Overview of Wireless Connection Security Standards in Company's Digital Infrastructure and Their Weaknesses

Roman Veynberg [1][0000-0001-8021-5738], Oleg Litvishko [1][0000-0002-2722-5109], and Dmitry Pisarev [2]

[1] Plekhanov Russian University of Economics,
36 Stremyanny lane, Moscow, 115998, Russia
veynberg@gmail.com, Litvishko.OV@rea.ru
[2] University of Warwick, Coventry CV4 7AL, United Kingdom
d.pisarev@warwick.ac.uk

Abstract. With the growth of wireless Wi-Fi traffic, detecting known and unknown attacks in networks remain challenging. Machine learning algorithms and neural networks support efficient tools for traffic analysis and intrusion detection. However, there are limited studies that compare the performance capabilities of these techniques for detecting attacks in networks of the 802.11 family of standards. There are several basic authentication standards for wireless networks. Each of them has its own advantages and disadvantages. Each has its own, rather complex, principle of operation. A large number of auxiliary diagrams and screenshots of the D-Link Airplane XtremeG Wireless Utility with the necessary settings are typical. The article discusses the main security problems of Wi-Fi wireless networks based on the 802.11 family of standards. Known vulnerabilities and possible methods of parrying them are given. The wireless networks of the IEEE 802.11 family of standards have more than 20 years' history of development and are widespread everywhere from homes to enterprise environments today. In this article, the architecture, an organization of communications and embedded security mechanisms of wireless networks will be discussed.

Keywords: wireless intrusion detection, Wi-Fi, decision tree, artificial neural network, machine learning.

1. Introduction

Human activity through the interaction of various devices across networks in everyday life increases daily. Most devices today can connect to the Internet and the number of connected appliances will reach 20.4 billion by 2020 (Gartner, 2019). The world is becoming more connected and with this comes a continuous increase in the amount of information exchanged between these devices.

Wireless technologies are attractive in the Internet era because they simplify connections and reduce the cost of devices. According to Cisco (2016), Wi-Fi and mobile traffic will grow 12% by 2021 from 2016 and will be 63% of all IP traffic. The dependence of humanity on this technology continues to grow, and by the end of 2018, the number of public access points will reach 340 million, which is seven times more than 2014 (Omar et al., 2016). The first standard of the Wi-Fi family,

Proceedings of the 10th International Scientific and Practical Conference named after A. I. Kitov "Information Technologies and Mathematical Methods in Economics and Management (IT&MM-2020)", October 15-16, 2020, Moscow, Russia

known as the IEEE 802.11, was released in 1997 and was followed with many amendments as it maintained the basis for wireless network products.

Wireless networks also attract criminals as new intrusion techniques and attack vectors develop rapidly. Since the first version of the standard, developers-built security mechanisms to provide confidentiality of communications for all nodes in a Wireless Local Area Network (WLAN). The first attempt to implement Wired Equivalent Protection (WEP) was nearly immediately recognized as vulnerable to attacks, which threatened the confidentiality of the transmitted information. Subsequent development of protective mechanisms increased the ability to cope with threats and developers focused on the confidentiality and availability of wireless networks during attacks. However, the growth of computer processing power and ease of availability of software designed to assist with hacking help even low-skilled attackers perform attacks.

Wireless Intrusion Detection Systems (WIDS) are an integral part of modern security for wireless networks. These systems cope with the threats 24/7 and consider the human factor. Moreover, intruders can plan their actions to pass through WIDS exploiting human weaknesses (Martellini et al., 2017). For example, attackers can provoke a WIDS to generate alerts for a long time so that it appears as a common event to those monitoring the system, such as the case of the 22-hour unavailability of eBay due to the attack "when the IDS system constantly alarmed, but everyone was too busy to answer" (Cherry, 2000).

Nevertheless, WIDS has become one of the most effective tools allowing a quick response to threats. These systems combine different approaches to the analysis of traffic and data, including machine learning techniques. The application of machine learning in WIDS grew rapidly because the algorithms help to automate detection of attacks and malicious behavior in networks using clustering (Shamshirband et al., 2014), attack classification (Thing, 2017) or anomaly-based detection (Usha and Kavitha, 2017). Along with conventional algorithms, such as Random Forest or AdaBoost, Artificial Neural Networks (ANN) also show great performance in the analysis of traffic flow (Al-Jarrah et al., 2015).

