Évf. 5 szám 1 (2023): Bánki Közlemények/Bánki Reports Autumn (2023)

Tisztelt Olvasó!

A Bánki Közlemények 2023. évi 1. száma zömében a számítási intelligencia módszerein alapuló mé rendszerek gyakorlati alkalmazhatóságát bemutató tanulmányokat közöl, melyek az Óbudai Egyete Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán működő Fuzzy Rendszerek Tudományos Műhely támogatásával készültek.

A kötet a Magyar Fuzzy Társaság idei jubileumi éve előtt is tiszteleg, hiszen a társaság idén ünnepli fennállásának 25. évfordulóját. A Magyar Fuzzy Társaság a Neumann János Számítógép-tudományi Társaság szakosztályaként működik, érdeklődési köre magában foglalja mindazokat a diszciplináka amelyeket a „Soft Computing", „Intelligent Techniques", „Computational Intelligence" összefoglaló nevekkel illetnek. Működése így nem korlátozódik pusztán a fuzzy logikára és a fuzzy halmazok elméletére, hanem magában foglalja a fuzzy technológiákat, neurális hálózatokat, genetikus algoritmusokat, a bizonytalanság modellezését, hibrid rendszereket és ezek alkalmazásait is.

A lágy számítási módszerek méltán népszerűek a mérnöki feladatok megoldásában, hiszen képesek figyelembe venni és kezelni az adatokban és a kiértékelés folyamatában felmerülő bizonytalanságo pontatlanságot, szubjektivitást, valamint optimalizálási feladatokban és komplex rendszerek esetén hatékony megoldást nyújtanak. A kötet tanulmányainak sokszínűsége lehetőséget ad a fuzzy logika mesterséges neurális hálózatok szerteágazó alkalmazási lehetőségeinek bemutatására.

Bepillantást nyerhetünk az iparban alkalmazható neurális háló alapú minőségellenőrzés megvalósításába. Különböző eljárásokkal meghatározhatók a gyenge pontok, amiket célszerű vizsg tanulmány munkaállomásokat vizsgál az ajánlatkészítés, felmérés fázisától kezdve, a soron követke tervezési lépést, majd a gyártást és végezetül a szerelést is figyelembe véve.

Egy másik tanulmányban szintén a mesterséges neurális hálózati modellt alkalmazták a távközlési vállalattól elpártoló ügyfelek számának előrejelzésére. A lemorzsolódás okainak feltárása nagyon fo vállalat jövőbeli marketingdöntéseinek meghozatalában. Az így létrejövő ügyfél-besorolási modell pontossága növelhető az ügyféladatok kiegyensúlyozott halmazának képzésével.

Kriptográfia témakörében a kötet egy olyan tanulmányt közöl, ami a tudományterületen jól használ Python könyvtárakkal foglalkozik. Egy vállalati modellen keresztül szemlélteti, hogy az adatok hogya haladnak át a protokollon és hogyan dolgozzák fel azokat. A titkosítás során a gépi tanulás módszer dolgozik.

A kötetben megtalálható a mesterséges intelligencia orvosi alkalmazhatóságát bemutató tanulmán amely a legnagyobb hangsúlyt a hematológiában való alkalmazásra helyezi. Az ilyen algoritmusok többnyire nagyobb pontossággal és hatékonysággal rendelkeznek, mint amit az ember nyújtani tud tanulmányban bemutatott példa a vörösvértestek, fehérvérsejtek és vérlemezkék kimutatásával foglalkozik.

Egy optimalizálási probléma evolúciós algoritmussal történő megoldása is helyet kapott a kötetben feladat a klasszikus „Utazó ügynök” problémához hasonló útvonal optimalizációval foglalkozik. A viz feladat a Formula-1-es versenynaptár, illetve a nagydíj helyszínek földrajzi elhelyezkedésének koord alapján az optimális, vagyis a legrövidebb útvonal meghatározása.

A fuzzy megközelítés öntözőrendszerbeli alkalmazhatóságával foglalkozó tanulmány célja az ültetet növények vízigényének becslése, és a szükséges öntözési idő kiszámítása annak érdekében, hogy elérhető legyen a talaj ideális nedvességtartama, és ezzel a növények számára a megfelelő mennyis víz biztosítható legyen.

A szerkesztőség nevében hasznos olvasást kívánok!

Dr. habil Laufer Edit

Vendégszerkesztő

Megjelent: 2023-11-29

Technical Mathematics (Műszaki Matematika)

Cryptography and cryptographic packages in Python

Una Sredovic

PDF (English)

Technical Informatics (Műszaki Informatika)

Application of Artificial Intelligence in Medicine

Tatjana Muratović

PDF (English)

Marketing using artificial neural networks

Anja Stijepović

PDF (English)

A Formula-1-es versenynaptár optimalizációja genetikus algoritmus segítségével

Gabriella Polyak, Miklós Póth

PDF (English)

Fuzzy Rule-Based Investigation of System Reliability with Reliability Block Diagram Method

Hamid Ali Hama Salih

PDF (English)

Feladatmegoldókészség fuzzy szabálybázisú becslése

Vera Stein, László Pokorádi

PDF (English)

Előrejelzések készítése Fuzzy-Markov alapú idősor-elemzés alapján

László Hanka

PDF (English)

Öntözőrendszer vezérlés fuzzy logikával

Martin Tibor Hegedűs

PDF (English)

Safety Science (Biztonságtudomány)

Drónok okozta veszélyhelyzetek és balesetek valamint azok megelőzésének lehetőségei

Marton Balint

PDF (English)

Drónok használata terrorszervezetek által

Marton Balint

PDF (English)

Nyelv

Magyar

English

Bánki Közlemények - Bánki Reports (ISSN 2560-2810)

BÁNKI KÖZLEMÉNYEK
V. ÉVFOLYAM 1. SZÁM

Cryptography and cryptographic packets in Python

Una Sredović
University of Donja Gorica, Podgorica, Montenegro
una.sredovic@udg.edu.me

Abstract — **Nowadays, we usually mean that the information we receive/ send digitally is secure and that only those to whom we in- tended it and the person sending it have access. Cryptography deals with the ques- tions of how, why and by what methods data of any type flows. Algebra, combinatorics and probability are the mathematical branches on which data encryption and de- cryption are based. All information passes through the protocol under some key - sym- metric or asymmetric. Each of them has its own methods, which in turn have advantages or disadvantages, and are still used today, al-though they are constantly being developed and improved. Such an information exchange system is important for security. although at-tacks (or their types) have been detected and classified over time, constant caution against new "hacker" methods and variations is always necessary. Recently, the Python pro- gramming language has been widely used, for example in databases, where it is extremely important that data remains anonymous or circulates securely. In this regard, many packages have been developed that have facili- tated their encryption and are regularly up- dated. As artificial intelligence and machine learning develop in parallel, models are pro- duced that facilitate tracking and analysis without constant human monitoring, and one such example is the placement of products by a company from a foreign user to a user, based on some of his data.**

Keywords: Cryptography, Symmetric key, Asymmetric key, Python, Machine learning

1 INTRODUCTION

The modern age in which digital devices, both computers and mobile devices such as phones, tablets or smart watches, have developed, has contributed to the development of electronic communication. Such com- munication must be secure at all times, since the in- dividual does not have a visible path through which any message passes, but it is an abstract, digital path.Cryptography (a word of Greek origin, derived from the words kryptós- meaning “hidden” and graphein- mean- ing “to write”) is a science that deals with methods for forming and keeping information secret. Throughout history, even today, it has always been important to pass on information, that is, to turn it into a message. As we live in a digital age where artificial intelligence and robotics are evolving rapidly, we can get a machine that would construct or decrypt codes much faster and more efficiently than human. In order for a machine to function independently, machine learning is required. Machine learning is a set of algorithms whose model is used to analyse data based on previously processed information (usually based on images). It was first mentioned in the middle of the 20th century and has been constantly evolving since then. It is closely related to statistics, but also to other mathematical disciplines. As an extremely large amount of data flows in the process of cryptography or cryptanalysis, a person can easily lose and "waste" a lot of time, which for some more complex algorithms requires a machine, but for basic calculations and some already discovered methods, it is extremely easier for computer. Machine learning is important because it gives enterprises a view of trends in customer behavior and business operational patterns, as well as supports the development of new products. Many of today's leading companies, such as Facebook, Google and Uber, make machine learning a central part of their operations. Machine learning has become a significant competitive differentiator for many companies.

2 EVOLUTION

Before analysing cryptography in more detail, we will try to put together the development of encoding and decoding. Although they seem obvious and too sim- ple, the methods and ideas used by the Egyptians and the ancient Greeks are still used today. Some even be- lieve that thanks to them, Hitler and World War II were stopped. Today we distinguish three historical periods in the development of cryptography: ancient period (until 1918) - Caesar’s algorithm and Wisner’s code; technical period (from 1918 to 1975) - Playfair’s algorithm and Enigma; paradoxical period (since 1975)-AES and DES system [1].

Enigma: The forerunner of the Enigma was a device similar to today's rotor, which served for key generation. There was a recess in the machine that would turn and move the position of the letter each time the button was pressed. German scientist Arthur Scherbius set the initial conditions that were later upgraded since it would be repeated after the sixth rotation of the letters, which gave an insufficiently large number of combinations, ie 26*26*26 = 17576. Later it was developed to 10,000,000,000,000,000 combination, so it was accepted in the army and used during World War II rate. Enigma was developed in England, mostly thanks to Alan Turing and Marian Rejewski, who concluded that every German message must be encrypted twice at the beginning - and thus came across the first clue to decryption, after which it was much easier to reach other segments. With the help of 5 rotors, they managed to find out the keys that the Germans would send every day, and change exactly them at midnight.Adjusting the weights between neurons enables the learning ability of an artificial neuron.

Keys in cryptography

The function of copying a message into some incomprehensible text in order to maintain secrecy and the

basic message is called key. Based on the ideas of previous encryption methods, much larger keys are being formed today, for the simple reason that to- day there are more advanced machines that can count much faster than humans. Today, two types of keys are used: symmetric (same key used by both parties) and asymmetric key (two keys where each party uses a different one). An example we can find in everyday life is the activation key for Windows operating system.

If two people have the ability to exchange the key verbally or outside the communication channel, and then continue to exchange messages over the key agreed upon, the symmetric key can work. The main opera- tion used to generate such keys is XOR (exclusive or) which is the addition of two numbers per module 2. Let A be the message and B the key, then the value (A xor B) = M passes through the communication chan- nel, while the other part gets the original message by calculating M xor B. pseudo-random string generators are often used to form deterministic encryption algo- rithms, although such strings are similar to random strings. There are two types of symmetric key:

Block cipher With such code, the message is broken into several blocks/segments with the help of a key and it passes to its recipient. Some of the algorithms that use the symmetric key block code are AES, DES, IDEA, Blowfish, RC6, RC6.

Stream cipher Instead of being stored in memory, such codes are encrypted with a key during the pas- sage of the code through the communication channel. An example of a symmetric key flow code is the RC4 algorithm.

Since Alice and Bob do not always have the ability to exchange a key outside the communication chan- nel in the real world, symmetric keys are rarely used today. The above algorithms are mostly inapplicable, although some of their more advanced forms are used, such as 3DES). We may encounter these algorithms in some transactions, message authentication, or hashing.

Asymmetric keys were first mentioned in *IEEE Transactions on Information Theory* in 1976 as a discovery by Whitfield Diffie and Martin Hellman. There are twokeys to this algorithm - private and public. The pub- lic key is for encryption only, while the private key is used for decryption and is owned by anyone who wants to receive a message. Unlike the symmetric algorithm, there is no danger of "intercepting" the message, because in that case the attacker would have access onlyto the text that is encrypted under public key, and it is available to everyone. Three parameters are importantin this algorithm: The pair (K_p, K_s), where K_p is the public key and K_s is the private key; Enc encryption algorithm; Dec decryption.

Example 1: As an example, we can take prime p =21489151 (although p is not large enough in real life). We can pick an arbitrary g like g = 1609879. Then A picks x = 3916708 at random and com- putes X = gxmodp = 13164781 and sends it to A. Then B picks y = 16766518 at random and computes Y = gymodp = 4109137 and sends it to B. In paral- lel, B computes K = Xymodp = 13275737. A can also compute K = Y xmodp = 13275737 [2]

In order for such a code to be of good quality, it is necessary to form a large enough p, which is not at all simple. That is why the Euler function and the following theorem are important to us:

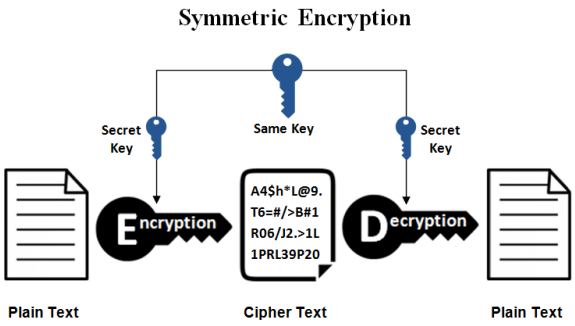
Theorem 1. Let a and b be nonzero integers. Then there exist integers r and s such that gcd(a, b) = ar +bs

and:

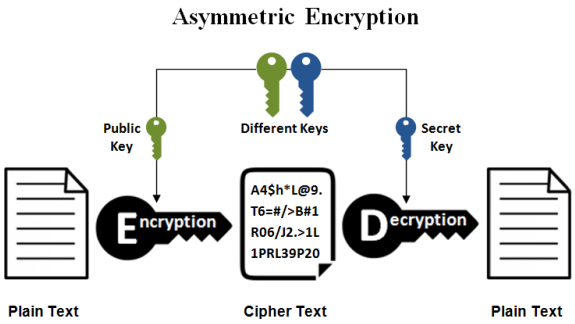
Corollary 1. Let a and b be two integers that are relatively prime. Then there exist integers r and s such that ar+bs = 1.

Definition 1. $\phi(n)$ is the number of non-negative integers less than n that are relatively prime to n. In other words, if n>1 then $\phi(n)$ is the number of elements in Un, and $\phi(1)=1$.

RSA model Let p and q be two prime numbers. Let n = pq and $\phi(n)$ = m = (p 1)(q 1) where ϕ is the Euler function. We are looking for a number E that is mutually prime with m (we need such an E to satisfy the gcd (E, m) = 1). By Euclidean algorithm we can get the number D, so that DE 1 modulo m. When we have calculated this, we publish the numbers E and n as the public key. In order for Bob to send Alice a mes- sage x, he needs to send a new number/code y = xE; while Alice, in order to decipher the message, needs to solve x = yD where only she knows D.



1. figure: Scheme of symmetric encription[3]



2. figure: Scheme of asymmetric encription[3]

Symmetric or asymmetric key algorithms? Although it is in much wider use asymmetric key, it has some disadvantages compared to symmetric. Namely, symmetrical keys do not require strong hardware due to a simpler algorithm, they need more time (precisely because of the more complex key) but they are more reliable than the symmetrical one keys and work where they can't (if

Alice and Bob can't exchange key outside the communication channel).

3 SECURITY OF CRYPTOGRAPHIC ALGORITHMS

The key is usually represented in a binary system and is formed large enough for the brute-force algorithm to be insignificant when it is discovered. In addition to keeping the message secure, the secrecy of the key is also important.

If the attacker does not have any new knowledge about the basic message after reading the encrypted message, we say that the cryptosystem has perfect security. The system that provides perfect security is called one - time pad and its basic features are:

1. The number of basic messages is less than or equal to the number of keys
2. The key is chosen randomly from the domain of uniform probability.
3. The key is used for one encryption only

Definition 2 (Protocol). A protocol is a set of rules and conventions for sending a message over a network.

It is a service that is provided by a protocol layer of Protocol is safe if the following is provided:

- Data integrity: ensures consistency and accuracy of the message
- Data confidentiality: data protection from unauthorized persons
- Authenticity: confirmation of message originality
- Access control: Checks if the client has legal access to the data
- Nonrepudiation: prevents the recipient from modifying the content (most commonly used for digital signatures)
- Resource availability: procedure in case of cancellation, error or detection of an attack

The higher the number of keys, the less likely an attacker is to hit the right one. However, if the attacker were to find out the length of the key or basic message, security is still at a high level considering the length of the message is insufficient to reveal the context of the same. [2]

SSH protocol: If there are a computer and a server (or two computers) that should connect, but for some reason, they can't do it with a secure communication channel, SSH ("Secure SHell") is a network protocol that allows users exchange of data in such a situation. When the client (computer) should connect to the server, the client forms two keys - private (Ks) and public (Kp). Then sends the public key to the server (which is legitimate, anyone can have the public key), where the server stores that key (Kp) in memory and forms a new key (Kv) and sends it back to the client two (Kp, Kv). Since with the private key (X), the client can erase which is (Kv), he sends such a key back to the server based on which he can confirm the identity of the client with whom he communicates and form a new, secure channel.

No matter how many rules you set, there will always be the idea that any cryptosystem is an "easy target" for revealing trusted or any other data. The knowledge so far about the interception and attack on the cryptosystem is divided into two groups: passive and active attacks.

Passive attacks: Passive attacks are similar to machine learning in that they aim to "learn" what the keys are based on monitoring the message flow. There is no possibility to modify the content but can abuse it. The most common forms of passive attack are:

- Analyzing the flow - Alice and Bob communicate believing they have a secure channel, but the attacker observes the frequency of their messages

- Posting a message - Although he cannot change it, the basic message of the attacker may publish or share

Active attacks: Types of active attacks, except that they can change its content, can also redirect the message to an unwanted location; answer or pretend to the right recipient for a certain period. Such attacks are more difficult to detect than passive ones, so their algorithms are quite more complex.

4 EXAMPLE IN PYTHON

Packages that were used in this example are:

Pandas: Pan(el) da ta s is "open - source" code used to analyse, process and sort data as well as their tables. The data types supported in this package are Data Frame - a data structure formed of types and columns, where each column contains the value of one attribute, and each type represents a set of values of all attributes; Data - an argument that represents data and is mandatory for definition; index, columns, dtype are optional arguments and serve to present the table more accurately. It is important in cryptography because of the simple manipulation of data, which generally has a lot.

Numpy: Mainly used with Pandas, it is also "open - source" and works with arrays. It is useful because it can easily work with arrays and matrices of large dimensions. ndarray is the main data structure in this package, in which all members of the array must be of the same type.

Paillier: One of the packages from the Python Library formed for data encryption. It is used for homomorphic encryption and its main advantage is that encrypted numbers can be multiplied by unencrypted ones. The parameters of this package are

- Publickey - the key based on which the message is encrypted;
- ciphertext - encrypted message in the form of an integer;
- exponent - mostly a negative number, the one that represents the exponent in the encryption equation

JSON: A package that works with JSON (JavaScript Object Notation) data is used to store and share data. It is easy to read because its elements are shown in pairs (name, value).

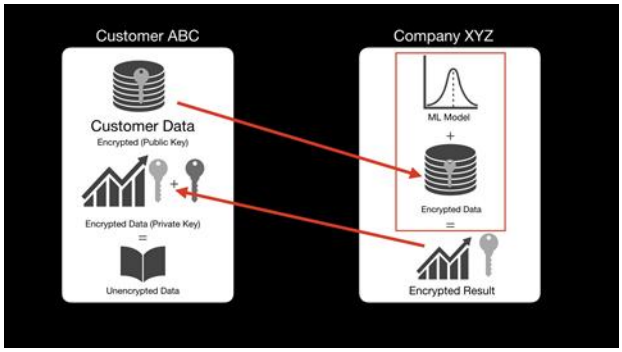
This example is a mini - version of large companies, a model that shows how data passes through the protocol and how it is processed. The idea is to present the product on the client based on his salary, the data from the table we received in csv format. Since privacy is mandatory, all messages and all data that would be useful for the client/company are sent in the form of a code (number). It would be unthinkable for every company to have a human being behind every computer waiting for the codes to arrive, then to analyse them and based on that analysis send back a product that he assumes is interesting/attractive to the client. In order for a machine to do all that, machine

learning is needed. With the help of the packages, the computer analyses, remembers and tries to guess which product to return as feedback and thus make a profit. It is clear that such an analysis requires as many attributes as possible, as well as data, and of course a longer period of time in order for the analysis to be more accurate.

In this example, we have the ABC client and the XYZ firm that get some data encrypted with an asym- metric cryptography model, using a public key. In com- bination with its machine algorithm and the obtained information about the client, it can extract its data (products) which will be returned to the client also with the help of a public key. Since the customer has his private key, he will use it to decrypt the message received from XYZ and thus read the product/message he received. [4]

Process:

1. Machine learning will be based on 4 coefficients: age, gender, lifestyle and healthy diet. The first file is the part where we form the machine learning model. Based on the data from the table, we train a machine that should predict which data will be important to the client. Such a model is used by XYZ, which is based on a linear regression type algorithm.



3. figure: Scheme of coding and decoding data [5]

2. The second file contains improvised data that is encrypted using a public and private key. Such keys are stored in a single JSON file in which all data is encrypted. What XYZ gets is just a dictionary with completely unclear values (large volume). The answer part is used to load products from the company.
3. Since it now has its own model for machine learning and the data it received from the client, the company, with the help of mathematical calculations, extracts the data that it will return to the client. There is a function named "getData" that displays what the com- pany sees as the information it received (it must be the same as in the JSON file). "computeData" will be able to generate the product to be presented to the client with the help of the coefficients from file 1 and the information just obtained. Of course, just as it must be secure, it will be encrypted with a public key and such code will be sent back at the target group. With the private key, that group will be able to decipher the message and thus find out the product it received from the company.

5 Conclusion

Consciously or unconsciously, we use cryptography and its methods every day. Using ATM, online payments and messages via social networks are life situations for which data encryption (in the form of numbers) is necessary. It is believed that the breaking of the German Enigma by Alan Turing, Joan Kankors, Hugh Alexander and Joan Clark stopped the Second World War, which created the Turing machine - the forerunner of today's computers. Thanks to increasingly advanced machines and programming languages, one no longer cares about the daily security of information exchange, although there is always the side that tries to access them illegally. Clearly, as economics, politics, and technology evolve, there will be an increasing need for cryptography development as well.

References

[1] Shyam Nandan Kumar. Review on network security and cryptography. International Transaction of Electrical and Computer Engineers System, 3(1):1–11, 2015.

[2] Bašić, B. D., Čupić, M., Šnajder, J. (2008). Umjetne neuronske mreže. *Zagreb: Fakultet elektrotehnike i računarstva*, 7–15.

[3] David Bishop. Introduction to Cryptography with java Applets. Jones & Bartlett Learning, 2003

[4] Example,https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences, Last access 26.03.2023.

[5] Example,howpublished=https://www.youtube.com/watch?v=nlsd2los50, note = last access: 21.04.2022.

[6] Python,howpublished=https://github.com/satssehgal/homomorphicencryption/blob/master/pic.jpg, note = last access: 21.04.20

Application of Artificial Intelligence in Medicine

Tatjana Muratović

University of Donja Gorica, Podgorica, Montenegro

email: tatjana.muratovic@udg.edu.me

***Abstract* — Blood is one of the most essential parts of the human body, and it comprises of the Red Blood Cells, White Blood Cells, and Platelets. Complete blood count characterizes the condition of well-being. Hence, segmentation and identification of blood cells is very important. Up to this day, many hospitals and health centers still use the old conventional method which involves manual counting of blood cells using haemocytometer along with other laboratory equipment's and chemical compounds, which is a time-consuming and tedious task. In this work, the author presents a machine learning approach for automatic identification and counting of three types of blood cells using Detectron2, a popular PyTorch based modular computer vision model library. Detectron2 detector has been trained on public blood cell detection data hosted at Roboflow. Overall, the computer-aided system of detection and counting enables us to count blood cells from smear images in less than a second, which is useful for practical applications.**

Keywords: Machine learning, Deep learning, Medicine, Blood Cells

1. INTRODUCTION

The development of artificial intelligence has gained new momentum since the beginning of the 21st century. Some important problems that were supposed to remain unresolved for a long time, they are just being resolved. Superior results are being achieved in some domains in which computers could not be compared to humans. Although it came to the fore only at the beginning of the 21st century, this area has a long history of development. Conceived in the works of Alain Turing, in the 1940s, it has been actively developing since the 1950s, when the first perceptron was constructed, the first system that teaches simple laws and is a distant forerunner of modern neural networks [11].

The application of artificial intelligence in medicine is the use of machine learning models to search medical data, which helps to better understand the patient's state of health. Thanks to advances in computer science and informatics, artificial intelligence (AI) is soon becoming an integral part of modern medicine. Artificial intelligence algorithms and other AI-powered applications are used to support healthcare professionals in the clinical setting [7].

Currently, the greatest use of artificial intelligence in medicine is in the establishment of medical diagnoses and analysis of medical images. Tools or support in establishing diagnoses help service providers to make the right decisions about patients' treatments, medications, mental health and other needs by giving them quick access to information or research that is relevant to a particular patient. In medical imaging, AI tools are used to analyze CT scans, X-rays, MRI as well as other tests.

Also, the COVID-19 pandemic, which has created major challenges for many healthcare systems, has accelerated the process of testing new technologies that rely on artificial intelligence. Research and results of these tests are still being purchased, and general standards for the use of artificial intelligence in medicine are still not defined. However, the possibility of AI being useful to clinicians and researchers as well as patients is constantly increasing. At this point, without doubt can be said that AI will become a key part of the digital systems that shape modern medicine [8].

2. ARTIFICIAL INTELLIGENCE

Artificial intelligence is perhaps the oldest field of computer science, which deals with all aspects of mimicking cognitive functions to solve problems in the real world and building systems that learn and think like humans. Therefore we often call it machine intelligence to compare it to human intelligence. Programs that allow computers to function in a way that is similar to human intelligence, are called artificial intelligent systems. British mathematician Alan Turing (1950) was one of the founders of modern computer science as well as artificial intelligence. He defined intelligent behavior of computers as the ability to reach the human level of performance in

cognitive tasks, and this later became known as the "Turing test". The area of artificial intelligence is at the intersection of cognitive sciences and computer science. Artificial intelligence is now attracting huge interest because of the success in machine learning [11].

2.1 Machine Learning

Machine learning is a branch of artificial intelligence that deals with techniques and methods that allow computers and other machines to learn based on experience, without explicit programming (Derived from the first definition of machine learning as a branch of science given by Arthur Semuel in 1959: A discipline that allows computers to learn without explicit programming). Enormous advances in machine learning have been driven by the development of new statistical algorithms along with the availability of large data sets and low cost calculations. Today, an extremely popular method is deep learning [4].

2.2 Deep Learning

Deep learning is part of the wider family of machine learning algorithms based on convolutional neural networks which have a long history. Deep learning is very popular today because it achieves amazing results even on human level. The best example is the recent achievement of the Thrun group, where they succeeded in applying deep learning to classify skin cancer with a level of competence that can be compared with human dermatologists [5].

3. NEURAL NETWORKS

An artificial neural network in the broadest sense of the word is an artificial replica of the human brain, which attempts to simulate the learning process. An analogy with the real biological model is actually quite shaky because with many details replicated, there are still many phenomena of the nervous system that have not been modeled by artificial neural networks. Furthermore, the characteristics of artificial non-neural networks that do not agree with those of biological systems. A neural network is a set of interconnected simple process elements, units or nodes, whose functionality is based on a biological neuron. In doing so, the power of the network comes from the connections between individual neurons, ie. the weights that are reached in the learning process based on a learning data set. The neural network processes data by distributed parallel operation of its nodes. The basic building block of a neural network is called a neuron. In the literature often uses the name Unit. Neurons connections have their own weight, which we can identify with the synapse and their strength. If the neuron signal is strong enough, the neuron will pass the signal to the subsequent neurons [8]. The value that a neuron needs to reach to pass a signal is called a threshold (Bias). The weights of connections between neurons and the threshold adapt during the learning phase. Various models have evolved from the basic idea of neurons that differ mainly in the way they transmit signals. We group neurons into layers, and all layers form a neural network. Input signals are sometimes called the input layer, however it does not consist of neurons. Except the input layer the network must also have an output layer. When the network consists only of input layer (input data) and output data layer then we will say that it is a single-layer neural network. When the network between input and output layer has one or more layers of neurons, than these layers are called hidden layers. Neurons in the same layer are not interconnected, but each neuron in the layer is associated with some neurons in the next layer [1]. One input data can consist of several signals. It is common to the input data to be divided into a learning set, a validation set, and a test set to ensure the proper operation of the network on unprecedented data. If we do not ensure proper sharing of this data, overtraining problems can occur. It is a phenomenon in which the network is fully adapted to the training data and loses the ability to adapt to new instances of the problem (overfitting). The test data set is only used to evaluate the network, so this data must not be used in learning algorithms [2]. If we focus on one hyperparameter, the natural way would be to try to train the network several times, each time with a different value of the selected hyperparameter and opt for the one that gives the best results on the set for testing. However, when a neural network is put into use, it can be assumed that its performance is significantly worse than that of the test set. The reason is that we are re-training and testing the network implicitly adapted to a set of test data, so the network does not actually have the ability to adapt to new data [2]. The solution to this problem is an additional set of data that we call a validation set. After the learning phase is over and when the network achieves satisfactory results on the data set for validation, then on the test data we can check if it is ready for actual use.

4. MODEL OF ARTIFICIAL NEURON AND NEURAL NETWORK

At first sight, it might be wrong to conclude that artificial neural networks represent a mathematical model of real neural network, but that is not the case. To some extent, artificial neurons are inspired by the way biological neurons function, but their mathematical model represents a significant simplification of the work of real neurons and the only real relationship between a biological neuron and an artificial neuron is that both are connected with the goal of learning and realization of some functionality. Biological neurons realize their functionality through impulses, while,

although there are pulse neurons networks, artificial neurons represent only a mathematical model of the elementary constituent of a larger architecture that can be trained to solve a specific problem and which, again by convention, is called a neural network, so the alternative name for an artificial neuron is a newly formed term perceptron [6].

Therefore, the artificial neuron is a simple classifier which accepts the input vector, denoted by χ, the weight vector representing the synaptic weights for the artificial neuron, denoted by ω and we apply an activation function φ on their scalar product, which is typically a nonlinear function.Therefore, a mathematical model of a neuron, when it comes to the model in the picture can be represented by an equation

$$y = \varphi (\chi * \omega)$$

The values of the elements of the weight vector, can be adjusted manually either on the basis of experiments or on the basis of the propagation of gradients in a process called supervised learning. One neuron does not represent a significant classifier model, but if we have many, their usefulness and classification power increase when they are connected into an architecture called an artificial neural network. In its simplest form, an artificial neural network represents layers of artificial neurons [6].

5. APPLICATION OF ARTIFICIAL INTELLIGENCE IN IDENTIFICATION AND COUNTING BLOOD CELLS

A complete blood count (CBC) is a very important test. The three main types of blood cells are red blood cells(RBCs), white blood cells (WBCs) and platelets [3]. Red blood cells, ie. erythrocytes are the most abundant cell type in the body. Their main role is to transport oxygen from the lungs to the tissues and carbon dioxid in the opposite direction. Erythrocytes have the shape of a biconcave lens. This form of erythrocyte provides maximum elasticity and flexibility, allowing them to go through very narrow capillary spaces without rupture of the cell membrane. Average diameter is about 7,8 μm to a thickness of 2,4 μm on the periphery, or 1 μm or less in the central part of the cell [3]. Erythrocytes consist of about 70% water, while the remaining amount is mostly hemoglobin whose concentration ranges from 140g / l (in women) to 160g / l of blood (in men) and which is the respiratory pigment. The cell consists of a membrane (lipo protein structure) and a cytoplasm without a nucleus and most other cellular organelles. The cell membrane of erythrocytes ensures the shape and plasticity of red blood cells and the stability of their internal environment. It is a very dynamic structure, important to sustain its existance. The number of red blood cells in healthy people depends on various factors. Most often on gender, age, altitude. The percentage of blood that makes up erythrocytes is called hematocrit and is 40-45% [10]. White blood cells, ie. leukocytes make up only 1% of the total number of cells in the blood. Their role is multiple. Immunological is most often mentioned, ie. their role in defense from disease. Leukocytes originate in the bone marrow, but part of the development of some types of leukocytes also takes place in the thymus, lymph glands and nodes, as well as the spleen. They are very important for the interpretation of laboratory blood analysis. In one liter of blood, in case of adults, there are between 4-11 billion white blood cells. Leukocytes differ from other cell types in appearance, representation, place of origin and function. According to the shape nuclei and membranes they are divided into granulocytes (with granular cytoplasm and lobes by that nucleus) and agranulocytes (with homogeneous cytoplasm and round nucleus). The most important organ when it comes to white blood cells is the thymus gland (thymus), which is located below the sternum, because it is essential for the development of one of the subtype of lymphocytes, T lymphocytes. Leukocytes contain about 80% water, a large amount of glycogen that serves as a source of energy, lots of nucleoproteins, histamine and heparin. Of the physical characteristics, the most important is an amoeboid movement as it passes from the blood to the tissues. The shape of the leukocytes varies. All peripheral blood leukocytes are round in shape. Granules in the cytoplasm have specific granules that are dyed with acid and base dyes, and there are also neutral granules. The lifespan of leukocytes is different. Some leukocytes are formed in the bone marrow and they stay there until the need arises. For example, granulocytes once they are released and after they reach the bloodstream they stay there for another 5 days [10]. Platelets are small blood components whose main role is to stop bleeding by plug formation and blood coagulation. Since the number of these blood cells is huge, the traditional way of manual counting of blood cells using a hemocytometer is very long, and often wrong, because the accuracy largely depends on the skill of the person performing the analysis. Therefore the automation of counting different blood cells would greatly facilitate the whole process. With the development of machine learning, applications that are used for image classification and object detection become more accurate. As a result, methods based on machine learning are applied in different fields. Specifically deep learning methods have different applications in medicine, such as detection of abnormality and localization on chest X-rays, automatic segmentation with detection of local errors in MRI images of the heart, detection of diabetic retinopathy on retinal fundus images. So it is worth considering in-depth learning methods that can be used to identify and count blood cells [3].

6. MATERIALS AND METHODS

Google Colab was used to analyze the data and create the model. Because it supports many popular machine learning libraries, it provided a suitable environment. Python and its libraries (PyTorch, Pandas, Numpy, Matplotlib) were used for implementation. We used Roboflow to collect and prepare data. Roboflow is a Computer Vision development framework for data collection, containing public collections of data that is available to users, and also allows users to access their data collections. We used the popular PyTorch library Detectron2 for detection and classification of objects. Detectron2 is a system that lets the most modern computer vision technologies to be included in the workflow. Detectron2 includes all the models that were available in the first version, such as Faster R-CNN, Mask R-CNN, RetinaNet and DensePose. It also features several newer models such as the Cascade R-CNN, Panoptic FPN, and TensorMask [13]. We used a Faster RCNN neural network. We classified the data into two groups: the learning group (80% of the data) and the group for testing (20% of data). We used 765 COCO (Common Objects in Context) image.

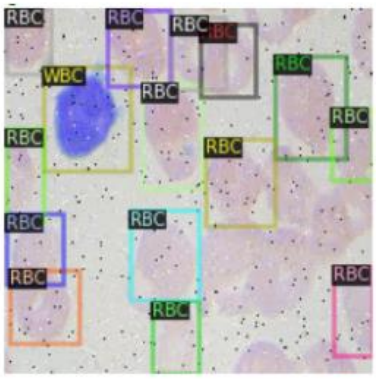


Figure 1. Example of a learning model

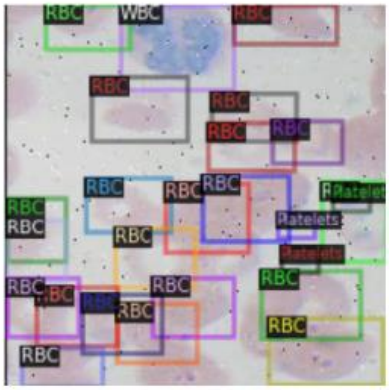


Figure 2. Example of a learning model

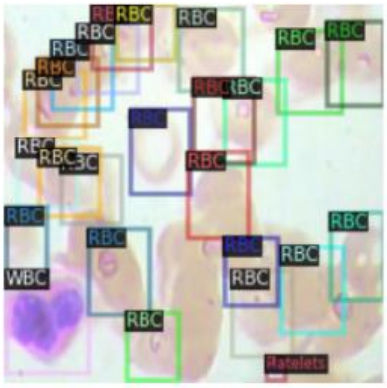


Figure 3. Example of a learning model

7. RESULTS

The following are examples of results obtained for imported data.

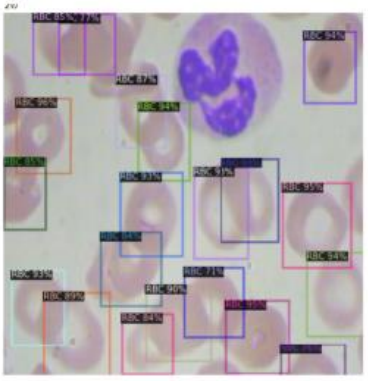


Figure 4. Example of a result

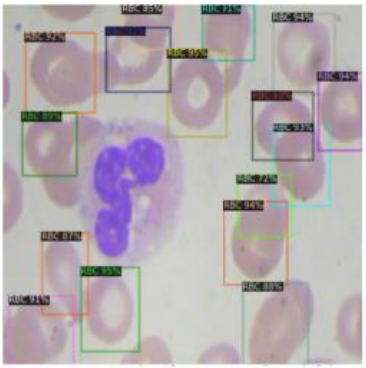


Figure 5. Example of a result

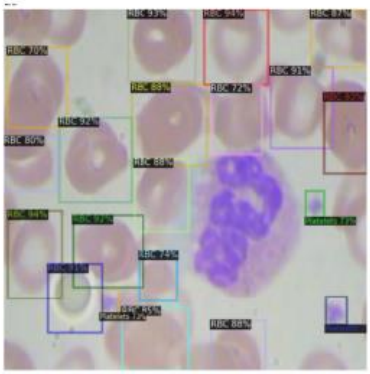


Figure 6. Example of a result

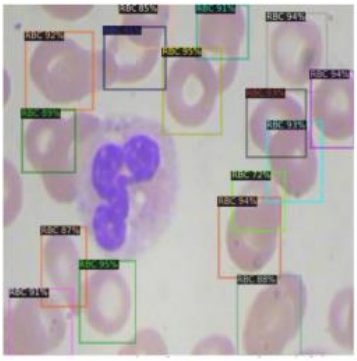


Figure 7. Example of a result

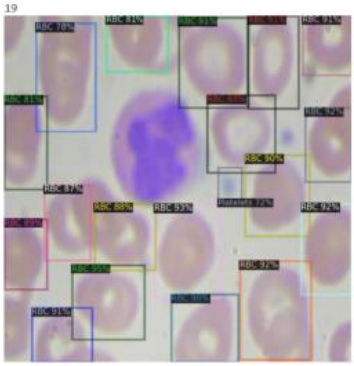


Figure 8. Example of a result

8. CONCLUSION

As we have already mentioned, the application of artificial intelligence grows day by day more and more. In this growth, machine learning stands out as its largest branch, while deep learning is developing within it, which has increasingly significant application. In this paper, we have dealt with the application of artificial intelligence in medicine, while the greatest emphasis is placed on its application in hematology. In medicine,the greatest benefit of using artificial intelligence comes from considerable saving of time and human capacity when performing tasks that are logical and repetitive. Also, most importantly, such algorithms mostly have better accuracy and efficiency than the human could provide. The example given concerned with the detection of red blood cells, white blood cells and platelets, the accuracy of this algorithm was very high. Similar algorithms aided by artificial intelligence are widely used for detection of pneumonia, various changes in the proteins, feeling of comfort of patients via AI assisted phone calls… What is certain to us is that they make life much easier at the moment.

