IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/45ICT/2025/4531525/
Vol. 2025 (21), Article ID 4531525

Identification of characteristics of Rouge Access Point based on SNMP and SYSLOG protocols*

Piotr AUGUSTYNIAK, Miłosz NIERBIŃSKI and Piotr ZWIERZYKOWSKI

Institute of Communication and Computer Networks, Faculty of Computing and Telecommunications, Poznań University of Technology, Poznan, Poland

Correspondence should be addressed to: Piotr AUGUSTYNIAK, piotr.augustyniak@doctorate.put.poznan.pl

* Presented at the 45th IBIMA International Conference, 25-26 June 2025, Cordoba, Spain

Abstract

The paper analyzes the vulnerabilities of Wi-Fi networks, particularly highlighting the dangers posed by public wireless networks. It focuses on two specific attack types: Evil Twin and Rogue Access Point (AP), which are presented as practical and serious threats to network security. The study explores the detection of these attacks through the analysis of logs generated by SNMP and SYSLOG protocols, emphasizing the importance of correlating events over time rather than relying on isolated incidents. Experimental research was conducted in a test environment where various attacks were simulated. The results showed that monitoring and identifying unauthorized access points is possible through careful analysis of SNMP and SYSLOG data. The study revealed that single events, such as device disconnections or deauthentication frames, are not enough to identify threats. Instead, a temporal correlation of these logs provides a clearer indication of an attack in progress. During the setup and experimentation, several technical challenges were encountered, including issues with device configuration and software stability. These difficulties contributed to a deeper understanding of cybersecurity, Linux system administration, and vulnerabilities in Layers 2 and 3 of the OSI model. The research concludes that Rogue AP and Evil Twin attacks, despite being well-known, continue to be relevant threats, particularly in poorly secured networks. Therefore, effective defense requires not only advanced monitoring tools but also proper training and awareness for network administrators and users. The analysis presented in the paper is based on experience gained in a real network.

Keywords: Rogue Access Point, wireless LAN, SNMP, SYSLOG, MITM (Man in the Middle), WLAN Security

Introduction

The contemporary development of information and communication technologies, and the Internet in particular, has a significant impact on the functioning of both society and individuals. Solutions providing elastic access to network resources play an important role in this process. A key role in this process is played by wireless (WLAN) and mobile networks, which have become an integral part of everyday life due to their flexibility and mobility. However, the increase in popularity of these technologies brings with it new challenges in terms of cyber security.

In this paper we address the issue of security in wireless local area networks (WLANs). There are many threats in such networks, such as weak authentication, lack of proper encryption or vulnerabilities due to device configuration errors. One less common but significant threat is attacks using foreign access points, such as Rogue Access Point or Evil Twin, which can lead to the interception of sensitive data and other serious incidents [1,2].

Cite this Article as: Piotr AUGUSTYNIAK, Miłosz NIERBIŃSKI and Piotr ZWIERZYKOWSKI, Vol. 2025 (21) "Identification of characteristics of Rouge Access Point based on SNMP and SYSLOG protocols" Communications of International Proceedings, Vol. 2025 (21), Article ID 4531525, https://doi.org/10.5171/2025.4531525

Recognizing and identifying foreign access points can be a challenge for many network administrators. This paper presents the possibilities of using SNMP (*Simple Network Management Protocol*) and SYSLOG (*System Logging Protocol*) protocols to detect abnormal events. In combination, the two protocols offer a set of tools to monitor key network parameters, detect abnormal events and identify potential threats. The work aims to both analyze the effectiveness of these tools and develop methods that can be applied in real network environments. Lessons learnt from the paper will help to improve security in wireless networks, which is crucial in the face of today's challenges and threats. The research presented here is part of a broader effort to develop methods for analyzing or monitoring network traffic, which will allow us to detect the presence of unauthorized access points at an early stage.

The article consists of 5 sections. Section two presents an introduction to the issues of monitoring wireless local area networks, with particular emphasis on SNMP and SYSLOG protocols. Section three is devoted to the problem of detecting hostile access points. Section four presents the research environment, methodology and results of the conducted research and discussion of the results. The work concludes with a brief summary highlighting the practical significance of the presented research.