This article helps to do overview of wireless connection security standards in company's digital infrastructure (WIDS) and find most common weaknesses to prevent cyber-attacks.

2. Literature review

Some researchers tried to explore conventional Machine Learning (ML) and ANN techniques for detecting attacks in networks [1-8, 15-20]. For example, Buczak and Guven (2016) conducted an overview of both approaches arguing the methods can be implemented for wired and wireless networks. However, this comparison includes several limitations (9-11). First, wired networks have a different architecture than wireless such that wireless networks are more vulnerable because it is easier to gain access to a node for attacks. Second, attacks exist that exploit the vulnerabilities of specific wireless standards. Third, protection of Wi-Fi networks is a challenge for defenders due to specific limitations, such as the variety of devices, limited bandwidth, the poor performance of endpoints, and mobility (Liao et al., 2012). Finally, the research does not provide practical experiments and performance evaluations [12-14].

The number of studies comparing ML and DL performance is limited, and existing methods have significant limitations [21-30]. First, some research uses datasets such as KDD that considered as obsolete (Sabhnani and Serpen, 2004). However, even recent studies continue to incorporate it for evaluating the performance of IDS (Dong and Wang, 2016). Second, many studies either consider conventional or ANN algorithms for WIDS [30-35]. However, both ML and ANN models must be tested on an identical sample of data to measure performance with the same preprocessing and normalization phases. While a few algorithms are less sensitive to data preprocessing, such as Decision Trees and Random Forests, most are sensitive to these phases. As a result, the metrics of algorithms with different preprocessing stages of data may differ (Raschka, 2015, Yin, D. and Cui, K., 2011).

3. Evolution of embedded security methodology of 802.11 standard

For more than 20 years, the standard has seen many versions and undergone many amendments. Some of them are focused on legislative complaints, others on technical improvements and on enhancing security [7-13]. Overview of Lashkari *et al.* (2009), Hiertz *et al.* (2010) and Noh, Kim and Cho (2018) were analyzed to identify the most significant enhancements of security mechanisms for the standards. Figure 1 presents an evolution of the security and significant improvements of the 802.11 family standards.

WEP. Security mechanisms have been built into wireless networks since the first version of the 802.11 standard [3,7,8,10, 25.35]. WEP was one of the first security mechanism that was developed by a group of volunteer IEEE members to prevent eavesdropping (confidentiality), unauthorized access to a wireless network (access control), and tampering with transmitted messages (data integrity). WEP uses two methods of authentication: Open System and Shared Keys, and provides the security by encryption through the RC4 algorithm.

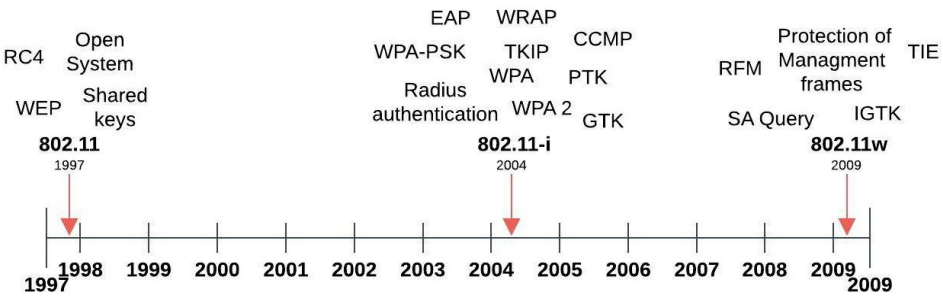

Fig. 1. Evolution and significant improvements of 802.11 family standards

WEP mechanism has many fundamental weaknesses. First, it has problems in the RC-4 algorithm because uses RC4 improperly and keys can be brute-forced. Second, it allows an attacker to modify a message undetectably without knowing the encryption keys. Third, it uses weak key management and updating key mechanism

and cannot prevent attacks such as reply attack and the forging of authentication messages [8]. As a result, WEP was recognized as being unsecured [16,19,20].