REFERENCES

[1] Bojana Dalbelo Bašić, Marko Čupić, and Jan Šnajder. Umjetne neuronske mreže. Zagreb: Fakultet elektrotehnike i računarstva, 2008.

[2] Dan Claudiu Cireşan, Ueli Meier, Luca Maria Gambardella, and Jürgen Schmidhuber. Deep, big, simple neural nets for handwritten digit recognition. Neural computation, 22(12), 2010.

[3] Nilkanth Mukund Deshpande, Shilpa Gite, and Rajanikanth Aluvalu. A review of microscopic analysis of blood cells for disease detection with ai perspective. PeerJ Computer Science, 7, 2021.

[4] Issam El Naqa, Ruijiang Li, and Martin J Murphy. Machine learning in radiation oncology: theory and applications. Springer, 2015.

[5] Yanming Guo, Yu Liu, Ard Oerlemans, Songyang Lao, Song Wu, and Michael S Lew. Deep learning for visual understanding: A review. Neurocomputing, 187, 2016.

[6] Neha Gupta et al. Artificial neural network. Network and Complex Systems, 3(1), 2013.

[7] Jianxing He, Sally L Baxter, Jie Xu, Jiming Xu, Xingtao Zhou, and Kang Zhang. The practical implementation of artificial intelligence technologies in medicine. Nature medicine, 25(1), 2019.

[8] Werner Horn. Ai in medicine on its way from knowledge-intensive to data-intensive systems. Artificial Intelligence in Medicine, 23(1), 2001.

[9] Richard Lippmann. An introduction to computing with neural nets. IEEE Assp magazine, 4(2), 1987.

[10] Lorenzo Putzu and Cecilia Di Ruberto. White blood cells identification and classification from leukemic blood image. In International Work-Conference on Bioinformatics and Biomedical Engineering. Copicentro Editorial, 2013.

[11] Alan M Turing. Computing machinery and intelligence. In Parsing the turing test. Springer, 2009

BÁNKI KÖZLEMÉNYEK
V. ÉVFOLYAM 1. SZÁM

Marketing using artificial neural networks

Anja Stijepović
University of Donja Gorica, Podgorica, Montenegro
anja.stijepovic2@udg.edu.me

***Abstract* — Due to the emergence of numerous digital innovations, many business sectors are being reshaped at an astonishing pace. One of the technologies that is increasingly affecting every aspect of our lives is artificial intelligence. In this paper, we examine the impact of artificial intelligence in the context of marketing. The main application of artificial neural networks is in the field of predictive analytics, therefore these networks provide effective tools for predicting consumer behavior as well as for evaluating success of marketing campaigns. In order not to be overshadowed by their competition, companies and organizations must adopt new, fast and accurate methods of artificial intelligence when analysing their customer data. The artificial neural network model analysed in this paper is a prediction of the outflow of customers (churn) from a telecommunications company. Discovering the reasons for churn is very important in making future marketing decisions of a company. The accuracy of the resulting customer classification model could be increased by training on a balanced set of customer data.**

***Keywords*:** artificial neural networks, marketing, data sets, churn

1 INTRODUCTION

With the development of science and technology, our lives rely much more on digital products and services than they did in the previous decades. Numerous companies, aware of frequent technological innovations, are increasing automation and the use of artificial intelligence in everyday business. The technology of artificial intelligence is important because it enables human capabilities - understanding, reasoning, planning, communication and perception - to be performed by software more efficiently, effectively and at a low cost. Automation of these capabilities creates new opportunities in most business sectors and user applications.

Artificial neural networks are computer systems developed as a generalization of mathematical models of biological nervous systems in the human brain. Their ability to collect, memorize and use experimental knowledge (learn by example), influences their wide application. Artificial neural networks and machine learning are revolutionizing the world of marketing as well. Large amounts of data on customers, trends and products can now be processed faster and smarter in order to organize successful marketing campaigns. Neural networks, fed with enough data, are able to provide more accurate insights and predictions, helping marketers assess expectations and provide consumers with a better experience. Data analysis can answer the main challenge of digital advertising: „How to place an advertisement on the right platform and in front of relevant viewers?". Artificial neural networks provide companies with a deep insight into their customers and thus optimize the return on investment in advertising. Not only will companies be able to increasingly personalize interactions in the future, but they will also be able to predict future customer behavior based on the data collected.

2 ARTIFICIAL NEURAL NETWORKS

Following the example of biological nervous systems, which are composed of billions of neurons, artificial neural networks are created. Artificial neural networks consist of interconnected processing elements - artificial neurons [1]. With their help, computers are able to perform tasks that the human brain easily and successfully performs on a daily basis, such as recognizing shapes and voices, learning from examples, remembering and making decisions. Computers are machines that do routine work faster and better than humans. However, intelligence, awareness, creativity and feelings are human traits that computers lack. Therefore, artificial models inspired by the human brain allow computers to take over, facilitate or speed up many human tasks.

Artificial neurons have a simpler structure, but similar functions as biological ones. They, too, have a local memory in which they memorize the data they process and then pass it on through communication links. Using input data and weighting coefficients, artificial neurons calculate the output data, and then, with the help of some activation function, produce the final outputs. The 1. figure shows the architecture of an artificial neuron; $x_1, \dots, x_4$ are the input data, $w_1, \dots, w_4$ are weights, θ is the middle output, f is the activation function, and O is the final output [1]. The output signal of a neuron is given by the following relationship, where the variable net is defined as the scalar product of weight and input vectors:

$$O = f(net) = f\left(\sum_{j=1}^{n} \omega_j x_j\right). \quad (1)$$

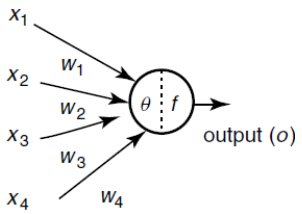


Figure 1: Architecture of an artificial neuron [1]

The activation function that is later used for producing inputs of the hidden layers is the ReLu function, defined by the following equation:

$$f(x) = \begin{cases} 0, & x < 0 \\ x, & x \geq 0 \end{cases}. \quad (2)$$

The most common form of the activation function is the sigmoid function, which produces final output values between 0 and 1. The sigmoid function is defined by the following relationship:

$$f(net) = \frac{1}{1 + e^{-a \cdot net}}, \tag{3}$$

where the parameter a determines the slope of the function [2].

Adjusting the weights between neurons enables the learning ability of an artificial neuron [1]. Learning allows artificial neural networks to become more accurate in predicting outcomes. Networks are fed with a large amount of data which teaches them basic rules and improves their performance of various tasks. They are considered trained when a particular set of inputs leads to the desired final outputs.

The 2. figure shows an example of the artificial neural network architecture. We can conclude that artificial neural networks are graphs, whose nodes are neurons, and directed branches with weights represent the connections between inputs and outputs [4]. Usually, each layer of the network receives inputs from the previous layer or the environment, and sends its outputs to the next layer. Deep neural networks are composed by multiple hidden layers, and are used in deep learning (subset of machine learning).

3 How can artificial neural networks improve marketing?

In order to have a successful marketing campaign, a company must know its customers, that is, it must store data about them and then identify information relevant to further advertising of products and services. A company must observe the relationships with customers, find out where they are located, what age they are, which products they buy most often, the quantity and frequency of purchases, sensitivity to promotional activities and such [5]. All this data is stored in a large database of the company, which cannot be managed without the help of some computer software.

If we recall the ability of neural networks to learn from examples, it is clear that they can be taught to successfully analyse these types of data. The most common application of artificial neural networks is in the field of predictive analytics, which is an important part of creating a marketing plan for a business. Marketers can predict the future with a high probability and make the right decisions based on the expected results of advertising.

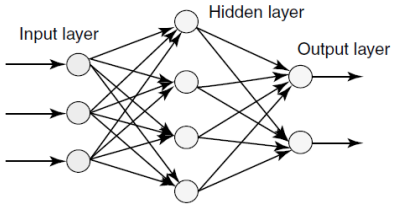


Figure 2: Architecture of an artificial neural network [1]

With the help of artificial intelligence, companies can optimize the return on investment in advertising by placing ads in front of relevant viewers. In addition to analysing simple data about custumers, like their name, address or age, patterns of behaviors should be considered during the formation of a marketing plan as well. In this context, hidden layer neurons can be viewed as invisible variables, which can be analysed using the weights of the connections between them and thus reveal important behaviors or attitudes [6].

Additionally, with the methods of artificial intelligence, it is possible to form propensity models. These models are designed to "identify potential customers who are more likely to respond to an offer" [7]. When creating a marketing campaign, the target audience and campaign goals are defined. Propensity models, by connecting customer characteristics with expected behavior, recommend strategies for achieving desired goals. They represent an opportunity to determine the value of a customer in the long run, i.e. how long the customer will remain loyal to the company. If a company has recognized its best customers, then it must make an effort to keep them [5].

So far, various applications of artificial neural networks in the field of marketing have been observed, including modeling consumer responses to market stimulations, new product development, sales forecasting, identifying consumer needs and expectations, market segmentation and creation of marketing strategies [6].

Another application of artificial neural networks is in the analysis of customer outflow (churn). One of the main rules that must be met during the formation of a company's marketing plan is that advertising to previous customers is cheaper and more effective than advertising to people who have not been in contact with the company before. [5] If a company loses valuable customers, it does not only lose the potential revenue from them, but it also must incur additional costs to replace old customers with new ones. The book [5] estimates that reducing customer outflows by only 5% per year could lead to a significant increase in profits (25%). Therefore, a company must pay special attention to retaining valuable customers whom the artificial intelligence model classified as „churned" (likely to end transactions with a company). For example, telecommunications company T-Mobile analyses transactional data to determine valuable customers who are likely to change service providers. Then, T-mobile provides these customers with better offers and privileges in order to keep them in the company. [5] In the following research, we will analyse a model for predicting the outflow of customers of a telecommunications company.

4 Data collection and processing

The „Telco Customer Churn" dataset found on the Kaggle website was used to create the classification model analysed in this research. Each row of this dataset represents a customer of one telecommunications company, and each column contains certain customer attributes. There are 21 columns and 704 customers (rows). The column named „Churn" contains „Yes" or „No" answers depending on whether the customer has left the company in the previous month. It is important to determine whether a customer will leave the company, but also the reason for the potential churn, therefore we consider the „Churn" column as a dependent variable (dependent on other columns). Other columns contain information about the services which each user signed up for (telephone, multiple lines, internet, online security, online backup, device protection, technical support and streaming of television and movies), account information (tenure, contract, method of payment, electronic payment,

monthly and total charges), as well as demographic data on customers (gender, age and whether they have partners and dependents).

There are two types of data in this dataset: categorical and numerical. Most columns contain only Yes / No (or Female / Male) which are easily converted into numbers 1 or 0 and fed to the artificial neural network. The columns that posed a problem are „InternetService“, „Contract“ and „PaymentMethod“ which contain three or more textual responses. The problem was solved by the method of „one-hot encoding“, a process by which categorical variables are transformed into a form that can be given to a deep learning algorithm. In this way, each of these columns was divided into three or more columns, which now contain only 0 or 1. For example, in the initial column „Contract“, three unique answers were observed: „Month-to-month“, „One year” and „Two year”. A new dataset has been created which, instead of the „Contract“ column, contains „Month-to-month“, „One year“ and „Two year“ as separate columns with values of 0 (if the buyer does not have this type of contract) or 1 (otherwise). The numeric data from the „Tenure“, „MontlyCharges“, and „TotalCharges“ columns were scaled down to numbers between 0 and 1 so they can be comparable to other binary values in the dataset. Additionally, 11 rows which had no value for the total costs of the customer, but did for his monthly costs, were deleted from the initial dataset. The "customerID" column has been removed from the initial dataset because it does not affect the customer's decision whether to leave or not. In this way, data cleansing was performed before creating a deep learning model.

5 Methodology

Google Colab was used to analyse the data and create a predictive model, and the code was found on GitHub [3]. As Google Colab works in the cloud and supports many popular machine learning libraries, it has provided a suitable environment for model implementation. The implementation was done in Python, and the libraries used were Pandas, Numpy, Matplotlib, Scikit-learn and TenserFlow. Pandas and Numpy were used to sort and process the data, Matplotlib was used to visualize data via histograms, Scikit-learn was used to evaluate the performance of the machine learning algorithm and to calculate the interdependence of variables, and TenserFlow and Keras were used to create an artificial neural network.

After cleansing, the data was classified into two groups: the training group (80% of the data) and the testing group (the remaining 20%). The training dataset is used to fit into the model for its training, and the testing dataset is used to evaluate the machine learning model. The train-test split method was used to assess the performance of the created model over data that was not used in its training (data that the model had not seen before).

The artificial neural network was created with the Keras.Sequential command. The network had a fully-connected structure with an input layer, two hidden layers and an output layer. Fully connected layers were defined using the Dense class. The input shape was (26,) which represents the number of columns that the "Churn" column is depended on. That means the model expects rows of data with 26 variables. The first hidden layer had 20 neurons, the second hidden layer had 12, and the output layer had 1 neuron.The ReLu (rectified linear unit) activation function was used to obtain outputs from the hidden layers, and the sigmoid function was used for producing final output values between 0 and 1. The outputs were then transformed into numbers 0 or 1 for easier analysis. The output 0 means the model predicted the customer as not churned, and 1 as churned.

After the model was defined, it was compiled. Since churn prediction is a binary classification problem, cross entropy was used as the loss argument (defined in Keras as “binary_crossentropy“). The optimizer was defined as the efficient stochastic gradient descent algorithm “adam“. The classification accuracy was defined via the metrics argument. The model was then fitted and ran for 100 epochs.

Finally, with the classification report, the accuracy of the model with actual and predicted values was calculated. A summary of the results was presented by the confusion matrix, which showed us how many times the classifier was accurate on the testing dataset (how many customers were or were not classified as churned).

6 Discussion and results

During dataset analysis, it was noticed that most clients did not leave the company in the previous month, i.e. that the majority of values (73,42% of the total number of customers) in the „Churn“ column is equal to „No”. This fact is confirmed by the graph in the 3. figure, which shows the number of „Yes” and „No” answers in the „Churn” column. As the Yes/No response classes are not evenly distributed, the observed dataset is unbalanced, leading to the assumption that the model will not be successful in predicting customers who have left the company because it is trained with less data on such customers. The assumption was later confirmed by the classification report.

In order to discover the categorical values that have the biggest affect on the outflow of customers, mutual information was calculated (a measure of the interdependence between 15 independent variables and the dependent variable „Churn”). In the 4. figure we can see that the variable „Contract” has the highest mutual information (9,82%), therefore, among the observed variables, it most affects the outflow of customers. „Gender”, „PhoneService” and „MultipleLines” have mutual information that is close to 0, which means that these variables do not affect the outflow of customers. Variables that do not have a strong association with the target variable („Churn”) could be excluded from the creation of customer churn prediction models.

.

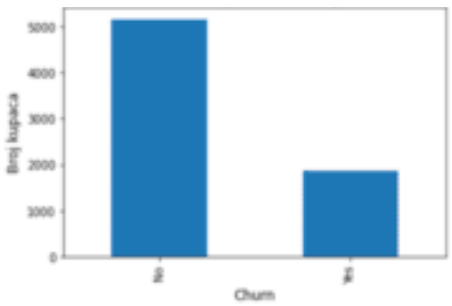


Figure 3: Graphic visualization of customer churn

Contract	0.098182
OnlineSecurity	0.064528
TechSupport	0.062873
InternetService	0.055394
OnlineBackup	0.046659
PaymentMethod	0.044423
DeviceProtection	0.043784
StreamingMovies	0.031918
StreamingTV	0.031803
PaperlessBilling	0.019119
Dependents	0.014270
Partner	0.011383
MultipleLines	0.000798
PhoneService	0.000069
gender	0.000037

Figure 4: Mutual information between categorical variables and the "Churn" variable

The „SeniorCitizen“ column was not considered in the previous analysis because it only contains numbers 0 and 1 in the initial dataset. Therefore, we separately analysed the variable „SeniorCitizen”, as well as the variable „Contract”, which showed the highest degree of dependence on the variable "Churn". The results are shown on the graphs in the 5. and 6. figure, where the red colour represents customers who are churned, and green represents those who are not.

In the 5. figure we can see that almost 80% of non-senior customers are not churned, which is less than 60% amongst senior customers. Thus, the outflow rate of senior citizens is almost twice as high as the outflow rate of young citizens. The company can use this information by giving older customers better offers that would prevent them from leaving the company. Based on the graph in the 6. figure, we conclude that clients with monthly contracts have higher outflow rates compared to clients with annual contracts.

Numerical variables „tenure” and „TotalCharges” were considered as well. In the following graphs shown in the 7. figure, the x −axis represents the number of months spent in the company (in the first graph) or the amount of total costs (in the second graph), while the y −axis represents the number of customers. We notice that the higher the total charges and the fewer months spent in the company, the greater the outflow of customers. This shows that loyal customers, i.e. customers who have been associated with the given telecommunications company for a long time, are unlikely to leave the company, whereas the opposite is true for newer customers. The company also needs to calculate whether it is more profitable to reduce the total costs of certain customers, or to lose those customers.

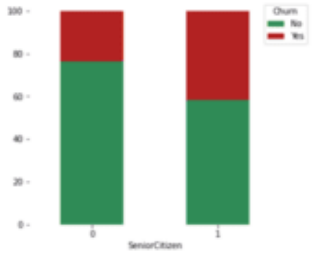


Figure 5: Churn rate of seniors and younger customers

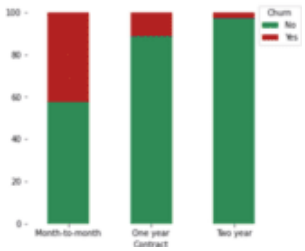


Figure 6: Churn rate of customers who have different types of contracts in the company

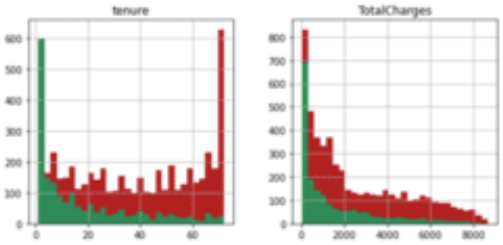


Figure 7: Customer churn depending on the number of months in the company and total charges (respectively)

After analysing the variables that could potentially affect the outflow, a model of artificial neural networks was created, which predicts the customer churn with a certain accuracy. The performance of the model was assessed by the classification report shown in the 8. figure.

The accuracy of the model (the ratio of correct predictions and all predictions) is 0.78. However, the accuracy of the model does not give enough information about its performance, because the model, as mentioned above, is built on an unbalanced data set. Therefore, we calculated separately the precision of the model in classifying customers who have not left the company (“churn” is 0), and the precision of the model in classifying customers who have left the company (“churn” is 1). Our assumption turned out to be correct, since the model is fed by a much larger number of data on customers who remained in the company, then the forecast for such customers is more accurate. This is confirmed by the classification report in which the accuracy for class 0 is equal to 0.83, while the accuracy for class 1 is equal to 0.64. Precision for class 1 is the ratio of the number of customers that the model correctly classified as churned, and the total number of customers it classified as churned. The recall for class 0 is the ratio of the number of customers that the model correctly classified as non-churned and the number of customers that are actually non-churned. As shown in the classification report, the recall for class 0 is 0.88, but the recall for class 1 is 0.55.

The „confusion matrix” shown in the 9. figure gives us information about the number of correct and incorrect classifications for 0 and 1. The columns of the matrix contain the predicted classes, while the rows represent the actual classes. So, out of 1407 data that entered the model’s testing group, 408 (185 + 223) were actually 1 (left the company), and 999 (875 + 124) were 0 (stayed in the company). However, the model predicted that 347 (223 + 124) of data is equal to 1, and 1060 (185 + 875) is equal to 0. Thus, the correct classifications of the model are on the main diagonal of the matrix, and incorrect are outside it.

	precision	recall	f1-score	support
0	0.83	0.88	0.85	999
1	0.64	0.55	0.59	408
accuracy			0.78	1407
macro avg	0.73	0.71	0.72	1407
weighted avg	0.77	0.78	0.77	1407

Figure 8: Classification report

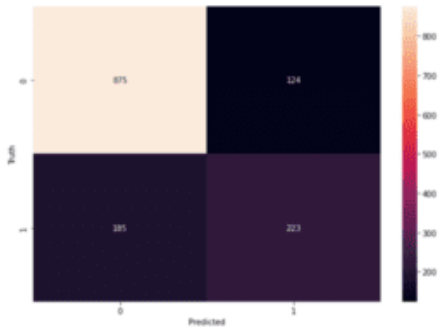


Figure 9: Confusion matrix

7 Conclusion

In this paper, the concept of artificial neural networks, as well as their application in marketing, were explained. The model of deep learning analysed in this paper solves the problem of classifying customers into groups of customers who have or have not left a particular company in the previous month. The model was trained with 80% of data from the given dataset and then tested on the remaining 20%. The model has proven successful in classifying customers who remain in the company, however, its accuracy in classifying customers who have left the company needs to be improved by further research. Better performance of the created model is expected by increasing the dataset (by balancing it), which would feed the neural network with enough of different data. Adding more hidden layers to the used neural network may improve the accuracy of the model. Of course, in order for a company to make the right marketing decisions, customer data must be further analysed statistically. Variables that do not have a strong correlation with the target variable „Churn" could be excluded from the creation of the classification model. Additionally, a successful model could be created by other methods of machine learning.

Outflow of customers is a problem that all companies face, however, it can be prevented by proper prediction. Analysis of big amounts of data can help companies detect valuable customers who plan to leave. After recognizing such customers, the company should strive to improve the services and products that those customers are dissatisfied with. Thus, the company must analyse the results of the successful predictive model in order to make successful marketing decisions and lose as few customers as possible.

References

[1] Abraham, A. (2005). Artificial neural networks. *Handbook of measuring system design*, 901–903.

[2] Bašić, B. D., Čupić, M., Šnajder, J. (2008). Umjetne neuronske mreže. *Zagreb: Fakultet elektrotehnike i računarstva*, 7–15.

[3] Grover, K. (2021). *Deep-learning-keras-tf-tutorial/churn.ipynb at master · codebasics/deep-learning-keras-tf-tutorial.* Retrieved from https://github.com/codebasics/deep-learning-keras-tf-tutorial/blob/master/11_chrun_prediction/churn.ipynb. (Last accessed 13 May 2022).

[4] Jain, A. K., Mao, J., Mohiuddin, K. M. (1996). Artificial neural networks: A tutorial. *Computer* , *29* (3), 31–44.

[5] Lamb, C., Hair, J. F., McDaniel, C., Summers, J., Gardiner, M. (2009). *Mktg*. Cengage Learning Australia, 293–303.

[6] Silva, M., Moutinho, L. (2015). Artificial neural networks in marketing. *Wiley Encyclopedia of Management*, 1–5.

[7] Thiraviyam, T. (2018). *Artificial intelligence marketing,* 449–451.

BÁNKI KÖZLEMÉNYEK
V. ÉVFOLYAM 1. SZÁM

A Formula-1-es versenynaptár optimalizációja genetikus algoritmus segítségével

Optimization of the Formula-1 race calendar using genetic algorithm

Polyák, G., Póth, M.*
Faculty of Technical Sciences, University of Novi Sad, Serbia
* Subotica Tech –Collage of Applied Sciences
gabriellapolyak8@gmail.com
pmiki@vts.su.ac.rs

***Összefoglalás* — Genetikus algoritmusok alatt olyan keresési technikák egy csoportját értjük, melyekkel optimumot vagy egy adott tulajdonságú elemet lehet keresni. A genetikus algoritmusok speciális evolúciós algoritmusok, technikáikat az evolúcióbiológiából kölcsönözték. Számos alkalmazási területe van, azaz számos problématípust meg lehet oldani a segítségével. A munka célja egy optimalizálási probléma megoldása genetikus módszerrel. Tekinthetjük ezt egy Az utazó ügynök problémához hasonlónak, ugyanis útvonal optimalizációról van szó. Alapul a Formula-1-es versenynaptár, illetve a nagydíjhelyszínek földrajzi elhelyezkedésének koordinátái szolgálnak. Az optimalizálás két módon történt, a Microsoft Excel egyik bővítményével, az Excel Solverrel, illetve Matlabban íródott programban. Az Excel Solver működési elve, hogy a megszorítások figyelembevételével megvizsgálja a lehetséges megoldásokat, majd azok közül kiválasztja a számunkra legkedvezőbbet. A Matlabban írt program a genetikus algoritmus során használt módszereket alkalmazza, mint amilyen a szelekció, mutáció, keresztezés és a visszahelyezés. A munkában az említett két programban kapott eredmények kerülnek összehasonlításra és összegzésre.**

***Kulcsszavak*:** útvonal-optimalizáció, genetikus algoritmus, Formula-1, problémamegoldás

***Abstract* — Genetic algorithms are a group of search techniques, which can be used to search for an optimum or an element with a given property. Genetic algorithms are special evolutionary algorithms, borrowing their techniques from evolutionary biology. They have many fields of application, i.e. many types of problems can be solved with their help, such as e.g. subset selection, structure development, technical design, etc. The aim of this work is to solve an optimization problem using the genetic method. This could be considered similar to the Traveling salesman problem (TSP), as the topic is route optimization. The study is based on the Formula 1 race calendar and the geographical location of the grand prize venues. The optimization was done in two ways, with an add-on of Microsoft Excel, Excel Solver, and a program written in MATLAB. Excel Solver is based on: examining the possible solutions taking into account the constraints, then selecting the one that fits the most. The program written in MATLAB uses methods used in the genetic algorithm, such as selection, mutation, crossing, and insertion. In this work, the results obtained in the two programs are compared and summarized.**

***Keywords*:** route optimization, genetic algorithm, Formula-1, problem solving

1 BEVEZETÉS

Rohamosan gyorsuló és fejlődő világunkban egyre összetettebb problémákba ütközünk. Váratlan fordulatok akármikor történhetnek, a megoldások pedig nem várathatnak magukra.

A munka célja egy optimalizálási probléma megoldása evolúciós módszerrel. Tekinthetjük ezt egy Az utazó ügynök problémához (Travelling Salesman Problem, TSP) hasonlónak, ugyanis útvonal optimalizációról van szó. Alapul a Formula-1-es versenynaptár, illetve a nagydíjhelyszínek földrajzi elhelyezkedésének koordinátái szolgálnak.

A 2021-es évi végleges versenynaptár került optimalizálásra, először a Microsoft Excel beépített alkalmazásával, a Solverrel, majd pedig Matlabban írt programmal, ami az evolúciós algoritmus módszereit használja, mint amilyen a szelekció, mutáció, keresztezés és a visszahelyezés. Mivel a Solver egy beépített funkció így nem lehet tudni, hogy valójában mi történik miközben a program fut, csak a bemeneti adatokat lehet ismerni, illetve miután lefutott a program, a kimeneti adatokat, azaz az eredményeket. Ez volt az oka annak, hogy egy program lett megírva Matlabban, hogy tudjuk pontosan hogyan is történik az optimalizáció. Miután mindkét módszerrel megtörtént az optimalizáció, az eredmények kielemzésére került sor, majd pedig a kapott adatok kerültek összehasonlításra.

Ugyanazzal a módszerrel a Formula – 1 1950 óta íródó történelmében, azaz az összespálya közötti optimális útvonal is kiszámításra került.

Mivel a 2020-as szezon elég kaotikusra sikerült, a szervezők igyekeztek enyhíteni ezt a 2021-es szezonra, azonban ismét elég sok problémába ütköztek. A 2020-as szezonhoz hasonlóan ismét több futam megrendezése is elhalasztásra került, illetve le lett mondva. Végül a 2021-es szezon 21 nagydíjhelyszínből és 22 megrendezett futamból

állt össze. Az ausztriai Red Bull Ringen 2 nagydíj is lett szervezve Osztrák, illetve Stájer Nagydíj néven.

2 GENETIKUS ALGORITMUSOK

A biológiai evolúcióban az élőlények, mint komplex rendszerek fejlődését figyelhetjük meg. Az élőlények evolúciója egy olyan folyamat, melynek során az élőlények megtanulnak változó környezetükhöz alkalmazkodni. Ez az alkalmazkodás nem egyformán sikeres minden élőlény számára, így egyre változatosabb formák mellett szelekciónak is szemtanúi vagyunk. Darwin (1859) „A fajok eredete" című műve óta ez az evolúciós folyamat egyre inkább a kutatás tárgyát képezi.

A genetikus algoritmusok heurisztikus keresési megközelítések, amelyek az optimalizálási problémák széles skálájára alkalmazhatók. Ez a rugalmasság a gyakorlatban kedvezővé teszi őket számos optimalizálási probléma szempontjából [6]. A genetikus algoritmus modellje természetesen távol áll a tényleges biológiai evolúciós folyamattól, csak néhány fogalom, technika állítható párhuzamba, mint amilyen a populáció, egyed, szelekció, mutáció, szaporodás, és a tényleges élőlények generációi helyébe a folyamatosan változó populációk sora lép, az1. ábrán a genetikus algoritmus átalános felépítése látható.

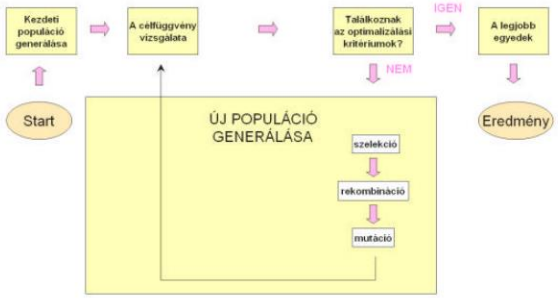
```
start
kezdeti populáció inicializálása
kiértékelés
ismételd amíg a populáció nem konvergál
    szelekció
    keresztezés
    mutáció
    kiértékelés
stop
```

1. ábra - A genetikus algoritmusok általános felépítése

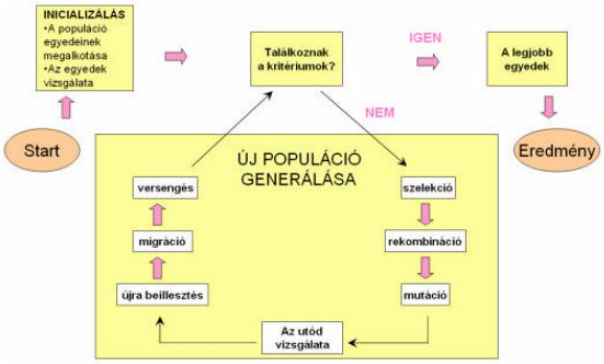
Bár a genetikus algoritmus születését egyértelműen a biológiai evolúció motiválta, a kialakított modell más jellemzőit is kiemelhetjük. Tekinthetjük kereső eljárásnak, tanuló algoritmusnak, vagy populációs alapú algoritmusnak, amelyben biológiai analógiák, vagy információcsere jellemzők alapján képezünk egyes műveleteket. E megközelítés alapján az evolúciós algoritmust a mesterséges intelligencia probléma független kereső eljárásai, vagy a tanuló algoritmusai közé sorolhatjuk, vagy akár az operációkutatás populáció alapú algoritmusának is tekinthetjük [1].

2.1 A genetikus algoritmusok működési elve és módszerei

Az evolúciós algoritmus a probléma megoldását egy evolúciós eljárással keresi. Az eljárás ciklikusan működik, minden ciklusban egyidejűleg több egyeddel (megoldással) dolgozva. Egy populációból válogatással, majd különböző kereső műveletekkel állít elő újabb utódokat, a 2. ábrán egy egyszerű genetikus algoritmus szerkezeti felépítése látható, míg a 3. ábrán egy összetettebbé [5]. Az egyes egyedek rátermettségét a fitneszfüggvénnyel méri, amely a rátermettebb egyedekhez nagyobb (kisebb) számot rendel, mint a kevésbé rátermett egyedekhez. Minden iteráció végén értékeli az egyedeket és utódokat, vagy csak az utódokat, és újabb populációt alakít ki belőlük. A ciklusok, azaz generációk mindaddig ismétlődnek, amíg egy kívánt feltétel nem teljesül (pl. a generációk száma elér egy kívánt értéket).



2. ábra - Egy egyszerű genetikus algoritmus szerkezeti felépítése



3. ábra - Egy összetettebb genetikus algoritmus szerkezeti felépítése

2.1.1 Egyed és populáció

Az algoritmus egy kezdeti egyedhalmazzal indul, amelyet populációnak nevezünk. Mindegyik egyed potenciális megoldás a problémára. Az egyedek pedig génekből állnak, általában bináris reprezentációval. Mivel a módszer egyszerre több egyedet „kezel", így a globális optimum megtalálásának esélye megnő. A populáció az egyedek fejlődésén keresztül fejlődik. Tehát minél fittebbek az egyedek, annál közelebb kerül a populáció is a feladat (egy) megoldásához.

2.1.2 Fitnesz függvény

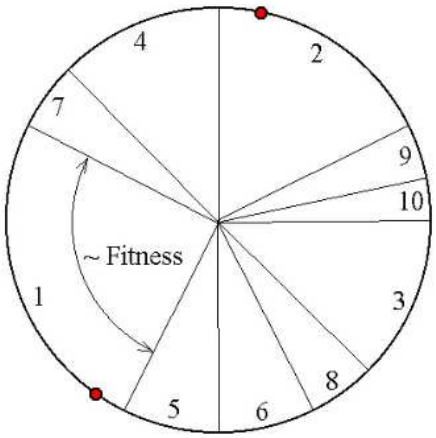
Az egyedek rátermettsége a fitnesz függvény segítségével értékelődik ki, vagyis számszerűsíti azt, hogy mennyire fitt (mennyire versenyképes). A függvény mindig problémafüggő.

2.1.3 Szelekció

A szelekció, vagy kiválasztás folyamata alatt azt a folyamatot értjük, amikor is egyedeket választunk ki a populációból, hogy azok tulajdonságait tovább örökítsük a következő generációba [8]. Két, a fitnesz értékeik alapján kiválasztott egyed alkot egy szülőpárt. Minél nagyobb a fitnesz értéke egy egyednek, annál nagyobb eséllyel kerül kiválasztásra, de kevés esélyt gyengébben teljesítő egyedek is kapnak [7].

Többfajta szelekciós technikáról beszélhetünk:

- Rátermettség arányos szelekció (roulette wheel selection vagy fitness proportional selection, 4. ábra): Amikor is a nagyobb fitnesz értékű egyedek nagyobb eséllyel kerülhetnek kereszteződésre, de esélyt kaphatnak a gyengébben teljesítő egyedek is, bár jóval kisebb valószínűséggel (eséllyel). Ez esetben a teljes populációból választunk véletlenszerűen az arányokat figyelembe véve. Illetve fontos megjegyezni azt is, hogy egy egyed többször is kiválasztásra kerülhet.



4. ábra - Rulettkerék szelekció

- Párok versenyeztetése (tournament selection): Amikor véletlenszerűen kiválasztott egyedek közül az kerül keresztezésre, amelyiknek nagyobb a fitnesz értéke.
- Rangsorolás (rank selection): Abban az esetben használják, amikor az algoritmus az optimum köré gyűlik, így minden egyes egyednek relatíve egyforma szelet jut a rulett keréken. Így a rátermettség helyett a rátermettségi rangsor szerint osztják el arányosan a lehetőséget a kiválasztódásra.

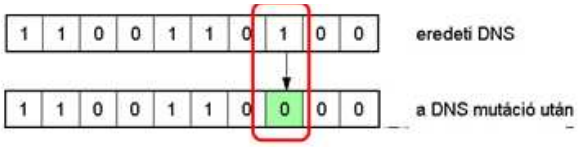
- Elitista szelekció (elitism selection): Elitista szelekcióról beszélünk, ha a legrátermettebb egyed(ek) mindig átkerül(nek) változatlanul az új populációba. Garantálva ezzel, hogy az eddig megtalált legjobb megoldásnál rosszabbul nem tud teljesíteni a teljes populáció.

2.1.4 Mutáció

Mutáció esetén véletlenszerűen megváltoztatunk egy egyed egy-egy génjét, egy példa az 5. ábrán látható. Lehet ez:

- Bitek 0-ról 1-re való cseréje és fordítva
- Gén cseréje a felső és alsó határ között egyenletes eloszlással generált véletlen számmal
- A kiválasztott génhez hozzáad egy Gauss eloszlású véletlenszerű értéket; ha ez kívül esik az adott gén megadott alsó vagy felső határán, akkor az új génértéket levágják a határnál

Kezdetben a mutációk az állapottér hatékony feltárását eredményezik, a későbbiekben a lokális minimumokból való kizökkentés a szerepük. A globális optimum közelében tartózkodó populáció esetében azonban kérészéletűek, hiszen kevésbé lesznek fittek társaiknál.