Monitoring wireless local area networks

Network monitoring is one of the key aspects for ensuring the security of IT infrastructure. Wireless networks, due to their open characteristics, require special attention in terms of monitoring. A process that allows early detection of threats or anomalies in network traffic, but also ensures its smooth operation [3]. Effective monitoring of wireless networks involves several critical fields of operation. The first is the control of the operation of devices within it. This includes both user end devices and access points. This ensures that if a new device is present on the network, monitoring will allow it to be investigated quickly, dramatically reducing the chance of malicious devices such as unauthorised access points. Another important aspect is to examine the performance of our infrastructure, gaining insight into metrics such as packet loss, reordering or duplication, transmission delay or jitter. By examining performance, we have a direct insight into the parameters that describe the performance of our network. If we find anomalies, we can quickly take remedial steps. An equally important aspect of monitoring is having full visibility of the infrastructure in order to quickly identify malfunctions if necessary. For example, the occurrence of a failure in one area can significantly affect the performance of another section of the network, or an entire service. It also reduces the complexity of dealing with possible problems by quickly identifying the area where they occur [4,5].

Main advantages of WLAN monitoring

Network problems can significantly disrupt infrastructure operations, especially in distributed and complex environments, nevertheless the use of network monitoring can significantly improve the quality of service provided, here are the most important ones:

- *Early detection of threats and incidents*. Threats to the network will not always occur regardless of its level of security, so it is crucial to put in place tools to address them as soon as possible and thus ensure that the possible impact of such incidents is minimized.
- *Ensuring business continuity*. Monitoring the network by enabling administrators to respond quickly to incidents helps to ensure the continuity of network operations.
- *Documenting and reporting in line with engineering best practice and company policy*. There are rules to be followed in computer networks. Monitoring enables documentation and reporting that can provide future proof that the network meets the imposed requirements and, for example, avoid potential financial penalties.
- *Performance optimisation*. Monitoring makes it possible to observe individual parts of the network, and this makes it possible to identify low-performance elements.
- *Improved network security*. By monitoring and detecting threats on the network, sensitive data and users are significantly less vulnerable to the effects of potential attacks such as data loss, devices being taken over or privacy breaches. Systematic analysis of network traffic also enables rapid response to unusual events, identification of the source of the problem and minimisation of the risks associated with ransomware, phishing or unauthorised access attacks. These measures are reflected in increased stability and trust in the network infrastructure

SNMP and SYSLOG protocols

With the increasing complexity and compilation of today's networks, consisting of a variety of devices such as routers, switches, servers, access points, IoT devices and monitoring systems, managing network infrastructures is becoming an increasingly difficult task. The necessity to monitor the status of devices and ensure that they are operating optimally can be a challenge. The Simple Network Management Protocol (SNMP) can be used for this

purpose, which allows administrators to monitor the status of network devices, collect data on their performance and remotely manage their configuration [5]. A diagram of how the SNMP protocol works is shown in Fig.1.

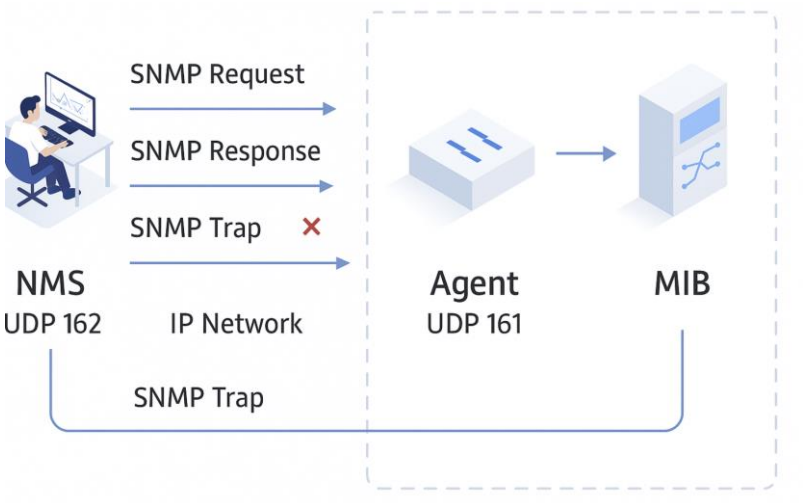

Figure 1. Functional diagram of SNMP

System Logging Protocol (Syslog), is a protocol designed to centrally collect and monitor logs from network devices . Hence, it plays a key role in the management of complex network infrastructures, including WLANs. More specifically, it allows structured diagnostic and operational information to be sent from devices such as routers, switches or access points to a central server. It is notable that, despite the lack of an initial formal specification, syslog has been widely adopted as a standard, demonstrating its practical importance and usefulness in managing network infrastructure. A diagram of how SYSLOG works is shown in Fig.2.