WPA. The Institute of Electrical and Electronics Engineers and Wi-Fi Alliance tried to develop more robust and secure mechanism for wireless networks and Wi-Fi Protected Access (WPA) was introduced in 2004 to fix the serious security weaknesses of WEP. The main improvements are providing a stronger encryption process such as Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES). WPA was adopted for enterprise security and supports Extensible Authentication Protocol (EAP) and a Radius server for user authentication, access control and management. The WPA-PSK was developed as an adaptation of the mechanism for home users because WPA depends on Radius as the authentication server. WPA-PSK is a simplified mechanism of the original WPA and it is based on a passphrase as a pre-shared key as will be presented in Figure 7.

WPA was designed to fix the vulnerabilities of WEP. However, weaknesses of WPA have been discovered by many researchers. Moskowitz (2003) demonstrated the weaknesses of WPA against a dictionary attack in November 2003. Tews and Beck (2009) proposed a successful attack on WPA. They used the implementation of WPA with support of IEEE 802.1e Quality of Service (QoS) features. During this attack, a plain text from the encrypted message was recovered in 15 minutes.

WPA2. The draft of the IEEE 802.11i was revealed in 2004, and it was finally published as the IEEE 802.11-2007 standard in 2007 (Society and Committee, 2007). The specification is the next generation of IEEE 802.11 and frequently referred to as WPA2. The basic mechanisms for generating keys and efforts which were used to protect traffic confidentiality and integrity will be discussed below.

Generating a key in WPA2 specification is a hierarchical structure. The initialization of the primary key depends on the authentication method. The authorization method can be based on a PSK if the pre-shared key is used as the authentication method.

As can be seen from Figure 2, STA generates a PSK using Password-Based Key Derivation function 2 (PBKDF2). The next step is generating PMK from PSK. A fresh PTK is composed of three parts: Key Confirmation Key (KCK), Key Encryption Key (KEK) and Temporal Key (TK) that are used to protect unicast traffic from AP and STA.

The 802.11i standard defines the Master Session Key (MSK) as the top-level key if WLAN uses the 802.11X family standard for authorization. The active version of the 802.1X-2010 standard is different from PSK authentication and involves the following parties in the authentication process: a supplicant is a STA that wants to connect to a WLAN, an authenticator device is an AP and authentication server such as Radius [6]. The standard uses the Extensible Authentication Protocol over an IEEE 802 Local Area Network (EAPOL) as the authentication framework PTK is composed of an EAPOL-Key Key Confirmation Key (KCK), EAPOL-Key Encryption Key (KEK) and a TK.

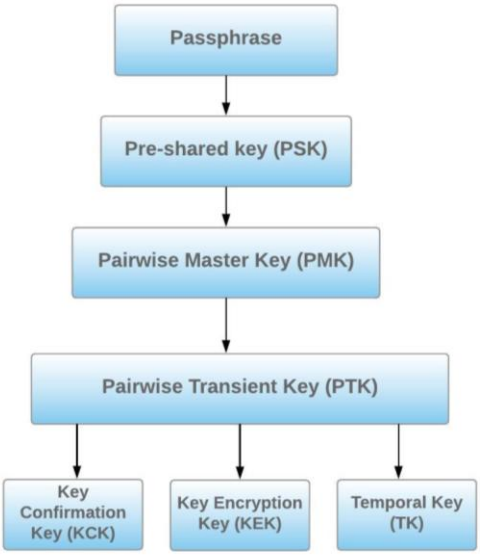

Fig. 2. WPA2-PSK key hierarch

WPA2 provides traffic confidentiality and integrity through the support of three protocols: Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol (CCMP), Wireless Robust Authenticated Protocol (WRAP) and Temporal Key Integrity Protocol (TKIP).

CCMP uses the Advanced Encryption Standard (AES) algorithm as the basis for encrypting data. It splits data into 128-bit pieces and encrypts them using a key of the same size. TKIP and WEP are based on RC4, but the main difference between TKIP and WEP is the centralized management of packet integrity, which is performed at the AES level. WRAP can be used instead of CCMP as the encryption method and is considered more secure because it is based on the Offset Codebook (OCB) mode of AES [7]. However, the OCB mode is listed as an optional method of 802.11i because of licensing issues.

WPA2 provides a robust and secure approach for wireless networks and solves several security issues. Nevertheless, it is susceptible to Denial of Service (DoS) attacks during re-authentication and re-association phases (Tsitroulis, Lampoudis and Tsekleves, 2014). Li *et al.*, (2012) and Yin and Cui (2011) succeeded in efforts to enhance the security of WPA2, but at the same time, they have emphasized that growing computing capabilities make it much easier to exploit the vulnerabilities of the standard.