5. ábra – Mutáció

2.1.5 Keresztezés

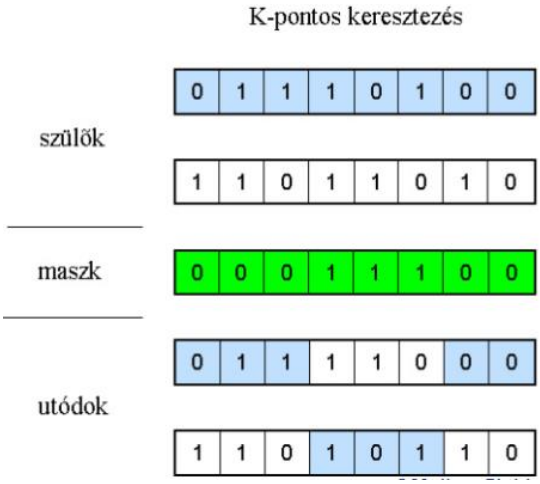
Keresztezés vagy rekombináció alatt értjük azt a folyamatot, amikor két kiválasztott egyedet valamilyen „módszer” alapján egyesítjük. Minden egyes szülőpár esetén két utódot hozunk létre. A genetikus algoritmus előnye főleg a keresztezésből származik, így ez a rész van kerül a legrészletesebb ismertetésre.

A kereszteződés történhet többféleképpen, mindig a problémához kell igazítani a módszert:

- Egypontos keresztezés – A szülőket két részre osztja, és ezeket a részeket cseréli fel egymással, példa a 6. ábrán látható.

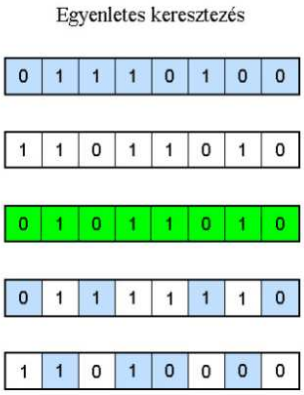
6. ábra - Egypontos keresztezés

- K-pontos keresztezés – A szülőket k+1 részre osztja, majd ezekből hozza létre az utódokat, példa a 7. ábrán látható.



7. ábra - K-pontos keresztezés

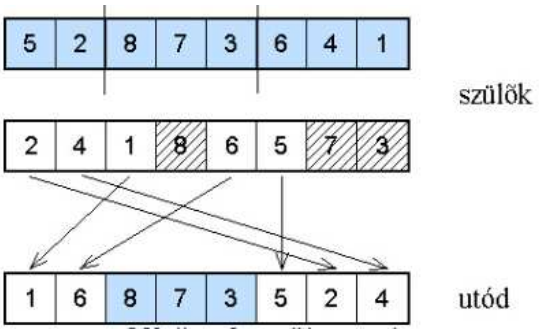
- Egyenletes keresztezés (uniform crossover) – Minden pont meghatározott valószínűséggel származhat, egyik vagy másik szülőtől, példa a 8. ábrán.



8. ábra - Egyenletes keresztezés

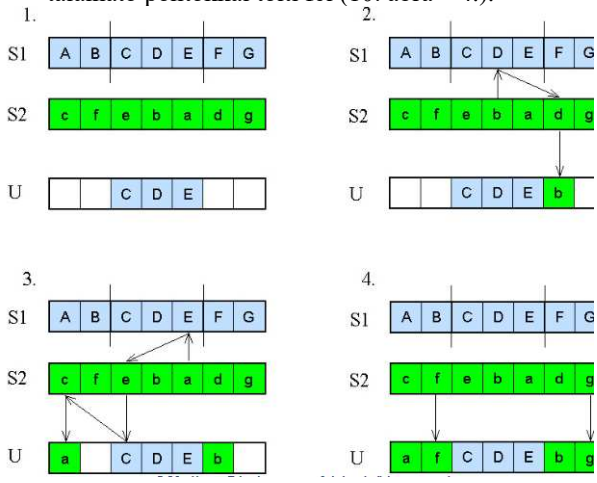
- DAVIS sorrendi keresztezés (Order crossover, OX) – Az első permutáció véletlenszerűen kiválasztott szakasz (8,7,3) átmásolásra kerül az utód ugyanazon

részére. A maradék helyek a második permutációból (szülőből) töltődnek fel, a sorrendet betartva, de a már felhasznált pontokat kihagyva, példa a 9. ábrán található. Az utód az első szülőtől relatív sorrendi, abszolút helyzeti és szomszédsági, míg a másodiktól csak relatív sorrendi információkat örököl.



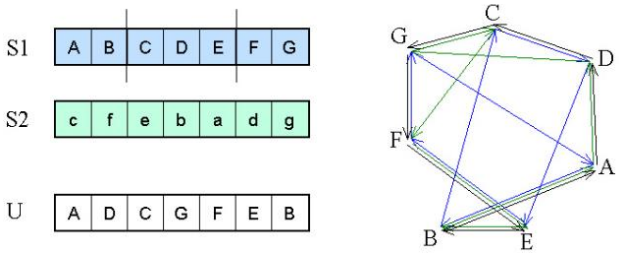
Ábra 9. ábra – Order crossover (OX)

- Részletes megfeleltetésű keresztezés (Partially mapped crossover, PMX) – Ezt az operátort Goldberg és Lingle alkották meg 1985-ben. Az eljárás a sorrendi keresztezésnél megismert módszertől abban különbözik, hogy a második szülőtől származó pontokat másképp helyezi el (10. ábra). Az S1 szülőtől átmásolt CDE részlet után (10. ábra – 1.), először azokat a pontokat helyezi el az U utódban, melyek még nem szerepelnek benne és az S2 szülőnél azokon a helyeken vannak, melyeket az utódnál már betöltöttünk, ezek a b és az a pontok. A b pont elhelyezése úgy történik, hogy megnézi melyik pont van az S1-ben a helyén, ez a D pont, ezután arra a helyre teszi a b pontot, amit a d foglal az S2-ben (10. ábra – 2.). Az a pont elhelyezése: a helyén S1-ben E van, de e helyén U-ban már C, ezért tovább kell folytatni a módszert: c helye U-ban még üres, tehát ide kerül a (10. ábra – 3.). A maradék helyeket az S2-ből ugyanazon a helyen található pontokkal tölti fel (10. ábra – 4.).



10. ábra - Partially mapped crossover (PMX)

- Order crossover 2 - Ez a módszer véletlenszerűen kiválaszt K pontot az első szülőből, megkeresi ezek helyét a másodikban, és a K pontot a második szülőben elfoglalt helyekre, de az első szülőben meghatározott sorrendben, helyezi el az utódban. A maradék pontokat a második szülőből közvetlenül másolja át az utódba.
- Élkeresztezés - Az élkeresztező eljárás az utazó ügynök problémához készített speciális operátor. Az algoritmus a permutációk szomszédsági tulajdonságait veszi figyelembe, mert ez határozza meg egy útvonal hosszát. Az eljárás először kifejezi a szülőkből a szomszédsági információkat, és tárolja őket egy táblázatban, tulajdonképpen egy mindkét szülő éleit tartalmazó gráfot rajzol fel. Ezután a táblázat (gráf) alapján egy új egyedet (útvonalat) hoz létre. Az új egyedet létrehozó eljárás többször is zsákutcába juthat az útvonal keresése közben – a 11. ábrán egy lehetséges utódot mutat [4].



11. ábra – Élkeresztezés

2.1.6 Visszahelyezés

Az utódok létrehozása után ki kell alakítani az új populációt, amelyben már az utódok is helyet kapnak. Az új populáció többféleképpen állítható elő. Az utódok lecserélhetik az előző populációt, valamilyen arányban az előző populáció egyedeiből és az utódokból fog állni, vagy pl. a fitneszfüggvény alapján dönti el az algoritmus, melyek lesznek az új populáció egyedei [1].

2.2 Alkalmazási területek

Hogyha megértjük az adaptív rendszerek működésmódját, ez alapján mesterséges adaptív rendszerek fejleszthetők [2].

Adaptáción olyan folyamatot értett, amely valaminek a struktúráját állandóan módosítja, ezzel környezetében egyre jobb hatásfokot ér el. Adaptív rendszerként a biológiai evolúciót vizsgálta, amely az alkalmazkodást azzal teszi lehetővé a változó környezeti feltételekhez, hogy állandóan változó genetikai struktúrákat generál, és örökléssel terjeszti őket.

Valamilyen szempontból egyre jobb hatásfokú, vagy egyre jobban alkalmazkodó struktúrák előállítása tulajdonképpen egy optimalizációs folyamat. Természetesen az optimum elérését összességében nem biztosítja az adaptív rendszer, de optimalizációs problémák megoldásához könnyen továbbfejleszthető. Így az evolúciós algoritmusra, mint optimalizációs módszerre szokás tekinteni, amely a legösszetettebb problémák esetén alkalmazható. Számos feladatnál, amelynek megoldása optimalizálásra visszavezethető, sikerrel alkalmazható az evolúciós algoritmus.

Az optimalizálás mellett a legkülönbözőbb területeken találkozunk az evolúciós algoritmus alkalmazásával. A mérnöki munka tervezési folyamatában legyen az akár áramkör, repülőgép tervezés, gazdasági folyamatok szimulációja, munkaütemezés, piaci árak meghatározása, szabályzók

tervezése, információ visszakeresése stb. egyaránt találunk sikeres alkalmazásokat.

A problématípusok, amelybe besorolható az alkalmazási területek többsége:

1. Részhalmaz kiválasztás: az objektumok egy halmazából ki kell választani egy részhalmazt (pl. hiba diagnosztika)
2. Szcenárió generálás: a rendszer szimulálása, hogy különböző feltételek mellett vizsgálhassuk a rendszer dinamikáját, fejlődési tendenciáját (pl. gazdasági folyamat modellezés)
3. Paraméter beállítás: adott struktúrájú rendszer paramétereinek becslése (pl. paraméter becslés matematikai képletekhez, neurális hálókhoz).
4. Struktúra fejlesztés: optimális, megfelelő minőségű rendszerstruktúra kialakítása (pl. neurális háló struktúra, klaszterek kialakítása).
5. Hozzárendelési problémák: objektumok egy halmazát egy másik objektum halmazra képezzük le, figyelembe véve a megadott feltételeket
6. Műszaki tervezés: műveletek olyan sorrendjének a meghatározása, amelynek egy kiindulási állapotot egy kívánt állapotba transzformálnak [1]

3 ÚTVONAL-OPTIMALIZÁLÁS

3.1 Excel Solver

A Solver típusú programok olyan matematikai optimalizálási alkalmazások, amellyel matematikai feladatot lehet megoldani. Cél olyan általános modell megalkotása, melynek segítségével számos hasonló probléma megoldható. A Microsoft Excel bővítménye az Excel Solver működési elve, hogy a megszorítások figyelembevételével megvizsgálja a lehetséges megoldásokat, majd azok közül kiválasztja a számunkra legkedvezőbbet.

Excel Solver segítségével az ún. célértékcellában található képlet optimális (minimális, maximális vagy adott célértéket felvevő) értékét lehet megkeresni a megkötések vagy korlátozások felállításával a munkalapon szereplő többi képletcella értékeiben. Ehhez a Solver a cellák olyan, döntési változóknak vagy egyszerű változócelláknak nevezett csoportját használja fel, amelyek a képletek kiszámításához használhatók a célérték-vagy a korlátozáscellában. A Solver úgy módosítja a döntési változócellák értékeit, hogy megfeleljenek a korlátozáscella megkötéseinek és a célértékcellához kívánt eredményt hozzák létre [3].

3.1.1 A 2021-es versenynaptár

A 2021-es versenynaptár végül 21 nagydíjhelyszínből és 22 megrendezett futamból állt. Egy alkalommal volt dupla hétvége, ami azt jelenti, hogy egymást követő két hétvégén ugyanazon a nagydíjhelyszínen két különböző néven futó nagydíjat rendeztek.

Az 1. táblázatban lehet látni a pályák nevét és a földrajzi koordinátáikat.

1. táblázat - A pályák elnevezései és földrajzi koordinátái

	Circuit	Latitude	Longitude
1	Bahrain International Circuit	26.0325	50.510556
2	Imola Circuit	44.34111	11.713333
3	Algarve International Circuit	37.232	-8.632
4	Circuit de Barcelona-Catalunya	41.57	2.261111
5	Circuit de Monaco	43.734722	7.420556
6	Baku City Circuit	40.3725	49.853333
7	Circuit Paul Ricard	43.250556	5.791667
8	Red Bull Ring	47.219722	14.764722
9	Silverstone Circuit	52.078611	-1.016944
10	Hungaroring	47.582222	19.251111
11	Circuit de Spa-Francorchamps	50.437222	5.971389
12	Circuit Zandvoort	52.388819	4.540922
13	Monza Circuit	45.620556	9.289444
14	Sochi Autodrom	43.410278	39.968271
15	Istanbul Park	40.951667	29.405
16	Circuit de Americas	30.132778	-97.64111
17	Autódromo Hermanos Rodriguez	19.406111	-99.0925
18	Interlagos Circuit	-23.70111	-46.69722
19	Losail International Circuit	25.49	51.454167
20	Jeddah Corniche Circuit	21.631944	39.104444
21	Yas Marina Circuit	24.467222	54.603056

A következő lépés a pályák földrajzi koordinátái között kiszámítani a távolságot euklideszi módszerrel.

A 2. táblázatban balról láthatjuk az optimalizálás előtti távolságokat, sorrendet és az összegüket, ez a sorrend az, amit a valóságban meg is valósítottak, tehát a versenynaptár sorrendje. Jobbról láthatjuk az optimalizálás utáni eredményeket, láthatjuk a megváltozott sorrendet.

Az eredeti összeg 630,497(66 288.536 km) volt, míg optimalizáció után az eredmény 396,3041(41 957,074 km) lett. Ez jelentős javulást jelent, ki tudjuk jelenteni, hogy az Excel Solver kitűnően végezte munkáját.

2. táblázat - Az útvonal hossza optimalizálás előtt és után

1	42.9002		7	3.9101
2	21.5516		4	11.7251
3	11.7251		3	71.8457
4	5.5952		18	67.8491
5	42.5658		17	10.8244
6	44.1556		16	99.0851
7	9.8117		9	5.5665
8	16.5127		12	2.4197
9	20.7608		11	9.3635
10	13.5832		8	4.5010
11	2.4197		10	12.1271
12	8.2679		15	10.8456
13	30.7583		14	10.3413
14	10.8456		6	16.5993
15	127.5059		21	3.3108
16	10.8244		19	1.0884
17	67.8491		1	12.2256
18	109.7883		20	35.5806
19	12.9383		2	2.7408
20	15.7558		13	2.6550
21	4.3816		5	1.6993
1			7	
Total	630.4969		Total	396.3041

3.1.2 Az összes eddigi, azaz 73 pálya

A Formula – 1 1950 óta íródó történelmében a 2020-as évig összesen 73 pálya szerepelt. Érdekes optimalizációs feladat megtalálni azt a legrövidebb utat, amivel az összes pályát be lehet járni. Ennél a feladatnál jóval nagyobb táblázatokról van szó, 73x73=5329 cellából állóról. Szintén a pályák földrajzi koordinátái és a közöttük lévő euklideszi módszerrel kiszámított távolság alapján történt az optimalizáció.

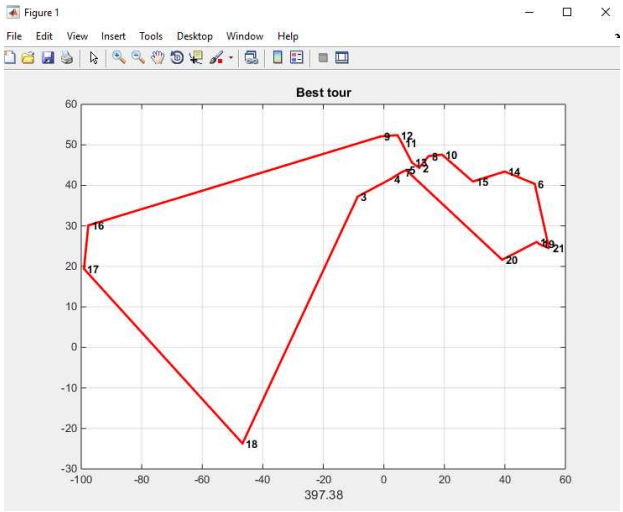
Mikor ABC sorrendbe lettek állítva a pályák, a közöttük lévő távolság összege 5232,484 (553 973,546 km) volt, ezután használatra került az Excel Solver és optimalizáció után ez a távolság 953,542 (100 953,399 km) lett. Solver ismét remekül teljesített, sokkal rövidebb optimális útvonalat talált, mint amilyen az eredeti volt.

3.2 Matlab

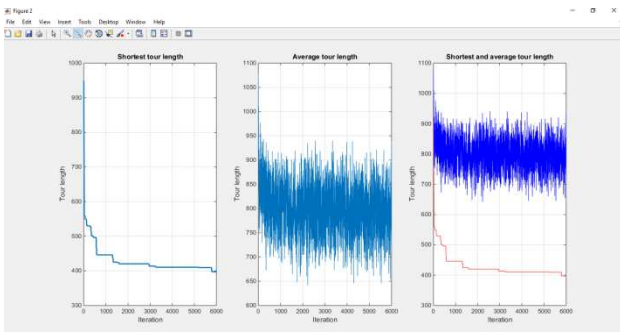
A Matlabban írt program az evolúciós algoritmus során használt módszereket alkalmazza, mint amilyen a szelekció, mutáció, keresztezés és a visszahelyezés. A program egyszerre 8 egyednél keresi az optimális útvonalat, tetszőleges számú generációra tudjuk lefuttatni a programot. Ahhoz, hogy minél jobb, azaz optimális, eredményt kapjunk, célszerűbb minél több generációra futtatni a programot, egy bizonyos pontig, amíg látjuk az eredmény javulását.

3.2.1 A 2021-es versenynaptára

A 12-es ábrán lehet látni a koordinátarendszerben megadott pályák koordinátáit és az optimalizáció után eredményként berajzolt optimális útvonalat. Az optimalizáció után a kapott eredmény, azaz az optimális útvonalhossz 397,38 (42 071,415 km).



12. ábra - Az optimalizáció utáni útvonal grafikonon ábrázolva

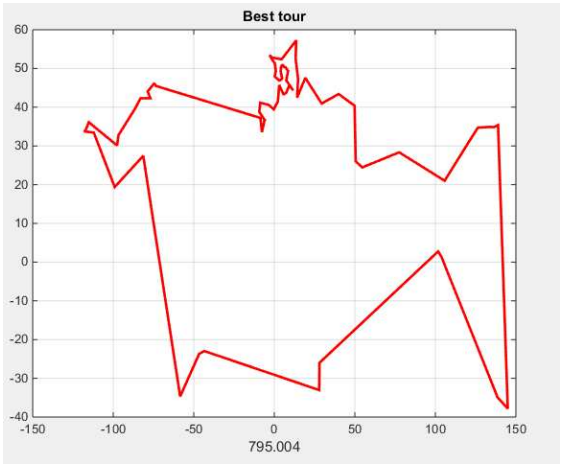


13. ábra - A legrövidebb, az átlagos útvonal és a kettő összevetve egy grafikonon

A program 6000 generációra lett lefuttatva (13. ábra), ha növeljük a generációszámot ettől nagyobbra, nincs jelentős javulás, nem produkált a program ettől rövidebb útvonalat. Az ábrán három grafikon látható, balról a legrövidebb útvonalak értéke van bejelölve, a középsőn az átlagútvonalak, jobbról pedig mindkettő összevetve. Mindhárom grafikon a generációk futtatásának függvényében alakul.

3.2.2 Az összes eddigi, azaz 73 pálya

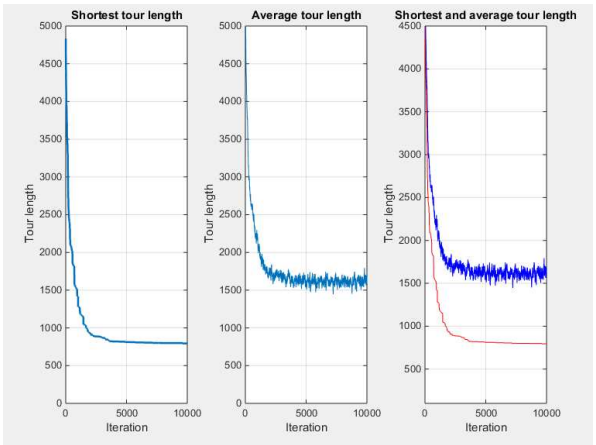
Egy kicsit egyszerűbb feladat után egy bonyolultabb lett feladva a Matlabban íródott programnak. Ugyanazokkal a koordinátákkal dolgozott ugyanolyan sorrendben, mint az Excel, azonban más eredményt produkált. Az optimális útvonal az alábbi ábrán látható. A program 50 egyedre és 10.000 generációra lett lefuttatva (14. ábra).



14. ábra - Az optimalizáció utáni útvonal és annak hossza

Láthatjuk, hogy a program lefutása után a kapott eredmény 795,004 (84 168,664 km) lett, ami jobb, mint az Excelben kapott. A 15. ábrán az optimális útvonal látható rávetítve a világtérképre.

15. ábra - Az optimalizált útvonal rávetítve a világtérképre



16. ábra - A legrövidebb, az átlagos útvonal és a kettő összevetve egy grafikonon

A 16. ábrán látszik, hogy az optimalizáció hasonlóan indult, mint Excelben, 5000 körüli értkétől, azonban az optimális útvonal hossza kevesebb lett.

A programot lehet futtatni Részletes megfeleltetésű keresztezéssel (PMX) és Order crossoverrel (OX) illetve keresztezés nélkül is. Hasonló eredmények születnek mindhárom alkalommal. Mikor keresztezés nélkül fut a program, lényegesen gyorsabban lefut, viszont korai konvergencia következik be, azaz gyorsan eléri az optimumot, utána pedig már nem javul tovább.

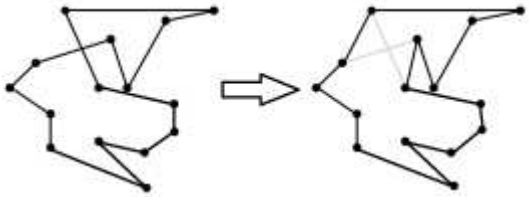
3.2.3 2-opt módszer

1958-ban Croes találta ki a módszert Az utazóügynök probléma megoldására. Ez egy javító algoritmus, tehát már egy meglévő utat fejleszt.

Alapelve:

- Vesz kér élet a körútból. Legyen ezek súlya s (a, b) és s (c, d)
- Összeköti a két élhez tartozó négy csúcsot (nem lehet a két élnek közös csúcsa) úgy, hogy új körutat kapjunk. Ezt csak egyféleképpen tehetjük meg úgy, hogy továbbra is körutat kapjunk.
- Az élek új súlyai s (a, c) és s (b, d). Ha ezek kisebbek, mint s (a, b) és s (c, d) akkor az eredeti éleket lecseréljük a kisebb összsúlyú élekre.

Az algoritmus akkor áll le, ha már nem tudunk cserét végrehajtani (17. ábra).



17. ábra - 2-opt. példa

A programba a 2-opt. módszer is beépítésre került, amelynek pozitívuma, hogy a program futása közben látható ahogy az élnek cserélődnek és ahogy rövidül az útvonalhossz. Szintén hasonló eredményeket kaptunk, mint az előbb említett módszerekkel. A versenynaptár optimalizálásakor 40 848,594 km-t, míg az összes nagydíjhelyszín esetén 86 181,925 km-t.

4 Összegzés

A munka az elméleti és gyakorlati részből áll. Az elméleti részben főleg az evolúciós algoritmusok fogalma, működési elve, alkalmazási területei kerülnek feldolgozásra. Milyen eljárásokat használ, mik a kulcs fogalmak. Számos alkalmazási területe van, azaz számos problématípust meg lehet oldani a segítségével, mint a pl. részhalmaz kiválasztás, struktúra fejlesztés, műszaki tervezés stb.

A gyakorlati részben útvonal-optimalizációra került sor a Microsoft Excel Solver nevű bővítményével, illetve Matlabbal. Mindkét módszer ugyanazokon az alapokon nyugszik, evolúciós algoritmust használ. Amíg a Solver egy beépített funkció, nem tudjuk valójában mi történik, addig Matlabban, pontosan látjuk, milyen lépések mennek végbe, hogyan is történik valójában az optimalizáció. A 2021-es versenynaptár került optimalizálásra, ami 21 nagydíjhelyszínt tartalmaz, tehát 21 koordinátapár közötti utat kellett optimalizálni, tehát a legrövidebbet megtalálni. A koordináták között euklideszi módszerrel került kiszámításra a távolság, ezekkel a távolságokkal lett a későbbiekben dolgozva.

Solver csak egy bizonyos mennyiségű beviteli adattal tud jó eredményeket elérni, ugyanis mikor az eddigi összes nagydíjhelyszín, azaz a szám szerint 73 koordinátáit és a közöttük lévő távolság lett beviteli adatként megadva, közel sem tudott olyan mértékű optimalizálást végrehajtani, mint előtte kevesebb adattal.

Ami a versenynaptárt illeti Excelben kilométerben kifejezve az optimalizálás előttiútvonal hossza 66 288.536 km, míg az optimalizált 41 957,074 km, Matlabban (keresztezéssel és 2-opt-tal is) optimalizálás után 40 848,594 km-t kaptunk, közel 1000 kilométernyi a különbség a két módszer között.

Ami az összes eddigi, azaz 73 pályát érinti, az optimalizáció előtti útvonal hossz kilométerbe átszámítva 553 973,546 km (viszonyítási alapként ez több mint tizenháromsorosa az egyenlítő hosszának), Excelben optimalizálás után 139 465,186 km, míg Matlabban86 131,107 km. Matlabban az optimális útvonal több mint50000 kilométerrel rövidebb, mint Excelben. Mindkét módszerrel jóval rövidebb utat találtunk az eredetinél, azonban ebben a feladatban Matlabban írt program jobban teljesített az Excelnél. A 2-opt. módszerrel optimalizálás után 86 181,925 km-t kaptunk, tehát mindössze 50 kilométernyi különbség van ekkora távra a keresztezési módszerek és a 2-opt. módszer között, tehát mindkettő sokkal jobban teljesített, mint az Excel. A következő lépés a 3-opt módszer beépítése lenne a programba.

5 Irodalomjegyzék

[1] Borgulya István: Evolúciós algoritmusok, Dialóg Campus Kiadó, 2004, ISBN 963 9542 41 5

[2] John Henry Holland: Adaptation in Natural and Artificial Systems, 1975

[3] Bence Keresztury: Genetic Algorithms and the Traveling Salesman Problem, 2017

[4] Takács Á., dr. Kamondi L. - A genetikus algoritmusok

[5] Kulcsár Z. – Az utazóügynök probléma és alkalmazásai, 2017

[6] Kramer, O. (2017). Genetic Algorithms, Studies in Computational Intelligence, 11-19. Doi: 10.1007/978-3-319-52156-5_2

[7] Shukla, A., Pandey, H. M., & Mehrotra, D. (2015). Comparative review of selection techniques in genetic algorithm. 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE). Doi: 10.1109/ablaze.2015.7154916

[8] Sastry, K., Goldberg, D., & Kendall, G. (2005). Genetic Algorithms. Search Methodologies, 97-125. https://doi.org/10.1007/0-387-28356-0_4

[9] Algoritmi veštačke inteligencije, edicija Grokking, Rishal Hurbans Kompjuter biblioteka – Beograd (2021) ISBN: 978-8673105611

[10] Michael Negnevitsky: Artificial Intelligence, A Guide to Intelligent Systems. Pearson Education Canada; 3rd edition (2011) ISBN: 978-1408225745

Fuzzy Rule-Based Investigation of System Reliability with Reliability Block Diagram Method

Hamid Ali Hama Salih
Óbuda University Institute of Mechatronics and Vehicle Engineering, Budapest, Hungary
Hamid.Ali.Hama.Salih@gmail.com

Abstract — **This study analyzes the dependability of a simple network architecture using a fuzzy method that is similar to a stochastic one. This concept is taken from the Fuzzy Fault Tree Analysis (FFTA), which considers the OR and AND gate connections between sets and the maximum and minimum of the membership function inside each set. A Fuzzy Reliability Block Diagram (FRBD) has a maximum of the membership functions in case of parallel connection and a minimum of the membership functions in case of series connection.**

Keywords: Fuzzy reliability, failure data, fuzzy possibility, membership function.

1 INTRODUCTION

The system is comprised of one or more subsystems, all of which are interconnected and share components to accomplish their respective duties. A system can be anything from a single machine to a network made up of the same components that are currently considered to be components. Regarding presentation options, the system is entirely flexible. This greatly depends on the context.

Reliability refers to the extent to which actual system performance matches expectations. This relationship is accounted for by stochastic system model assumptions, which provide a metric for system reliability that is based on component reliability. In order to establish the overall system's reliability, it is necessary to characterize and analyze the properties of each component. A new method for possibilities uncertainty analysis of a simple structure system's reliability has been demonstrated. In this context, the primary objective of this paper is to present a methodology to determine the fuzzy reliability of a simple structure system and investigate the block diagram method, as well as determine the fuzzy rule base to solve a case study.

Sharma and Mukesh K, respectively, demonstrated If a system's behavior can be adequately specified within the framework of probability measure, then its reliability can be defined as the probability that it effectively performs its designated function over a specified time period. In practice, however, system parameters are typically imprecise (fuzzy) due to missing or unavailable information, and the probabilistic approach to traditional reliability analysis is insufficient to account for such inherent uncertainties. To achieve this objective, fuzzy reliability, a novel concept introduced and formalized within the framework of probability theory, is employed.[1]

Qimi Jiang and Chun-Hsien Chen presented a computational model of fuzzy dependability with a focus on the application of random general stress-fuzzy general strength to the resolution of engineering problems. This computational model is founded on a mathematical transition that enables the calculation of fuzzy probability using the computational method of conventional probability. On the basis of this computational model, a numerical technique is provided for calculating the imprecise dependability of mechanical elements, sensors, and so on. This paves the way for the analysis of the dependability of systems composed of components whose dependability is uncertain. The case study validates the efficacy of the method by evaluating the fuzzy reliability analysis of a sensor type used in railway systems. The computational results confirm the algorithm's compatibility with engineering practice.[2]

Fabio Biondini, Franco Bontempi, and Pier Giorgio Malerba developed a very general method for determining the safety of reinforced and prestressed concrete structures. Numerous sources of ambiguity are well-known to influence the exact values of the parameters that regulate the geometrical and mechanical characteristics of such structures. Such characteristics cannot be regarded as fixed parameters in the real world. In the current study, all of these unknowns are modeled using a fuzzy criterion, in which the model is not specified by a singular value but by a range of possible values. Different serviceability and ultimate limit states are used to characterize the reliability issue at the load level. The membership function of the safety factor is computed by solving an associated anti-optimization problem for each limit state's critical interval. The overall strategy of this solution procedure is guided by a genetic algorithm that generates random values for the parameters of the material and geometric nonlinear structure assessments.[3]

Reliability has emerged as a key factor in the design and operation of today's enormous, complex, and expensive mechatronics systems. Modern mechatronics systems cannot operate without the durability and dependability of their constituent parts. However, failure physics modeling and familiarity with probability and statistics are required for the field of reliability theory. Therefore, mathematical dependability models are indispensable to this scientific discipline. Possibly the most prevalent method employed in reliability analysis today is one that evaluates the system as a whole by evaluating its individual components.

1.1 Structure of Paper

The structure of the paper is as follows: The first section presented the introduction which includes the problem statement and objective of the paper along with the literature review. In section 2, a synopsis of the Fuzzy Reliability Block Diagram (FRBD) is presented. The Fuzzy Rule Base (FRB) is presented in section 3. Section four presents the conclusion.

2 FUZZY RELIABILITY BLOCK DIAGRAM (FRBD)

There is always the risk of anything going wrong, whether it involves a technique, a component, a piece of equipment, a system, or a person. A deterministic, oversimplified, and utopian viewpoint allows for 100% reliability. When it comes to functioning in the real world, none of us is perfect. Nothing is impervious to the wear and tear that time and circumstance inevitably inflict. Predicting and avoiding failures is the focus of reliability engineering. In order to evaluate reliability issues, it is important to know the why, how, and how often failures occur, as well as the cost of failure in terms of money, effort, and goodwill. [4]

All problems with system dependability can be traced back to specific tangible defects, which can then be corrected. In reality, almost all prospective failures are inadequately understood, making failure prediction a probabilistic challenge in reliability analysis.

2.1 Series Connection Structure

Any structure or system in which some subset of *n* components is required for proper operation is said to be "series-dependent." All of the pieces in a series system must be operational for the system as a whole to be in a condition where failure is impossible. In a series-configured system, if any part of the system fails, the whole thing will go down with it.[5]

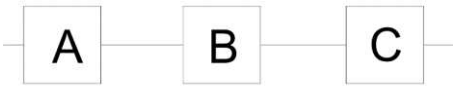


Figure 1: Reliability block diagram for series systems. (WILEY, 2021)

Table 1: Fuzzy set representation series structure data.

μ_{sys}	y	A	B	C
	$\mu_{sys}(y)$	0.9	0.8	0.75

Element (A, B, and C) are connected in series.

$$\mu_{sys} = min\ (\mu_A; \mu_B; \mu_C); \mu_{sys} = 0.75 \qquad (1)$$

The Fuzzy Reliability Block Diagram of series connection works when all the sets of the universe or system work which comes from the minimum possibility of membership function in the set or between the sets because the Fuzzy Fault Tree Analysis of series connection comes from the maximum possibility of membership function (OR-gate) in the set or between the sets.

2.2 Parallel Connection Structure

A parallel structure or system is one in which the system is considered to be operational if any one of its *n* components is doing its job.[5]

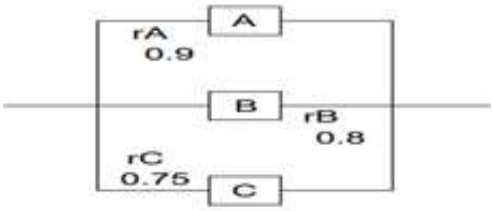


Figure 2: Reliability block diagram for parallel systems. (WILEY, 2021)

In order to provide a failsafe mechanism, it is usual practice to use parallel systems. The Fuzzy Reliability Block Diagram of parallel connection works when one of the sets of the universe or system is working which comes from the maximum possibility of membership function in the set or between the sets because the Fuzzy Fault Tree Analysis of parallel connection it comes from the minimum possibility of membership function (AND-gate) in the set or between the sets.

Table 2: Fuzzy set representation of parallel structure data.

μ_{sys}	y	A	B	C
	$\mu_{sys}(y)$	0.9	0.8	0.75

$$\mu_{sys} = max\ (\mu_A; \mu_B; \mu_C); \mu_{sys} = 0.9 \qquad (2)$$

2.3 Combined Connection Structure

The term "redundancy" is used to describe the practice of replicating essential parts or processes in order to boost system reliability (as with a backup or fail-safe) or performance (as with GNSS receivers or multi-threaded computer processing). [6]

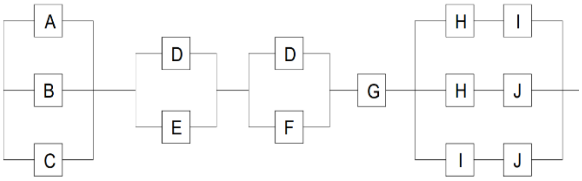


Figure 3: Reliability block diagram study case example.[7]

Table 3: Fuzzy set representation data of study case example.

μ_{sys}	y	A	B	C	D	E
	$\mu_{sys}(y)$	0.9	0.8	0.75	0.85	0.65

μ_{sys}	y	F	G	H	I	J
	$\mu_{sys}(y)$	0.95	0.55	0.7	0.8	0.6

Element (A, B, and C) are connected in Parallel and they become a block 1.

μ_1= max (max (μ_A, μ_B), μ_C);

Element (D and E) are connected in parallel and they become a block 2.

μ_2= max (μ_D, μ_E);

Element (D and F) are connected in parallel and they become block 3.

μ_3= max (μ_D, μ_F);

There is a series connection between block (1,2, and 3) and element G and they become block 4.

μ_4= min (min (μ_1, μ_2), min (μ_3, μ_G));

Element (H and I) are connected in series and they become block 5.

μ_5= min (μ_H, μ_I);

Elements (H and J) are connected in series and they become block 6.

μ_6= min (μ_H, μ_J);

Element (I and J) are connected in series and they become block 7.

μ_7= min (μ_I, μ_J);

There is a parallel connection between blocks (5, 6, and 7) and they become block 8.

μ_8= max (max (μ_5, μ_6), μ_7);

The fuzzy reliability of the system will be a series of connections between blocks (4 and 8).

μ_{sys}= min (μ_4, μ_8)

μ_{sys} = 0.5500

3 FUZZY RULE-BASE

In 1965, L. A. Zadeh developed the concept of fuzzy sets for the first time. The objective was to provide a line of reasoning that may be useful in solving problems that have proven difficult to solve in the past. The main innovation was a little tweak to the traditional mathematical concept of sets. This simultaneously defined a membership function and a membership degree, resulting in a blurring of previously separate categories.[8]

Four of the most important components of a Fuzzy rule-based inference system are shown in Figure 4.