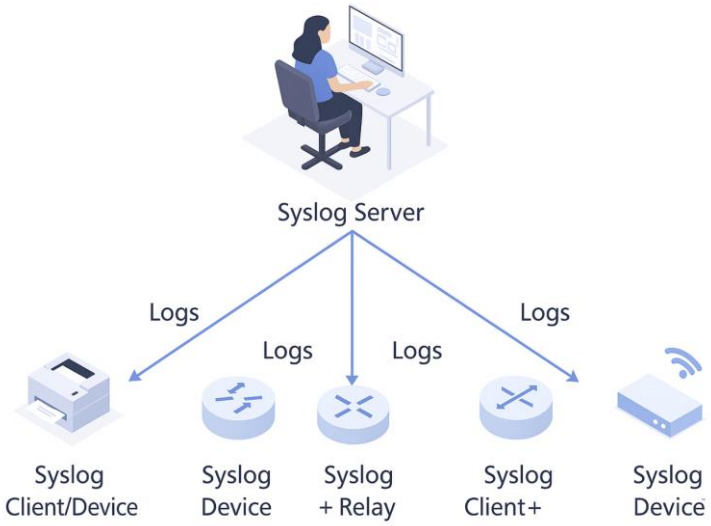

Figure 2. Syslog operation diagram

The SNMP and syslog are protocols that are commonly used in the area of network monitoring and maintenance. They work completely differently, therefore it is useful to understand the differences between them in order to determine which protocol best suits the needs of our network and to consider the prospect of using them both at the same time.

SNMP is used to capture and organize information about devices on the network, such as performance metrics and configuration data in a central management system. Syslog is used to record and store messages that have been created and sent by devices on the network for troubleshooting and analysis. Syslog focuses on collecting information and analysing data to troubleshoot network problems, while SNMP is mainly used to monitor devices and manage their configuration [7].

The SNMP and syslog protocols should not be seen as competitors, or judged within the framework of which one is better/worse. Their simultaneous use will provide us with a definite increase in the effectiveness of network

monitoring and analysis, while also raising the level of network security. Nevertheless, the choice of a particular solution or the aforementioned combination of them should depend on the nature of the wireless network to be monitored, its infrastructure, its users and their requirements, and the goals of the organization in which it is located.

Detection of foreign access points

An Alien Access Point is a network device that acts as a Wi-Fi access point that functions within a specific network infrastructure, but is not authorized with it in any way. The key element to defining an access point as a foreign, fake or unauthorized access point is the network administrator's lack of permission for it to operate on the network, making it a potential security risk.

The literature distinguishes several types of foreign access points depending on their installation method, intent or threat potential:

- *Evil Twin* also referred to more commonly as SoftAP or Spoofed AP. Represents a malicious device created to intercept network traffic. The following types of Evil Twin can be distinguished:
    - Co-existing with a legitimate AP or Evil Twin operating in parallel with a legitimate AP, passing user traffic through the right AP.
    - Replacing the legitimate AP or Evil Twin takes over the function of the legitimate AP, disconnecting it from the network and acting in its place
    - Co-existing with a legitimate AP, that is, an Evil Twin operating in parallel with a legitimate AP, but not passing user traffic through the right AP.
- *Improperly Configured AP* (Improperly Configured AP). These types of APs are not created as a result of malicious activity, but are created as a result of mistakes by administrators. Despite the lack of malicious intent, they can become a security vulnerability and allow an attacker to access an organization's resources.
- *Unauthorized AP* (Unauthorized Access Point). These access points are installed by employees or end users without the knowledge or consent of the administrator. Often their installation may be aimed at improving their own network convenience, but lack of oversight can make such a device a security risk. They are characterized by a physical connection in a wired network [8].

A foreign Access Point can be identified by a set of characteristics, which will be divided into those necessary, without which the Access Point will not be classified as foreign, and those that are not necessary but are important.

Conditions necessary in the identification of a foreign AP

Several cases of identification can be distinguished:

- *Unauthorized device in the network*. The access point operates on the network without the administrator's knowledge or consent, making it a potential security risk. It is not registered with network management systems such as SNMP, syslog, or WLAN central controllers, which are used to monitor and manage network infrastructure. The device's lack of presence in these management systems is a key feature and one of the primary criteria for identifying a foreign access point.
- *Unauthorized MAC address*. The MAC address of a foreign AP should not be in the list of trusted devices. In addition, often these devices may additionally use (MAC spoofing), that is, MAC address spoofing techniques to impersonate other APs or use them to dynamically change the MAC address to avoid detection.
- *Connection to the organization's internal network*. Foreign Access Points can be physically connected to an organization's network infrastructure, allowing traffic to pass between devices. Such connections can act as bridges for unauthorized traffic, increasing the risk of data interception or attacks on internal systems.

Characteristics not necessary but important in identifying a foreign AP

Several cases of identification can be distinguished:

- *Uncommon SSID*. One of the frequently used of tactics, at the same time a common feature of a foreign Access Point, is to give SSIDs inviting each other to connect, for example, “Free Wi-Fi,” or to set the same SSID as an already existing AP, which significantly misleads users.