802.11w. The predecessors of the IEEE 802.11w standard focused on the confidentiality and integrity and paid little attention to the availability of wireless networks. Consequently, the security mechanisms of wireless networks were vulnerable to DDoS attacks, because management frames remained unprotected. In 2009, the IEEE 802.11w-2009 (IEEE, 2009) standard was approved focusing on these issues. The Robust Management Frames (RMF) mechanism of the standard

provide cryptographic protection of Deauthentification, Disassociation and Action frames.
A new PTK was presented in the WPA2 mechanism and responsible for protecting unicast management frames. The new encryption key focusing on broadcast management frames was introduced in IEEE 802.11w, namely the Integrity Group Transient Key (IGTK). Moreover, the new the Security Association Query (SA Query) mechanism was implemented to defend from Association Request attacks. It generates SA Query Request and Response which corresponds between nodes and helps to verify the association procedure. The procedure is interrupted if the STA Query Response message is not recognized as valid by the AP.
Another significant improvement is the Timeout Information Element (TIE). The timer allows an AP to store a session if it receives another SA Request at the time of waiting for the response from an STA. The AP expects to wait for a response from the STA for a certain time and does not respond to requests from third-party clients.
Nevertheless, the final improvement in the wireless security mechanism is not free from vulnerabilities. For example, an attacker can create a successful DDoS attack by sending Deauthentication frames repeatedly and preventing the association between the AP and STA during the handshake phase [15]. Moreover, the 802.11w standard is vulnerable to malicious radio frequency (RF) broadcasts which has been known for many years [2].
In summary, these results show that even the final implementation of the 802.11 standards has vulnerabilities. Before proceeding to examine wireless security, it is necessary to give an overview of existing attacks on 802.11 networks.

4. Results: building security architecture and communication lines within WIDS

The wireless networks are based on the final revision of the standard (IEEE Std 802.11 -2016, 2016) and use the following radio frequencies 2.4 GHz, 3650 MHz, 4.9 GHz, 5 GHz, 5.9 GHz, 60 GHz. The most common frequency is 2.4 GHz that can be distinguish into 11-14 channels depending on the region [1].
The networks can be organized into two modes: The Infrastructure and Ad-Hoc modes. As can be seen from Figure 3, Client Stations (STA) communicate through an organizational device, namely the Access Point (AP) in the infrastructure mode. A group of stations using the same radio frequency is known as a Basic Service Set (BSS) that can be interconnected via a Distribution System (DS) into an Extended Service Set (ESS). Wireless Local Area Network (WLAN) systems are defined as systems that include the DS and one or more APs.
The Ad Hoc mode is a term used as a general description of an Independent Basic Service Set (IBSS). IBSS forms peer-to-peer connections between STAs within their range and does not rely on APs.

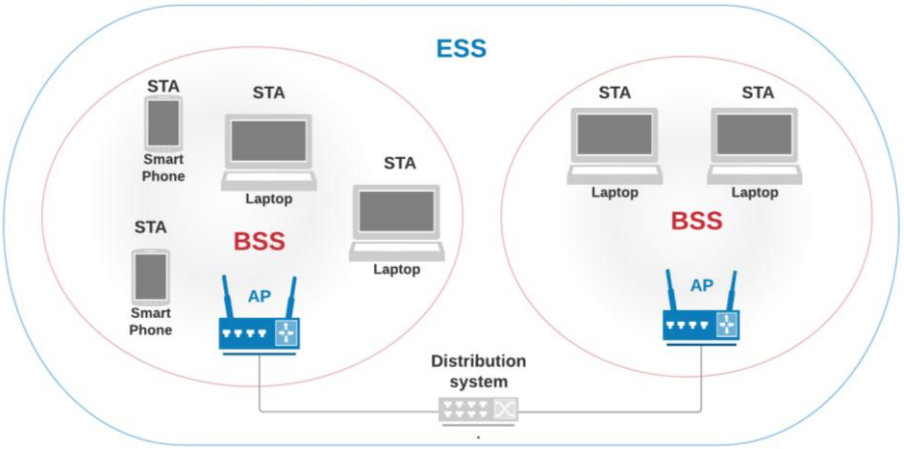

Fig. 3. Architecture of an infrastructure mode of the 802.11 standard

These two modes have different traffic behavior and vulnerabilities. This research is focused on the description of the architecture and security issues of the infrastructure mode. A brief overview of communications is provided below. The communication structure of the Wi-Fi can be described in the context of Open Standards Interconnect (OSI) seven-layer communications model (ISO/IEC 7498-1, 1994).