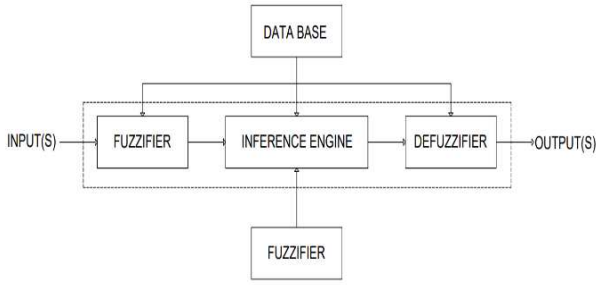


Figure 4: Fuzzy inference system architecture.[8]

Both the input and the output variables are characterized by means of fuzzy sets in the Fuzzifier. At this point, you may substitute metaphorical language and interval numbers for straightforward, simple values.[8]

All of the available knowledge from subject matter experts is collected in the Rule Base and organized according to the identified problem. In order to create the fuzzy rules, we use the conditional expression "IF...(antecedent(s)) ... THEN... (consequence(s)) to build and connect the variables for input and output. Inside the Inference Engine, the rules are activated.[9]

The strength of the current depends on how strongly the independent variables that were utilized to generate the Fuzzy output set are connected to one another. Fuzzy inference comes in many forms, including the Sugeno type, the Mamdani type, and the Tsukamoto type.[10]

One of the most common kinds of inference system, the Mamdani type is used to convey expert knowledge in light of historical data. Here, the conclusion is shown by way of an example. Let's go through the steps of explaining a simple system that has two input variables (x_1 and x_2) and a single output variable (y). The distribution of the variables within their respective classes is shown in Figure 5.[11]

In the situation where x_1 = a and x_2 = b, there are two rules that might be triggered:

$$R_1: IF\ X_1 = A_2\ AND\ X_2 = B_3\ THEN\ Y = C_3 \quad (3)$$

$$R_2: IF\ X_1 = A_3\ AND\ X_2 = B_3\ THEN\ Y = C_2 \quad (4)$$

According to the first rule, the red line represents (a) member's second degree in A_2, whereas the green line represents (b)'s second degree in B_3. The conditions are all interconnected in an AND fashion. Hence, the rule's effectiveness is equal to the lowest membership value. As a result, the red color denotes a C_3 activation state.[10]

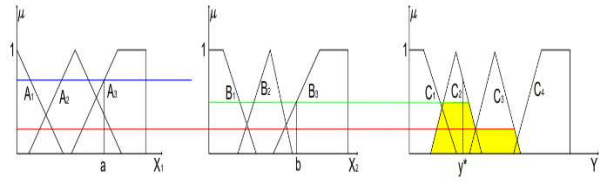


Figure 5: The Mamdani deduction or conclusion.[8]

$R_1: IF\ X_1 = A_2\ AND\ X_2 = B_3\ THEN\ Y = C_3 R_2: IF\ X_1 = A_3\ AND\ X_2 = B_3\ THEN\ Y = C_2$On the other side, the second rule has also been brought into play. The levels of membership are represented by lines that are blue (in the case of A_3) and green (for B_3) respectively. The AND connection may be thought of as reducing their firing power to their minimum, as seen by the green level in the second rule. It is going to be the level (for C_2). In conclusion, the response to the active rules is the conjunction of all the outcomes (the shaded yellow area in Figure 5).[11]

In order to make a more objective evaluation of the resulting Fuzzy set, the next step is to transform it into a form that is more amenable to such an analysis. Specifically, this is a step that the Defuzzifier does before the translation is complete. The illustrative Figure 5 demonstrates the complexities of the result and the resulting perplexity. Therefore, defuzzification is crucial. Hence, a result (y * in Figure 5) that is easier to interpret is attainable. There are a number of different approaches to defuzzification, but no overarching paradigm has been offered for choosing the most effective one. The best solution is the one that is created specifically for the problem at hand.[12]

A fuzzy inference system might be useful if the problem being investigated is shrouded in uncertainty, there is a dearth of information, there are too many outside influences, or the connection between the two is hard to identify.[12]

3.1 Case Study Example for Fuzzy Rule Base (FRB)

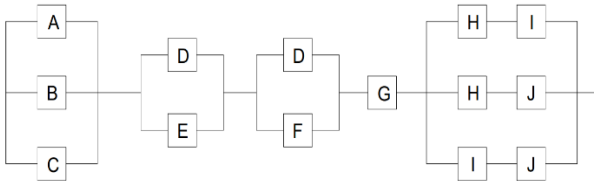


Figure 6: Fuzzy rule base study case example.[7]

Table 3: Fuzzy rule base representation of study case example data.

μ_{sys}	y	A	B	C	D	E
	$\mu_{sys}(y)$	0.9	0.8	0.75	0.85	0.65

μ_{sys}	y	F	G	H	I	J
	$\mu_{sys}(y)$	0.95	0.55	0.7	0.8	0.6

Type	Num. Membership Function	Range
Mamdani	1	[0 1]

Membership Function type	Mf-value
S-shape mf	[0.25 1]

Num. Input	Num. Output	Num. Rules	Defuzzification
18	9	9	Centroid

AND-gate	OR-gate	Implication	Aggregation
min	max	min	max

$$R_1: IF\ (A = mf(\mu_A))\ OR\ (B = mf(\mu_B))\ OR\ (C = mf(\mu_C))\ THEN\ (\mu_1 = mf(\mu_1))$$

$$R_2: IF\ (D = mf(\mu_D))\ OR\ (E = mf(\mu_E))\ THEN\ (\mu_2 = mf(\mu_2))$$

$$R_3: IF\ (D = mf(\mu_D))\ OR\ (F = mf(\mu_F))\ THEN\ (\mu_3 = mf(\mu_3))$$

$$R_4: IF\ (G = mf(\mu_G))\ AND\ (\mu_1 = mf(\mu_1))\ AND\ (\mu_2 = mf(\mu_2))\ AND\ (\mu_3 = mf(\mu_3))\ THEN\ (\mu_4 = mf(\mu_4))$$

$$R_5: IF\ (H = mf(\mu_H))\ AND\ (I = mf(\mu_I))\ THEN\ (\mu_5 = mf(\mu_5))$$

$$R_6: IF\ (H = mf(\mu_H))\ AND\ (J = mf(\mu_J))\ THEN\ (\mu_6 = mf(\mu_6))$$

$$R_7: IF\ (I = mf(\mu_I))\ AND\ (J = mf(\mu_J))\ THEN\ (\mu_7 = mf(\mu_7))$$

$$R_8: IF\ (\mu_5 = mf(\mu_5))\ OR\ (\mu_6 = mf(\mu_6))\ OR\ (\mu_7 = mf(\mu_7))\ THEN\ (\mu_8 = mf(\mu_8))$$

$$R_9: IF\ (\mu_4 = mf(\mu_4))\ AND\ (\mu_8 = mf(\mu_8))\ THEN\ \mu_{System} = mf(\mu_{System})$$

$$\mu_{System} = 0.766$$

[Rules]

1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0, 1 0 0 0 0 0 0 0 0 : 2
0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0, 0 1 0 0 0 0 0 0 0 : 2
0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0, 0 0 1 0 0 0 0 0 0 : 2
0 0 0 0 0 0 1 0 0 0 1 1 1 0 0 0 0 0, 0 0 0 1 0 0 0 0 0 : 1
0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0, 0 0 0 0 1 0 0 0 0 : 1
0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0, 0 0 0 0 0 1 0 0 0 : 1
0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0, 0 0 0 0 0 0 1 0 0 : 1
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 0, 0 0 0 0 0 0 0 1 0 : 2
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1, 0 0 0 0 0 0 0 0 1 : 1

4 Conclusion

The following conclusions can be deduced from the results of analysis:

1. The conventional reliability of a system depends on the probability of the system functioning, whereas the fuzzy reliability of a system depends on the possibility that the system is functioning.

2. In the Fuzzy Reliability Block Diagram (FRBD), the maximum of the membership function is represented by an OR gate connection and is applied for parallel connection whereas the minimum of the membership function is represented by an AND gate connection and is applied for series connection.

3. Calculations are required to determine the criteria of the classic reliability of the system in order to determine which sets can provide the best results, whereas in fuzzy reliability the criteria are the connection structure, and the concept of maximum and minimum is used to determine the criteria of fuzzy reliability.

4. The element with the most significant role in this study is element *G* for the Fuzzy Reliability Block Diagram (FRBD), because element *G* is connected in series with the other elements. This means that if element G's reliability is zero, the entire system's

Reliability is also zero.

5. Fuzzy Reliability Block Diagram (FRBD) can be utilized during troubleshooting when maintenance professionals rely on their generalized experiences. This thinking should be investigated using fuzzy set theory (also known as possibility theory) because these experiences can be interpreted through linguistic variables.

6. In the Fuzzy Rule Base the Mamdani inference system, the S-shape function as a membership function, and the centroid method for defuzzification has been determined, the defuzzifier value represents the fuzzy reliability of the system.

Acknowledgements

I am indebted to my advisor, [**László Pokoradi**], for their unwavering support and counsel throughout my master's program. Their knowledge and patience have been indispensable to me and crucial to this paper's success.

I am appreciative to [**Óbuda University**] for granting me permission to conduct research and for all the resources and support they provided.

I would also like to thank [**Committee**] for serving on the committee for my paper and for providing insightful

feedback and suggestions. Their guidance and insights were crucial in shaping my research and enabling me to write this paper.

REFERENCES

[1] Sharma, M. K. (2017). Possibility and Probability Aspect to Fuzzy Reliability . *Global Journal of Pure and Applied Mathematics., 13*(7), 3641-3655.

[2] Qimi Jiang, C.-H. C. (2003). A numerical algorithm of fuzzy reliability. *Reliability Engineering & System Safety, 80*(3), 299-307.

[3] Fabio Biondini a, F. B. (2004). Fuzzy reliability analysis of concrete structures. *Computers & Structures, 82*(13-14), 1033-1052.

[4] Zhen-zhou, G. S.-x. (2003). Procedure for computing the possibility and fuzzy probability of failure of structures. *Journal: Applied Mathematics and Mechanics, 24*(3), 338.

[5] WILEY. (2021). *RELIABILITY ENGINEERING* (Third Edition. kiad.). Piscataway, NJ, USA: ELSAYED A. ELSAYED.

[6] Coit, D. W. (29 Oct 2010). Maximization of System Reliability with a Choice of Redundancy Strategies. *IIE Transactions, 35, 2003*(6), 535-543.

[7] Castanier, B. (2020). *Reliability Engineering: Introduction to the concepts and methods.* Rue de Rennes: Polytech Angers.

[8] Lukács, J. (2021). The Investigation of the Applicability of Fuzzy . *Acta Polytechnica Hungarica, 18*(11), 19.

[9] Jesus, M. J. (January 1999). A proposal on reasoning methods in fuzzy rule-based classification systems. *ELSEVIER, 20*(1), 21-45.

[10] Pokorádi, L. (2022). Fuzzy rule-based hierarchical overall risk analysis of battery testing laboratories. *SJR Scopus - Computer Science (miscellaneous), 23*(1), 89-97.

[11] E.H. Mamdani, S. A. (January 1975). An experiment in linguistic synthesis with a fuzzy logic controller. *International Journal of Man-Machine Studies, 7*(1), 1-13.

[12] Ayres, N. (2021). A Mamdani Type Fuzzy Inference System to Calculate Employee Susceptibility to Phishing Attacks. *Applied Sciences, 11*(1), 19.

Feladatmegoldókészség fuzzy szabálybázisú becslése

Fuzzy rule-based model of task solving skills

Stein Vera, Pokorádi László
Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Budapest, Magyarország
stein.vera@bgk.uni-obuda.hu, pokoradi.laszlo@bgk.uni-obuda.hu

***Összefoglalás* – Napjainkban egyre nagyobb teret kapnak az olyan jellegű kutatások, melyek azt vizsgálják, hogy a felsőoktatásból kikerülő hallgatók milyen oktatási módszerek segítségével válhatnak a munkaerőpiaci elvárásoknak mind jobban megfelelő szakemberekké. A tanulmány egy ilyen kutatás részeként egy mikrokísérlet nyomonkövetése, és kiértékelése fuzzy következtetési rendszer alkalmazásával. A tanulmányban áttekintjük a rendszer bemenetéül szolgáló tárgyi tudást mérő relevancia, és a motiváltságot mérő alapossági gény mutatószámok képzésének módszerét, valamint az alkalmazott fuzzy következtetések definícióit a hallgatói feladatmegoldó-készségre vonatkoztatva. Az eljárás és a defuzzifikálás során nyert minősítő végeredmények tükrében pedig lehetővé válik az egyes hallgatói teljesítmények objektívebb értékelése.**

Kulcsszavak: fuzzy, feladatmegoldókészség, alapossági gény, relevancia, teljesítményértékelés

***Abstract* – Nowadays, there is a growing body of research on what educational methods can help students that are graduating from higher education to become better-equipped professionals to meet the demands of the labour market. This study is part of such research, monitoring and evaluating a micro-experiment using a fuzzy inference system. In this paper review the method of training the subject knowledge relevance as an input to the system, and the method of generating the motivation thoroughness metrics, as well as the definitions of the fuzzy inference applied to student task solving ability. In addition, in the light of the procedure and the qualitative results obtained during the defuzzification process, a more objective assessment of each student's performance becomes possible.**

Keywords: fuzzy, task solving, need for thoroughness, relevant results, performance assessment

1 BEVEZETÉS

Jelen tanulmány egy komplex kutatás részét képezi, melyben azt vizsgáljuk, hogyan hat a rendszertechnika tudományának elsajátítása a mérnökhallgatók projektszemléletére.

Már önmagában a projektszemlélet definiálása, összetevőinek meghatározása, és ezek mérhetővé tétele is bőven meghaladja e mikrokísérlet kereteit, melyben azt tanulmányozzuk, hogy egy feladat megoldása során tapasztalható tárgyi tudás és a szorgalom, az alaposság igénye, hogyan alakítják a hallgatók feladatmegoldó készségét.

Az irodalomkutatás során tanulmányunk megközelítéséhez szervesen illeszkedő elemzéseket nem találtunk. Voskoglou ugyan kidolgozott egy fuzzy modellt a tanulócsoportok tudásának és készségeinek értékelésére [9], de a kiinduló adatbázist eleve már szubjektív oktatói értékelés használatával alakította ki, és a javasolt módszer a tanulócsoportok készségeit szabálybázis alkalmazása nélkül értékelte.

Johanyák [10] a következő félév hallgatói csoportlétszám és laborórák számának tervezéséhez készített modellt a hallgatói eredmények előrejelzéséhez, ahol a vizsgaeredményt fuzzy szabályinterpoláción alapuló következtetés segítségével jósolja meg. Itt pedig elsősorban az előrejelzésen, nem pedig a hallgatók teljesítményének értékelésén van a hangsúly.

A tanulmány az alábbi fejezetekből áll: A 2. fejezetben ismertetjük majd a lágyszámítási módszerrel feldolgozott adatok összegyűjtésének módszerét, és az ezekkel kapcsolatos elgondolásainkat. Ezt követi a harmadik fejezetben a fuzzy következtetési rendszer részletes bemutatása. Majd a negyedik fejezetben pedig számításaink eredményéből vonunk le következtetéseket.

2 A MIKROKISÉRLET ISMERTETÉSE

A feldolgozott adatokat egy önkéntesen megoldható, pozitívan motivált feladat kiadása során gyűjtöttük másodéves mechatronika szakos mérnökhallgatók munkáiból.

A feladat kérdésfelvetése inkább közelíti a munkavégzés során előforduló problémákat, mint a matematikában, fizikában és a műszaki felsőoktatás alapozó tantárgyaiban kiadott feladatok túlnyomó többsége. A hallgatók ugyanis nem kaptak kiindulási adatokat, és behelyettesítendő képleteket, megoldási sémákat, nem követhették a jól megszokott, „konzerv” feladatkidolgozási módszereket. Sőt, pont az volt az elérendő cél, hogy a megoldáshoz szükséges alapadatokat meghatározzák, és bemutassák azt a gondolatmenetet, melynek során eljutottak a megoldásig.

Bármilyen képzésben veszünk is részt, mindenki szembesült már tanulóként ezzel a problémával, amikor a teljesítményét értékelik. Ilyenkor az az elvárásunk, hogy ne csupán a tárgyi tudásunk, de a logikai készségünk, a szorgalmunk, a motiváltságunk, és a többiekhez

mért teljesítményünk is érvényre jusson a kapott osztályzatban, értékelésben. Objektív eredményt várunk egy teljesen szubjektív műfajban.

Természetesen a tanárok is törekszenek a mind tárgyilagosabb teljesítményértékelési rendszer kialakítására, de ez azért igen összetett és nehéz feladat. Így aztán ritkán fordulhat elő, hogy mindkét fél azonos mértékben elégedett.

Ha csak a tárgyi tudás megítélését vizsgáljuk, önmagában ez is rengeteg kérdést vet fel. Mondhatnánk, hogy egy teszt elég objektív lehet ennek méréséhez, de ha alaposabban belegondolunk, a jól mérő tesztkérdés helyes megválaszolásának könnyen lehet akadálya egy pillanatnyi zavar, hibásan értelmezett szöveg, ugyanakkor viszont a tanultak értő ismerete szükséges hozzá, ami túlmutat egyetlen kérdésen. Akármennyi pontot is érjen a kérdés, gyakorlatilag a megítélése mégiscsak bináris. Jó, vagy nem jó.

Erős túlzás lenne tehát azt állítani, hogy egy teszt kellően finom skálán alkalmas a tárgyi tudás mérésére. Ezt a módszert tehát elvetettük, maradt a hagyományosnak mondható, esszé jellegű, kifejtős kidolgoztatási mód.

További kérdés az is, hogy egy probléma kapcsán milyen módon hasonlíthatók össze egymással a leadott megoldások. Mi legyen az a szint, amihez mérünk, hol legyen a teljes megoldás?

Mikrokísérletünkben nem határoztuk meg a megoldás optimális szintjét, hanem – az egymáshoz mérhetőség kedvéért – az összes megoldás adatait összesítettük, és ehhez képest határoztuk meg az egyes feladatok %-os relevanciaszintjét.

A szorgalom mércéjének a kidolgozás alaposságigényét vettük alapul – függetlenül a leírtak helyességétől –, hogy hány egyenlettel, és magyarázó ábrával kívánta a feladat kidolgozója alátámasztani az eredményeit. Ennek optimális szintjét – a 100 %-ot – itt azonban a leadott munkák számtani átlagában határoztuk meg, mivel a szorgalom megítélése lényegesen szubjektívebb, mint a tárgyi tudás értékelése.

Az adatállomány felvétele éles értékekkel, többségében binárisan történt – az 1. ábra szerint – annak érdekében, hogy a későbbiekben mind lágyszámítási, mind matematikai statisztikai módszerekkel kiértékelhető adatállományt kaphassunk.

1. táblázat: Adatállomány

		hallgató1	…
releváns adatok	***adat1***	1	
	adat2	0	
	…		
irreleváns adatok	***hibás adat1***	0	
	hibás adat2	1	
	…		
releváns képletek száma		2	
irreleváns képletek száma		0	
magyarázó ábra van/nincs		1	
irodalomkutatás van/nincs		0	

Ebben a tanulmányban a lágyszámítás adta megoldási lehetőség kerül górcső alá.

3 A FUZZY KÖVETKEZTETÉSI RENDSZER BEMUTATÁSA

Az „emberi gondolkodásban a kezdetek óta jelen van az igény a kétértékű, túlságosan merev logikától való eltérésre, a nem szélsőségekben való gondolkodásra.” [4]

Gyakori az az irodalmi megközelítés tehát, hogy a fuzzy logikát – kiemelve azt a tulajdonságát, hogyan „lágyítja”, árnyalja a problémák megközelítését – a Boole kétértékű logikával hasonlítják össze, és definiálják az „elmosódott halmazok logikája”-ként. [2]

A pohár így félig tele van. De ugyanaz a pohár félig üres is, hiszen sok olyan feladat megoldása is cél lehet, ahol pedig a probléma fuzzy megfogalmazása teszi egyáltalán lehetővé, hogy az amúgy túl komplex, nehezen, vagy nem számszerűsíthető dolgokra mégis valamilyen számszerű megoldást találjunk, ahogy ez esetünkben is történik. Ez a megközelítés is tetten érhető Pokorádi [6] meghatározásában, miszerint a: „ fuzzy teóriájának egyik fő célja olyan módszerek kidolgozása, melyekkel szabályokba foglalhatók és megoldhatók a túlságosan bonyolult, hagyományos vizsgálati módszerek segítségével nehezen megfogalmazható problémák.”

„A fuzzy következtetési rendszerek egyik legelterjedtebb típusa a természetes nyelvi szabályokat használó Mamdani típusú következtetési rendszer” [8], melyet ebben a tanulmányban is használunk majd.

3.1 A bemenetek létrehozása és fuzzifikálásuk

A bemeneti paramétereink kialakításakor a legkevésbé szigorú megközelítésre törekedtünk, amely így nem veszi figyelembe sem az irreleváns adatok létét, sem azok számosságát. Ugyanezt az elvet alkalmaztuk az egyenletek, és magyarázó ábrák tekintetében is.

A modell egyik bemenete a relevancia, mely [0; 1] tartománybeli értéke azt képviseli, hogy az adott hallgató hány százalékát találta meg azon kiindulási adatoknak, melyek az összes megoldást tekintve bármikor előfordultak. A számított relevancia értékek így a [0,18; 0,9] tartományban szóródtak.

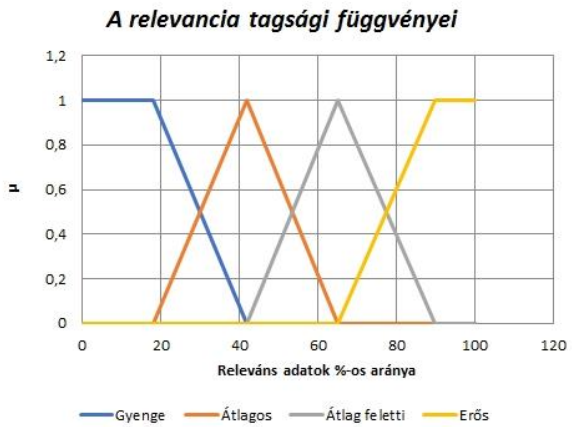
Négy kategória került megkülönböztetésre (1. ábra): a gyenge, az átlagos, az átlag feletti, és az erős minősítésű megoldásvariáció.

Az átlagos kategória csúcspontjának helyét a teljes adatállomány számtani átlaga határozza meg.

A nem szélsőértéket adó kategóriák tagsági függvényeinek alakja háromszög, ezzel biztosítjuk a mind egyenletesebb átmenetet az egyes kategóriák között. Ugyanez a törekvés adta az átlag feletti szinthez tartozó mag értékét is.

A legenyhébb értékelésre való törekvés abban is megnyilvánul, hogy egyértelműen gyengének kizárólag a leggyengébb leadott munka relevancia szintjét tekintettük. Ez indokolja ezen tagsági függvény alakjának eltérését a háromszög alaktól.

Ugyanezen gondolat mentén az egyértelműen erős szintet a legmagasabb relevancia értéket elért hallgató eredményével adtuk meg. Ezért e két kategória meghatározásánál alkalmaztunk trapéz alakot.



1. ábra: Relevancia függvények

2. ábra: Alaposságigény függvények

A tagsági függvények definícióit Koncz és szerzőtársai [1] által használt alakban írjuk fel:

$$\mu_{Gyenge}(x) = \begin{cases} 1 & , \quad x \le 18 \\ max\left(\frac{42-x}{24}, 0\right), & x > 18 \end{cases} \tag{1}$$

$$\mu_{Átl.}(x) = \begin{cases} max\left(\frac{x-18}{24}, 0\right), & x \le 42 \\ max\left(\frac{65-x}{23}, 0\right), & x > 42 \end{cases} \tag{2}$$

$$\mu_{Átl.fel.}(x) = \begin{cases} max\left(\frac{x-42}{23}, 0\right), & x \le 65 \\ max\left(\frac{90-x}{25}, 0\right), & x > 65 \end{cases} \tag{3}$$

$$\mu_{Erős}(x) = \begin{cases} max\left(\frac{x-65}{25}, 0\right), & x < 90 \\ 1 & , \quad x \ge 90 \end{cases} \tag{4}$$

A modell másik bemenete az alaposságigény. Mutatószámát úgy képeztük, hogy az összes adat (relevanciától függetlenül), képlet, és magyarázó ábra darabszámának összegét viszonyítottuk hallgatónként a vizsgált teljes hallgatóállomány átlagához. Az értékek így a [0,29; 2,22] tartományban szóródtak.

A szintek elkülönítésére és a függvénygörbék alakjaira vonatkozó elvek itt is pontosan ugyanazok, mint a relevancia tagsági függvényeinél alkalmazottak (2. ábra). Az átlagos szint magja – természetesen – itt a 100% lett.

$$\mu_{Gyenge}(x) = \begin{cases} 1 & , \quad x \le 29 \\ max\left(\frac{100-x}{71}, 0\right), & x > 29 \end{cases} \tag{5}$$

$$\mu_{Átl.}(x) = \begin{cases} max\left(\frac{x-29}{71}, 0\right), & x \le 100 \\ max\left(\frac{160-x}{60}, 0\right), & x > 100 \end{cases} \tag{6}$$

$$\mu_{Átl.fel.}(x) = \begin{cases} max\left(\frac{x-100}{60}, 0\right), & x \le 160 \\ max\left(\frac{222-x}{62}, 0\right), & x > 160 \end{cases} \tag{7}$$

$$\mu_{Erős}(x) = \begin{cases} max\left(\frac{x-160}{62}, 0\right), & x < 222 \\ 1 & , \quad x \ge 222 \end{cases} \tag{8}$$

Már a bemenetek meghatározásakor is megfigyelhető az oktatói megközelítés hatása, hiszen nyilván nem mindegy, hogy milyen adatok alapján, és milyen egyedi optimumszint meghatározásával alakítottuk ki a fuzzifikálandó bemeneti paramétereinket. Itt is törekedtünk a legkevésbé szigorú megközelítés érvényre juttatásában, mivel még a gondolatmenet alátámasztását szolgáló képletek és ábrák helyességét sem vizsgáltuk, csupán azok számossága befolyásolta az alaposságigény számítását.

De azért igazán majd a szabályrendszer (2. táblázat) kialakításában lesz tetten érhető az oktatói szabadság, és a megítélés szubjektivitása.

3.2 A szabálybázis

Az értékelési szabálybázis felvételekor *ÉS* kapcsolatokat, és így minimum operátort alkalmaztunk az egyes szabályok képzésekor, így a 2. táblázatban látható 16 szabály jött létre.

2. táblázat: Értékelési mátrix

		relevancia			
	MIN	gyenge	átlagos	átlagon felüli	erős
alaposság -igény	gyenge	NFM	NFM	ELF	MF
	átlagos	NFM	ELF	MF	P
	átlagon felüli	NFM	MF	P	P
	erős	ELF	P	P	P

3.3 A kimenet tagsági függvényei

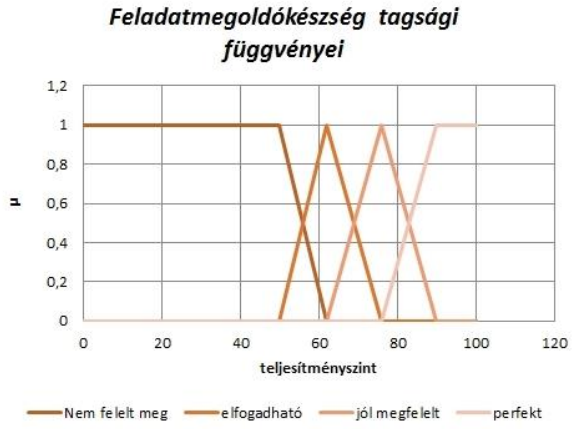
A feladatmegoldókészség tagsági függvényeinek (3. ábra) meghatározásakor az alapot az oktatói gyakorlatban igen gyakran alkalmazott értékelési skála adta.

A fuzzy következtetéseinknél így tehát – a bemenetekhez hasonlóan – szintén négy szintet különböztetünk meg, mely teljesen hasonlóvá teszi így az értékelést az oktatásban tradícionálisan alkalmazott osztályozási módszerhez. Ezek a

- *NFM* – nem felelt meg;
- *ELF* – elfogadható;
- *MF* – jól megfelelt;
- *P* – perfekt.

Ennek megfelelően az – egyáltalán bármilyen szempontból – elfogadható szint alsó küszöbét 50%-os teljesítményben definiáltuk, a 90%-os eredmény pedig már a kimagasló kategóriát képviseli. Ezen szélsőértékek mentén határoztuk meg trapéz alakú tagsági függvényeinket.

A köztük elhelyezkedő háromszög alakú elfogadható, és jól megfelelt szintekhez tartozó függvények magját pedig rendre a 60%, és a 75% adja.



3. ábra: Feladatmegoldókészség függvények

$$\mu_{NFM}(x) = \begin{cases} 1, & x \le 50 \\ max\left(\frac{62-x}{12}, 0\right), & x > 50 \end{cases} \tag{9}$$

$$\mu_{ELF}(x) = \begin{cases} max\left(\frac{x-50}{12}, 0\right), & x \le 62 \\ max\left(\frac{76-x}{14}, 0\right), & x > 62 \end{cases} \tag{10}$$

$$\mu_{MF}(x) = \begin{cases} max\left(\frac{x-62}{14}, 0\right), & x \le 76 \\ max\left(\frac{90-x}{14}, 0\right), & x > 76 \end{cases} \tag{11}$$

$$\mu_{P}(x) = \begin{cases} max\left(\frac{x-76}{14}, 0\right), & x < 90 \\ 1, & x \ge 90 \end{cases} \tag{12}$$

3.4 Aggregáció

Az általunk választott aggregációs módszer – a maximum operátor alkalmazása – egyetlen fuzzy halmazt képez az implikációs szabályok fuzzy halmazainak kimenetéből azok Zadeh-féle uniójával (4. ábra).

Mivel ez a t-konorma a legkisebb, az egyes képességek együttes hatásának figyelembevételénél ez látszik a legcélszerűbb aggregációs eljárásnak. [3]

Számításainkat a Matlab Fuzzy Logic Toolbox segítségével végeztük el. A programban megadott, és az ábrákról leolvasható értékeket %-ban kell értelmezni.

3.5 Defuzzifikáció

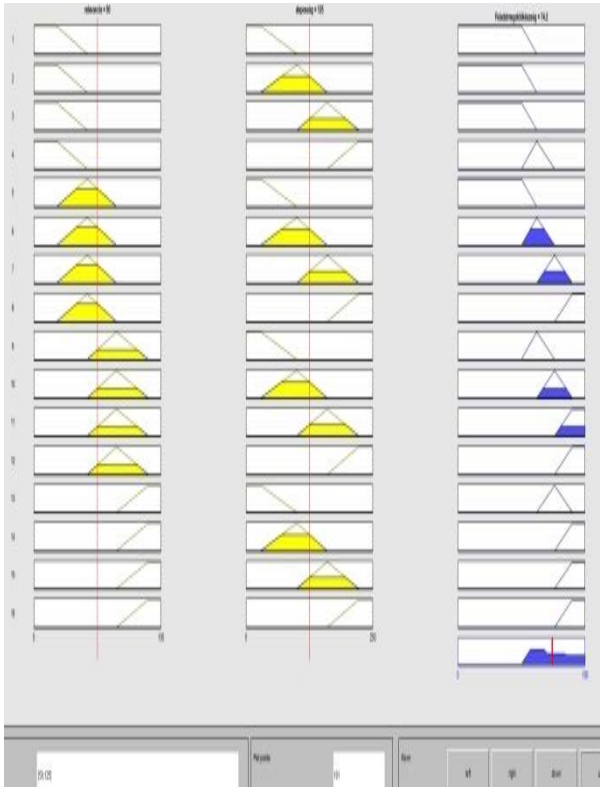
Mivel a defuzzifikáció során kapott görbe alatti terület – gyakorlatilag – a hallgatók mérhető teljesítménytényezőinek együttes hatását szemlélteti, így elemzésünk során két defuzzifikációs módszer használata lehet indokolt. Az egyik a Centroid of Area (CoA), a másik pedig a Bisector of Area (BoA).

A BoA által kapott egyenes többnyire egybeesik a CoA módszer adta centroid vonallal, illetve számottevő különbség nem nagyon van a kettő között.

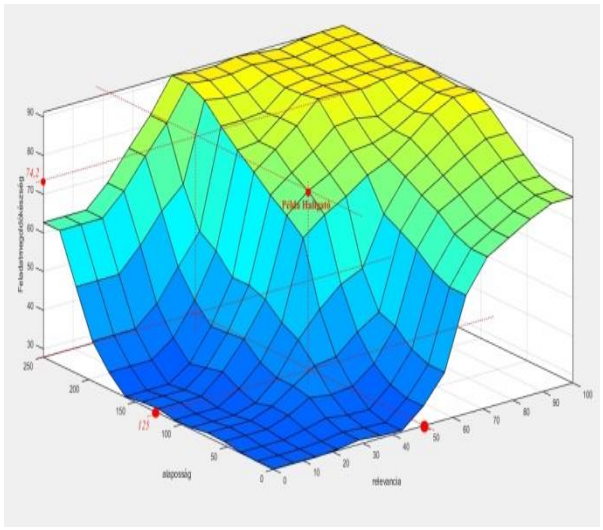
Mért adatok hiányában elemzésünkben nem lehetséges vizsgálatot végezni arra nézve, melyik módszer ad pontosabb eredményt, így választásunk a CoA defuzzifikációra esett. [3]

Számításainkban egy Példa Hallgató 50 %-os relevancia, és 125 %-os alapossági-gény bemeneti adataihoz tartozó defuzzifikált érték 74.2 % lett. (4. és 5. ábra)

Oktatói szemmel nézve az eredményt teljesen reálisnak tűnik, hogy egy gyengébb tárgyi tudású, de átlag feletti szorgalommal rendelkező hallgató által készített feladat eléri a közepes szintet.



4. ábra: A szabályok és aggregáció



5. ábra: Példa Hallgató a defuzzifikációs felületen

4 KONKLÚZIÓ

Számításaink eredményeként ötfokú skálán értékelhetővé válnak az eredendően nagyon nehezen minősíthető hallgatói teljesítmények (3. táblázat), és így lényegesen reálisabb osztályozatok adhatók, mintha az oktató csupán a szubjektív benyomásaira hagyatkozott volna, vagy kizárólag a releváns adatok mennyiségét értékelte volna.

Mindkét utóbb említett módszer önmagában nagyon félrevezető lehet, és egymásnak teljesen ellentmondó értékelést eredményezhetnek adott hallgatók esetében.

Erre utaltunk a bevezetésben, hogy a fuzzy megközelítés alkalmazása bizonyos esetekben megoldhatóvá tesz megoldhatatlannak látszó komplex feladatokat is.

3. táblázat: Hallgatók értékelésének eredményei

	relevancia	*alaposság-igény*	*CoA Matlab*	*érdemjegy*
H1	65%	186%	92%	5
H3	29%	86%	35%	1
H4	47%	122%	72%	3
H5	35%	115%	46%	1
H6	24%	57%	32%	1
H7	18%	36%	28%	1
H8	53%	143%	79%	4
H9	53%	100%	70%	3
H10	59%	165%	87%	4
H11	47%	158%	79%	4
H12	35%	93%	42%	1
H13	59%	100%	72%	3
H14	59%	97%	67%	3
H15	47%	86%	50%	2
H16	35%	107%	44%	1
H17	24%	72%	32%	1
H18	18%	79%	29%	1
H19	41%	111%	61%	3
H20	18%	64%	29%	1
H21	41%	82%	43%	1
H22	53%	100%	70%	3
H23	18%	54%	29%	1
H24	53%	79%	48%	1
H25	47%	72%	42%	1
H26	24%	29%	29%	1
H27	24%	50%	32%	1
H28	24%	43%	31%	1
H144	71%	193%	90%	5
H145	94%	222%	91%	5

Megvizsgálandó az a tény, hogy mindkét bemenet képzésekor felhasználtuk a relevánsan megtalált adatok számosságát, amely felvetheti a kérdést, hogy mennyire függetlenek egymástól, és duplán vettük-e figyelembe ugyanazt az adatot.

Alapvetően a helyes adatok többszöri felhasználása a hallgatók szempontjából nem hátrányos, egyébként pedig a korreláció a két bemenet között nem lesz túl erős, így ez nem hibája a modellnek.

További vizsgálat tárgya lehet majd, hogy milyen egyéb mutatók képezhetők az eredetileg felvett adatállomány segítségével, melyek az alapkutatás szempontjából nagyobb relevanciával bírnak.

Az így nyert teljesítményértékelések felhasználhatók a jövőben egy matematikai statisztikával történő elemzésre is.

IRODALOMJEGYZÉK

[1] Koncz A., & Johanyák, Zs. Cs., & Pokorádi, L. (2022). Fuzzy rule-based hierarchical overall risk analysis of battery testing laboratories, Proceedings Of The Romanian Academy, Series A, Volume 23, Number 1/2022, 89–97.

[2] Halmai, A. (2011). Mérés és irányítástechnika, Edutus, TAMOP-4.1.2.A/2-10/1, 167.

[3] Tóth-Laufer, E. & Rövid, A. & Takács, M. (2012). Error Calculation of the HOSVD-based Rule Base Reduction in Hierarchical Fuzzy Systems, FUZZY SETS AND SYSTEMS 307 pp. 67-82., 16 p.

[4] Kóczy, L. T., & Tikk, D. (2012). Fuzzy rendszerek, Typotex, ISBN 978-963-2797-09-0

[5] Pokorádi, L. (2016). Modellek a műszaki biztonságtudományban. *Gradus*, 3(2), 92-100.

[6] Pokorádi, L. (2008). Rendszerek és folyamatok modellezése, Campus, ISBN 978-963-9822-06-1, 181-212.

[7] Pokorádi, L. (2013). Rendszertechnika, TERC, ISBN 978-963-9968-71-4

[8] Tóth-Laufer, E. & Takács, M. & J Rudas, I. (2012) Conjunction and Disjunction Operators in Neuro-Fuzzy Risk Calculation Model Simplification, In: Szakal, A (szerk.) 13TH IEEE INTERNATIONAL SYMPOSIUM ON COMPUTATIONAL INTELLIGENCE AND INFORMATICS (CINTI 2012), New York, Amerikai Egyesült Államok : IEEE pp. 195-200. , 6 p.

[9] Voskoglou, M. (2013). Fuzzy Logic as a Tool for Assessing Students' Knowledge and Skills, Educ. Sci. 2013, 3., pp. 208-221.

[10] Johanyák, Zs. Cs. (2019). Fuzzy rule interpolation based model for student result prediction, Journal of Intelligent & Fuzzy Systems, vol. 36, no. 2, pp. 999-1008, DOI: 10.3233/JIFS-169875

BÁNKI KÖZLEMÉNYEK
V. ÉVFOLYAM 1. SZÁM

Előrejelzések készítése Fuzzy-Markov alapú idősor-elemzés alapján

Hanka László
Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Természettudományi és Alapozó Tantárgyi Intézet; Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Természettudományi Tanszék, Magyarország
hanka.laszlo@bgk.uni-obuda.hu, hanka.laszlo@uni-nke.hu

***Összefoglalás* — Az élet, az alkalmazott és egzakt tudományok számos területén találkozunk idősorokkal. E témában az az alapvető kérdés, hogy hogyan lehetséges a megfigyelések során kapott adatsorra egy olyan matematikai modellt felállítani, amely a felhasználó által előírt hibahatáron belül szolgáltatja a megfigyelt adatokat is és amely modell alapján előrejelzéseket lehet adni az idősor további adataira a megfigyeléseket követő néhány időpontjára vonatkozólag. A témakörben számos módszer fellelhető a szakirodalomban. Ebben a cikkben két nagy horderejű matematika elméletnek, a Markov-láncok elméletének és a Fuzzy logikának az egyesítésével kapott modellel, egy speciális Fuzzy-Markov folyamattal fogjuk modellezni az idősort és ennek alapján adunk majd előrejelzést a jövőre nézve.**

***Kulcsszavak*:** idősor-elemzés, előrejelzés készítés, Markov-lánc, Fuzzy-logika, Fuzzy mátrix-aritmetika, Fuzzy-Markov folyamat

1 BEVEZETÉS

Az egzakt és alkalmazott tudományok, a gazdasági de még a hétköznapi élet is számos területen kínál példákat idősorokra [1], [2], [3]. Egyszerűen fogalmazva az idősor, ideális esetben, azonos időközönként végzett megfigyelések sorozata. Ilyen például egy részvény napi árfolyama, egy repülőtér napi utasforgalma, egy ország évi gabonaexport mennyisége, a hőmérséklet napi/havi átlagértéke vagy maximális étéke egy adott földrajzi helyen, egy egyetemre évente beiratkozott hallgatók száma, stb.