- *Unusual behavior in network traffic*. Undoubtedly, analysis of network traffic can reveal anomalies indicating the presence of a foreign Access Point, such as sending deauthorization frames, sudden jumps in the amount of information sent, or abnormally high traffic volumes.
- *Improved signal strength*. An attacker, when carrying out an attack, will often choose to increase the signal strength which is also a feature that can make it easier to identify such an AP.

Rogue AP and Evil Twin attacks

Rogue AP and Evil Twin are two different but equally significant threats to wireless networks. The former can result from both user ignorance and intentional action by attackers, while the latter is a pre-planned malicious attack. The key difference is the purpose and intentionality of these actions, which translates into different detection and countermeasure strategies. Implementation of advanced monitoring tools and user education are the cornerstones in protecting wireless networks from such threats.

Use of SNMP and SYSLOG protocols for practical identification of attacks

The test environment was designed to analyze attacks on wireless networks, such as Rogue AP and Evil Twin, and their detection capabilities using syslog and SNMP protocols. The test environment consisted of :

- Linksys WRT54GL router with Fresh Tomato software version 2024.5 freshtomato-K26MIPSR1RT - 2024.5: supports syslog and SNMP monitoring and features to log client activity events.
- Linksys WAP54GL router with dd-wrt software: supports syslog and SNMP monitoring with limited network statistics analysis capabilities.
- ParrotOS computer. It runs a Syslog server - rsyslog, which is installed by default in ParrotOS - and uses tools such as Wireshark to capture network traffic.
- Client devices. An iPhone 15 smartphone and a Lenovo ThinkPad laptop that simulate typical network user traffic.
- Network card in monitoring mode. The same card as in the earlier analysis was used, namely ALFA AWUS036ACH. Used for Deauthentication attacks and Layer 2 traffic analysis.

The environment was set up in a controlled environment, with client devices connecting to one of two access points. For testing, Rogue AP and Evil Twin attacks were orchestrated, simulating scenarios in which a client could be tricked into connecting to an unauthorized access point.

The research considers the following scenario. We assume that a user unknowingly connects to Evil Twin In this scenario, a user using a mobile device is within range of both an authorized access point and a fake AP (Evil Twin). After the attacker sends deauthorization frames, the device automatically tries to reconnect to the network. Because of the stronger Evil Twin signal, the device connects to the fake AP.

Phase 1: Connect the customer to the authorized access point

Initially, for an attack opportunity to occur, the device must connect to a real access point.

Syslog:

Jan 26 03:32:45 router DHCPREQUEST for 192.168.1.101 from 8A:C8:71:41:0F:54 via br0

The client (MAC: 8A:C8:71:41:0F:54) sends a DHCPREQUEST request to obtain an IP address (Fig. 3). The request is directed to the br0 (bridge) network interface, which handles communication between clients on the local network.

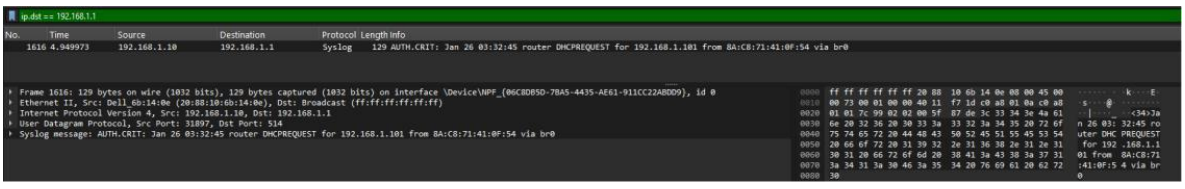

Figure 3. The process of sending a DHCPREQUEST request

Jan 26 03:32:46 router DHCPOFFER for 192.168.1.101 to 8A:C8:71:41:0F:54 via br0

The router assigns an IP address (192.168.1.101) to the client with the MAC address 8A:C8:71:41:0F:54 (Fig. 4). The DHCPOFFER message is part of the DHCP protocol in which the server informs the client that the requested address is available. The process takes place over the br0 interface, which acts as a network bridge.

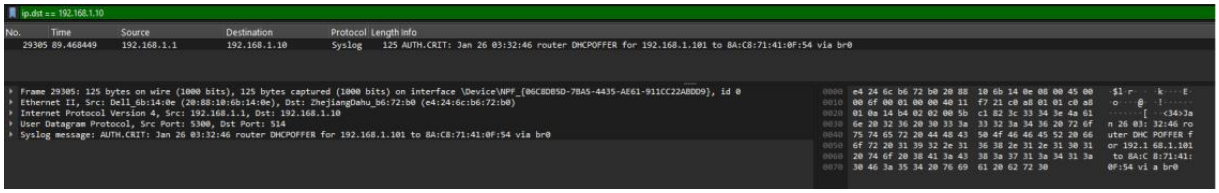

Figure 4. The process of assigning an IP address in response to DHCPREQUEST

Jan 26 03:32:47 router wlan0: WPA handshake completed for client 8A:C8:71:41:0F:54

WPA authentication successful (Fig. 5). The client with MAC address 8A:C8:71:41:0F:54 has undergone the Wi-Fi Protected Access (WPA) protocol handshake process, which has confirmed its identity and established an encrypted connection to the access point via the wlan0 interface (Fig 5). The handshake process involves the exchange of security keys, which ensures the integrity and confidentiality of data transmissions over a Wi-Fi network.