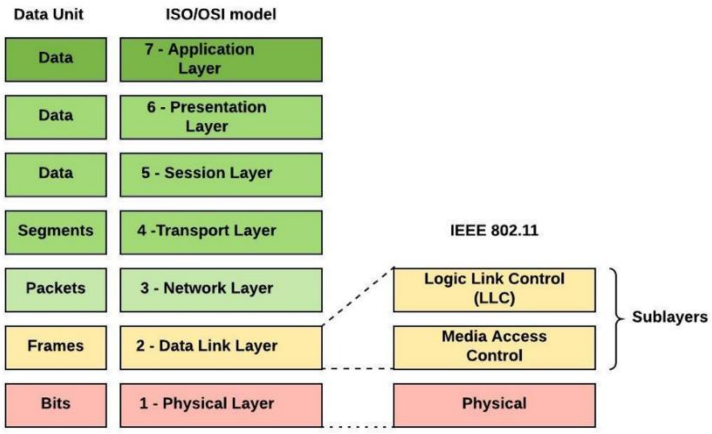

Fig. 4. Mapping of IEEE 802 layers to ISO/OSI reference model

As can be seen from Figure 4, standards in the IEEE project 802.11 target two layers: Physical (PHY) and Data Link layers. The PHY layer specifies modulation, coding techniques and responsible for media and signal transmission. The Data Link Layer is divided into two sublayers: Logic Link Control (LLC) and Media Access Control (MAC). The LLC sublayer receives information form layers 3 to 7 and

transfers to MAC sublayer. MAC sublayer is responsible to add information from second layer such as source, destination and BSS.
As shown in Figure 4, frames are basic transfer units of Data Link Layer. The family of IEEE 802.11 standards has different types of frames. Figure 5 presents a generic data frame. Data frames have the same structure consisting of a header, the frame body, and Frame Check Sequence (FCS) but, depending on the specific type, some of the fields may not be used [4]. Data frames are divided into management, control and data sections and each of them fulfils a different purpose and specify transmission of data as well as management and control of wireless links.

Fig. 5. Generic data frame

Management frames are responsible for establishing and retaining connections between an AP and client devices. Management frames have different subtypes such as Authentication, Deauthentication, Association request, Reassociation response, Disassociation, Beacon, Probe request, Probe response. For instance, beacon frames are responsible for announcing the presence of APs and their capabilities such as transmission rates and optionally other data like used channel and applied security mechanisms. Beacon frames include information about the network such as the Service Set Identification (SSID), which defines the name of the network. Access points send beacon frames every few milliseconds when they have a network to offer. The timing of beacon frames must be defined by APs for the entire BSS. The STA sends a deauthentication frame to another STA or an AP to terminate the connections. A deauthentication frame is one-way communication and must be accepted.
Figure 6 demonstrates the establishment of communication through a search for the available networks by sending probe requests. The client can explicitly request the network to which it wants to connect or send 0 bytes as SSID which is also known as Broadcast SSID. The AP is answered by a probe response packet.