Minden egyes esetben az az első feladat, hogy a megfigyeléssel kapott adatsort analizáljuk, egy olyan matematikai modellt készítünk, amely a megfigyelések adatsorát elfogadható hibahatáron belül szolgáltatja. Ez tekinthető a matematikai modell tesztjének. Ha ez jól működik, ami azt jelenti, hogy a modell a felhasználó által előírt hibahatáron belül szolgáltatja a megfigyelési adatokat, akkor a modell segítségével extrapolálunk, azaz olyan jövőbeli időpontokra vonatkozólag adunk előrejelzést, jóslatot, amelyre vonatkozólag értelemszerűen még nem volt megfigyelés.

A fenti példák esetében ez tehát jelentheti egy részvény árfolyamát vagy a repülőtér utasforgalmát néhány napra előre, egy ország következő évi gabona exportját, jelentheti a következő napi/havi átlag vagy maximális hőmérsékletet az adott helyen, vagy a jövő évben egy egyetemre beiratkozott hallgatók számának a becslését, előrejelzését, stb.

A szakirodalomban számos módszer található amely ezt a problémakört tárgyalja. Tekintettel a SzaFARi konferencia tematikájára, ebben a cikkben egy fuzzy logika alapú matematikai modellt mutatunk be melynek struktúráját a sztochasztikus folyamatok elméletének, pontosabban a Markov-láncok elméletének segítségével fogjuk kialakítani.

A cikkben egy idősor bemutatása után a Markov-folyamatok elméletének alapgondolatait ismertetjük, mint alapvető eszközt, utána a 4. pontban annak a leírása következik, hogy hogyan alkalmazható idősorokra a fuzzy logika. Ezután az 5. pontban az említett két elmélet ötvözeteként a fuzzy-Markov folyamat idősorokra történő alkalmazása következik, amely a cikk lefontosabb része, végül pedig a 6 .pontban a bemutatott elmélet alkalmazását mutatjuk be a bevezetőben megadott idősor adatokra vonatkozólag.

2 A VIZSGÁLT IDŐSOR BEMUTATÁSA

Mielőtt bemutatnánk az alkalmazott elméletet, lássunk egy példát idősorra.

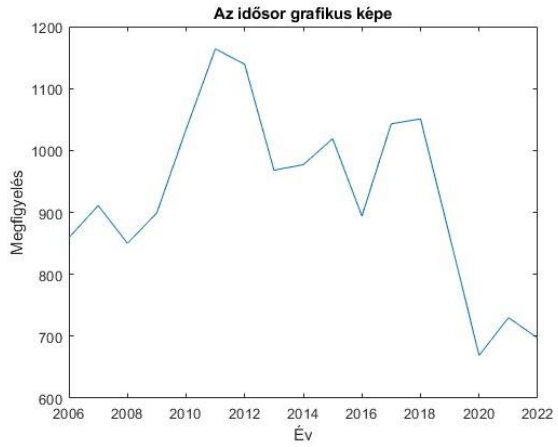
1. táblázat: A vizsgált idősor adatai és az adatok megváltozása

Sorszám	*Év*	*Adat (y_n)*	*Változás(Dy_n)*
1	2006	859	
2	2007	911	52
3	2008	850	-61
4	2009	899	49
5	2010	1034	135
6	2011	1164	130
7	2012	1139	-25
8	2013	968	-171
9	2014	977	9
10	2015	1019	42
11	2016	894	-125
12	2017	1043	149
13	2018	1051	8
14	2019	861	-190
15	2020	669	-192
16	2021	730	61
17	2022	697	-33

Az idősor legyen egy teljesen hipotetikus adatsor, amely nem kötődik közvetlenül semmilyen konkrét megfigyeléshez, így koncentrálhatunk tisztán a matematikai módszerekre függetlenül attól mit is jelentenek konkrétan a megfigyelési adatok. Legyen az idősor az 1. táblázatban közölt adatsor.

Felvettünk tehát hipotétikus adatokat (y_n) 2006 és 2022 között minden évben, tehát feltesszük, hogy az elmúlt 17 évre vonatkozólag vannak megfigyelések. Ez jelenti a rendelkezésre álló idősort. Feladat előrejelzést készíteni a következő évekre, tehát 2023., 2024., … stb. évekre. A táblázatban feltüntettük nem csak a megfigyelést, hanem a megfigyelt adatok évenkénti változását is a $Dy_n = y_n - y_{n-1}$ különbséget, ugyanis, mint a következő pontokból kiderül, a Fuzzy-Markov modellnek [4], [5] éppen ez a különbség képezi az alapját.

Célszerű az idősort szemléltetni. Az 1.ábrán látható az idősor grafikus képe.



1. ábra

A hagyományos idősor elemzési eljárások [1], [3] első lépése az lenne, hogy megvizsgáljuk az idősort, van-e benne tipikus trend, azaz növekedés vagy csökkenés, illetve tapasztalható-e szezonalitás, más szóval van-e periodikus összetevője az idősornak. A grafikus kép segít ennek eldöntésében. Ha van akkor a szokásos módszertan ezen komponensekre való additív felbontás, dekompozíció lenne. Mint látható ebben az esetben egyik viselkedésforma sem jellemző. Azonban a Fuzzy-Markov alapú elemzési módszer ezeket a tulajdonságokat nem is kell hogy hangsúlyozza. Ez a modell a Dy_n különbségek osztályokba sorolásával jellemzi az idősort. A módszer első lépése a Markov-lánc segítségével történő leírás. A Markov-láncok elmélete releváns részének bemutatása következik a 3. pontban.

3 MARKOV-LÁNCOK

Diszkrét idejű Markov-láncnak [6], [7], [8] nevezünk egy sztochasztikus folyamatot, ha az rendelkezik az "emlékezet nélküli" tulajdonsággal. Azaz ha egy sztochasztikus folyamat adott n időpontbeli állapotának valószínűség eloszlása csak a közvetlenül megelőző n - 1 időpontbeli állapottól függ és független minden korábbitól. Ezt a tulajdonságot az alább formulával szokás értelmezni:

$$P\left(S_n \middle| S_{n-1}, S_{n-2}, ..., S_1\right) = P\left(S_n \middle| S_{n-1}\right) \qquad (1)$$

melynek jelentése a következő. Annak az eseménynek a feltételes valószínűsége, hogy az n időpontban a rendszer az S_n állapotban van kizárólag az n időpontot közvetlenül megelőző n -1 időpontbeli S_{n-1} állapottól függ és nem függ korábbi állapotoktól. Ezen feltétel teljesülése esetén az egymást követő időpontokban a Markov-lánc diszkrét valószínűség eloszlásait az alábbi formulával tudjuk leírni:

$$\boldsymbol{\pi}_{n+1} = \boldsymbol{\pi}_n \mathbf{R};\ n = 0,1,2.... \qquad (2)$$

ahol a $\boldsymbol{\pi}_0; \boldsymbol{\pi}_1; \boldsymbol{\pi}_2; .....n = 0,1,2....$ sorvektorok a Markov-lánc diszkrét valószínűség eloszlásai az egymást követő időpontokban, az $\mathbf{R}$ mártix pedig a folyamat ún. átmeneti valószínűség mátrixa. Példaként legyen az $\mathbf{R}$ mátrix az alábbi 3×3-as mátrix

$$\begin{matrix} & & hova \\ honnan & \mathbf{R} = \end{matrix} \begin{bmatrix} 0,5 & 0,3 & 0,2 \\ 0,5 & 0,1 & 0,4 \\ 0,4 & 0,3 & 0,3 \end{bmatrix} \qquad (3)$$

Ez a mátrix egy olyan folyamatot ír le amelynek 3 állapota van, és az egyes állapotok közötti átmenetek valószínűségei találhatók a mátrix soraiban olyan értelemben, hogy a sorok jelképezik az induló állapotot ("*honnan*") és az oszlopok a végállapotot ("*hova*"). Következésképpen minden sor egy diszkrét valószínűség eloszlás, ami miatt ezt a mátrixot sor-sztochasztikus Markov mátrixnak nevezzük. Ha feltételezzük, hogy a rendszer a kiinduló állapotban a $\boldsymbol{\pi}_0 = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$ eloszlással adott, akkor a (2) formula szerint a diszkrét idejű Markov-lánc a következő időpontokban az alábbi diszkrét eloszlásokkal írható le:

$$\begin{aligned} \boldsymbol{\pi}_1 &= \boldsymbol{\pi}_0 \mathbf{R} = \begin{bmatrix} 1\,0\,0 \end{bmatrix} \begin{bmatrix} 0,5 & 0,3 & 0,2 \\ 0,5 & 0,1 & 0,4 \\ 0,4 & 0,3 & 0,3 \end{bmatrix} = \begin{bmatrix} 0,5\,0,3\,0,2 \end{bmatrix}; \\ \boldsymbol{\pi}_2 &= \boldsymbol{\pi}_1 \mathbf{R} = \begin{bmatrix} 0,5\,0,3\,0,2 \end{bmatrix} \begin{bmatrix} 0,5 & 0,3 & 0,2 \\ 0,5 & 0,1 & 0,4 \\ 0,4 & 0,3 & 0,3 \end{bmatrix} = \begin{bmatrix} 0,48\,0,24\,0,28 \end{bmatrix}; \\ \boldsymbol{\pi}_3 &= \boldsymbol{\pi}_2 \mathbf{R} = \begin{bmatrix} 0,48\,0,24\,0,28 \end{bmatrix} \begin{bmatrix} 0,5 & 0,3 & 0,2 \\ 0,5 & 0,1 & 0,4 \\ 0,4 & 0,3 & 0,3 \end{bmatrix} = \begin{bmatrix} 0,472\,0,252\,0,276 \end{bmatrix}; \\ &stb. \end{aligned} \qquad (4)$$

Ez a valószínűség eloszlás sorozat – sztochasztikus folyamat – mutatja hogyan változik a rendszer eloszlása az egyes állapotok között ahogy múlik az idő.

A továbbiakban az idősor elemzés egy olyan módszerét mutatjuk be, amely a diszkrét idejű Markov-láncok fent bemutatott struktúráját és logikáját alkalmazza, természetesen bizonyos értelemben általánosított formában. A kérdés az lesz, hogy egy idősor esetében mit tekintünk állapotnak és hogy mit jelent az állapotok közötti átmenet és végül a legfontosabb kérdés nyilván az lesz, hogy mi az átmeneti valószínűség mátrix megfelelője idősor kontextusban. Ezeket a kérdéseket tisztázzuk a következő pontokban.

4 A FUZZY LOGIKA ALKALMAZÁSA IDŐROKRA

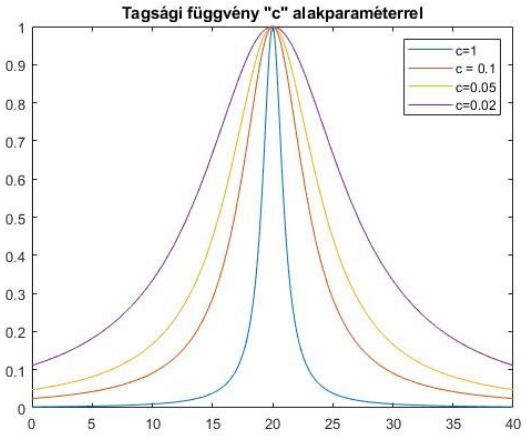
A következő lépés a fuzzy logika alkalmazása, a fuzzifikálás [9], [10]. Alapvető kérdés, hogy mire vonatkozólag definiálunk fuzzy halmazokat. Visszatekintve az 1. táblázatra, abban azért szerepelnek a Dy_n megváltozások, mert az alapgondolat az, hogy nem az idősor megfigyelt értékeire vonatkozólag, hanem a változások értékeire vonatkozólag definiálunk fuzzy halmazokat. Figyelembe véve a táblázatbeli változás-értékeket, kialakítunk hét egyenlő hosszúságú intervallumot az alábbi lingvisztikai változókkal:

[-200,-150]: Drasztikus csökkenés
[-150,-100]: Jelentős csökkenés
[-100,-50]: Számottevő csökkenés
[-50, 0]: Enyhe csökkenés
[0, 50]: Enyhe növekedés
[50,100]: Számottevő növekedés
[100,150]: Jelentős növekedés

Ezután eldöntjük, hogy milyen típusú tagsági függvényeket rendelünk a fenti változókhoz [9], [11]. Ebben a dolgozatban az alábbi függvény alkalmazását javasoljuk:

$$\mu(x) = \frac{1}{1 + c \cdot (x - m)^2}; \qquad (5)$$

ahol c egy alak- vagy skálaparaméter, m pedig egy középérték, amelyre a görbe szimmetrikus. A függvény grafikus képe különböző c értékek és azonos m = 20 középérték esetén látható a 2. ábrán.



2. ábra

A javasolt függvény előnye, túl azon hogy könnyen kódolható az, hogy a c parameter változtatásával egyszerűen "hangolható". Mint könnyen látható, ha a paraméter értéke növekszik a görbe egyre jobban koncentrálódik az m középérték körüli környezetre, így a többi lingvisztikai változó hatása egyre jobban kiküszöbölhető, míg fordítva ha a parameter értéke csökken a lingvisztikai változók egymásra hatása egyre dominánsabb. Mint a cikk végén látni fogjuk, ez egy nagyon hasznos tulajdonsága ennek a tagsági függvénynek, mert mint kiderül, a c parameter értéke jelentősen befolyásolja az idősorra illeszkedő matematikai modell pontosságát, a c parméter értékének csökkentése jelentősen növeli a pontosságot.

A továbbiakban tehát az (5) képlettel értelmezett tagsági függvényt fogjuk alkalmazni a fentiekben definiált hét intervallum mindegyikére:

$$\mu_k(x) = \frac{1}{1 + c \cdot (x - m_k)^2}; \; k = 1, 2, ..., 7; \qquad (6)$$

ahol c természetesen ugyanaz a skálaparaméter mindegyik intervallumra, m_k pedig a k-adik intervallum középértéke. A kapcsolódó fuzzy halmazok jelölésére az A_k (k = 1,2,…,7) jelölést fogjuk alkalmazni. A 3. ábrán látható a hét intervallumra vonatkozólag a tagsági függvények rendszere, c = 0,0001 skálaparaméter esetén.

3. ábra

A c paraméter értékének ezen megválasztását a későbbiekben indokoljuk.

2. táblázat: A vizsgált idősor változás adatainak fuzzifikálása

Sorszám	*Év*	*Változás(Dy_t)*	*Fuzzy halmaz(A_k)*
1	2006		
2	2007	52	A_6
3	2008	-61	A_3
4	2009	49	A_5
5	2010	135	A_7
6	2011	130	A_7
7	2012	-25	A_4
8	2013	-171	A_1
9	2014	9	A_5
10	2015	42	A_5
11	2016	-125	A_2
12	2017	149	A_7
13	2018	8	A_5
14	2019	-190	A_1
15	2020	-192	A_1
16	2021	61	A_6
17	2022	-33	A_4

A következő lépés az, hogy meghatározzuk az 1. táblázat szerinti Dy_t értékeknek mely fuzzy halmazhoz tartozik a maximális tagsági értéke. Ezen osztályozás szerint értelmezzük majd az idősor egyes "állapotait".

Ez után pedig az következik, hogy az idősort folyamatnak, állapotok közötti átmenetnek tekintjük, ahol az állapotokat azzal a fuzzy halmazzal jellemezzük, amelyben az adott változás maximális tagsági értékkel szerepel, az átmenet pedig azzal van figyelembe véve, hogy a változás értéke mely fuzzy halmazból mely fuzzy halmazba kerül.

Ezeket a tapasztalt átmeneteket, a kronológiai sorrend mellőzésével, láthatjuk az alábbiakban:

$$\begin{aligned} A_1 &\rightarrow A_1, A_5, A_6 \\ A_2 &\rightarrow A_7 \\ A_3 &\rightarrow A_5 \\ A_4 &\rightarrow A_1 \\ A_5 &\rightarrow A_1, A_2, A_5, A_7 \\ A_6 &\rightarrow A_3, A_4 \\ A_7 &\rightarrow A_4, A_5, A_7 \end{aligned} \tag{7}$$

Az átmenetek időbeli sorrendje azért nincs figyelembe véve, azért indifferens, mert azok a fuzzy logikai műveletek, amelyeket majd alkalmazunk, kommutatívok, így a sorrendiség nem számít, csak az, hogy az idősor teljes egészét figyelembe véve, mely átmenetek voltak tapasztalhatók.

5 FUZZY-MARKOV FOLYAMAT

Most következik az a pont, amikor alkalmazni lehet a Markov-láncok elméletének (2) formulával leírható struktúráját és ötvözhetővé válik a fuzzy logika és a Markov-láncok elmélete [4], [5]. A kérdés az, hogy a (2) formulában szereplő **R** átmeneti valószínűség mátrixnak mi a fuzzy megfelelője. Természetesen itt nem valószínűségek lesznek a mátrix elemei, hanem a definiált fuzzy halmazok felhasználásával értelmezzük az **R** mátrix komponenseit az alábbiakban bemutatott eljárással. Cél, hogy az egész idősort jellemezzük egyetlen mátrix segítségével olyan módon, hogy az tartalmazzon információt az összes tapasztalt átmenetre vonatkozóan.

3. táblázat: Az A_1, A_2,… A_7 fuzzy halmazok a tagsági értékek vektoraként értelmezve

A_1	1,000	0,286	0,091	0,043	0,024	0,016	0,011
A_2	0,286	1,000	0,286	0,091	0,043	0,024	0,016
A_3	0,091	0,286	1,000	0,286	0,091	0,043	0,024
A_4	0,043	0,091	0,286	1,000	0,286	0,091	0,043
A_5	0,024	0,043	0,091	0,286	1,000	0,286	0,091
A_6	0,016	0,024	0,043	0,091	0,286	1,000	0,286
A_7	0,011	0,016	0,024	0,043	0,091	0,286	1,000

Ezért figyelembe vesszük a (7) átmeneteket és megállapodunk abban, hogy az egyes fuzzy halmazokat az egyes intervallumok középértékéhez tartozó tagsági értékek vektorával azonosítjuk. Az alábbi 3. táblázatban foglaltuk össze az ilyen módon kapott fuzzy halmazokat.

Ezek után következhet az **R** átmenet matrix generálása az alábbi módszerrel. Figyelembe véve a (7) formulával figyelembe vett átmeneteket, ha létezik egy $A_k \rightarrow A_j$ átmenet, akkor ennek az átmenetnek megfelelően, generálunk egy $\mathbf{R}_{kj}$ mátrixot, amely a modell szerint magában foglalja az átmenetre jellemző információt numerikus adatok formájában. Ezt a mátrixot a klasszikus diadikus szorzat fuzzy matrix-aritmetikai megfelelőjével értelmezzük [9], [10], [11] az alábbi módon:

$$\begin{gathered} A_k \rightarrow A_j \Rightarrow \mathbf{R}_{kj} = A_k^T \cap A_j \in \mathbf{R}^{n\times n}; \\ \text{azaz} \\ \mathbf{R}_{kj}(m,p) = \min\left(A_k(m); A_j(p)\right) \end{gathered} \tag{8}$$

ahol a "T" felső index a transzponálás műveletét jelenti. Azonosítva a fuzzy halmazt a hozzá tartozó sorvektorral tehát arról van szó, hogy az A_k sorvektor tanszponáltjaként kapott oszlopvektornak és az A_j sorvektornak készítjük a diadikus szorzatát a szorzás műveletének fuzzy aritmetikai megfelelőjével a minimum operátorral. A művelet eredménye természetesen egy 7×7-es kvadratikus mátrix.

Példaként a 2. táblázatban, sorrendben az első $A_6 \rightarrow A_3$ átmenetnek megfelelő $\mathbf{R}_{63}$ mátrix a következő:

$$\begin{aligned} \mathbf{R}_{63} &= A_6^T \cap A_3 = \\ &= \begin{bmatrix} 0{,}016 \\ 0{,}024 \\ 0{,}043 \\ 0{,}091 \\ 0{,}286 \\ 1{,}000 \\ 0{,}286 \end{bmatrix} \begin{bmatrix} 0{,}091 & 0{,}286 & 1{,}000 & 0{,}286 & 0{,}091 & 0{,}043 & 0{,}024 \end{bmatrix} = \\ &= \begin{bmatrix} 0{,}016 & 0{,}016 & 0{,}016 & 0{,}016 & 0{,}016 & 0{,}016 & 0{,}016 \\ 0{,}024 & 0{,}024 & 0{,}024 & 0{,}024 & 0{,}024 & 0{,}024 & 0{,}024 \\ 0{,}043 & 0{,}043 & 0{,}043 & 0{,}043 & 0{,}043 & 0{,}043 & 0{,}024 \\ 0{,}091 & 0{,}091 & 0{,}091 & 0{,}091 & 0{,}091 & 0{,}043 & 0{,}024 \\ 0{,}091 & 0{,}286 & 0{,}286 & 0{,}286 & 0{,}091 & 0{,}043 & 0{,}024 \\ 0{,}091 & 0{,}286 & 1{,}000 & 0{,}286 & 0{,}091 & 0{,}043 & 0{,}024 \\ 0{,}091 & 0{,}286 & 0{,}286 & 0{,}286 & 0{,}091 & 0{,}043 & 0{,}024 \end{bmatrix} \end{aligned} \tag{9}$$

Elkészítve a (7) formula szerinti összes átmenethez tartozó $\mathbf{R}_{kj}$ mátrixot, a teljes idősor jellemzését azzal az **R** mátrixszal írjuk le amelyet úgy kapunk, hogy képezzük az összes $\mathbf{R}_{kj}$ átmenetmátrix összegét, azaz fuzzy értelemben a maximum operátort alkalmazzuk az alábbiak szerint:

$$\begin{gathered} \mathbf{R} = \bigcup_{(k,j)} \mathbf{R}_{kj} \in \square^{n\times n} \\ \text{azaz} \\ \mathbf{R}(m,p) = \max_{(k,j)} \left(\mathbf{R}_{kj}(m,p)\right) \end{gathered} \tag{10}$$

Elvégezve a fenti műveleteket az alábbi **R** mátrixot kapjuk:

$$\mathbf{R} = \begin{bmatrix} 1,000 & 0,286 & 0,091 & 0,286 & 1,000 & 1,000 & 0,286 \\ 0,286 & 0,286 & 0,091 & 0,286 & 0,286 & 0,286 & 1,000 \\ 0,286 & 0,286 & 0,091 & 0,286 & 1,000 & 0,286 & 0,286 \\ 1,000 & 0,286 & 0,286 & 0,286 & 0,286 & 0,286 & 0,286 \\ 1,000 & 1,000 & 0,286 & 0,286 & 1,000 & 0,286 & 1,000 \\ 0,286 & 0,286 & 1,000 & 1,000 & 0,286 & 0,286 & 0,286 \\ 0,091 & 0,286 & 0,286 & 1,000 & 1,000 & 0,286 & 1,000 \end{bmatrix} \quad (11)$$

A bemutatott matematikai modellnek tehát az a lényege, hogy a teljes idősort vizsgáljuk, és a fentiekben bemutatott módon generált **R** mátrix tartalmazza bizonyos értelemben a szükséges információkat az idősor egészére, annak alakulására vonatkozólag. Ezt a mátrixot használjuk fel a modellezésre és előrejelzés készítésére a továbbiakban.

Az idősor modellezéséhez első lépésben azt tesszük, hogy minden egyes évhez rendelünk egy vektort, amely az adott évbeli változás tagsági értékeinek vektora. Ha az *n*-edik évről van szó, akkor az A_n vektor előállítása az alábbi formula alapján számítjuk:

$$\mu_k\left(Dy(n)\right) = \frac{1}{1 + c\left(Dy(n) - m(k)\right)^2};$$
$$k = 1,2,3,...,7; \quad (12)$$
$$n = 2006, 2007, ..., 2022;$$

Rögzített *n* évhez minden *k*-ra kiszámítjuk a fenti értéket. Eredményképpen a 4. táblázatbeli vektorokat kapjuk:

4. táblázat: Az egyes évekhez rendelt fuzzy halmazok

A_{2006}	0,019	0,031	0,058	0,144	0,587	0,654	0,158
A_{2007}	0,071	0,196	0,836	0,436	0,119	0,051	0,028
A_{2008}	0,020	0,032	0,061	0,154	0,653	0,597	0,148
…	…	…	…	…	…	…	…
A_{2021}	0,047	0,106	0,362	0,940	0,229	0,079	0,039
A_{2022}	0,940	0,286	0,286	0,286	0,362	0,286	0,286

Ezek után pedig a idősor modellezése a Markov-láncok elméletének analógiájképpen úgy történik, hogy egy adott *n* évbeli megfigyelt adatról a következő évi megjósolt adatra, tehát az előrejelzésre az

$$A_n = A_{n-1} \circ \mathbf{R};$$
$$A_{n-1} : \text{megfigyelés az } (n-1)\text{-edik évben} \quad (13)$$
$$A_n : \text{előrejelzés, jóslat az } n\text{-edik évben}$$

formula alapján térünk át, ahol **R** a (10) és (11) szerinti mátrix, a "o" művelet pedig a mátrixok fuzzy típusú sor-oszlop szorzása a szokásos min-max műveletek alkalmazásával [9], [10], [12].

A (13) képlet alapján nyilvánvaló hogy jóslatként, előrejelzésként egy sorvektort, más szóval egy fuzzy halmazt kapunk. A (13) összefüggés tehát azt jelenti, hogy Markovi szemléletben az idősor egy "állapota" a 4. táblázatban látható és (12) formula alapján értelmezett fuzzy halmazzal értelmezhető. Az új "állapot" a következő időpontban pedig a (13) szerinti sorvektor-mátrix szorzás eredményeképpen adódó új fuzzy halmazzal egyenértékű.

Az utolsó lépés ennek a fuzzy halmaznak a defuzzifikálása. Defuzzifikálásra a legegyszerűbb és leggyakrabban alkalmazott módszert javasoljuk, a súlypont módszert, mely az alábbi formula alapján határozható meg:

$$\text{prognózis}(n) = \frac{\sum_{k=1}^{7} \mu_k\left(A_n(k)\right) m(k)}{\sum_{k=1}^{7} \mu_k\left(A_n(k)\right)};$$
$$m(k) : \text{a k-adik intervallum középértéke} \quad (14)$$
$$A_n(k) = \text{az n évhez tartozó prognosztizált tagsági értékek}$$

A prognózis, azaz a defuzzifikált érték nem más, mint az idősor következő évbeli értékére vonatkozó jóslat. Éppen ennek meghatározása a jelen dolgozat fő célja. Mielőtt bemutatnánk a módszer által szolgáltatott eredményeket, röviden indokoljuk, hogy miért a súlypont módszert javasoljuk defuzzifikálásra. Ha a formulát kissé átalakítjuk, azt kapjuk, hogy a jósolt érték a

$$\text{prognózis}(n) = \frac{\mu_1\left(A_n(1)\right)}{\sum_{k=1}^{7} \mu_k\left(A_n(k)\right)} m(1) + \frac{\mu_2\left(A_n(2)\right)}{\sum_{k=1}^{7} \mu_k\left(A_n(k)\right)} m(2) + ...$$
$$... + \frac{\mu_7\left(A_n(7)\right)}{\sum_{k=1}^{7} \mu_k\left(A_n(k)\right)} m(7) = \text{Várható érték} \quad (15)$$

formulával is egyenértékű, ami nyilvánvalóan tekinthető egy várható értéknek [6], [7], mivel a normált tagsági értékek vektora

$$\left(\frac{\mu_1\left(A_n(1)\right)}{\sum_{k=1}^{7} \mu_k\left(A_n(k)\right)}; \frac{\mu_2\left(A_n(2)\right)}{\sum_{k=1}^{7} \mu_k\left(A_n(k)\right)}; ...; \frac{\mu_7\left(A_n(7)\right)}{\sum_{k=1}^{7} \mu_k\left(A_n(k)\right)} \right) \quad (16)$$

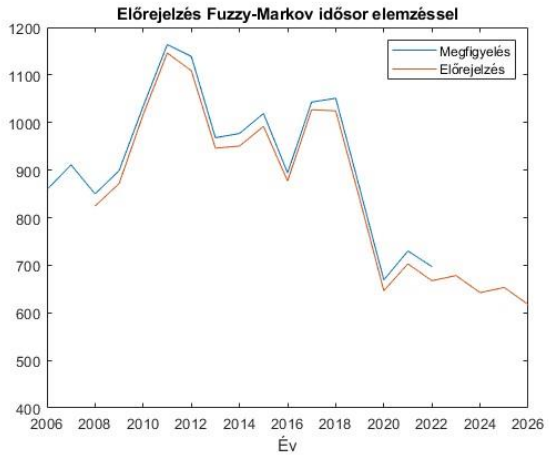
nyilván egy diszkrét valószínűség eloszlást alkot. Ilyen terminológia esetén, tehát hogy a defuzzifikált értékre úgy tekintünk mint egy valószínűségi változó várható értékére, még mélyebbnek tekinthető a kapcsolat a valószínűség elmélettel és így a Markov-láncok elméletével.

6 AZ IDŐSOR MODELLEZÉSE ÉS PROGNÓZISOK KÉSZÍTÉSE

Ebben a pontban bemutatjuk a fentiekben javasolt módszer alkalmazását az 1. táblázatban közölt idősorra vonatkozólag.

Alkalmazva a (13) képlet által definiált Markov-lánc jellegű algoritmust a 4. táblázatban foglalt fuzzy halmazokra a (11) által adott **R** mátrix felhasználásával úgy, hogy a tagsági függvényeket az (5) képlet értelmezi

c = 0,0001 alakparaméter alkalmazása mellett, akkor először is a 4. ábrán látható eredményt kapjuk.



4. ábra

Mint azt az ábra is mutatja, a modell jól működik, a prognózis-idősor jól illeszkedik a megfigyelésekhez. Numerikusan az 5. táblázat tartalmazza a közelítésre vonatkozó adatokat és annak relatív pontosságát %-os formában a 2008-2022 időintervallumra vonatkozólag.

5. táblázat: Az idősor közelítése prognosztizált adatokkal

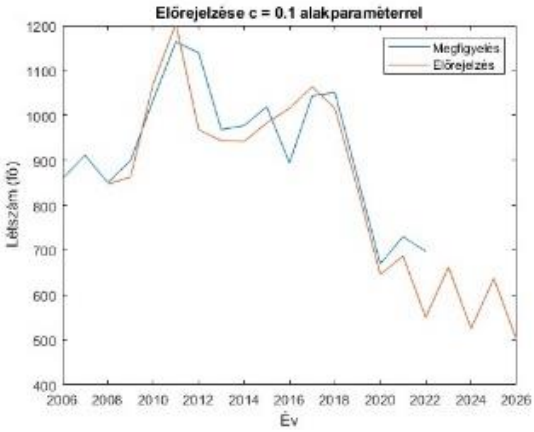
ssz.	Év	Megfigyelt adat	Prognózis	Relatív hiba %
1	2008	850	824,36	3,02
2	2009	899	871,81	3,02
3	2010	1034	1016,82	1,66
4	2011	1164	1146,20	1,53
5	2012	1139	1108,83	2,65
6	2013	968	946,18	2,25
7	2014	977	950,61	2,70
8	2015	1019	991,89	2,66
9	2016	894	877,18	0,88
10	2017	1043	1026,87	1,55
11	2018	1051	1024,63	2,51
12	2019	861	838,57	2,60
13	2020	669	646,58	3,35
14	2021	730	702,89	3,71
15	2022	697	667,46	4,24

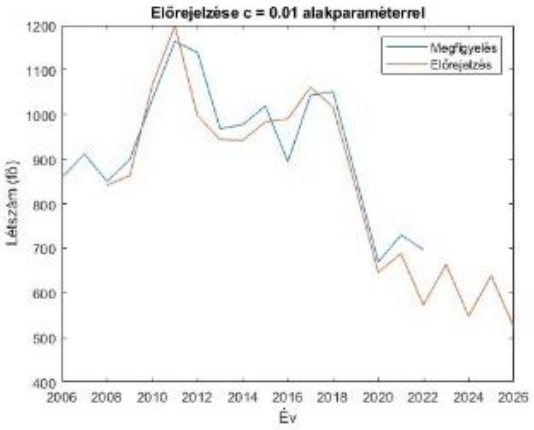
A közelítés pontosságára vonatkozó előírás vagy igény a felhasználó által van meghatározva. Véleményünk szerint az átlagosan 2-3%-os relatív pontosság kielégítőnek tekinthető.

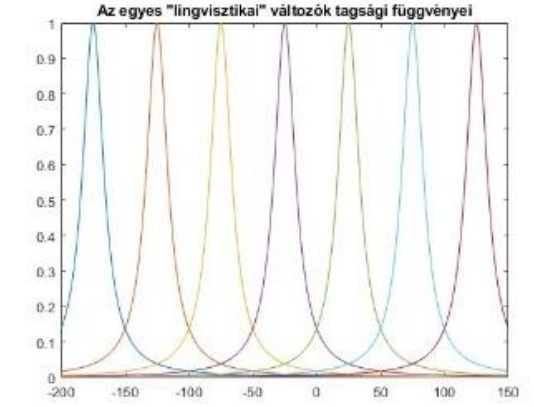
A jövőre vonatkozó előrejelzések, melyek értékei Y_{2023} = 678, Y_{2024} = 642, Y_{2025} = 653 és Y_{2026} = 617 az 5. táblázat adatai, a tapasztalt relatív pontosság alapján válnak jogossá és elfogadhatóvá. Ezzel a bevezetőben kitűzött programot teljesítettük.

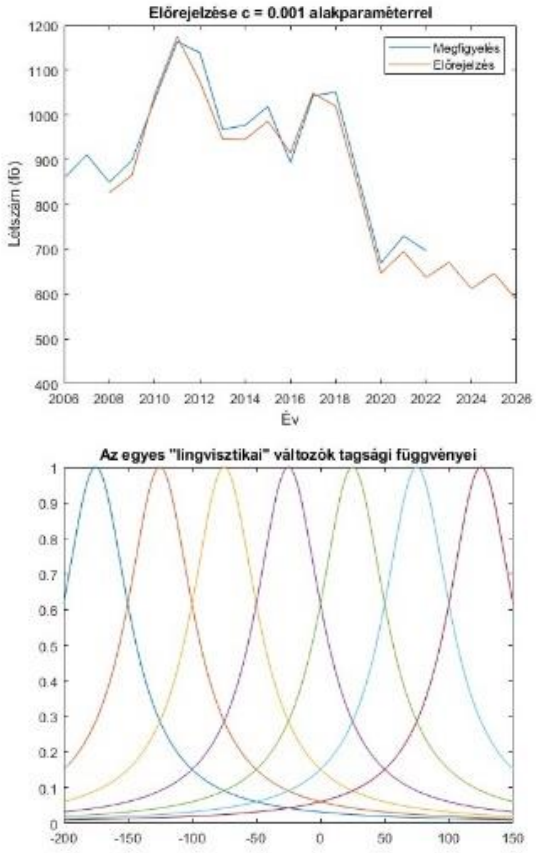
Befejezésképpen még azt vizsgáljuk meg, milyen hatása van a prognózis minőségére a c alakparaméter választásának. Mint korábban már megadtuk, az 5. táblázat illetve a 4. ábra grafikonja c = 0,0001 paraméter érték esetén született. Nyilván felmerül a kérdés, hogyan módosul a helyzet, ha c-nek más értéket adunk.

Az 5. ábrán látható az eredmény grafikusan rendre c = 0,1; c = 0,01; c = 0,001 paraméter értékek esetén.









5. ábra

Amit az ábráról leolvashatunk az, hogy minél jobban "elkentek" a tagsági függvények, más szóval minél nagyobb hatása van egymásra a rendszerbeli fuzzy halmazoknak, vagyis minél nagyobbak a tagsági függvény értékek, a közelítés pontossága annál jobb. Csupán vizuálisan összehasonlítva a 4. ábrát és az 5. ábra c = 0,001 paraméter érékhez tartozó ábráját, úgy tűnhet hogy az utóbbi pontosabb. Azonban a számítások azt mutatják, hogy ez nem igaz, a relatív hiba jellemzően 1%-kal rosszabb c = 0,001 esetén. Ha még tovább csökkentenénk a c értékét, elérhetnénk egy átlagos 2%-os relatív hibaszintet, ha erre szükség van, de nagyságrendi javulás a hibát tekintve már nem érhető el.

Hangsúlyozzuk, hogy a fenti számítások egységesen az (5) formula által definiált tagsági függvény esetére lettek elvégezve. A probléma vizsgálata elvégezhető más alakú függvényekkel is, amely eljárás lehetőséget ad a módszer esetleges továbbfejlesztésére, pontosítására.

7 Következtetések

A fentiekben bebizonyítottuk, hogy a fuzzy logika módszertana a Markov-láncok elméletével ötvözve egy alkalmas és hatékony módszer idősorok elemzésére, modellezésre és prognózisok készítésére. Az idősor egy állapotát, alkalmas tagsági függvény, és alkalmas paraméter választása esetén az adott időpontbeli változásnak megfelelő fuzzy halmaz jelenti, és a prognózis, az előrejelzés úgy adható meg, hogy a Markov-lánc következő állapotát egy újabb fuzzy halmazzal adjuk meg, amely a változás jósolt mértékének megfelelő fuzzy halmaz. Az idősor soron következő tagja pedig innen valamely defuzzifikációs módszerrel adódik. A számításokhoz és az ábrák készítéséhez a Matlab szoftvert használtuk. Minden ábra és táblázat saját készítésű.

Hivatkozások

[1] Box, Jenkins, 'Time Series Analysis, Forecasting and control', Wiley, 2016.