Figure 5. Completion of the WPA handshake for the client

SNMP:

SNMPv2-MIB::sysUpTime.0 = Timeticks: (183056) 0:30:30.56

The router's operating time is 183056 ticks of the system clock, which corresponds to 30 minutes and 30.56 seconds (Fig. 6). This value is measured since the last time the device was started and represents an indicator of the stability and continuity of the router. It is one of the key variables monitored with SNMP and is useful in analysing the device's status and reliability [1].

Figure 6. Device operating time indicator in system clock ticks

IF-MIB::ifInOctets.1 = Counter32: 174864823

The received data over the interface is 174864823 bytes. This value is stored as a 32-bit counter (Counter32), which records the total amount of data received by the network interface since the router was started (Fig. 7). Monitoring this variable allows analysis of incoming traffic and detection of potential anomalies, such as spikes in data transmission that may indicate an attack or network congestion.

[1] The system clock tick is the smallest unit of time measured by the device's system clock, corresponding to a specific time interval, e.g. 1/100th of a second, depending on the system implementation.

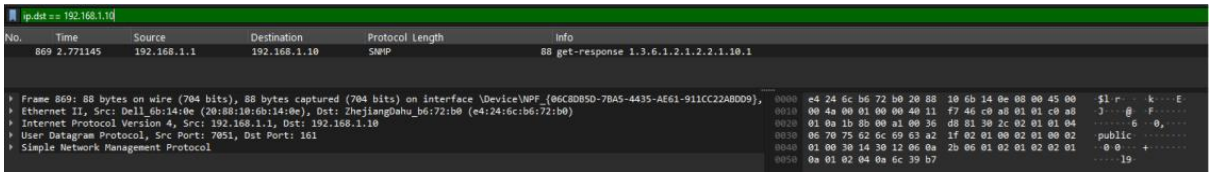

Figure 7. Number of bytes received by the network interface

IF-MIB::ifOutOctets.1 = Counter32: 674825485

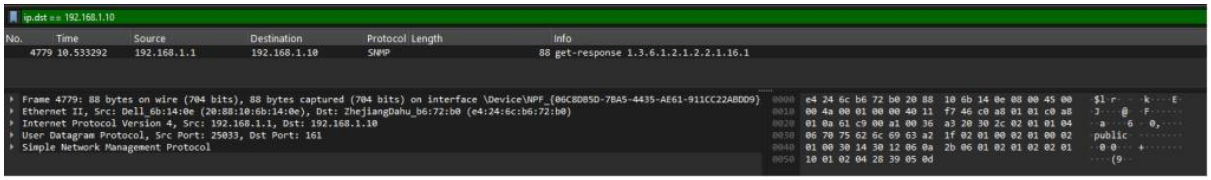

Figure 8. Number of bytes sent over the network interface

The data sent over the interface is 674825485 bytes. This value, stored as a 32-bit counter (Counter32), represents the total amount of data sent over the network interface since the router was started (Fig. 8). Analysis of this counter is useful in detecting potential congestion or abnormal outgoing traffic patterns, which may indicate, for example, the transmission of large files or the operation of malware.

SNMPv2-SMI::enterprises.9.9.315.1.2.2.1.8.1 = INTEGER: 2,
where:

- SNMPv2-SMI is a standard prefix specifying that the variable is from the MIB database for the SNMP v2 protocol,
- *enterprises.9.9.315 : namespace for Cisco devices and the specific variables that occur in them,*
- *1.2.2.1.8.1 : a location in the MIB structure indicating the number of active clients for a particular interface.*

The number of active clients is 2. This value represents the current number of devices connected to the access point via a given interface (Fig. 9). Monitoring this variable allows the network load to be monitored in real time, as well as detecting potential anomalies such as a sharp drop in the number of clients (e.g. due to a deauthorisation attack) or an abnormal increase (e.g. indicating unauthorised connections to the network).
Monitoring this variable allows the analysis of network load and the detection of changes that may indicate an anomaly, such as customers being disconnected as a result of a deauthorisation attack.