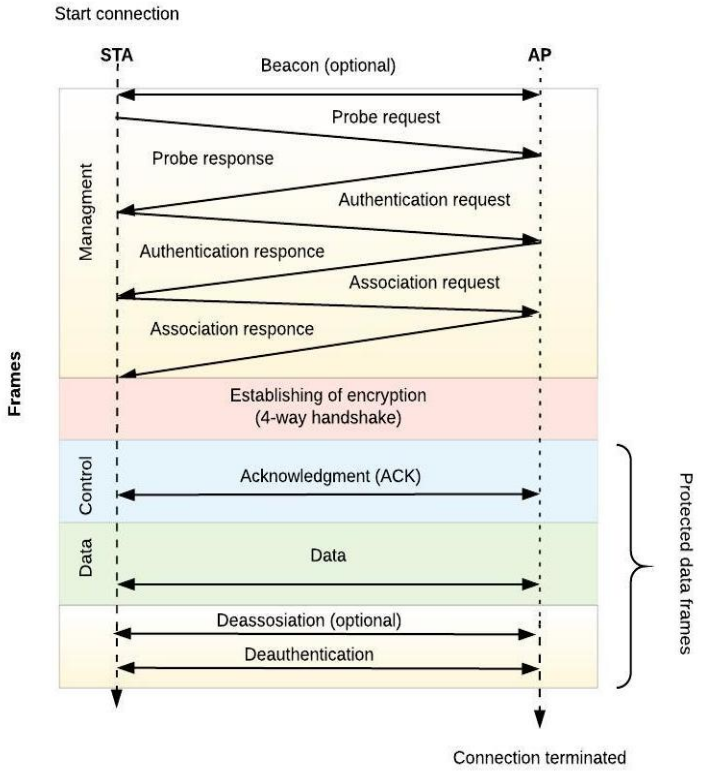

Fig. 6. Frame exchange between two parties using 802.11i
(frame exchanges of 4-way handshake (WPA-PSK) is shown simplified)

After this packet is received, the client sends an authentication request which must be answered by authentication response. The client sends an association request if the previous exchange of authentication packet was successful and waits for association response. The next step is the handshake and it depends on the security mechanism chosen for establishing connections.

Figure 7 demonstrates a successful four-way handshake using a Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) as an example. A Pre-Shared Network Key (PSK) is used to start communication it can be in the range from 8 to 63 ASCII characters. A Pairwise Master Key (PMK) is generated based on the combination of the pre-shared key and the SSID of the network. The STA and AP negotiate a temporary Pairwise Transient Key (PTK). These temporary keys are dynamically generated each time the client connects based on MAC addresses and they exchange random numbers of A-nonce from the access point and S-nonce from the STA side. This helps to ensure uniqueness and non-repeatability of the keys.

The AP checks the PMK from the STA using the Message Integrity Code (MIC) which is a cryptographic hash of the packet [35]. It helps to prevent tampering because if MIC is not valid that means that PTK and PMK are also not correct as PTK is obtained from PMK. Other security features of 802.11 standards will be discussed in more detail later.

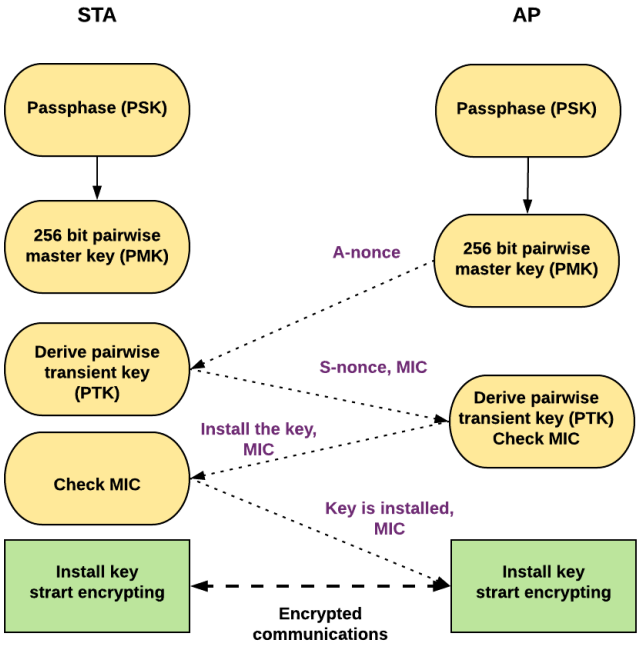

Fig. 7. Four-way WPA-PSK handshake

Control frames assist and coordinate the delivery of data from clients to APs. They have one the of the following subtypes: Request to Send (RTS), Clear to Send (CTS), Acknowledgment (ACK) and Power-Save Poll (PS-Poll). RTS and CTS are optional data frames, that help to reduce frame collisions, which are introduced by the hidden node problem because it requests permission to occupy the channel before data transfer [12]. For example, a STA sends a RTS packet with an integrated duration header and other STAs reply by CTS packets, that they are willing to stop sending packets until the time lasts specified in the duration header. ACK data frames are responsible for error-checking process.
Data frames are used to carry actual information from other layers after communication is established. They can be categorized according to function. For example, basic data frames are used for delivery and receiving data but null data frames care no payload such as information about the sleep state of devices.