[2] Lynwood A., Johnson, L.A, Montgomery, D.C, and Gardiner, J.S., Forecasting and Time Series Analysis. 2nd Edition. McGraw-Hill,Inc, 1990.

[3] Box, Jenkins, Reinsel, Ljung: 'Time Series Analysis', Springer, 2016.

[4] Guangming: Fuzzy Markov chains based on the fuzzy transition probability, IEEE Chinese Control and Decision Conference, 2014

[5] Avrachenkov, Sanchez: Fuzzy Markov chains, Fuzzy Optimization and Decision Making, 2002

[6] Ross: Stochastic processes, John Wiley and sons, USA, 1996

[7] Karlin - Taylor: An introduction to stochastic modeling, Academic Press, London, 1998

[8] Knill: Probability and Stochastic Processes with Applications, Overseas Press, India, 2006

[9] László, Pokorádi ; Sinan, Kocak ; Edit, Tóth-Laufer: Fuzzy Failure Modes and Effects Analysis Using Summative Defuzzification Methods, ACTA POLYTECHNICA HUNGARICA 18 : 9 pp. 111-126. , 16 p. (2021)

[10] Kóczy, Tikk: Fuzzy rendszerek, Typotex, Budapest, 2001

[11] Paasino-Yurkovich: Fuzzy control, Addison-Wesley, USA, 1998

[12] Meghdadi-Akbarzadeh: Probabilistic Fuzzy Logic and Probabilistic Fuzzy Systems, IEEE International Fuzzy Systems Conference, 2001

BÁNKI KÖZLEMÉNYEK
V. ÉVFOLYAM 1. SZÁM

Öntözőrendszer vezérlés fuzzy logikával

Hegedűs Martin Tibor
Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Budapest, Magyarország
s8x0cu@stud.uni-obuda.hu

***Összefoglalás* — Jelen cikk megvizsgálja a fuzzy logika alkalmazási lehetőségeit az automata öntözőrendszerek esetében, ehhez röviden ismerteti a jelenlegi technológiákat, eljárásokat, ezek fontosabb előnyeit és hátrányait. Továbbá megvizsgálja az automatika alkalmazásának nehézségeit, ezekre megoldást kínál egy fuzzy logika alapú öntözésvezérlő modell tervezésével és megvalósításával, illetve továbbfejlesztési lehetőségeket is ajánl a cikk végén.**

***Kulcsszavak*:** fuzzy, fuzzy rendszer, öntözés, öntözőrendszer, locsolás, locsolórendszer

1 BEVEZETÉS

A kertben a gyep, valamint a virágok, bokrok és fák megfelelő öntözése elengedhetetlen ahhoz, hogy egészségesek és szépek legyenek a növények. Ehhez azonban körültekintően kell végezni az öntözésüket, nem elég csak úgy nagyjából meglocsolni őket. Erre a feladatra egy öntözőrendszer telepítése ideális választás, amennyiben a helyi igényekhez és körülményeknek megfelelően van megtervezve. A szakirodalomban több megoldás is található, ezek közül a következőkben a gyakrabban használtakat fogom kifejteni:

A kézi öntözés időigényes, azonban ha odafigyelünk, akkor a legnagyobb vízmegtakarítás érhető el, ugyanis az egyszerre locsolt terület meglehetősen kicsi, így a kilocsolt vízmennyiséget jól lehet szabályozni. Továbbá mivel az öntözés közben aktívan figyeljük azt, így azonnal tudunk reagálni, amikor egy területre már elegendő vizet juttattunk ki. A kézi locsolás történhet közönséges locsolócsővel („slaggal”), vagy a cső végére csatlakoztatható kézi locsolófejjel is. Utóbbi előnye, hogy a vizet jobban szétszórja, ezzel kevésbé terheli a füvet, illetve kevésbé mossa el a földet.

Automata öntözővel (pl köresőztetővel, impulzus szektoresőztetővel vagy négyszögesőztetővel) a gyep locsolása jóval kevesebb időt igényel a felhasználótól, mivel az öntözés nagy részében az automatikus esőztető végzi a locsolást. Azonban a kert gyakran nagyobb, mint amekkora területet lefednek ezek az esőztetők, így 15-60 percenként át kell helyezni őket. Ezenkívül elindítani és leállítani is manuálisan kell őket.

A beavatkozás- és felügyeletmentes megoldás az automatikus öntözőrendszer telepítése, amely a föld szintjéből kiemelkedő szórófejekkel végzi az öntözést, közben ezeket egy automatikus vezérlő kapcsolja be és ki a beállított program alapján. Ez a megoldás jelentősen költségesebb (százezres nagyságrend, a pár ezer forintos kézi/félautomata locsolókészülékekhez képest), azonban nagy területekre vagy az emberi beavatkozás/felügyelet lehetőségének hiányában (pl. füvesített köztereknél, parkoknál) nincs más megoldás, mint a teljesen automata öntözőrendszer telepítése. Azonban ez a megoldás nyújtja a legjobb és legegyenletesebb gyepminőséget is.

Az ültetett gyep, valamint a többi növény a talajból szívja fel a nekik szükséges vizet, illetve a táp- és ásványi anyagokat, amelyeket vissza kell táplálni a talajba. A táp- és ásványi anyagokat elegendő az ültetés közben kiegészíteni, mivel a különböző földalatti állatok és más növények az évek során folyamatosan visszapótolják a felhasznált tápanyagokat. Azonban a vizet legalább heti, de gyakran heti 2–5 alkalommal is pótolni kell, ugyanis a fölösleg egyrészt elszivárog a talaj mélyebb rétegeibe, másrészt elfolyhat az alacsonyabban fekvő területekre. Nem őshonos növények esetén csak az esőre támaszkodni nem lehet, mivel ezen növények vízigénye eltér az adott terület természetes csapadékmennyiségétől, nagyobb szárazságok esetén kiszáradhatnak. [1, 2]

A vezérlés megvalósítására a szakirodalomban több módszer is található. Megoldás lehet a cikkben is választott fuzzy logika alapú módszer, ahol a bemenetek kiértékelése – és ezzel az öntözőrendszer vezérlése – fuzzy logika segítségével történik. Másik megoldás lehet a mesterséges intelligencia használata, ahol a bejövő adatokat egy neurális háló dolgozza fel, és ebből állapítja meg a szükséges kimeneti értékeket. [3, 4]

Jelen cikkben a korábban említett ültetett növények vízigényét fogom megbecsülni, és ehhez kiszámolni a szükséges öntözési időt, hogy elérjük a talaj ideális nedvességtartamát, és ezzel a növényeknek a megfelelő mennyiségű vizet biztosítsuk.

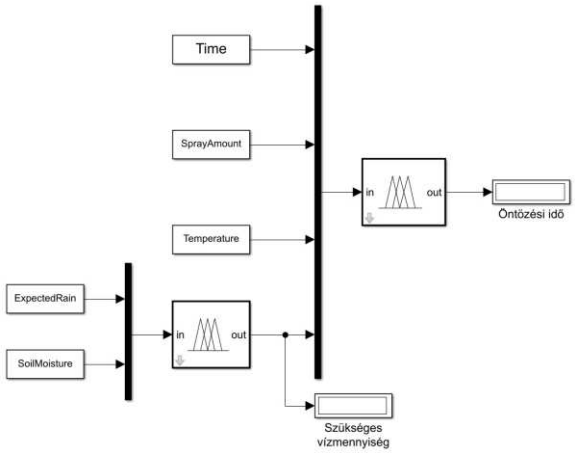
2 FUZZY MODELL

2.1 A rendszer felépítése

A modell célja meghatározni az alább sorolt bemeneti paraméterekből a szükséges vízmennyiség kijuttatásához szükséges időt. Ehhez hierarchikus modellt alkalmaztam, ugyanis ha az összes bemenetet egy rendszerre kapcsolom, a szabályok száma elérte volna az ezres nagyságrendet, amely rendszer komplexitását és ezáltal számításigényét is jelentősen megnöveli.

A rendszer felépítését az 1. ábra szemlélteti.

A modell 2 alegységből épül fel. Az első egység feladata kiszámolni a szükséges vízmennyiséget a talaj nedvességéből és a várható csapadékból. Az 1. táblázat összefoglalja, hogy a két bemenetből milyen módon keletkezik a „Szükséges vízmennyiség” kimenet.



1. ábra: A teljes modell simulinkben felépítve

1. táblázat: A talaj nedvessége és a várható csapadék logikai kapcsolata

		Várható csapadék			
		semmi	**szitál**	**esik**	**zuhog**
Talaj nedvessége	**száraz**	sok	valamennyi	kevés	semmi
	nyirkos	valamennyi	kevés	semmi	semmi
	nedves	kevés	semmi	semmi	semmi
	átázott	semmi	semmi	semmi	semmi

A második egység feladata meghatározni a locsolási időt a 2.3. bekezdésben sorolt bemenetből, illetve a fentebb említett egység kimenetéből. Mivel ez az egység 300 szabályt tartalmaz, jelen cikkbe nem tudom beilleszteni, azonban a működésének logikáját a következő pszeudokód írja le:

```
inputs: time, amount, temp, water
  if time == 1 or time == 5:
  return max(round(
      ((water+5) - (amount+1)) / 2
    ), 0) + 1
elseif time == 3 and temp == 3:
  return max(round(
    (water-1) - (amount-1)/4
  ), 1)
else:
  return 1
```

Fontos szempont, hogy az öntözésnek csak éjjel illetve délben van értelme, a többi időpontban nem lenne jó a hatásfoka. Ebből kifolyólag ha éjjel van, akkor alapos öntözést végzünk, hosszasan, jól átáztatva a talajt:

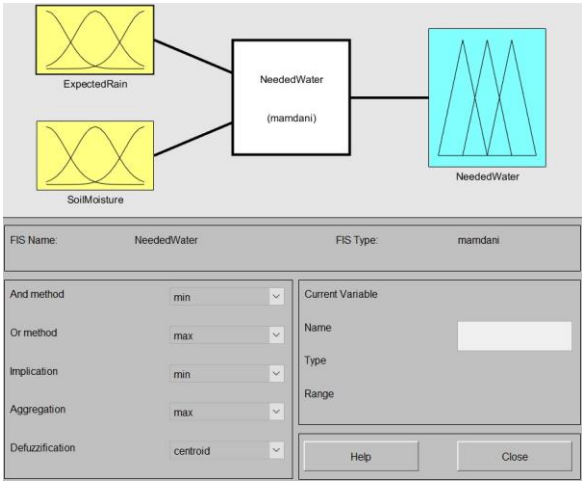
```
((water+5) - (amount+1)) / 2
```

Délben pedig csak akkor kell „lehűteni” a gyepet, amikor nagyon meleg van, így itt csak pár percre kapcsoljuk be az öntözőrendszert:

```
(water-1) - (amount-1)/4
```

2.2 *Szükséges vízmennyiség meghatározása*

A szükséges vízmennyiség meghatározására szolgáló alrendszer felépítését a 2. ábra szemlélteti.

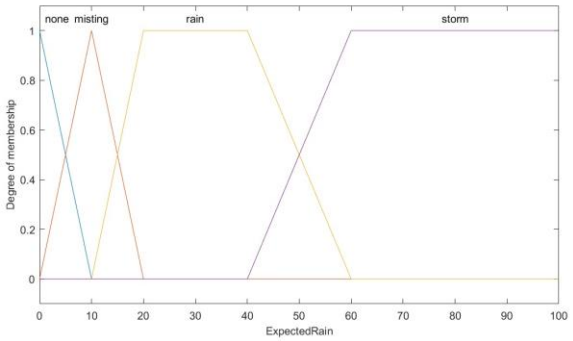


2. ábra: A szükséges vízmennyiséget meghatározó fuzzy logika

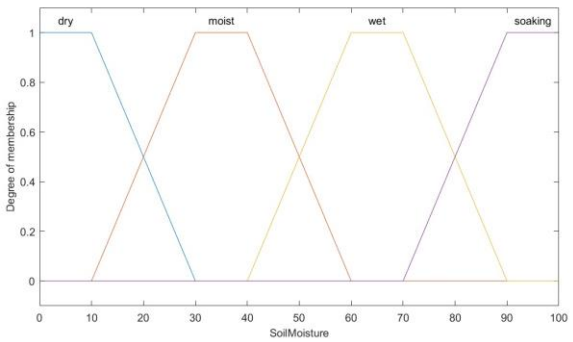
2.2.1 *Bemenetek*

Várható csapadék (ExpectedRain): A meteorológia szerint előrejelzett várható csapadék mennyisége milliméterben az adott napra. Értéke változhat napközben is. Célja a vízpazarlás csökkentése eső esetén.

Talajnedvesség (SoilMoisture): Egy vagy több nedvességmérő szenzor segítségével mért pillanatnyi talajnedvesség, százalékban kifejezve (ahol 0% a teljesen száraz talaj, 100% amikor már nem tud több vizet felvenni). A növények vízigényének meghatározására ezen bemenet a felelős, így a rendszer az épp aktuális igényekhez tud alkalmazkodni.



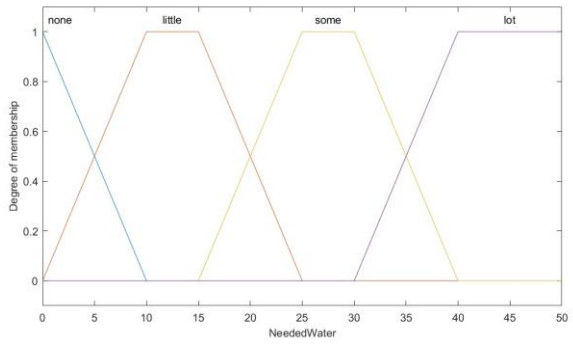
3. ábra: A várható csapadék tagsági függvényei



4. ábra: A szükséges vízmennyiség tagsági függvényei

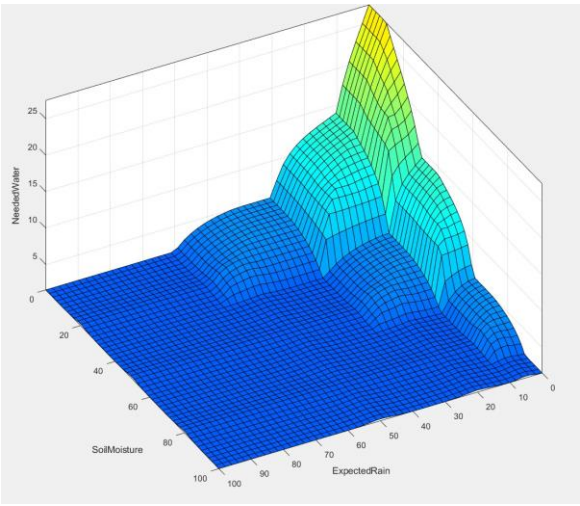
2.2.2 Kimenet

Szükséges vízmennyiség (NeededWater): A jelenleg szükséges vízmennyiség mm-ben kifejezve. Értékétől függ az éjszaka illetve délben kilocsolt víz mennyisége.



5. ábra: A szükséges vízmennyiség tagsági függvényei

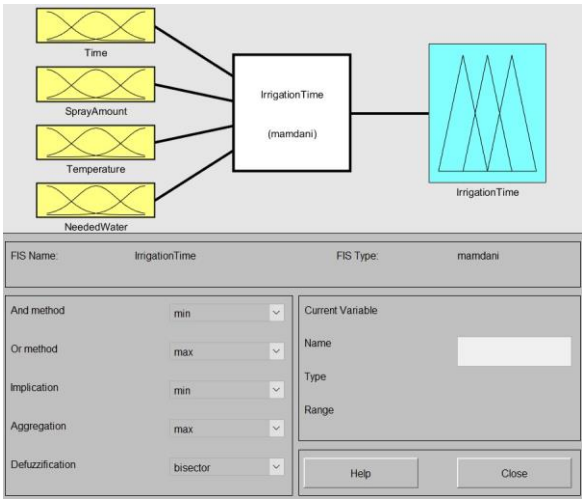
Az alrendszer által képezett kimeneti felület a 6. ábrán látható.



6. ábra: A szükséges vízmennyiség a két bemenet függvényébenű

2.3 Öntözési idő meghatározása

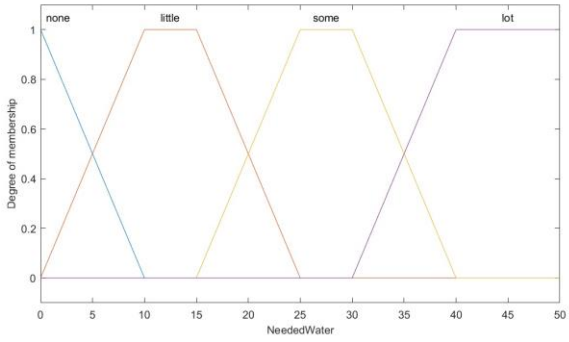
Az öntözési idő meghatározására szolgáló alrendszer felépítését a 7. ábra szemlélteti.



7. ábra: Az öntözési időt meghatározó fuzzy logika

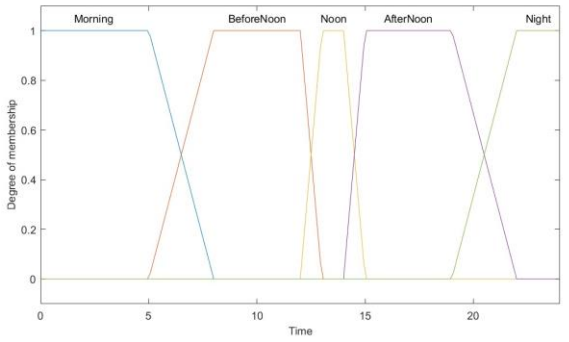
2.3.1 *Bemenetek*

Szükséges vízmennyiség (NeededWater): A jelenleg szükséges vízmennyiség mm-ben kifejezve. Értékétől függ az éjszaka illetve délben kilocsolt víz mennyisége.



8. ábra: A szükséges vízmennyiség tagsági függvényei

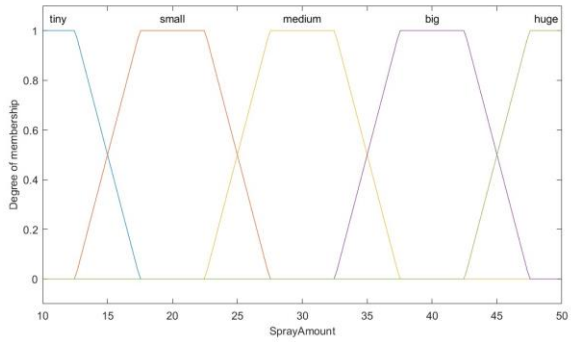
Pillanatnyi idő (Time): A paraméter értéke [0;24[közötti lehet, a pillanatnyi időt adja meg órában, tört számként. 5 trapéz alakú tagsági függvényt tartalmaz, melyek az éjszakai és a déli órák megkülönböztetésére szolgálnak a nap többi részétől. A déli órák körüli függvények meredekebbek, hogy ezen időszak élesebben határolódjon el az éjszakánál, mivel ekkor csak egy rövid időre kell bekapcsolni az öntözést.



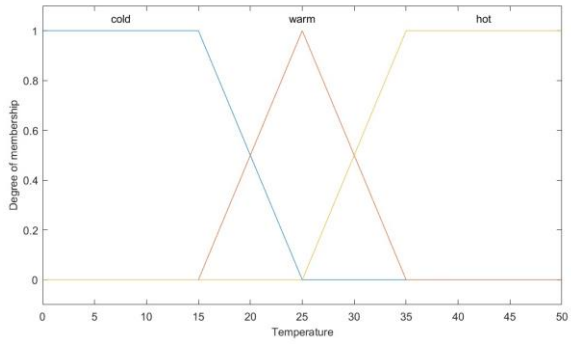
9. ábra: A pillanatnyi idő tagsági függvényei

Kilocsolt vízmennyiség (SprayAmount): A paraméter értéke az adott területre kilocsolt víz mennyisége, milliméterben értelmezve. A rendszer futása alatt értéke konstans marad, csak az öntözőrendszer változtatása esetén és a tavaszi beüzemeléskor kell frissíteni. A frissítése egy egyszerű méréssel történik: kihelyezünk 2-5 egyenes (függőleges) falú edényt vagy poharat az öntözési területre, majd egy ismert időtartamra (célszerű minél hosszabbra, pl 5 vagy 10 percre) bekapcsoljuk az öntözést. Az idő letelte után megmérjük az edényekben összegyűlt vízmennyiség magasságát, azaz hogy hány milliméter került bele. Ezen értékek átlagát vesszük, majd osztjuk a percben értelmezett öntözés időtartamával, így megkapjuk az öntözési teljesítményt mm/min-ben, ez lesz a paraméter értéke.

Hőmérséklet (Temperature): A levegő pillanatnyi hőmérséklete árnyékban, az öntözött terület közelében mérve, °C-ban értelmezve. Jelentősége a melegebb időszakban van, ugyanis nyáron a déli nagy kánikulák miatt a gyep túlhevülhet vagy kiszáradhat, de ezt egy rövid öntözéssel megakadályozhatjuk. Erre megoldást nyújtva a bemenet feladata meghatározni, hogy kell-e délben „lehűtő” öntözést végezni.



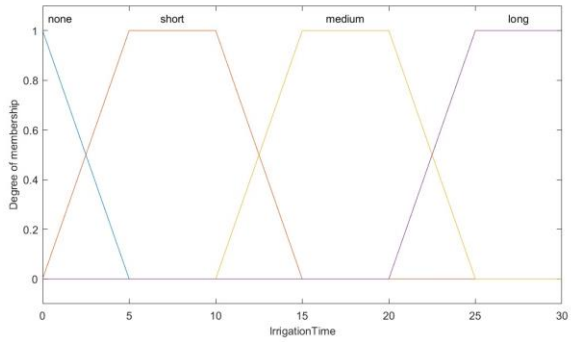
10. ábra: A kilocsolt vízmennyiség tagsági függvényei



11. ábra: A hőmérséklet tagsági függvényei

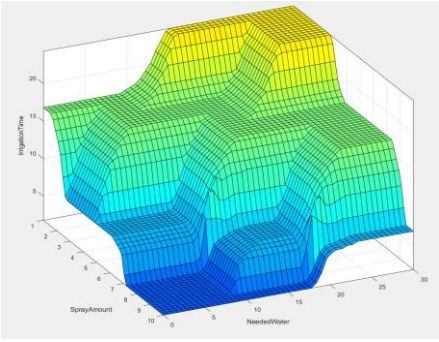
2.3.2 *Kimenet*

Locsolási idő (IrrigationTime): A rendszer kimenete, az éppen aktuálisan szükséges mennyiségű idő percben értelmezve ahhoz, hogy kielégítsük a növények vízigényét.



12. ábra: A locsolási idő tagsági függvényei

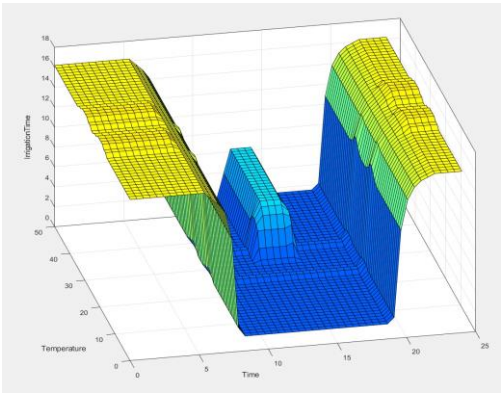
Az alrendszer által képezett kimeneti felület a 13. ábrán látható.



13. ábra: Az öntözési idő a Kilocsolt és a Szükséges vízmennyiség függvényében

3 AZ ELKÉSZÜLT RENDSZER

Az alábbi képeken látható az elkészült modell:



14. ábra: Az öntözési idő az Idő és a Hőmérséklet függvényében

4 ESETTANULMÁNY

A következőkben megvizsgálok néhány kritikusabb esetet, illetve hogy ezen esetekben hogyan viselkedik a modell. Kritikusnak kell tekintenünk azon eseteket, amikor a hőmérséklet nagyon magas (>30°C), illetve amikor a talaj nedvessége szélsőséges (<15% / >85%). A SprayAmount értéket minden esetben 5mm/minre állítottam be, mivel az öntözőrendszer paraméterei nem változnak meg a normál üzem közben.

A különböző bemenetekre adott kimenetet a 2. táblázat tartalmazza. Az öntözési idők esetében a 4-6 percnél kisebb értékeket 0-nak kell tekinteni, az okáról később írok.

2. táblázat: Az esettanulmány be- és kimenetei

Ssz.	T [h]	SprAmnt [mm/min]	Tmp [°C]	ER [mm]	SM [%]	IT [min]
1	22.0	5.0	27.0	01.3	37.0	15.6
2	22.0	5.0	27.0	14.6	37.0	06.6
3	22.0	5.0	27.0	14.6	74.0	06.6
4	22.0	5.0	18.0	02.7	68.0	06.6
5	22.0	5.0	18.0	18.3	68.0	06.6
6	22.0	5.0	18.0	18.3	23.0	09.3
7	10.0	5.0	27.0	14.6	37.0	01.5
8	10.0	5.0	38.0	14.6	37.0	01.5
9	10.0	5.0	38.0	00.0	37.0	01.5
10	12.5	5.0	27.0	14.6	37.0	01.8
11	12.5	5.0	38.0	14.6	37.0	01.8
12	12.5	5.0	38.0	00.0	37.0	06.3

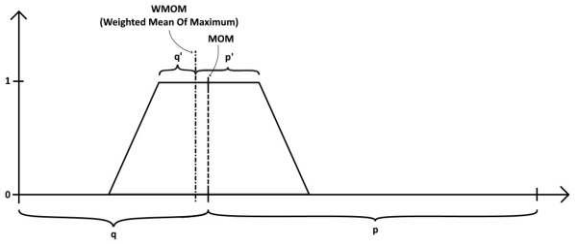
Az első 6 sorban az esti öntözésre adott viselkedést vizsgáltam. Megfigyelhető, hogy csak akkor locsol a rendszer, ha nincs várható eső és alacsony a talaj nedvességtartalma. Ez megegyezik az elvárt viselkedéssel, mely szerint akkor kell öntözni, ha már száraz a talaj és nem lesz eső se.

A 7-12. sorban a nappal-dél kapcsolatot térképezem fel. Itt a feladat, hogy csak 12 és 13 óra között öntözhet, és akkor is csak ha magas a hőmérséklet és nincs várható eső.

Amint az látható, csak a 12. sor bemenetei esetén kezdeményez locsolást, de ekkor is csak egy 6 perceset.

5 TOVÁBBFEJLESZTÉSI LEHETŐSÉGEK

A modell az alapvető követelményeknek megfelel, de hatékonysága javítható. A korábban említett hiba (miszerint a 4-6 percnél rövidebb időket 0-nak kell tekinteni) abból származik, hogy a két egységben a defuzzifikációs módszer centroid, de valójában jelen körülmények között egy úgynevezett weighted mean of maximum lenne a célszerű. Ezen módszer lényege, hogy a kimeneti érték nem a maximumok átlaga, hanem a maximumok intervallumának arányos pontja a maximum átlagának a teljes tartománybeli elhelyezkedésével. Egy szemléltető példa látható erre a 15. ábrán.



15. ábra: A WMOM defuzzifikációs módszer

Számítása az (1) képlet segítségével lehetséges.

$$value = (max(mf) - min(mf)) \cdot \frac{\frac{max(mf)+min(mf)}{2} - min(x)}{(x + min(mf)\ max(x)) + min(x)}$$

Ahol:

- x: a defuzzifikálandó tagsági függvény x tengelye
- mf : a defuzzifikálandó függvény értékei x-nél

value: a defuzzifikáció eredménye

6 ÖSSZEGZÉS

A modell az alapvető követelményeknek részben felel meg, a bemeneti paraméterek alapján a logika szerint elvárt kimenetet adja. A hatékonyság növelése és a kisebb hibák kiküszöbölése érdekében azonban további értelmezés szükséges, hogy a kimenet ténylegesen továbbítható legyen a vezérlésnek.

IRODALOMJEGYZÉK

[1] Tóthné Dr. Laufer Edit. *Fuzzy rendszerek mérnöki alkalmazása*. Óbudai Egyetem. 2019. (Elérés dátuma 2022. 05. 12.).

[2] *Efficient irrigtion for water conservation: guideline for water efficient urbn gardens and landscapes*. Angol. CS10057_10/20 verzió. State of Queensland. 2020. url: https://www.resources.qld.gov.au/__data/assets/pdf_file/0010/ 1463779/efficient-irrigation-guideline. pdf (elérés dátuma 2022. 05. 12.).

[3] Aydin, Ömer, et al. "An artificial intelligence and Internet of things based automated irrigation system." arXiv preprint arXiv:2104.04076 (2021).

[4] Mohammed, Benzaouia, et al. "An intelligent irrigation system based on fuzzy logic control: A case study for Moroccan oriental climate region." 2nd international conference on Embedded Systems and Artificial Intelligence (ESAI'21). 2021.

BÁNKI KÖZLEMÉNYEK
V. ÉVFOLYAM 1. SZÁM

Drónok okozta veszélyhelyzetek és balesetek, valamint azok megelőzésének lehetőségei

Use of drones by terrorist organizations

BÁLINT Márton
Óbudai Egyetem Biztonságtudományi Doktori Iskola, Budapest, Magyarország
balint.marton@phd.uni-obuda.hu

Összefoglalás - A drónok számos előnyös tulajdonsággal rendelkeznek, és ezek az előnyök a legváltozatosabb módokon aknázhatók ki. A drónok használata ugyanakkor számtalan veszélyt hordoz, és az ártó szándékú magatartások ezeknek csak egy szegmensét jelentik. Jelentős biztonsági kihívást jelentenek a gyakorlatlan, tapasztalatlan drónkezelők, azok, akik a nyilvánvaló veszélyekkel nem számolva kezelik pilóta nélküli eszközüket. Több esetben előfordult, hogy megszakadt a drón és az irányító egység közötti kapcsolat, vagy a kezelő – rossz szándékból vagy puszta figyelmetlenségből – olyan területre vezette az eszközt, ahol annak semmi keresnivalója nem volt. A drónbalesetek legtipikusabbja az, amikor az irányíthatatlanná váló drón járműre, épületre zuhan, emberrel ütközik. Jelen tanulmányban áttekintettük a drónok alkalmazásának lehetséges színtereit, összegyűjtöttünk néhány tipikusnak mondható drónbalesetet, végül arra a kérdésre keressük a választ, hogy a balesetek milyen módokon, milyen megoldások révén előzhetők meg

Kulcsszavak : drón, felhasználás, véletlen, baleset, biztonság, megelőzés

Abstract - Drone technology offers many advantages that can be used in a large variety of positive applications. At the same time drone usage can also be the source of numerous dangers. The malignant application of drones is only one segment of such dangers. Unskilled and inexperienced drone pilots represent a major security challenge, those who use pilot free flying devices without taking into consideration even the most evident risks. The loss of communication between the pilot and the drone is a regular occasion. Also, such drones fly – for harming purposes or by pure lack of attention – over areas where it should not be. The falling of an uncontrolled drone over a vehicle, building of collision thereof with one or several people is the most common example of drone accidents. The present paper will show an overview of possible drone application scenarios, will list some of the most typical drone accidents and will conclude by studying the means and solutions by which drone accidents could be avoided.

Keywords: drone, application, unintended, accident, security, prevention

1. BEVEZETÉS

Az angol drone szó eredeti jelentése here, vagyis hím méh, idővel azonban a zümmögés, zúgás jelentés is e kifejezéshez kötődött. Egy másik magyarázat szerint az angol Királyi Légierő (Royal Air Force) gyakorlatozás céljára kifejlesztett egy távolról irányítható repülni képes célpontot, amelyet egy Méhkirálynő (Queen Bee) néven emlegetett repülőgépet átalakítva konstruáltak meg. A gyakorlatozás során robotrepülőket teszteltek, melyek feladata volt a Méhkirálynő ártalmatlanítása, így kézenfekvőnek tűnt e robotrepülőket drone-oknak (vagyis hím méheknek) nevezni. Idővel ezt a mulatságos nevet kezdték használni más pilóta nélküli repülőkre is [1].

A távirányítású repülők, vagyis a drónok egy alcsoportját képezik a pilóta nélküli repülőgépek, habár e fogalmak terén az egyes forrásokban mutatkozik némi bizonytalanság. A pilóta nélküli repülőgép (Unmanned Aerial Vehicle, a továbbiakban: UAV) irányító személyzet és mindenfajta közvetlen emberi beavatkozás nélkül repül. A Remotely Piloted (Aerial) Vehicle (RPV; másként: Remotely Piloted Aircrat System, a továbbiakban: RPAS) elnevezés távolról irányított légijárművet takar, amely magában foglalja a távirányítású repülőt, a repülőre szerelhető vezérlő egységet, az irányító egységet és minden olyan eszközt, mely a repülési feladat végrehajtásához nélkülözhetetlen [1].

A pilóta nélküli repülőgépet elsősorban katonai célokra fejlesztették ki, és az 1960-as évek óta viszonylag széles körben alkalmazzák a harcászatban. Két fő sajátossága, éspedig az, hogy pilóta nélkül képes repülni, valamint az irányítása a távolból is megoldható, alkalmassá teszi minden olyan feladat végrehajtására, amely veszélyeztetné az ember életét, testi épségét, vagy amelynek a kivitelezéséhez „emberi tudás és/vagy képesség már nem lenne elég”[2].

A drónok tipizálásának többféle módja is ismeretes, csoportosíthatók méret, alkalmazási terület szerint. A legkisebb rovarméretűek, vannak néhány kilogrammos, de akár a tíz tonnát is elérő példányok. Ismeretesek forgószárnyas, merevszárnyas, illetve felhajtóerő elvén működő drónokat. Rotorszám szerint megkülönböztetjük a trikoptert, a kvadrokoptert, a

hexakoptert, az oktokoptert, vannak továbbá speciális gépek is, melyeknél a rotorok egy része felfelé, másik része lefelé áll. Sokféle lehet a meghajtó rendszerük is, a kisebb eszközöket rendszert akkumulátor működteti, a nagyobbakat villanymotor, a valamivel nagyobbakat (melyek pár száz kilogrammnyi terhet is képesek felemelni) robbanómotor. A legnagyobb pilóta nélküli gépek jellemzően légcsavaros gázturbinával, újabban sugárhajtóművel működnek [2].

2. A DRÓNOK ALKALMAZÁSI LEHETŐSÉGEI

A drónok a legváltozatosabb feladatokra alkalmazhatók. Leginkább nehezen megközelíthető helyszíneken, az emberi életre, a testi épségre veszélyt jelentő körülmények között vetik be ezeket az eszközöket, nemcsak harci cselekmények során, hanem veszélyes anyagok jelenléte esetén is. A feladatot képesek előre megírt program alapján végrehajtani, de manuálisan is irányíthatók távolról. Sokoldalú, alapvetően könnyen kezelhető szerkezetekről van. Bevethetők katasztrófavédelmi, tűzvédelmi iparbiztonsági feladatok ellátásánál, alkalmasak kémiai, biológiai, radiológiai, nukleáris veszélyeztetettség feltárására, az ilyen jellegű veszélyeztetettség elhárítására, mentesítési feladatokra. A pilóta nélküli eszköz egyik fő előnye a nevéből kikövetkeztethető: mivel nincsen rajta személyzet, ezért erősen szennyezett terület felett is alkalmazható, és sokkal tovább a levegőben maradhat, mint egy hagyományos repülőgép [3].

Egy tűzvédelmi kérdésekkel foglalkozó tanulmány megállapította, hogy míg egy drón nagyjából két percen belül használható felvételeket küld a tűzről, addig a gyalogos tűzoltó körülbelül 420 métert képes megtenni, ez a távolság pedig csak egy 67 méter sugarú tűzkári terület bejárást teszi lehetővé. Vagyis, a drónos felderítés vitathatatlanul hatékonyabb, hiszen segítségével bármilyen magasságból és bármilyen szögből végezhető megfigyelés, emellett – hőkamerával – alkalmas a rejtett tűzfészkek, parázsló zugok felkutatására, leégett területek ellenőrzésére is. Emellett, további előny az is, hogy a drón által közvetített audio- és videófelvételt biztonságos helyen egyidejűleg több személy is tanulmányozhatja, illetve a modern technikának köszönhetően a helyszíni képeket okostelefonon is meg lehet tekinteni [4].

Egy atlantai (USA) cég, a Sonin Hybrid egy olyan hibrid (benzin és elektromos) meghajtású drónt készített és árusít, amely akár 225 kilométer/órás sebességgel is képes haladni, de a normál sebessége is eléri a 96 kilométer/órát. A könnyű szénszálas anyagból készült Recruit három órán át a levegőben marad, és a teherhordó képessége is nagyobb, mint a vele azonos kategóriába tartozó gépek többségéé. A tizenkétszeres digitális és harmincszoros optikai zoomos kamerával felszerelt eszközt a gyártó elsődlegesen elsősegélynyújtásra ajánlja [5].

1. Ábra: Recruit típusú rendőrségi drón.

A pilóta nélküli gépek zöme beépített GPS helymeghatározóval van felszerelve, így műholdak támogatásával egy előre megtervezett röpvonalon is képes haladni vagy szektoronként fel tudja térképezni a kijelölt területet. Idézzünk fel egy hazai példát: a 2013-as dunai árvíz idején a honvédelmi szaktárca megbízásából fejlesztett drónok (X8, Bora, Ikran) Esztergom–Tát–Nyergesújfalu térségében egy harminc négyzetkilométeres körzetet berepülve közvetítették az élőképeket. Említhetők azonban külhoni megoldások is. A spanyol tűzvédelmi hatóság egy kategóriájában viszonylag nagynak számító, 2–4 kilogramm teherbírású merevszárnyú drónt használ, mely egyetlen feltöltéssel száz kilométerre is elrepül. Hőkamerával van felszerelve, fedélzeti számítógépére pedig egy speciálisan az andalúziai bozóttüzek elemzésére és stratégiai javaslatok adására képes programot telepítettek [6].

2. Ábra: X9 felderítő UAV.

3. Ábra: Bora felderítő UAV

4. Ábra: Ikran felderítő UAV.

Az intelligens drónok esetében egy Google Maps alapú térképen előre megjelölhetők azok a pontok (GPS koordináták), melyek érintésével kell az eszköznek haladnia. Be lehet programozni a repülési magasságot, miként azt is, hogy a kamera milyen irányban, mekkora dőlésszögben rögzítse a képet. Ha a tervezett útvonalon változatosak a domborzati viszonyok, az intelligens drónt be lehet úgy állítani, hogy menet közben vegye figyelembe a térkép által jelzett magasságot. A legmodernebb eszközök azonban már fel vannak szerelve lefelé néző optikai vagy ultrahangos szenzorokkal, márpedig e funkció bekapcsolásával elérhető, hogy a gép mindig egy meghatározott távolságra repüljön a talajtól [7].