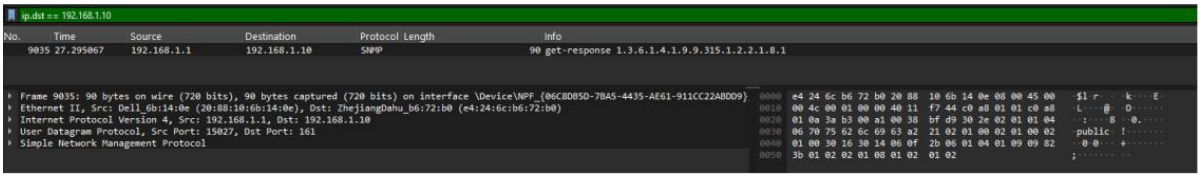

Figure 9. Number of active clients connected to the access point

Phase 2: Deauthorisation of the client by the attacke

A deauthorisation attack is launched on the client device using “aireplay-ng”.

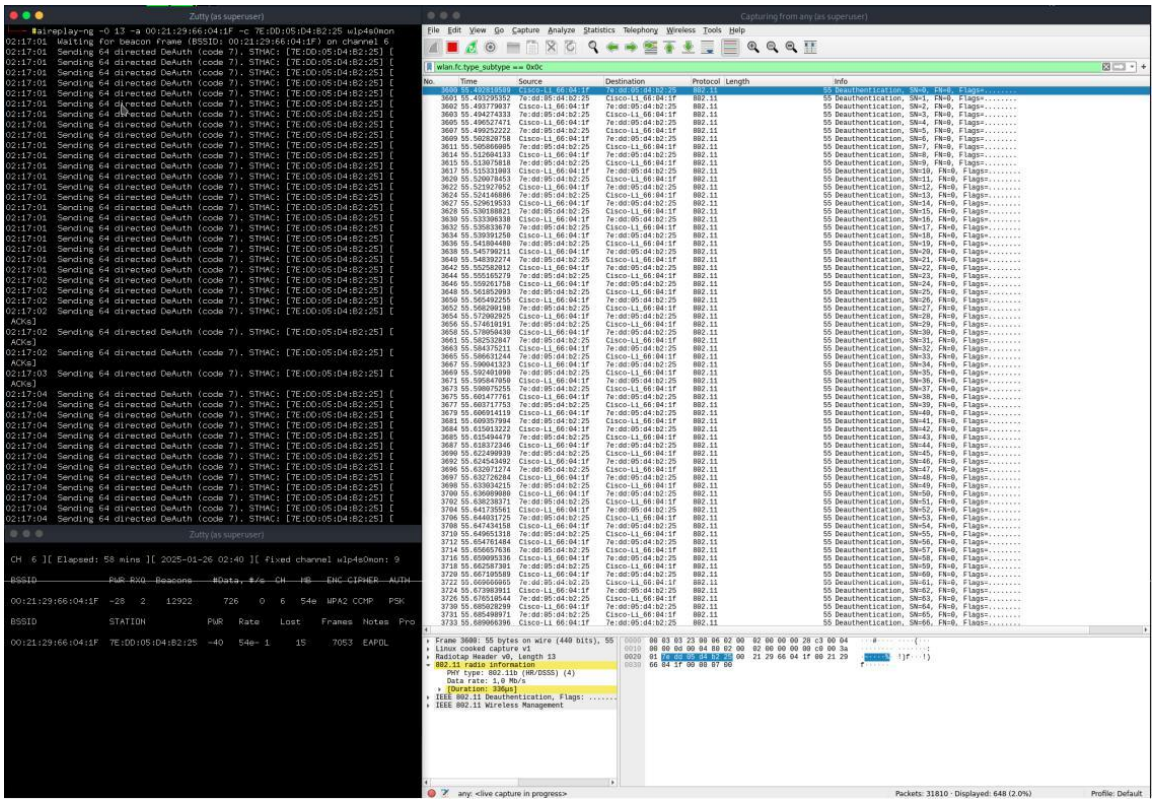

Figure 10. A screenshot from Wireshark showing the deauthorisation frames sent during the attack

Figure 10 shows: Frame type: Deauthentication (code 12), MAC address of the access point (Source), MAC address of the client (Destination), Number of deauthentication frames sent: 64 and Protocol: IEEE 802.11 Management.

The attacker sent a large number of deauthorisation frames in a short period of time, as shown in Figure 10, which had the effect of forcing the client to disconnect from the access point.

Syslog:

Jan 26 03:50:12 router wlan0: client disconnected (MAC: 8A:C8:71:41:0F:54)

The client with MAC address 8A:C8:71:41:0F:54 has been disconnected from the network (Fig. 11). This event can be the result of a number of reasons, such as client inactivity, device shutdown, change of access point (roaming) or a deliberate action such as a deauthentication attack. Monitoring these types of logs allows for quick identification of potential problems in the network, including possible Layer 2 attacks.