5. Discussion

With the growth of wireless Wi-Fi traffic, detecting known and unknown attacks in networks remain challenging. Machine learning algorithms and neural networks support efficient tools for traffic analysis and intrusion detection. However, there are limited studies that compare the performance capabilities of these techniques for detecting attacks in networks of the 802.11 family of standards. There are several basic authentication standards for wireless networks. Each of them has its own advantages and disadvantages. Each has its own, rather complex, principle of

operation. A large number of auxiliary diagrams and screenshots of the D-Link Airplane XtremeG Wireless Utility with the necessary settings are typical. In the article the authors tried to show evolution and common weaknesses of well-known security standards and through that provide more secured architecture and communication lines within popular WIDS.

6. Conclusion

The article discusses the main security problems of Wi-Fi wireless networks based on the 802.11 family of standards. Known vulnerabilities and possible methods of parrying them are given. The wireless networks of the IEEE 802.11 family of standards have more than 20 years' history of development and are widespread everywhere from homes to enterprise environments today. In this article, the architecture, an organization of communications and embedded security mechanisms of wireless networks are discussed. The main purpose of this article is to provide and create secured architecture and help specialists to avoid leaks of data, in time do updates and prevent black holes in security 802.11 standards.

7. Acknowledgments

This article was funded as part of the internal grant under the name "Preparation of scientifically based proposals for the development of the Russian market of financial technologies and alternative money as an element of the country's innovative policy" by PRUE.

References

1. Ballmann, B.: 'Understanding Network Hacks - Attack and Defense with Python'. In: Uster, Switzerland (2015)
2. Bertka, B.: '802 .11w Security : DoS Attacks and Vulnerability Controls', *Infocom* (2012)
3. Crow, B.: 'IEEE 802.11 Wireless Local Area Networks', *IEEE Communications Magazine*, 35(9), pp. 116–126. doi: 10.1109/35.620533 (1997)
4. Dayong N, Mikhaylov A, Bratanovsky S, Shaikh Z.A., Stepanova D. (2020), Mathematical modeling of the technological processes of catering products production. Journal of Food Process Engineering, 43(2). https://doi.org/10.1111/jfpe.13340
5. Gast, M.: '802.11 Wireless Networks: The Definitive Guide, Second Edition', *OReilly Media*, pp. 1–656. Available at: http://portal.acm.org/citation.cfm?id=581813 (2005)
6. Hiertz, G.: 'The IEEE 802.11 universe', *IEEE Communications Magazine*, 48(1), pp. 62–70 (2010)
7. IEEE (2009) 'IEEE Std 1149.7-2009', *IEEE Std 1149.7-2009*, pp. 1–985. doi: 10.1109/IEEESTD.2010.5412866.
8. Jeffree, T., Congdon, P. and Seaman, M.: '802.1X-2010 IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control', *IEEE Std 802.1X-2010*, pp. 1–222 (2010)
9. Krovetz, T.: *The OCB Authenticated-Encryption Algorithm*. Available at: https://tools.ietf.org/html/rfc7253 (2014)