Az amerikai fejlesztésű, hat méter szárnyfesztávolságú Viking 400-S (L3 Unmanned Systems) üzemideje tizenkét óra, teherbírása 45 kilogramm, egy speciálisan kialakított kameraházat helyeztek el rajta, melybe vegyi, nukleáris és radioaktív veszélyek felderítésére szolgáló készülék helyezhető el. A Lockheed Martin és a Kaman Aerospace által közösen fejlesztett-gyártott gép a Kaman K-MAX UAT, melynek teherbírása megközelíti a 2800 kilogrammot, akár mentésre is alkalmas.

5. Ábra: Viking 400-S drón.

6. Ábra: Kaman K-MAX UAT

A drón a rendészet eszköztárába is remekül beilleszthető, támogathatja a közlekedésrendészet, a baleseti helyszínelők munkáját, bűnmegelőzési célzattal megfigyelhetővé tesz tömegrendezvényeket, közterületen segíti a járőrök munkáját, alkalmas személyek követésére, veszélyeztetettek csoportjába tartozó (például kiskorú, idős, feltehetően öngyilkosságot elkövetni akaró) emberek felkutatására. Drónnal megközelíthetők közlekedésre alkalmatlan, nehezen bejárható, életveszélyes területek. Drónnal körözési feladat is végrehajtható, ugyanis nagykiterjedésű magán- és közterületek is átkutathatók ilyen módon [8].

A drónok rendészeti alkalmazására említhető példaként a west-midlands-i (Egyesült Királyság) rendőrség kísérleti modellje, melynek keretében drónok alkalmazásával figyelték a futballmérkőzésekre érkező szurkolókat; az angol légügyi szabályozás alapján a drónok a stadionok felett nem repülhetnek át, ám már az is kellő visszatartó erővel bírt, hogy megfigyelték a beléptetésre várókat, és már ott ki tudták emelni a tömegből a rendbontó magatartást tanúsítókat. A hatékonyság és a költséghatékonyság szempontjai kerültek előtérbe akkor, amikor a queenslandi (Ausztrália) rendőrség a helikoptereit pilóta nélküli gépekre cserélte: egyrészt azért, mert segítségükkel jóval gyorsabban tudtak intézkedni (például szükség esetén a helyszínre vezényelni élőerőt), másrészt azért, mert a drónok fenntartása, üzemeltetése jóval kisebb terhet ró a rendőrség költségvetésére [9].

A drónok polgári célú felhasználása is széles körű, és a tapasztalat azt mutatja, hogy egyre változatosabb feladatokra vetik be. Ha a gépet felszerelik a megfelelő szoftverrel, számos, emberi beavatkozást nem igénylő feladatot végre tud hajtani, márpedig ez – miként arra a koronavírus-világjárvány felhívta a figyelmet – nagyon is lényeges szempont.

A drónok mezőgazdasági célú alkalmazása is egyre inkább elterjed, használhatók az erdőgazdálkodásban, a precíziós növénytermesztésben, a legkülönfélébb típusú károk (aszálykár, vadkár stb.) felmérésében. Drón segítségével könnyedén azonosítani lehet a kritikus

területeket, például a termőföld azon részeit, ahol a gyomnövények, a kártevők elszaporodtak, ahol tápanyagpótlásra, öntözésre van szükség. Drónról akár a vetőmag, a növényvédő szer, a műtrágya is a talajra juttatható, mégpedig célzottan oda, ahol arra szükség mutatkozik. A Mecsekerdő Zrt. a vegetáció monitorozására használja a drónokat, a Baranya megyében található erdők felét ilyen módon felügyeli. A drónok felvételeket készítenek a faállományról, a szakemberek az így nyert képalapú adatok elemzésével időben felismerik a fák pusztulását, a természeti élőhelyek változásait [10] [11].

A drón alkalmas a szakhatóságok tevékenységének támogatására is. Például az Országos Vízügyi Főigazgatóság drónokkal monitorozza a természetes vizeket, így különösebb nehézség nélkül nyomon követhetők a vízszintingadozások, az érkező árvizek, a jégzajlás. A drónra szerelt hőkamerával észlelni lehet a víztározókon, csöveken vagy akár a gátakat védő homokzsákokon található sérüléseket [11].

Az áruszállítás terén és az építőiparban már jónéhány éve bevett eljárásnak számít a drónok alkalmazása, más iparágakra ez még nem feltétlenül jellemző, habár vannak külföldi jó gyakorlatok. Így például a drón segítheti a készletgazdálkodást, nagy területen tárolt eszközökről leltárt készíthet, egy megadott árucikket megkereshet. Drónnal munkabiztonsági megfigyelés végezhető, nyomon követhető adott termelési folyamat előrehaladása, az, hogy éppen hol tart a megvalósítás, van-e eltérés a tervektől. Már egészen korai fázisban feltárhatók a kockázatok, a rendszeres megfigyelések lehetővé teszik az eltérések kijavítását, szükség esetén a műszaki folyamat újra tervezését. Külhoni jó gyakorlatra példa a Gazprom megoldása: Oroszországban kétezer kilométer hosszúságú csővezeték kiépítése volt a feladat, a cég már a tervezés korai fázisában drónokat alkalmazott az építési terület megismerésére, majd később a munkafolyamat ellenőrzését, a projektmegfelelőség biztosítását segítették a robotrepülők [11].

A drón a magánbiztonság céljait is képes megfelelően szolgálni. A Kecskeméti Városrendészet például egy időben az éjszakai órákban drónokat reptetett a közterületek felett, így figyelte meg és azonosította be a szabályszegőket, akiket indokolt esetben még figyelmeztetni is tudott [11].

A fentieken túlmenően a filmipar is előszeretettel él a drónok nyújtotta lehetőségekkel, de a lakossági felhasználás is egyre népszerűbb, hobbieszközként szolgál, szabadtéri rendezvények vagy éppen családi események megfigyelésére és megörökítésére is alkalmas.

E cikk keretei nem elégségesek ahhoz, hogy kimerítő felsorolását adjuk a drónok lehetséges alkalmazási módozatainak, az azonban a fenti rövid áttekintés alapján is belátható, hogy egyre nagyobb volumenű, egyre szélesebb alkalmazási körű drónhasználattal kell számolnunk. Tény ugyanakkor az is, hogy a drónok használata biztonsági kérdéseket is felvet, a híradások gyakorta szólnak drónok okozta balesetekről. A következő fejezetben néhány példán keresztül szemléltetjük, milyen veszélyhelyzeteket idézhetnek elő a pilóta nélküli gépek.

3. DRÓNHASZNÁLAT MIATT BEKÖVETKEZETT BALESETEK, VESZÉLYHELYZETEK

Az Egyesült Államok Szövetségi Légügyi Hatósága (Federal Aviation Administration, a továbbiakban: FAA) már 2015 októberében arra hívta fel a figyelmet, hogy egyre több drón kerül magánszemélyek birtokába, ami december hónapban – lévén népszerű karácsonyi ajándékról van szó – akár egymillió újonnan üzembe helyezett gépet is jelenthet. Márpedig az, hogy repülési ismeretekkel nem rendelkező, a drónreptetésben járatlan emberek kezébe kerülnek az ilyen eszközök, a balesetveszély megnövekedését is eredményezheti, mutatott rá az FAA, mely 2015 első félévében közel hétszáz riasztást kapott azzal kapcsolatban, hogy pilóta nélküli eszközök túl közel repültek az utasszállító gépekhez. A veszélyt olyannyira fenyegetőnek érzik a légitársaságok, hogy például a Boeing már be is szerzett drónhatástalanító fegyvereket. Az FAA ugyanakkor tud olyan esetekről is, amikor UAV zavarta a kaliforniai erdőtüzek oltásában résztvevő helikoptereket, egy másik alkalommal pedig civilek drónokkal próbáltak kémfotókat készíteni a Trónok harca forgatásán [12].

A „drón-konfliktus” egyfelől tehát abból adódik, hogy az eszközöket olyan helyekre reptetik, ahol azoknak nincsen semmi keresnivalójuk. A másik fő veszélyforrást a gyakorlatlan felhasználók jelentik, akik a drónreptetés során számos váratlan nehézséggel szembesülnek, ez különösen zsúfolt, sűrűn beépített nagyvárosi környezetben fordul elő. Zavaró tényező lehet az erős szél, a rádióantennák és -tornyok interferenciája, irányítási problémákat okozhatnak a magas épületek körül hirtelen megváltozó szél- és fényviszonyok, a rossz láthatóság; ezek a körülmények könnyen vezetnek ahhoz, hogy az eszköz látótávolságon kívül kerül, az operátor pedig elveszíti az irányítást felette. Nézzünk néhány példát a drónok okozta balesetekre, balesetveszélyes helyzetekre.

2013-ban a Virginia állambeli (USA) Motorsports Parkban rendezett bikafuttatáson szabadult el egy UAV, a közönségbe csapódott, és súlyosan megsebesített néhány nézőt. 2014-ben egy céges rendezvényen repült egy kisebb drón egy fotósnak, megvágta az állát, az orrát pedig levágta. Ugyanebben az évben egy drón éppen csak elkerülte az ütközést – 700 láb magasságban – egy Airbus A320 utasszállítóval. 2015 januárjában az Egyesült Államok

mexikói határán zuhant le egy kábítószert szállító pilóta nélküli gép, a kvadrokopter roncsait és mintegy három kilogramm metamfetamint a határátkelő közelében, egy áruház parkolójában találták meg. A mexikói rendőrök szerint túl nagy volt a rakomány, azért esett le a drón [13] [14] [15].

7. Ábra: Kábítószert szállító drón.

2015. január 26-án egy drón hatolt be a Fehér Ház feletti légtérbe, a biztonsági szolgálat a terrortámadás lehetőségét is felvetette, később kiderült, hogy erről szó sem volt, csak az eszköz a tulajdonosa számára irányíthatatlanná vált.

2015 májusában a naganoi (Japán) zenei fesztiválon egy tizenötéves fiú drónja esett a nézők közé, szeptemberben egy 49 éves férfi által irányított UAV csapódott a világörökségi helyszínen található Himedzsi kastélyba [16].

2015 decemberében Marcel Hirschert, a négyszeres világkupa-bajnok síelőt csaknem agyonütötte egy drón a Madonna di Campiglio-i műlesikló versenyen: éppen siklott le a pályán, amikor közvetlenül a háta mögött becsapódott egy meghibásodott drón. A sportoló nem sérült meg, és ugyan érzékelte a problémát, de csak utólag tudta meg, mi történt [17].

Az FAA egy tanulmányban arra mutatott rá, hogy a repülőgépek számára sokkal kockázatosabb drónnal ütközni, mint madárral. A drón egyes elemei esetében ugyanis jóval nagyobb az anyagsűrűség, mint a madárcsontban (ez különösen igaz az akkumulátorra, a kamerára), így a nagy erővel becsapódó eszköz komoly károkat képes okozni. A kutatók szimulációs kísérletet végeztek, mely során azt modellezték, mi történik, ha egy 1,2 kilogrammos Phantomot, illetve egy 1,8 kilogrammos PrecisionHawk Lanchester modellt

8. Ábra: PrecisionHawk Lanchester típusú drón.

irányítanak egy sűrített levegővel működő szerkezetből egy nagygép (jelen esetben egy Boeing 737-es és egy Learjet 31A bizjet) testének különböző pontjaihoz. A modellezés eredményeként kiderült, hogy 250 csomós sebességnél a pilótafülke ablakait viszonylag kisebb kár éri, közepes a károsodás, ha a becsapódás a szárnyak belépő élét éri, és közepes vagy annál nagyobb a kár, ha a drón a nagygéppel annak függőleges vagy vízszintes vezérsíkján találkozik [18].

2017 szeptemberében New Yorkban egy katonai helikopter ütközött egy kisméretű drónnal, 2018 januárjában egy charter-gép ütközött egy UAV-val, azt megelőzően pedig Hawaii-on került sor egy hasonló incidensre, amikor a pilóta nélküli eszköz egy helikopter rotorjának repült. Baleset egyik esetben sem történt, a nagyobb gépek kisebb sérülésekkel megúszták. Nem volt ilyen szerencséje annak a Robinson R22-es kétszemélyes helikopternek, mely 2018 elején Dél-Kaliforniában lezuhant egy drón miatt. A helikoptert tanulópilóta vezette, ám az oktató észlelte az UAV – feltehetően egy Phantom kvadrokopter – közeledését, átvette az irányítást, és megpróbált kitérni az ütközés elől. Ez a manőver ugyan sikeres volt, ám közben a farokrotor belegabalyodott egy fa ágaiba, ennek következtében zuhant a helikopter a földre. Súlyosbítja a történtek megítélését, hogy a távirányítású drónt a Charlestoni repülőtér közelében repették, ott, ahol egyébként az ilyen eszközök üzemeltetése tilos. A Robinsonban 180 ezer dolláros kár keletkezett, és bár személyi sérülés nem történt, az eset úgy vonult be a „drón-konfliktusok” történetébe, mint az „első igazi drón-baleset” [19].

Szakértők e baleset kapcsán rámutattak, hogy ha az UAV nagygéppel, többszáz utast szállító kereskedelmi géppel, teherszállító repülővel találkozik, és a drónt nem darálja be a hajtómű, a katasztrófa esélye elhanyagolható. A könnyű gépek, a viszonylag alacsonyan repülő (rendőrségi, mentő stb.) helikopterek ugyanakkor jóval nagyobb veszélyben vannak, és nem is feltétlenül a drónnal történő ütközés következtében lehet a lezuhanásukra számítani, hanem – mint azt a dél-karolinai eset is mutatja – akkor, amikor a pilóta az ütközést elkerülendő kénytelen veszélyes manővereket végrehajtani [19].

Személyi sérüléssel járt az a 2021-es eset, melynek során a chilei haditengerészet Bell UH-57B Jetranger III típusú helikoptere ütközött egy drónnal. A két fős személyzettel járőröző helikopter a Punta de Tralca nevű, szállodákkal teli üdülőhely felett járt, amikor ismeretlen körülmények között nagy erővel nekicsapódott egy kisméretű UAV (feltehetően egy 570 grammos Mavic Air 2), mely a szélvédőt áttörve megsebesítette a helikopter utasát, és csak a szerencsén múlt, hogy nem a pilótát találta el. A katona az arcán sérült meg, kórházba is kellett szállítani. A hatóságoknak nem sikerült az eszközt azonosítaniuk, mert az – megsértve ezzel a helyi jogszabályokat – nem volt regisztrálva, és nem is szerepelt rajta a tulajdonosra utaló jelzés [20].

Magyarországon is történt már drónbaleset. Egy huszonhárom éves szingapúri férfi Budapesten a Duna fölé reptette a drónját, hogy felvételeket készítsen, ám feltehetően a Szabadság-híd vastömege leárnyékolta az eszközt, mely így nem kapott jelet az irányító egységtől: a drón a hídon irányíthatatlanná vált, rázuhant egy gépjárműre, betörve a szélvédőjét [9].

4. Védelmi mechanizmusok

A drónok, habár hasznot hajtó alkalmazásuknak számos módja van, ugyanakkor jelentős veszélyeket is magukban rejtenek, különösen, ha gyakorlatlan személy próbálkozik az irányításukkal. Az alábbiakban megvizsgáljuk azokat a lehetőségeket, melyekkel elkerülhetők a drón-balesetek.

Az interneten több olyan írással is találkozunk, mely a kezdő drónhasználók számára nyújt praktikus tanácsokat. Az egyik – „Hogyan ne zuhanjon le a drónod” típusú, oktatást is kínáló – oldalon a következőket javasolják. A friss dróntulajdonos, mielőtt „élesben” is kipróbálná az eszközt, olvassa el többször is a felhasználói kézikönyvet, majd gyakoroljon néhány órát szimulátoron, hogy megszokja a vezérlőeszközöket. Miután elsajátította a kezelés alapjait, elkezdheti a reptetést, de kezdetben ne irányítsa a gépet 30–40 méternél magasabbra, és ekkor még ne működtesse a kamerát. Gyakorolja a „Hazatérés” funkciót, hazatéréshez pedig állítson be egy maximális repülési magasságot, elkerülendő a fákkal, épületekkel való ütközést. A kábelekre, vezetékekre külön kell a kezelőnek ügyelnie, az akadályérzékelők ugyanis a vékony akadályokat nem érzékelik, ez fokozottan érvényes a hátramenetre és a rosszul megvilágított terekre. Javasolt felszállást követően körülbelül fél percen át egy méter magasságon lebegtetni az eszközt, így bemelegszik az akkumulátor, és az is kiderül, ha valami probléma van vele. A vészleállító parancsot csak a rendeltetésének megfelelően szabad kiadni. Kerülni kell a drónhasználatot szeles időben, magasfeszültségű vezetékek közelében és minden olyan helyen, ahol nagy interferenciára lehet számítani (például nagy méretű fémtárgyak mellett). Nem tanácsos a madarakat megzavarni, a területüket óvó ragadozómadarak képesek akár meg is támadni a drónt [21].

Amerikai szakértők szerint megoldást jelenthet, ha a hobbicélú UAV-ok esetében a jogalkotók, illetve a gyártók korlátozzák azok képességeit (például megakadályozzák, hogy nagy sebességgel vagy meghatározott magasság felé repülhessenek). Az FAA egyfajta megoldást lát a felhasználók tájékoztatásában, ennek érdekében fel is vette a kapcsolatot a Walmart üzletlánccal, hogy kialakítsanak egy stratégiát, miként lehetne minél hatékonyabban felhívni a vásárlók figyelmét a biztonságos drónhasználatra [12].

A floridai rendőrség is az képzés erejében bízik, az állomány kiképzést kap a drónok biztonságos használatára, az oktatás megszervezését egy harmincéves tapasztalattal rendelkező repülésbiztonsági intézetre bízták. A rendőröket nemcsak a drónkezelésre készítik fel, hanem arra is, miként lehet hatékonyan fellépni az erőszakos, illetve illegális drónbehatolásokkal szemben [9].

A Nemzetközi Légi Szállítási Szövetség (International Air Transport Association, IATA) is az oktatás, valamint a megfelelő jogszabályok megalkotását szorgalmazta már 2018-ban, hangsúlyozva, hogy a tiltás, illetve a használatot teljesen ellehetetlenítő korlátozás nem célravezető, szükség van ugyanis a drónipar fejlődésére, hiszen a benne rejlő gazdasági potenciál egyáltalán nem elhanyagolható mértékű. Hasonló álláspontra helyezkedett az Európai Unió is, mely a dróngyártás és -használat szigorú szabályozása mellett tette le a voksát [22].

Jelen cikk írásának nem célja a drónhasználatra vonatkozó szabályanyag áttekintése, az ugyanakkor nem vitatható, hogy a szigorú jogi keretek meghatározása alapvető jelentőséggel bír mind az ártó szándékú drónhasználat elleni fellépés, mind a vétlen drónbalesetek megelőzése körében. A 2015-ben módosított japán polgári repülési törvény szerint például nem lehet drónt használni repterek, tömegrendezvények felett, magántulajdonú területek felett, ha ahhoz a tulajdonos kifejezetten nem járult hozzá. Repüléstilalmi övezetbe nem sorolt területek felett legfeljebb százötven méter magasságig repülhetnek és harminc méterre közelíthetnek meg embereket, épületeket, járműveket [15].

Dél-Koreában 2017-ben szigorították a drónokra vonatkozó szabályozást. Itt legfeljebb százötven méter magasságig repülhetnek a drónok, és mindenképpen látótávolságon belül kell az eszközt tartani, vagyis követelmény, hogy a kezelő szabad szemmel jól lássa azt. Az, aki regisztrált drónt akar reptetni, kötelező felelősségbiztosítást kell, hogy kössön, ennek fedezete átszámolva körülbelül 38 millió forintnak felel meg. A repülőtereket kilenc kilométerre lehet megközelíteni, tömegrendezvény felett tilos drónt reptetni, továbbá

Szöul teljes területe repüléstilalmi övezet, igaz, van néhány nagyobb park, ahol engedélyezett a drónhasználat [16].

A román hadsereg jóval drasztikusabb megoldást képzel el: 2021 márciusi sajtóértesülések szerint a hadsereg törvényi felhatalmazást akar kapni ahhoz, hogy az „ellenséges", vagyis a katonai, illetve az állami objektumokat, védendő rendezvényeket veszélyes mértékben megközelítő drónokat ártalmatlaníthassa, adott esetben lelőhesse. A kiszivárgott tervezet szerint indokolt a szigorú fellépés, ugyanis a kisméretű automata és távirányítású eszközök valós fenyegetést jelentenek a nemzetbiztonságra, amennyiben alkalmasak vegyi fegyver, robbanóanyag szállítására, a rájuk szerelt nagyfelbontású kamerák, érzékelők, lehallgató berendezések segítségével kémkedésre, katonai és kormányzati csatornák lehallgatására, harcászati gyakorlatok, műveletek illegális megfigyelésére, megzavarására. A törvényjavaslat ugyanakkor hangsúlyozza, hogy a drónok ártalmatlanítása során az arányosság elvét szem előtt tartva kell eljárni, vagyis, ha nem indokolt, nem kell fizikailag megsemmisíteni a túl közel repülő eszközt, elég az elektronikus berendezéseinek megzavarásával vagy egy mikrohullámú energianyalábbal feltartóztatni [23].

Mindezek mellett a fejlesztők is igyekeznek olyan megoldásokat kitalálni, melyek révén elkerülhetők a balesetek. Az intelligens drónok alkalmasak úgynevezett előre programozott útvonal repülésekre, amely azt jelenti, hogy kiválasztható az útvonaltervező szoftver internetes adatbázisából egy útvonal, és azt elég csak a drónra másolni: az eszköz azt repüli majd végig. Az előre tervezett útvonal-repüléseknél beépített biztonsági megoldások garantálják a balesetmentes repülést. Így például, be lehet programozni, mit tegyen a drón akkor, ha menet közben elveszíti a jelet. Rendszerint a drón ezt észleli és jelzi az irányító rendszernek, ettől függetlenül a tervezett utat változtatás nélkül lerepüli. Előfordulhat, hogy (például a nagy szél miatt) az út sokkal több ideig tart az előre eltervezettnél, ez azzal a veszéllyel jár, hogy az akkumulátor még a visszatérés előtt lemerül, a gép pedig lezuhan. Az intelligens drónok azonban előre észlelik, hogy a beprogramozott út végig repüléséhez nem lesz elegendő az akkumulátor töltöttsége, ezért megszakítják a repülést és automatikusan visszatérnek a kiindulási pontjukra [23].

A drónok gyártására specializálódott kínai DJI a tiltott légtérben való reptetést megakadályozandó beprogramozza az irányító szoftverbe a légtér azon részeit, ahová a gép nem tud berepülni. Az már más kérdés, hogy ez a funkció manuálisan kikapcsolható, tehát a rossz szándékú kezelők ellen ez nem jelent védelmet [10].

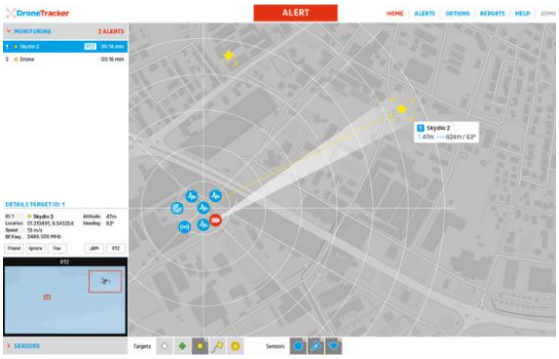
Radarokkal elérhető a drónok detektálása, habár önmagában egyik termék sem biztosít százszázalékos védelmet. Egy komplex megoldást kínál az amerikai Spotter RF radarrendszere, mely városi környezetben alkalmas a drónok detektálására. Apró érzékelőket helyeznek el a védendő pontokon (tetőn, épület sarkán, épület kiálló részein), így a rendszer – mely öt különböző hatótávolságú radarból áll – képes felismerni az objektum közelébe repülő pilótanélküli gépeket. A riasztási távolság annak függvényében alakul, hogy milyen érzékenységre vannak beállítva a szenzorok, ez lehet 130 méter, de akár 1300 méter is. A riasztást követően az operátor egy forgókamera segítségével beazonosíthatja a drónt, a rendszer megjeleníti a monitoron a főbb paramétereit, az pedig már a biztonsági protokollon múlik, hogy miként ártalmatlanítják az illetéktelen behatolót [10].

Bizonyított megoldás a frekvenciazavaráson alapuló elhárítás, ilyen elven működő elhárítórendszereket a francia hadsereg is előszeretettel alkalmazott Afganisztánban: az ellátmányt, a katonai felszerelést szállító teherautókra szerelték, így biztosítva az utat, ugyanis ezek az eszközök bombák ártalmatlanítására is alkalmasak [10].

Az Atos információtechnológiai óriásvállalat Drone Schield rendszere blokkol meghatározott frekvenciákat, ezáltal képes a navigációs műholdak és a légi járművek közötti kommunikációt megzavarni. Bonyolult, nagy szaktudást igénylő, ezek mellett rendkívül energiaigényes megoldásról van szó, a blokkolandó frekvenciák kiválasztása és beprogramozása pedig külön kihívást jelent. Az összes frekvencia válogatás nélküli blokkolása ugyanis nem javasolt, mert az akadályozná a saját kommunikációt is. A Drone Schield lényegében „pajzsként" leárnyékolja a védendő területet, mely körül két zónát alakít ki: ha a drón behatol az első zónába, elveszíti az irányítójától érkező jelet, erre a kereskedelemben kapható drónok legtöbbje úgy reagál, hogy visszarepül a kiindulási pontjára. Amennyiben a drón mégsem fordul vissza, hanem berepül a második zónába, ott már kénytelen lesz leszállni vagy pedig lezuhan: a második zónában ugyanis a rendszer mindenféle jelet blokkol. A Drone Schield-nek nyilvánvalóan nem az a célja, hogy a drón leessen, az ezzel járó balesetek, személyi sérülések kivédésre ugyanis nem alkalmas. A tapasztalat ugyanakkor azt mutatja, hogy a dróngyártók kreativitása végtelen, így például sokan közülük frekvenciaugrásokkal igyekeznek az elhárító rendszereket kijátszani. Habár akusztikai érzékelőkkel javítható a detektálás hatékonysága, ám nagyvárosokban ez a megoldás nem alkalmazható, hiszen az alapzaj miatt az egyébként sem túl érzékeny szenzorok nem észlelik a rotorzajt [9].

2013. szeptember 15-én Angela Merkel német szövetségi kancellár egy választási kampányrendezvényen vett részt, és egy emelvényen felállított asztal mellett ült politikustársaival, amikor

egy drón feléjük repült, alig két méterre megközelítve a színpadot, majd egy paravánnak csapódva a földre esett. Habár a „Kalózpárt" vállalta később az incidensért a felelősséget, az esetnek komolyabb következményei nem lettek. A Deutsche Telekomhoz tartozó Dedrone cég vezetője azonban arra gondolt, hogy a drónra akár robbanószerkezetet is szerelhettek volna az elkövetők, ezért mindenképpen szükségét érezte egy drónelhárító megoldás kidolgozásának. Így alkották meg a Dedrone-szoftvert, amely ötszörös szenzoros védelemmel ellátva védi civil drónok ellen a légteret és a kijelölt objektumokat [24].



9. Ábra: Dedrone szoftver megjelenítése

Ha nem áll rendelkezésre a legmodernebb technológia, a drónelhárításra akár formabontó eszközök is alkalmasak lehetnek. A holland rendőrség sasokat tanít be a drónok ártalmatlanítására, Japánban hálókat feszítenek ki a védendő létesítmény fölé. A tokiói rendőrség által alkalmazott módszer világviszonylatban is egyedülálló: a drónellenes egység körülbelül 1,8–3 méter hosszú, könnyű, de erős „Spreading Wings S900" hexakopterei háromszor két méteres hálóval vannak felszerelve, ezekkel fogják el a jogsértő drónokat, az eljárás a gyakorlatban ahhoz hasonlít, mint amikor a pók a hálóját a légy köré szövi. A rendőrök első lépésben beazonosítják a drónt, lehetőség szerint megkeresik a kezelőjét, akit figyelmeztetnek is, majd, ha ez hatástalan marad, úgy a rendőrségi drón a jogsértő eszköz fölé repül, amely beleakad a hálóba és repülésképtelenné válik. A befogott drónt végül óvatosan a földre helyezik, a sérülés okozása ugyanis nem célja a rendőrségi műveletnek. Kínában lézeres megoldással igyekeznek a drónokat detektálni, a francia Airbus infrakamera és radar kombinálásával lép fel a dróntámadások ellen. Oroszországban egy mikrohullámú ágyút fejlesztettek ki, amely kupolaként borul a védett területre, és tíz kilométer távolságra képes hatástalanítani bármely repülő jármű elektronikáját [9] [16].

2015 őszén mutatta be a Battle amerikai cég a drónelhárító puskáját. A Drone Defender nevű eszköz súlya nem több 4,5 kilogrammnál, hatótávolsága négyszáz méter.

10. Ábra: Drone Defender eszköz

A fegyvert a drónra kell irányítani, rádióhullámokat bocsát ki, így blokkolja az irányító egységtől érkező rádiójeleket, egyúttal pedig saját maga is küld jeleket, ezzel mintegy felülírva az eredeti parancsot, leszállásra kényszerítve a pilóta nélküli repülőt. A gyártó ellenséges szándékú, fegyvert, robbanóanyagot szállító drónok ellen ajánlja a Drone Defendert, mely az UAV-ok által rendszerint használt ISM és GPS frekvenciákon működik, így gyakorlatilag bármilyen típusú pilóta nélküli gép hatástalanítására használható. Jelenleg is ilyen eszközöket vetnek be a Fehér Ház, más kormányzati épületek, nagykövetségek, történelmi jelentőségű emlékhelyek védelmére. A drón „leszedésére" szolgáló fegyvert az Egyesült Államokban polgári célokra tilos alkalmazni, ennek ellenére léteznek olyan vállalkozások, melyek lakossági felhasználásra kínálnak ilyen jellegű eszközöket. A DroneShield ugyanazon az elven működik, mint a Drone Defender: előbb blokkolja az UAV-hoz érkező jelet, majd leszállásra készteti, az optikai szenzorral rendelkező eszközt pedig visszaküldi a kiindulási pontra. A gyártó weboldalán közölt leírás szerint a fegyver hatótávolsága kétezer méter. A DroneShield ugyanakkor nem mulasztja el felhívni a figyelmet arra, hogy a fegyver használata az Egyesült Államok területén a szövetségi törvények értelmében tilos és büntetendő [25].

A kínai Hikvision is gyárt drónellenes puskákat (Anti-Drone Gunja),

11. Ábra: Hikvision Anti-Dron fegyver.

ezek 2017 óta Magyarországon is elérhetők. A szerkezet kinézetét tekintve is puskára hasonlít, kezelése rendkívül egyszerű, csak a célra kell irányítani a szálkeresztet és lenyomni az elsütőbillentyűt. Az akkumulátor mindössze tíz-tizenöt lövésre elegendő, ezt követően a tartalék-akkumulátort kell használni. Az antidrónpuska egyrészt a navigációt blokkolja (GPS, GONASS 1,5 GHz), másrészt pedig a vezérlést (2,4 GHz), a segítségével „leszedett" drón nem sérül, nem károsodik [25].

Végezetül, tegyünk említést egy újabb fejlesztésről: a Vodafone 2018-ban kezdett el tesztelni 4G és IoT technológián alapuló drónkövető megoldást, mellyel akár a védett övezetekbe történő vétlen és szándékos berepülések is megelőzhetőkké válnak. Az elgondolás lényege: SIM kártyát és 4G modemet telepítenek a drónba, így mind az üzemeltetők, mind pedig az illetékes állami szervek valós időben nyomon tudják követni, hogy az merre repül [26].

5. ÖSSZEFOGLALÁS

Jelen cikkben áttekintettük a drónok alkalmazásának lehetséges színtereit, összegyűjtöttünk néhány tipikusnak mondható drónbalesetet, végül arra a kérdésre kerestük a választ, hogy a balesetek milyen módokon, milyen megoldások révén előzhetők meg. Ilyen megoldás lehet az oktatás, melynek keretében felhívják a drónt vásárolni szándékozók figyelmét a biztonságos és körültekintő drónhasználat szabályaira.

Összességében megállapíthatjuk, hogy a biztonságos kialakítás a gyártók, a biztonságos használat a kezelők felelőssége, az állam feladata pedig az, hogy kellően szigorú szabályozással meghatározza a biztonságos gyártás és a biztonságos használat kereteit, azonban a drónok elleni védekezésben elkerülhetetlen a technológia fejlesztés is, melyek segítségével növelni tudjuk a védekezés hatékonyságát úgy a rosszindulatú, mint a jóindulatú drónok okozta veszélyhelyzetek esetében. Ez a kérdés az ártó szándékú, terrorista szervezetek által megtervezett és elkövetett dróntámadások esetében különösen fontos, mivel nem szabad figyelmen kívül hagyni, hogy a terrorista szervezetek a rosszindulatú drónfelhasználás technológiáját folyamatosan fejlesztik céljaik hatékony eléréséhez, ami kihívást jelent a hatóságok, valamint védelmi megoldásokat fejlesztők számára is.

A következő tanulmány kifejezetten a terrorista szervezetek által használt dróntámadásokkal foglalkozik.

IRODALOMJEGYZÉK

[1] Manga László (2016): Drónok és alkalmazási területeik, avagy szóba jöhetnek-e egy esetleges nukleáris baleset esetén. Műszaki Katonai Közlöny XXVI. évf. 2016/2. 183–196. https://mkk.uni-nke.hu/document/mkk-uni-nke-hu/2016_2_014_Manga%20Laszlo.pdf Letöltve: 2021.04.03.

[2] Gyaraki Réka (2016): A drónok szabályozása Magyarországon. Magyar Rendészet, 2016 (1). pp. 43-54. http://real.mtak.hu/108480/3/AdronokszabalyozasaMagyarorszagon.pdf Letöltve: 2021.04.03.

[3] Restás Ágoston – Grósz Zoltán (2014): A mentesítés kérdései a pilóta nélküli repülőgépek katasztrófavédelmi alkalmazása során. Bolyai Szemle Különszám. Nemzeti Közszolgálati Egyetem, 2014. 59–74.

[4] Langlovagok.hu (2014) A drónok alkalmazási lehetőségei a tűzoltói beavatkozások során. Dr. Balogh Imre Emlékpályázat. Nyertes pályamű „drón" jeligével. 2014. http://www.langlovagok.hu/tanulmanyok/2014/dron_letaijanos_2014.pdf Letöltve: 2021.04.03.

[5] Go2fly.hu (2020): 225-tel képes száguldani a legújabb elsősegély-drón. 2020.09.25. https://go2fly.hu/225-tel-kepes-szaguldani-a-legujabb-elsosegely-dron/ Letöltve: 2021.04.04.

[6] Dronvilag.hu (2014): Itt az öt legjobb tűzoltó drón. 2014.03.24. http://dronvilag.hu/itt-az-ot-legjobb-tuzolto-dron/ Letöltve: 2021.04.04.

[7] Go2fly.hu (2021a): Mitől intelligens egy drón? – Programozott útvonal-repülés. 2021.02.01. https://go2fly.hu/mitol-intelligens-egy-dron-programozott-utvonal-repules/ Letöltve: 2021.04.04.

[8] Nyitrai Endre: A drónok alkalmazásának lehetőségei a rendőrségi feladatok ellátása során. Rendőrségi Tanulmányok III. évf. 2020/1. 94–119.

[9] Rottler Violetta (2018a): A drónok rendészeti alkalmazása. 2018. február. 21. Nemzeti Közszolgálati Egyetem RTK MÖRT, Budapest. https://www.detektorplusz.hu/index.php?m=23684 Letöltve: 2021.04.04.

[10] Nemzeti Agrárgazdasági Kamara (2016): Drónok hazai szabályozására várva. 2016.09.17. http://nak.hu/en/agazati-hirek/mezogazdasag/146-novenytermesztes/92320-dronok-hazai-szabalyozasra-varva Letöltve: 2021.04.04.

[11] PWC (2021): Drónok a láthatáron: rendezett jogi környezetben indulhat az üzleti hasznosítás. https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/PwC_Dronok-a-lathataron.pdf Letöltve: 2021.04.04.

[12] Hvg.hu (2015a): Félelem és aggodalom: a legtöbben ezt akarják majd karácsonyra. 2015.10.03. https://hvg.hu/tudomany/20151003_Felelem_es_aggodalom_a_legtobben_ezt_akar Letöltve: 2021.04.09.

[13] NBCWashington.com (2013): Drone Crashes Into Crowd at Great Bull Run in Va. Several people suffered minor injuries. 2013.08.23. https://www.nbcwashington.com/news/local/drone-crashes-into-crowd-at-great-bull-run/1952283/ Letöltve: 2021.04.09.

[14] Businessinsider.com (2014): Woman Nearly Has Her Face Destroyed By A TGI Friday's Mistletoe Drone. 2015.12.08. https://www.businessinsider.com/tgi-fridays-mistletoe-drone-accident-2014-12 Letöltve: 2021.04.09.

[15] BBC.com (2015): Drug delivery drone crashes in Mexico. 2015.01.22. https://www.bbc.com/news/technology-30932395 Letöltve: 2021.04.09.

[16] Rottler Violetta (2018b): A drónhasználat jogi szabályozásának nemzetközi trendjei és hazai helyzete. Magyar Rendészet 2018/4. 157—171.

[17] Hvg.hu (2015b): Majdnem agyonütötte egy drón a világklasszis síelőt. 2015.12.23. https://hvg.hu/sport/20151223_Majdnem_agyonutotte_egy_dron_a_vilagklass Letöltve: 2021.04.10.

[18] Airportal.hu (2017): FAA: a drónnal való ütközés a madár elütésénél is veszélyesebb. 2017.11.29. https://airportal.hu/faa-dronnal-valo-utkozes-madar-elutesenel-veszelyesebb/ Letöltve: 2021.04.10.

[19] Iho.hu (2018): Az első igazi drón-baleset: helikopter zuhant le egy Phantom miatt. 2018.02.21. https://iho.hu/hirek/az-elso-igazi-dron-baleset-helikopter-zuhant-le-egy-phantom-miatt-180221 Letöltve: 2021.04.10.