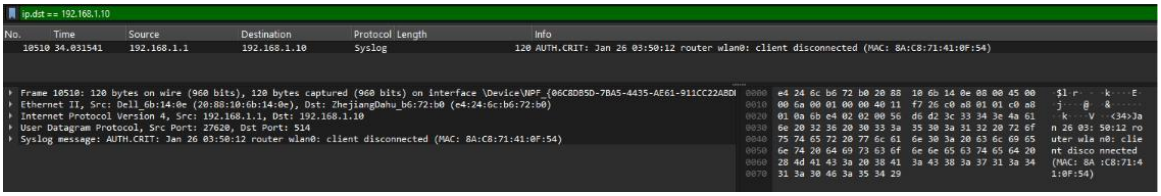

Figure 11. Client disconnection event with MAC address 8A:C8:71:41:0F:54 from wlan0 interface

SNMP:

SNMPv2-SMI::enterprises.9.9.315.1.2.2.1.8.1 = INTEGER: 1

The number of active clients has decreased to 1 (Fig. 12).

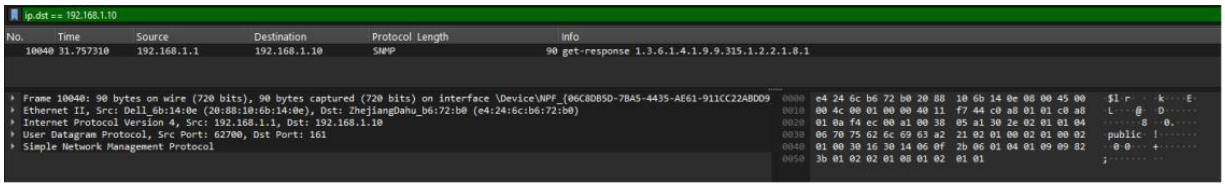

Figure 12: Reducing the number of active clients to 1

IF-MIB::ifInDiscards.1 indicates the number of packets correctly received, but discarded by the network interface (e.g. due to full buffers or filtering policies). This increase may be a sign of network congestion or a potential attack.

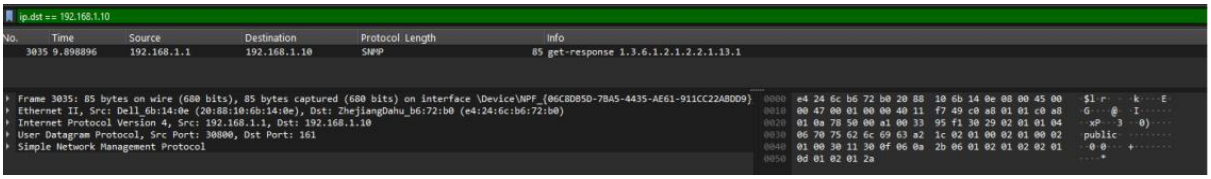

Figure 13: Number of correctly received but discarded packets on the network interface

The conducted tests made it possible to assess the effectiveness of wireless network monitoring using the syslog and SNMP protocols in the context of detecting Rogue AP and Evil Twin attacks (Fig. 13). One of the key conclusions from the analysis of the tests is the need for temporal integration of data from both protocols. Individual events logged in logs, while relevant, may not provide sufficient information to uniquely identify a potential attack.

Deauthentication frames can occur in a network as a natural part of its operation. For example, normal changes to access points (roaming) or signal disruptions may lead to the generation of such frames unrelated to attacker activity. Therefore, the mere detection of Deauth frames in monitored traffic cannot be considered clear evidence of an attack. By similarly, an event such as the disconnection of a client from an access point, which is recorded as “client disconnected” in the syslog logs, may result from user actions (e.g. switching off a device, leaving network coverage) or from natural changes in the network environment. Also, a decrease in the number of active clients in the SNMP logs, as recorded in the enterprises.9.9.315.1.2.2.1.8.1 variable, may be the result of normal network dynamics and not necessarily the result of an attack.

In order to effectively detect Rogue AP or Evil Twin attacks, it is crucial to analyse events recorded in both protocols at the same time. Time integration of the data provides a more complete picture of the network situation. For example, in a deauthorisation attack scenario, syslog can record deauthorisation frames sent at short intervals, indicating potential attack activity. At the same time, SNMP may record a decrease in the number of active clients and an increase in the number of dropped packets. Then, after a short period of time, the syslog can register disconnection with access point, which, in combination with the previous data, makes it clear that an attack may have occurred.