10. Kubat, M. (ed.). Cham: Springer International Publishing, pp. 91–111. doi: 10.1007/978-3-319-20010-1_5.
11. Lanze, F. *et al.* (2015) 'Hacker's toolbox: Detecting software-based 802.11 evil twin access points', in *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, pp. 225–232. doi: 10.1109/CCNC.2015.7157981.
12. Lee, W. and Stolfo, S. J. (2000) 'A framework for constructing features and models for intrusion detection systems', *ACM Transactions on Information and System Security*, 3(4), pp. 227–261. doi: 10.1145/382912.382914.
13. Legezo, D. (2016) *Research on unsecured Wi-Fi networks across the world*. Available at: https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/
14. (Accessed: 18 August 2018).
15. Liao, H.-J. *et al.* (2012) 'Intrusion detection system: A comprehensive review', *Journal of Network and Computer Applications*, 36, pp. 16–24. doi: 10.1016/j.jnca.2012.09.004.
16. Lin, F. and Cohen, W. W. (2010) 'Semi-supervised classification of network data using very few labels', in *Proceedings - 2010 International Conference on Advances in Social Network Analysis and Mining, ASONAM 2010*, pp. 192–199. doi: 10.1109/ASONAM.2010.19.
17. Lashkari, A.: 'A Survey on Wireless Security protocols (WEP , WPA and WPA2 / 802 . 11i)', *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, (Iv), pp. 48–52 (2009)
18. Li, Q.: 'Implementation and analysis of AES encryption on GPU', in Proceedings of the 14th IEEE International Conference on High Performance Computing and Communications, HPCC-2012 - 9th IEEE International Conference on Embedded Software and Systems, ICESS-2012, pp. 843–848 (2012)
19. Moskowitz, R.: *Weakness in Passphrase Choice in WPA Interface*. Available at: https://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html (2003)
20. Martellini, M. *et al.* (2017) *Information Security of Highly Critical Wireless Networks*. 1st edn. Springer Publishing Company, Incorporated, pp. 1–73. doi: 10.1007/978-3-319-52905-9
21. McAbee, S. T., Landis, R. S. and Burke, M. I. (2017) 'Inductive reasoning: The promise of big data', *Human Resource Management Review*, 27(2), pp. 277–290. doi: 10.1016/j.hrmr.2016.08.005.
22. Noh, J., Kim, J. and Cho, S.: 'Secure Authentication and Four-Way Handshake Scheme for Protected Individual Communication in Public Wi-Fi Networks', *IEEE Access*, 6, pp. 16539–16548 (2018)
23. Nyangarika, A., Mikhaylov, A. & Richter, U. (2019b). Oil Price Factors: Forecasting on the Base of Modified Auto-regressive Integrated Moving Average Model. International Journal of Energy Economics and Policy, 9(1), 149-160. https://doi.org/10.32479/ijeep.6812
24. Rahman, A. and Gburzynski, P.: 'Hidden problems with the hidden node problem', in *23rd Biennial Symposium on Communications*, pp. 271–273 (2006)
25. Sabhnani, M. and Serpen, G. (2004) 'Why machine learning algorithms fail in misuse detection on KDD intrusion detection data set', *Intelligent Data Analysis*, 8(4), pp. 403–415. doi: 10.1007/978-3-540-88623-5_41.
26. Scarfone, K. and Mell, P. (2007) 'Guide to Intrusion Detection and Prevention Systems (IDPS)', *National Institute of Standards and Technology*, 800–94(February), p. 127. doi: 10.6028/NIST.SP.800-94.
27. Scarfone, K. and Mell, P. (2012) 'Guide to Intrusion Detection and Prevention Systems (IDPS)', *National Institute of Standards and Technology*, 800–94(July), p. 111.

Available at: http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf. (Accessed: 17 August 2018).
28. Schmidhuber, J. (2015) 'Deep Learning in neural networks: An overview', *Neural Networks*, pp. 85–117. doi: 10.1016/j.neunet.2014.09.003.
29. Scikit-Learn (2018) *GridSearchCV*. Available at: http://scikit-learn.org/stable/modules/generated/sklearn.model_selection.GridSearchCV.html (Accessed: 17 August 2018).
30. Shamshirband, S. *et al.* (2014) 'D-FICCA: A density-based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks', *Measurement: Journal of the International Measurement Confederation*, 55, pp. 212–226. doi: 10.1016/j.measurement.2014.04.034.
31. Tews, E. and Beck, M.: 'Practical Attacks Against WEP and WPA', *Proceedings of the second ACM conference on Wireless network security*, pp. 79–85 (2009)
32. Tsitroulis, A., Lampoudis, D. and Tsekleves, E.: 'Exposing WPA2 Security Protocol Vulnerabilities', *International Journal of Information and Computer Security*, 6(1), p. 93 (2014)
33. Wang, W. and Wang, H.: 'Weakness in 802.11w and an improved mechanism on protection of management frame', in *2011 International Conference on Wireless Communications and Signal Processing, WCSP* (2011)
34. Wong, S.: 'The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards', *SANS Institute*, (October), pp. 1–9 (2003)
35. Yin, D. and Cui, K.: 'A research into the latent danger of WLAN', in *ICCSE 2011 - 6th International Conference on Computer Science and Education, Final Program and Proceedings*, pp. 1085–1090 (2011)