, it performs a multi-dimensional aggregation of parameters from normalized events for a defined time frame and evaluates the evolution of the aggregated values over time.

In the following it is described, how different attacks discussed in this paper can be detected.

Rogue APs, interfering devices, or protocol violations can be directly detected from events generated by sensors and corresponding pre-processing modules. Roque APs can furthermore be detected using the device inventory and logs from clients and passive sniffers that report on any AP detected.

If only a simple spectrum analyzer is available, i.e. one without the possibility to detect interfering devices directly, the channel utilization estimated by the spectrum analyzer can be correlated with the channel utilization estimated by a passive sniffer. Both should change similarly. But if only the channel utilization estimated by the passive sniffer decreases, i.e. fewer data is transmitted, but the channel utilization estimated by the spectrum analyzer stays the same, it can be assumed that the wireless channel is blocked by an interfering device or any other source of noise.

Rogue APs and other attacks like evil twins, man-in-the-middle or cheating on the backoff timing can also be detected using the anomaly detecting algorithm that uses the multi-dimensional data aggregation. For example, using the traffic flow data provided by the passive sniffers: {*Sniffer ID, Source MAC, Destination MAC, packet count*} and an aggregation of the *packet count* data individually per *Sniffer ID*, *Source MAC* and *Destination MAC*, different attacks cause detectable changes in these metrics. In case of additional noise, a reduction of the packet count for each aggregation can be noticed and roughly located, using the location of the passive sniffer. A rogue AP will create a new set of metrics for the MAC address used by the AP and the amount of traffic to and from other APs will decrease. Even if we have an evil twin that uses the same MAC address as the original AP and does not change the communication behavior, it will be detected if it is not located very near to the original AP because placing it in a different location (e.g. just outside the window of a factory building) will cause a change in the aggregated data per *Sniffer ID*.

Other parameter combination and metrics such as number of clients per AP or passive sniffer and signal strength per *Sniffer ID* and *Source MAC* extend detection capabilities even further as hardware (especially antenna) characteristics will now be included in the anomaly detection as well. It should be noted that using signal strength measurements comes with an important disadvantage. Even in an industrial environment that is well suited for the used anomaly detection algorithm because the network and system structure is mostly stable, the signal strength will vary due to changes in the physical environment (e.g. moving people, vehicles, machines) and technical properties of the devices used (e.g. power saving features). Depending on the environment, this can cause a significant rate of false-positive alerts or reduce the detection sensitivity. The main reason for this is, that a wide range of parameter values will be recognized as normal (baseline) behavior.

V. Future work

Currently, the SIEM system of GLACIER can only work on the data and knowledge gathered in a given environment and a given set of sensors/preprocessors. Future work will investigate options to retain knowledge about dependencies and correlations between sources. The primary goal is to allow substituting sources with cheaper versions of the same kind or completely different sources, e.g. replace a high-resolutions spectrum analyzer by a cheaper low-resolution version or even by utilizing signal strength information in captured packets and packet flow characteristics (throughput and latency). It will be investigated if it is possible to calibrate the detection algorithms in a given environment using high-precision sensors and later run with cheaper versions and if it is possible to reuse a model obtained in one factory environment in a similar or different one.

Acknowledgment

The authors give thanks to the BMBF for the financial support as well as all other partners involved in the research project GLACIER for their great collaboration. The project consists of the industrial partners rt-solutions.de GmbH, DECOIT® GmbH, and the research partner University of Applied Sciences and Arts of Hanover with the security group Trust@HSH. A special appreciation goes to the associated partner hanseWasser GmbH for its support and the possibility of prototype testing in their OT infrastructure.

References

[1] Grünert, Lars und Goran Sejdic (2017). Industrie 4.0-getriebene Geschäftsmodellinnovationen im Maschinenbau am Beispiel von TRUMPF. In: *Betriebswirtschaftliche Aspekte von Industrie 4.0*. Hrsg. von Mischa Seiter, Lars Grünert und Sebastian Berlin. Wiesbaden: Springer Fachmedien Wiesbaden, S. 29–45. ISBN: 978-3-658-18487-2

[2] Promotorengruppe Kommunikation der Forschungsunion Wirtschaft - Wissenschaft (2013). Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0: *Abschlussbericht des Arbeitskreises Industrie 4.0*. Hrsg. von Henning Kagermann, Wolfgang Wahlster und Johannes Helbig

[3] Gungor und Hancke (2009). Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches. *IEEE Transactions on Industrial Electronics*, Vol. 56, No. 10. October 2009.

[4] Zou, Zhu, Wang and Hanzo (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. In: *Proceedings of the IEEE* Vol. 104, No. 9. September 2016.

[5] Ehrlich, Trsek and Jasperneite (2018). Automatische Evaluierung von Anforderungen bezüglich der Informationssicherheit für das zukünftige industrielle Netzwerkmanagement. In: *Echtzeit und Sicherheit*, S. 49-58.

[6] GLACIER Project Website. Accessed on: Sep. 2, 2020. [Online]. Available: https://www.glacier-project.de

[7] Rong, Lee and Choi (2006). Detecting Stations Cheating on Backoff Rules in 802.11 Networks Using Sequential Analysis. *Proceedings of IEEE INFOCOM*. April 2006

[8] Mallesham Dasari (2017). Real time detection of MAC layer DoS attacks in IEEE 802.11 wireless networks. *Processings of 14th IEEE Annual Consumer Communications & Networking Conference*. January 2017.

[9] RF Explorer Vendor Website. Accessed on: Sep. 2, 2020. [Online]. Available: https://www.rf-explorer.com

[10] Rayanchu, Patro and Banerjee (2011). Airshark: detecting non-WiFi RF devices using commodity WiFi hardware. *Proceedings of the 2011 ACM SIGCOMM Internet measurement conference.* November 2011.

[11] Scapy Project Website. Accessed on: Sep. 2, 2020. [Online]. Available: https://scapy.net/

[12] Rong, Lee and Choi. Detecting Stations Cheating on Backoff Rules in 802.11 Networks Using Sequential Analysis. *Proceedings of INFOCOM 2006. 25th IEEE International Conference on Computer Communications*. April 2006.

[13] Elastic Common Schema (ECS) Reference. Accessed on: Sep. 3, 2020. [Online]. Available: https://www.elastic.co/guide/en/ecs/current/index.html