Only the correlation of these events, occurring in close time frames, allows the precise identification of malicious activity in the network. The mere detection of one of these elements, such as Deauth frames, without correlation with other events, could lead to false alarms. Thus, the integration of syslog and SNMP data, together with their time synchronisation, provides the foundation for effective security monitoring and analysis in wireless networks [9, 10].

Summary

An analysis of the vulnerabilities of Wi-Fi networks has shown that these technologies are exposed to a variety of threats, particularly in public wireless networks. An attempt was made to justify the selection of the Evil Twin

and Rogue AP attacks as representative examples of threats that pose real challenges to network security in practice.

This paper presents the ability to detect Rogue Access Point and Evil Twin attacks based on data generated by SNMP and SYSLOG. The paper focuses on the practical use of syslog and SNMP logs, emphasizing the importance of temporal integration of events as a key element in identifying threats.

In the research conducted, a number of experiments were carried out in a test environment, which confirmed the effectiveness of network monitoring and identification of foreign access points. The analysis of SYSLOG and SNMP logs made it possible to demonstrate that the integration of data from both protocols over time is a key element in identifying attacks. Single events, such as deauthorization frames, a reduction in the number of active clients or a disconnection of a device, are not sufficient to clearly identify a threat. Only the correlation of these data allows precise analysis and identification of potential attacks.

During the preparation of the test environment and the conduct of the research itself, many technical challenges were encountered, including difficulties related to the configuration of network devices and the stability of the software used. This allowed the authors to significantly expand their knowledge of cybersecurity, GNU/Linux configuration, and Layer 2 and Layer 3 vulnerabilities of the OSI model.

Analyzing the research, one can conclude that although Rogue AP and Evil Twin attacks have been known for many years, they still remain a real threat, especially in networks with a low level of security. An important part of protecting networks is not only implementing advanced monitoring mechanisms, but also educating administrators and users on ecurity best practices.

Acknowledgments

The authors thank the Polish Ministry of Education and Science for financial support (Applied Doctorate Program, No. DWD/6/0058/2022). This research was funded in part by the Polish Ministry of Science and Higher Education (No. 0313/SBAD/1311).

References

- P. Augustyniak, P. Zwierzykowski and O. Rogowicz: *"Concept and Phases of the Rogue Access Point Attack*" [in]: Artificial Intelligence and Machine Learning. 43rd IBIMA Conference, IBIMA-AI 2024, Madrid, Spain, June 26–27, 2024, Revised Selected Papers, Part-I , ed. Khalid S. Soliman - Cham, Switzerland: Springer Nature Switzerland, 2025 - s. 290-303
- P. Augustyniak, P. Zwierzykowski and O. Rogowicz: "*Theoretical and Practical Aspects of the Evil Twin Attack. The Attacker's Perspective and Defense Methodology"* [in] Artificial intelligence and Machine Learning. 41st IBIMA International Conference, IBIMA-AI 2023, Granada, Spain, June 26–27, 2023, Revised Selected Papers, ed. Khalid S. Soliman - Cham, Switzerland : Springer Nature Switzerland AG, 2024 - s. 224-236
- Adam Smutnicki. *Bezpieczeństwo sieci Wi-Fi* (cz. 1 i 2). Sekurak, https://sekurak.pl/bezpieczenstwo-sieci-wi-fi-czesc-1/ (Access 16th of April 2025)
- *Co to jest Monitorowanie sieci?,* nFlo, https://nflo.pl/slownik/monitorowanie-sieci/ (Access 16th of Aprlil 2025)
- *Monitors and Alerting*. DATADOG, https://docs.datadoghq.com/monitors (Access 16th of April 2025).
- G. Howard. *SNMP vs syslog*: *Which one should you choose*?, https://www.fs.com/de-en/blog/snmp-vs-syslog-which-one-should-you-choose-2255.html (Access 16th of April 2025).
- Bit Flip: *SNMP vs. Syslog. What's the Difference?*, https://thisvsthat.io/snmp-vs-syslog (Access 16th of April 2025).
- R. Gerhards: *The Syslog Protocol,* IETF, https://datatracker.ietf.org/doc/html/rfc5424 (Access 16th of April 2025).
- Jan Rześny. Netflow i syslog – jak połączyć obie technologie, aby uzyskać pełniejszy obraz infrastruktury it. Passus, https://www.passus.com/webinarium/netflow-i-syslog-jak-polaczyc-obie-technologie-aby-uzyskac-pelniejszy-obraz-infrastruktury-it/ , (access 16th of April 2025).
- Teletopix. Co to jest syslog i dlaczego się go używa? Teletopix, https://teletopix.org/pl/co-to-jest-syslog-i-dlaczego-sie-go-uzywa/#gsc.tab=0 (access 16th of April 2025)