[20] Airportal.hu (2021): Drón szakította át egy helikopter szélvédőjét Chilében. 2021.01.24. https://airportal.hu/dron-szakitotta-at-egy-helikopter-szelvedojet-chileben/ Letöltve: 2021.04.11.

[21] Djiars.hu (n.a.): Hogyan ne zuhanjon le a drónod 15 egyszerű lépésben. https://www.djiars.hu/blog/hogyan-ne-zuhanjon-le-a-dronod-15-egyszeru-lepesben Letöltve: 2021.04.11.

[22] Airportal.hu (2018): Egy drón miatt zuhant le egy helikopter az Egyesült Államokban. 2018.02.22. https://airportal.hu/dronnal-utkozott-es-lezuhant-egy-helikopter-az-egyesult-allamokban/ Letöltve: 2021.04.13.

[23] Go2fly.hu/MTI (2021): Ártalmatlanítaná az „ellenséges" civil drónokat a román hadsereg. 2021.03.18. https://go2fly.hu/artalmatlanitana-az-ellenseges-civil-dronokat-a-roman-hadsereg/ Letöltve: 2021.04.13.

[24] Suasnews.com (2017): Dedrone. 2017.

https://www.suasnews.com/2017/01/dedrone-supplies-drone-countermeasures-world-economic-forum-davos/ Letöltve: 2021.04.16.

[25] 24.hu (2016): Ezzel a fegyverrel lelőheted a drónokat az égről. 2016.11.30. https://24.hu/tech/2016/11/30/elkeszult-a-specialis-dronvadasz-puska/ Letöltve: 2021.04.17.

[26] HVG.hu (2018): A GPS után jegyezze meg az RPS-t: a Vodafone már javában teszteli a drónkövető hálózatot. 2018.02.21.

https://hvg.hu/tudomany/20180221_vodafone_dronkovetes_dronmeghatarozo_rendszer_rps_gps_u_space_sesar Letöltve: 2021.04.17.

BÁNKI KÖZLEMÉNYEK
V. ÉVFOLYAM 1. SZÁM

DRÓNOK HASZNÁLATA TERRORISTA SZERVEZETEK ÁLTAL

USE OF DRONES BY TERRORIST ORGANIZATIONS

Bálint Márton
Óbudai Egyetem Biztonságtudományi Doktori Iskola, Budapest, Magyarország
balint.marton@phd.uni-obuda.hu

Összefoglalás- A dróntechnológia lassan mindennapjaink részévé válik, előnyeire azonban a terroristák már több mint két és fél évtizede felfigyeltek, felhasználásuk a 2000-es évek elején szaporodott meg. A pilóta nélküli repülők legkreatívabb felhasználása pedig kétségkívül az Iszlám Államhoz kötődik. Jelen tanulmányban arra a kérdésre keressük a választ, hogy az elmúlt időszakban milyen céllal és milyen eredményességgel vetették be ezt az új technológiát a terrorista szervezetek. Meghatározzuk a pilóta nélküli repülő eszközök terrorista szempontból optimális tulajdonságait, számba vesszük az 1994 óta történt jelentősebb terrorista drónműveleteket. Végül az Iszlám Állam példáján keresztül elemezzük a drón támadások propaganda célú felhasználását, valamint az ISIL példáján keresztül rámutatunk a rosszindulatú drónhasználat kockázataira, azaz drónok használatának sikertelenségére és annak következményeire.

Kulcsszavak : drón, felhasználás, terrorista, propaganda, sikertelenség

Abstract - Drone technology is becoming part of our daily life. However, the attention of terrorist organizations to the advantages thereof has been risen more than 2,5 decades ago and the application of drones became widespread in the 2000's. Undeniably the most creative way of using pilot free flying vehicles it that of the Islamic State. The purpose of the present paper is to analyze for what purposes and with which success this new technology has been applied by terrorist organizations. We will identify the optimal features of a pilot free device from a terrorist point of view, list the major terrorist drone operations since 1994. Through the example of Islamic State we will study the propaganda-type usage of drone attacks and the examples of ISIL will show us the risks associated to malignant done attacks, their failures and consequences.

Keywords: drone, application, terrorist, propaganda, failure

1. BEVEZETÉS

Egy korábbi cikkben elemeztük a drónok használata által keletkezett veszélyes helyzeteket, melyek személyek, élőlények és különböző infrastruktúrák számára jelentenek véletlenük generált veszélyt. Ezt a gondolatmenetet jelen cikkben folytatjuk oly módon, hogy a drónok okozta veszélyek terrorista szervezetek általi kifejezetten szándékos és rosszindulatú felhasználását elemezzük.

A terroristák már az 1990-es évek közepén végeztek drónokkal tesztrepüléseket, a műveleti célú alkalmazásra azonban ekkor még nem került sor. Dokumentált éles bevetések először a 2000-es évek elején történtek, jobbára a Közel-Kelet konfliktuszónáiban. Amiért a téma napjainkban is aktuális, az az, hogy 2019-ben jelentősen megnövekedett az aktivitás e téren. Bár az Iszlám Állam – legalábbis a korábban ismert formájában – megszűnt, ám az általa képviselt eszmét valló csoportok tovább léteznek, és semmi sem akadályozza meg, hogy újabb, hasonló szerveződések jöjjenek létre. Márpedig, a robotikai forradalom, a mesterséges intelligencia (Artificial Intelligence, a továbbiakban: AI) térnyerése, az olcsó és bárki által hozzáférhető drón-technológia további fejlődése révén egyre újabb és újabb eszközök és módszerek jelennek meg a piacon, kiszámíthatatlan, hogy ezek közül melyek válnak halálos eszközzé egy terrorista csoport kezében. A Braun–Fleiss, szerzőpáros már arról ír, hogy a rosszindulatú csoportosulások akár „egy megállíthatatlan hadsereget" is létrehozhatnak a mesterséges intelligencia és a drónok keresztezésével, egy olyan hadsereget, mely „pilóta nélküli, öngondolkodó drónokból áll, amelyek minden emberi hozzájárulás nélkül képesek megválasztani célpontjaikat". [1]

A fokozódó veszélyt az Európai Unió Bizottsága is felismerte, újabb pénzügyi forrásokat biztosít a rosszindulatú drónhasználat ellen fellépő projektekre és – miként az a 2020 decemberében kiadott közleményéből kiderül – 2021 folyamán egy, „a városok nem együttműködő drónok elleni védelméről szóló uniós kézikönyv" kiadását tervezi.

A drónok ártó szándékú alkalmazása alapvetően két célt szolgálhat: egyrészt alkalmas lehet a szárazföldi és hagyományos légi hadműveletek támogatására vagy önálló fegyveres támadások végrehajtására (robbanószer, vegyi, biológiai fegyver stb. felhasználásával). Másrészt – és talán ez az izgalmasabb része a problémának – propagandaeszközként is kiváló, e vonatkozásban pedig „egy új, szimbolikus dimenziót vezet be". Harci támogatásként talán, önálló hadászati eszközként

bizonyosan nem tekinthető teljes értékű, valóban hatékony megoldásnak; a cél nem konkrét katonai előny elérése, sokkal inkább annak bizonyítására, még inkább demonstrálására szolgál, hogy az alkalmazója képes használni a modern légi technológiát. A szimbolikus használat kérdésköre – állítja az Archambault–Veilleux-Lepage szerzőpáros – leginkább az Iszlám Állam példáján figyelhető meg. Az állam nemzetközi jogi fogalmának egyik legfontosabb eleme a szuverenitás az adott állam fennhatósága alá tartozó területen, a szárazföldön, alatta a talajban, a hozzá tartozó tengerrészeken és a felette lévő légtérben. E területek – így a légtér ellenőrzése – az államok előjoga; a légtérbe éppen úgy nem lehet belépni az állam engedélye nélkül, miként azt a földi határátkelőhelyeken sem lehet megtenni. Egy hozzáértő ember azonban a kis méretű, alacsonyan repülő drónokat minden különösebb nehézség nélkül képes bereptetni a másik állam légterébe. A terroristák tehát a drónjaikkal szimbolikusan az állam szuverenitását sértik meg, a tekintélyét ássák alá [2].

2. A DRÓNHASZNÁLAT ELŐNYEI TERRORISTA SZEMPONTBÓL

Ha katonai drónokról van szó, hajlamosak vagyunk olyan gépekre gondolni, melyek szárnyfesztávolsága vetekszik a vadászgépek teljes hosszával, és több mint tizenkétezer méter magasról készítenek felvételeket, az operátor pedig több száz méter magasságból képes tetszőleges fegyverrel eltalálni a célpontot. Ez a leírás kétségkívül illik az állami hadseregek drónarzenáljára, ám az ilyen eszközök fejlesztése sok időt, magasan képzett szakemberek tudását, és legfőképpen dollármilliárdokat kitevő befektetést igényelnek, márpedig ezekkel a terrorszervezetek nem rendelkeznek. A kereskedelemben kapható kisebb drónok azonban számukra is elérhetők. Ezzel már részben meg is válaszoltuk a kérdést: milyen terrorista szempontból előnyös tulajdonságokkal bírnak ezek az eszközök?

Tény, hogy a drónok hatósugara nem túl nagy, de nehezen megközelíthető helyekre is eljuttathatók és eljuttathatók velük bizonyos szállítmányok is: egyes típusok (esetleg átalakítás után) ötven, de akár nyolcvan kilogramm rakománnyal terhelhetők, de még a kereskedelemben kapható egyszerűbb eszközök között is találni olyat, mely elbír huszonkét kilogrammot. Felfüggeszthető rájuk robbanóanyag, szállítható velük biológiai, vegyi fegyver, nukleáris fegyver, radioaktív anyag. Képfelvételek rögzítésére alkalmas eszközökkel is felszerelhetők. Megfigyelhetők általuk objektumok, személyek, katonai, rendőri erők mozgása. ATM közelében kifürkészhetők velük a PIN-kódok, beléptető rendszereknél a bejutást lehetővé tévő kódok. Kiválóan használhatók a rendőri munka megzavarására. Maga a drón is válhat fegyverré: adott célpontba irányítva „öngyilkos" drónként funkcionálhat; a rotorpengéivel, melyek rendkívül gyorsan forognak, életveszélyes sérülés vagy halál is okozható. A „kamikaze" drón ember által elkövetett öngyilkos merénylettel szembeni előnye könnyen felismerhető: az öngyilkos akciót vállaló ember az utolsó pillanatban meggondolhatja magát, mert megijed vagy éppen meglát a helyszínen egy gyermeket, akit megsajnál – ilyen veszélyekkel azonban a drónok esetében nem kell számolni [3, 4, 5].

A terrorista használatú drónok között vannak olyanok is, melyek miniatűr méretűek, akár egy tenyérben is elférnek, melyeket a nem avatott szem igen nehezen észlel, de a hangjuk sem különösebben feltűnő, köszönhetően az elektromotoroknak. Ugyanezen okból kifolyólag hőjelük gyakorlatilag nincs, eltérően például a dugattyús motoroktól. Leginkább műanyag vagy szénszálas kevlár az anyaguk, minimális fémtartalommal. Ebből következően pedig, a radarok egyáltalán nem, esetleg csak kis távolságból képesek észlelni, de még infravörös keresőrendszerek számára is kihívást jelent a felderítés, főként a napsütéses órákban, meleg időjárás esetén [6].

A téma kiemelkedő szakértője, Christopher Bolkcom, 2002-ben az Egyesült Államok Szenátusának Kormányzati Ügyek Bizottsága előtt tett nyilatkozatában hét olyan tényezőt azonosított, melyek terrorista szempontból kívánatossá tették a pilóta nélküli mini légijárművek használatát. Ezek a következők: (1) alacsony áron beszerezhető; (2) változatos kereskedelmi forrásokból hozzá lehet jutni; (3) pontos célba juttatást tesz lehetővé; (4) alkalmazási lehetőségei változatosak; (5) problémamentesen átjuttatható a légvédelmen keresztül; (6) tervezhető üzemidő; (7) csekély infrastruktúra szükséglet a telepítésnél, működtetésnél [2].

A szakértők egy része szerint azonban a terrorista drónok legfőbb előnye a váratlanság, az, hogy a meglepetés erejével jelennek meg, éppen ezért a segítségükkel végrehajtott támadás rendkívül erős pszichológiai hatás kiváltására alkalmas [2].

A pilóta nélküli légi járművek katonai célú felhasználásának története az első világháború idejére vezethető vissza. 1917-ben az Egyesült Királyság egy rádióvezérlésű Sowith Camel géppel hajtott végre kísérleteket, az elképzelés az volt, hogy a dinamittal megrakott gépből a brit városokat bombázó német zeppelinek ellen hajtanak végre támadást, ám a tesztrepülés csúfos kudarcba fulladt. A fejlesztések ettől függetlenül nem álltak le, és az 1930-as években már mind az Egyesült Királyságban, mind az Amerikai Egyesült Államokban általános gyakorlattá vált a pilóta nélküli gépek légvédelmi célokra történő használata [7].

Az, hogy a drónhasználat előnyeit a bűnözők, illetve a terroristák is felismerik, csak idő kérdése volt. Több kutató is kísérletet tett arra, hogy elkészítse a drónokkal végrehajtott terrorcselekmények katalógusát, a szakirodalomban a legfőbb hivatkozási alapot Gips (2002), Miasnikov (2005), Bunker (2015) és Don Rassler (2016) munkái jelentik [2].

A mindezidáig legkimerítőbbnek számító lista Bunker (2015) nevéhez fűződik: 1994 és 2015 márciusa között huszonnégy incidenst vett számba, ezek közül a legelső Japánban történt, a legtöbbért a Hezbollah felelős (hét esemény), ezt követi a sorban az Al-Kaida (hat esemény),

az Iszlám Állam (négy esemény) és a Hamász (két esemény) [7].

3. A TERRORISTA DRÓNHASZNÁLAT KEZDETEI

A pilóta nélküli légi járművek és a terroristák kapcsolódási pontjait tárgyaló szakirodalom elsőként a sorban az Aum Shinrikyo japán szektát említi meg, melynek tagjai – a tokiói metróban 1995. március 20-án végrehajtott terrorcselekményt megelőzően – azt tervezték, hogy a halálos ideggázt, a szarint drónok használatával juttatják a levegőbe, és e célból teszteltek is két, folyadékporlasztó tartállyal felszerelt, távirányítású mini helikoptert. A két jármű azonban a tesztrepülés során lezuhant [8].

Ugyancsak a tervezés fázisáig jutott az Al-Kaida, midőn a 2001-es genovai csúcstalálkozón „házilagos készítésű", úgynevezett improvizált robbanóeszközökkel (Improvised Explosive Device, IED) felszerelt drónokat akart bevetni a G8-ak vezetői ellen. Valamivel később, 2002-ben olyan elképzelései is voltak az Al-Kaidának, hogy anthrax baktériumot juttatnak drónnal a brit alsóház épületébe, illetve, hogy kereskedelmi repülőket támadnak meg robbanóanyaggal felszerelt UAV-okkal. A tesztrepülések azonban nem váltották be a hozzájuk fűzött reményt [9].

2002 augusztusában a kolumbiai hadsereg egyik alakulata kilenc távvezérlésű légi szerkezetet foglalt le a dzsungelben egy, a Kolumbiai Forradalmi Fegyveres Erőkhöz (FARC) tartozó táborban. Arra nézve, hogy a drónokat használták volna a terroristák, adat nem merült fel, de egyes feltételezések szerint saját készítésű robbanóeszközök szállítását tervezték [3].

Ugyancsak 2002-ben a Palesztin Nemzeti Felszabadítási Mozgalom (Fatah) IED-ekkel felszerelt drónokkal akart támadást indítani a jeruzsálemi zsidó negyed ellen, de a végrehajtásig nem jutottak el. Amiért figyelemre méltó az eset, az az, hogy az izraeli hatóságok ebben az időszakban több száz ilyen modellt fogtak el [3].

3.1. A Hezbollah és a Hamász által indított dróntámadások

A Hezbollah a 2000-es években felderítési célokra használt kisméretű pilóta nélküli – Mirsad 1-nek nevezett – repülőket, melyek izraeli területre bizonyítottan két esetben jutottak el. Az első jármű 2004 novemberében Nahariyya városáig repült és körülbelül fél órát töltött az izraeli légtérben, a sorsa azonban bizonytalan, lehetséges, hogy visszatért a Hezbollah bázisra, de az is elképzelhető, hogy a libanoni partok közelében a tengerbe zuhant. A 2005 áprilisi egy rövidebb, mintegy tizennyolc mérföld hatókörű támadás volt; a jármű sikeresen visszatért a bázisra. A Mirsad név ugyanakkor megtévesztő, ezek – Hassan Nasrallah sejk, a Hezbollah vezetőjének állításától eltérően – nem saját gyártású gépek voltak, hanem Iránból vásárolta a szervezet, 2006-ig legalább nyolc darabot. Izraeli források szerint a Mirsad 1 valójában egy iráni Mheger 4 drón, melynek törzshossza 2,9 méter, szárnyfesztávolsága mintegy három méter, 10 lóerős motor hajtotta, képes volt akár két kilométeres magasságba emelkedni, és 120 km/h maximális sebességgel repülni. Jelentések szerint harminc harcos még egy kiképzésen is részt vett Iránban, ahol megtanulták az UAV-ok kezelését. Egyes források úgy tudják, a Hezbollah vezetői azzal számoltak, hogy idővel Izrael belső részeit is elérhetik a Mirsadok, melyek akár 40–50 kilogramm robbanóanyagot is elbírnak [10].

2006. augusztus 13-án a Hezbollah három Ababil dróntámadást indított, egyet a libanoni Tyros közelében, kettőt pedig Izraelben, Nyugat-Galileában, illetve Haifához közel. A járművek 40–50 kilogrammos robbanófejjel voltak felszerelve; mindhármat az izraeli hadsereg F-16-os repülőgépei lőtték le. Elemzők feltételezése szerint az Ababil típusú UAV-okat az Iran Aircraft Manufacturing Industries (HESA) gyártotta. Az Ababil méreteit tekintve hasonlít a Mheger 4-hez: törzshossza 2,9 méter, szárnyfesztávolsága 3,25 méter, indítása pneumatikus hordozórakétával vagy rakétával történik, ejtőernyővel landol. Autopilóta üzemmódban is képes repülni, de távolról is irányítható. Motorja 25 lóerős, a gyártó körülbelül 300 km/h utazási sebességet garantál. Az Ababil 40 kilogrammos teher szállítására alkalmas [11] [10].

1. ábra Ababil 1 típusú drón.

A 2012 és 2014 második negyedéve közötti időszakban további Hezbollah, illetve Hamász támadásokra került sor. 2012. október 6-án a Hezbollah – iráni építésű, a szervezet egyik mártírja után Ayoub-nak nevezett – drónnal behatolt az izraeli légtérbe, hogy Dimona, pontosabban az ott működő nukleáris kutatóközpont felett készítsen légi felvételeket. A művelet – még úgy is, hogy a drónt lelőtte egy F-16-os – az izraelieket különösen érzékenyen érintette, mivel időben egybeesett egy nagyszabású katonai gyakorlat előkészületeivel. A The Jerusalem Post szerkesztőségi cikkében az akciót „súlyos provokációnak és Izrael szuverenitása nyilvánvaló megsértésének" nyilvánította, „még akkor is, ha a drón feladata csak az intelligencia összegyűjtése és/vagy Izrael védekezésének tesztelése volt"; „a kémkedés" – szögezte le a cikk „az agresszió egyik formája". Az al-Dzsazira (Al Jazeera English) cikkében ugyanakkor arra mutatott rá, hogy Izrael 2006 augusztusa óta 20 468 alkalommal lépett be a libanoni légtérbe, és bár ezt az esetek nagy többségében sugárhajtású repülőivel tette, de – mint azt az ENSZ Közgyűlésének Emberi Jogi Tanácsa 2006-ban

dokumentálta – drónokat is használt Libanonban, mégpedig nemcsak kémkedésre, hanem kórházak és gazdálkodó közösségek katonai bombázására [12].

2013. április 22-én Haifától nyugatra, a tenger felett egy másik Hezbollah drónt is lelőtt az izraeliek F-16-osa; az, hogy mi volt a célja ennek a dróntámadásnak, nem derült ki. Az első, drónok által rögzített sikeres támadás 2013 közepén történt, a Hezbollah (egy iráni gyártású, utóbb átalakított) drónnal két kisebb robbanószerkezetet dobott le a szíriai lázadók telepei felett. Kétségtelen, hogy a kereskedelemben kapható alkatrészek megfelelő átalakítása, fegyveres támadásra való alkalmassá tétele meglehetősen költséges és speciális szakmai tudást igénylő művelet [7] [13].

2014. július 14-én egy „házi készítésű", ötméteres Hamász UAV-ot lőttek le az izraeliek Ashdod közelében, az ország déli partvonala mentén. Ez volt az első eset, amikor a Hamász pilóta nélküli eszközt vetett be az izraeli légtér felett. A Washington Post tudósítása szerint a Hamász nyilvánosságra hozott egy videófelvételt egy repülőgépen szállított drónról, „négy kis rakétával vagy valamilyen apró felszereléssel a szárnyai alatt", az ugyanakkor nem derült ki, hogy a felvétel a szóban forgó drónt ábrázolta vagy egy másikat. Ugyan az eszközt gyorsan lelőtték az izraeliek – Patriot föld-levegő rakétával –, ám ez mégis egy újabb szintet jelentett a gázai konfliktusban: az IDF (Israel Defense Force) egyik magasrangú tisztje szerint az esetet úgy értékelték, hogy a Hamász – azzal, hogy immár nemcsak az erejét, hanem a tudását is fitogtatja – „megérett a tűzszünetre".

2. ábra Hamász drón

A Hezbollah a dróntámadásokkal – mutat rá Bunker (2015, 16–17) – legalább háromféle dolgot kívánt közölni. Egyrészt a korábbi izraeli jogsértésekre akarták felhívni a figyelmet (ez különösen a 2005. évi drónhasználatra lehet érvényes állítás); másrészt propagandacélokat szolgáltak ezek az akciók, megnövekedett képességeikkel és szakmai tudásukkal „dicsekedtek". Ez a fajta propagandacél a Hamásztól, az Al-Kaidától és – miként azt a későbbiekben látni fogjuk – az Iszlám Államtól sem állt távol. Végül, a drónműveletek figyelmeztetésként, egyfajta elrettentésként is szolgáltak: a régi „íjjal lövéshez" hasonlatosan – mutat rá Burger (2015) – azt igyekeztek közölni vele, hogy képesek ennél komolyabb támadásra, akár halálos erő alkalmazására is, és amennyiben az ellenség nem viselkedik az elvárásoknak megfelelően, akkor kénytelen lesz szembenézni a súlyosabb következményekkel. Bizonyosan ez lehetett a tényleges üzenet a dimonai atomkomplexum elleni dróntámadásnál [7].

3.2. Az Al-Kaidához köthető dróntámadások

Az Al-Kaidához köthető első dokumentált eset Pakisztánban történt: 2005. szeptember 13-én a pakisztáni hadsereg rajtaütött a Lashkar-e-Taiba szélsőséges iszlamista terrorszervezet egyik rejtekhelyén Észak-Vazirisztánban, ahol kínai gyártmányú – feltehetően felderítésre használt – távirányítású repülőgépeket foglaltak le [7].

Az ezt követő napon a virginiai Fairfax megyében (USA) letartóztattak, majd később el is ítéltek egy Ala Asad Chandiat (a/k/a Abu Qatada) nevű férfit terrorizmus támogatásának kísérlete miatt; az ítélet szerint Chandiat repülőgép-modellekhez való MP 1OOOSYS elektronikus automata pilóta rendszert vásárolt, azért, hogy azt drónhasználat céljából eljuttassa Pakisztánba, a Lashkar-e-Taiba terroristáinak [7; 14].

A további két – nagyobb nyilvánosságot kapott – incidens 2007-2008-ban történt, mindkettőben amerikai állampolgárok voltak érintettek. Az Al-Kaida által kiképzett Christopher Paul-t 2007-ben tartóztatta le a Szövetségi Nyomozó Iroda (FBI), mert terrorista célokra egy másfél méteres modell helikoptert épített. A következő évben pedig – az ugyancsak Al-Kaida szimpatizáns – Rezwan Ferdaus-t helyezték vád alá, aki C-4 robbanóanyaggal felszerelt, beépített GPS-szel rendelkező, távirányítású modellrepülőgépekkel indított támadást a Pentagon és a Capitolium épülete ellen. Utóbb mindkettőjüket börtönbüntetésre ítélték terrorizmus miatt [7].

3.3. Az Iszlám Állam drónműveletei

Az első három, bizonyítottan az Iszlám Államhoz (ISIL) köthető dróntámadásra 2014 augusztusában és szeptemberében került sor. 2014. augusztus 23-án Szíria északi részén, Raqqa közelében egy a 3. ábrán látható DJI Phantom FC40 kvadrokoptert vetettek be, később az eszköz felhasználásával készült videófelvételeket felhasználták az ISIL propagandaanyagaiban. 2014. január 30-án egy ismeretlen típusú drónt reptettek az iraki Falluja térségében, kifejezetten azzal a céllal, hogy internetes propagandaanyagokhoz felvételeket készítsenek a város elleni támadásokról. 2014. szeptember 12-én ugyancsak egy ismeretlen típusú drónt használtak az észak-szíriai Kobaniban videófelvételek rögzítése céljából, a felvételeken földi támadások és az öngyilkos merénylők után maradt pusztítás nyomai láthatók [7; 15].

3. ábra DJI Phantom FC40 kvadrokopter

2015. március 16-án (vagy ahhoz közeli időpontban) egy ISIL harcos az iraki Fallujah területén körülbelül húsz percig reptetett egy kisebb modell helikoptert, majd miután leszállt a drón, azt az autója csomagtartójába helyezve távozott a helyszínről. 2015-ben több alkalommal is megtörtént, hogy szíriai kurd katonák az ISIL-hez köthető, robbanóanyagokkal felszerelt drónokat lőttek le [7; 16, 17].

Az ISIL 2017 elején jelentette be, hogy felállította az Unmanned Aircraft of the Mujahedeen (A Mudzsahidek pilóta nélküli repülőgépei) nevet viselő drónműveleti egységét, mely – miként azt hivatalos hírlevelük, az al-Naba egyértelművé tette – szándékaik szerint nem más, mint „A new source of horror for the apostates!" (A rettegés egy új forrása a hitehagyottak számára!). Az elemzők arra hívják fel a figyelmet, hogy az Iszlám Állam a hadviselés legkülönfélébb technikáit és eszközeit bevetette, módszereiket – miként azt a Romaniuk–Burgers szerzőpáros találóan megjegyezte – egyszerre jellemezte a kísérletezés és az alkalmazkodás. Egyaránt inspirálódtak az afgán és a szovjet megoldásokból, kiemelt szerepet szánva a mélységi és felforgató műveleteknek. Eszköztárukból már csak emiatt sem maradhatott ki a drónok, illetve a drónok segítségével készített felvételek propagandacélra történő felhasználása. [4, 9]

El kell ismerni, hogy az ISIL rendkívül kreatív módon fejlesztette drón-technológiáját, újabb és újabb módszereket kipróbálva. 2017-ben egy ízben hagyták, hogy a Pesmergák két katonája lelőjön egy megfigyelő UAV-ot, és elszállítsák azt a bázisukra. Szétszerelés közben a drón felrobbant, melynek következtében két kurd harcos meghalt, két francia katona súlyosan megsebesült. Elrettentésként is használták a drónfelvételeket: 2017 januárjában például egy olyan propagandaanyagot tettek közzé, amelyen közel egy tucat példával szemléltették, mekkora pontossággal képesek az átalakított kvadkopterekkel földi célpontokra lőni. 2017 nyarán, amikor a koalíciós erők megkezdték Moszul visszafoglalását, az Iszlám Állam havi szinten százas nagyságrendben indított dróntámadásokat [4, 18, 19].

Ugyancsak 2017-ben, az ISIL kereskedelemben kapható drónokat olyan módon alakított át fegyverré, hogy az eszközre műanyag csöveket szereltek és azokba 40 milliméteres puskagránátot helyeztek. Az operátor terrorista az iraki csapatok fölé manőverezte a drónt, majd távvezérléssel utasítást adott a gránát leejtésére [4; 20].

A legnagyobb pusztítással járó drónhasználat 2017. október 24-én történt. Az Iszlám Állam egy drónról bombát dobott a Deir ez-Zor stadionra, mely szíriai hadsereg lőszerraktáraként funkcionált. A becsapódást követően hatalmas robbanások láncolata indult el, megsemmisítve a stadiont és az egész lőszerraktárt. A támadás közben a drón végig filmezett, kevéssel később az ISIL nyilvánosságra hozta a felvételeket, külön figyelmet fordítva arra, hogy azt minél többen lássák Deir Ezzor városában, ahol is a szír kormányerők akkor már közel egy hónapja folytatták a harcot az ellenőrzés megszerzéséért [21].

Az Iszlám Állam rendszeresen készített a drónok felhasználásával felvételeket, főként a támadások, az öngyilkos merényletek – propaganda célú – dokumentálása volt a cél. Ilyen felvételekhez leginkább kereskedelmi forgalomban beszerezhető drónokat, például DJI Phantom típusú eszközöket használtak. A felvételek ugyanakkor hírszerzési célokat is szolgáltak, a célpontokat előre felderítették, megvizsgálták, melyek a legkevésbé védett, legsérülékenyebb területek, a támadásokat így a lehető legpontosabban meg tudták tervezni [22].

Az Archambault–Veilleux-Lepage szerzőpáros a 2020 júliusában publikált tanulmányában arra vállalkozott, hogy megvizsgálja az Iszlám Állam 2016 októbere és 2018 decembere között keletkezett propagandaképeinek adatbázisát, abból a célból, hogy kiderítsék: a drónról készült felvételek közül mely típusúak vannak túlsúlyban. Az adatbázist a Georgia State University állította össze, a szervezethez köthető hírcsatornák anyagát, valamint 2015-ig az ISIL Twitter-fiókjait, azt követően a Telegram-profiljait szemlézve. Ekként a mondott időintervallumon belül összesen 19 749 képet sikerült összegyűjteni, ebből 524 fotó ábrázolt valamilyen drónhoz köthető tevékenységet. Ezt követően a kutatók minden képet egyenként elemeztek abból a szempontból, hogy mit ábrázol, és beazonosították azt is, hol készült a felvétel. A szerzőpáros a következő megállapításokat tette: az 524 fotóból 281 olyan drónról (leginkább módosított kvadrokopterről) készült, melyre valamilyen fegyvert, robbanóanyagot rögzítettek, a felvétel azt mutatta, hogy a drónról leoldják, ledobják stb. a szállítmányt. A fotók mindegyikén látható, hogy a lőszer, robbanóanyag rendben eléri a célpontot. Az 524-ből 160 képen valamilyen pusztító akció, nagyerejű merénylet, illetve mindezek konkrét következményei láthatók. Sok képen szerepel az öngyilkos merénylő neve és egy rövid ima („Allah fogadja el"). Ezek a képek – mutatnak rá a kutatók – „a vértanúság körüli pillanatokat" ábrázolják. Csak néhány olyan kép került az adatbázisba, mely nem mutatott konkrét akciót, pusztán csak magát a drónt, amint elrepül egy terület felett, ezekkel a képekkel az Iszlám Állam azt demonstrálja, hogy tényleges ellenőrzést gyakorol azon terület felett, melyen a drón átrepül, egyúttal pedig megkérdőjelezi az érintett ellenséges állam területi szuverenitását. Archambault és Veilleux-Lepage következtetése szerint az Iszlám Állam számára a drónhasználat katonai értékét felülmúlja annak

szimbolikus jelentősége: a drónfotók valójában az Iszlám Államról, mint szuverén államról szólnak.

4. ÚJABB TERRORISTA DRÓNTÁMADÁSOK

Bunker 2015-ben publikált művében 2015 márciusáig követte nyomon a terrorista célú dróntámadásokat, az Iszlám Állam azonban csak 2017 után mutatott e téren nagyobb aktivitást, de más terrorista csoportokhoz is köthetők az ezt követő időszakban jelentősebb műveletek.

2018. január 5-én egy szíriai lázadó csoport – melyet hivatalosan nem sikerült azonosítani – saját készítésű drónnal tervezett koncentrált támadást végrehajtani előbb a szíriai Khmeimim légi bázis, majd a Tartúsz kikötőjében lévő haditengerészeti bázis ellen, mindkettő az országban harcoló orosz hadsereg fontos támaszpontja. Összesen tizenhárom minigépet indítottak, a cél a minél nagyobb pusztítás volt, ennek érdekében repeszeket és robbanóanyagot szereltek a drónok szárnyaira. Az eszközöket azonban leleplezték az oroszok, egy részüket elektronikus eszközökkel sikerült is hatástalanítani, illetve megsemmisíteni, a többi gépet pedig elfogták, így a támadás teljes kudarcba fulladt [4].

2019. január 10-én egy huti felkelők egy robbanóanyaggal felszerelt drónnal hajtottak végre támadást Jemenben, az Al-Anad légi bázison nyolcezer fős katonaság részvételével, magas rangú helyi katonák és szövetséges vezetők jelenlétében megtartott katonai parádén. A támadás következtében hat katona elhunyt, sokan megsebesültek, köztük két magas rangú katonai tisztviselő is. Egy helyi riporter, Nabil al-Qaiti utóbb arról számolt be, hogy a színpad előtt állt, amikor észrevette a drónt, mely a felvonulás kezdete után még percekig a levegőben lebegett, körülbelül 25 méter magasságban. Éppen a hadsereg szóvivője, Mohammed al-Naqib kezdte meg beszédét a pódiumon, amikor a drón felrobbant. „Nagyon erős robbanás volt, és érezhettük a nyomást" – mondta Al-Qaiti, aki nagyon sok sebesültet látott maga körül, de neki nem esett baja. Az ENSZ szakértői úgy vélték, a merénylethez a hutik Iránból kaptak segítséget.

2019 nyarán a jemeni huti felkelők dróntámadásokat indítottak három, Szaúd-Arábia déli részén, a jemeni határ közelében található célpont ellen: az egyik a King Khalid légibázis, a másik az Abha repülőtér, a harmadik a Najran repülőtér volt. A felkelők katonai szóvivője bejelentette, hogy az Abha repülőtér elleni támadás sikerrel járt, a szállítmány „célba ért", és az Abha-i és a Najran-i reptereken is sikerült fennakadásokat okozni a légi forgalomban. Mindezt a szaúdi vezetés cáfolta, azt állították, hogy a drónokat elfogták és hatástalanították még azelőtt, hogy elérték volna a repülőtereket [37].

2019 augusztusában Szíria felől egy robbanóanyaggal megrakott „öngyilkos" drón hatolt be Izrael légterébe, az akciót az Izraeli Védelmi Erők meghiúsították. Elemzők szerint a merényletkísérlet mögött Javad Ghafari, a Forradalmi Gárda dandártábornoka állt, ő felügyelte ugyanis az iráni erőket Szíriában [24].

2019. szeptember 14-én a jemeni hutik a világ legnagyobb olajfinomítója ellen intéztek drónos merényletet, a szaúd-arábiai Aramcó kiemelten őrzött létesítményét huszonöt drónnal, illetve robotrepülővel támadták meg. Az objektumot egyszerre védte az amerikai Patriot légvédelmi rakétarendszer, a francia Shanine mobil légvédelmi rendszer, a német Skyguard, ám mindez hiábavalónak bizonyult, az alacsonyan repülő, jobbára műanyagból készült kistestű gépeket e rendszerek egyike sem volt képes időben észlelni [4].

Közép- és Dél-Amerika kábítószer kartelljei már korábban is előszeretettel alkalmaztak drónokat drogcsempészés céljaira: az egyik legtipikusabb módszer az, amikor a szállítmányt a drónra erősítik, a drónnal az országhatáron túl, az óceán nem vagy kevéssé ellenőrzött parti sávja felé repülnek, ahol a rakományt ledobják, azt pedig az erre szerződtetett személyek – magukat halászoknak álcázva – csónakokból összeszedik. A 2017-es híradások ugyanakkor már arról szóltak, hogy a kartellek esőerdőbeli rejtekhelyein a hatóságok olyan kis méretű repülő eszközöket is találtak, melyeket nagy valószínűséggel fegyveres támadásokban használtak a bűnelkövetők. A térségben ugyanakkor a drónok politikai célú használatára is akad példa. [25]

Caracasban 2018. augusztus 4-én Nicolás Maduro venezuelai elnök egy katonai felvonulás keretében katonák és civilek ezrei előtt tartott beszédet, amikor két, kamerával felszerelt, C4 robbanóanyaggal megrakott drón jelent meg a tömeg felett, majd két hangos robbanás hallatszott. A kormányerők szerint az ellenzék szervezte a támadást, a cél az elnök likvidálása volt. A merénylet azonban kudarcos véget ért, a DJI M-600 gépek egyike egy lakóépületnek csapódott, a másik pedig lezuhant és a földön robbant fel. Mindez ugyan látó- és hallótávolságon belül zajlódott, de emberéletben kár nem keletkezett, csak hét katona szenvedett könnyebb sérüléseket [26].

A drónok nem terrorista célú, de rosszhiszemű vagy gondatlan alkalmazása is járhat veszélyekkel. Gyakorta előfordul például, hogy menetrendszerinti repülőjáratok nem tudnak a tervek szerinti landolni, mert egy drón akadályozza a biztonságos leszállást (Serbakov, 2019). Bizonyosnak tűnik, hogy a terroristák ötleteket szereznek az ilyen és ehhez hasonló esetekből. Hírszerző ügynökségek például lehallgatták Al-Kaida tagok beszélgetését, melyben éppen azt tervezték, hogy robbanóanyaggal megrakott drónokat irányítanak majd az Egyesült Királyság, illetve az Egyesült Államok légikikötőiben várakozó repülőgépeknek [4].

5. ÖSSZEFOGLALÁS

A tanulmányban áttekintést nyújtottunk az elmúlt két és fél évtized drónnal végrehajtott terrorista akcióiról. Láthattuk, hogy a drónhasználatot három négy terrorszervezet illesztette be a harcászati, illetve politikai eszköztárába: a Hezbollah, a Hamász, az Iszlám Állam, valamint a jemeni huti lázadók esetében lehetett egy időben komolyabb ezirányú aktivitást megfigyelni. E szerveződések közül egyértelműen a Hezbollah az, amelyik a legrégebb óta (1997-től kezdődően) rendelkezik drónműveleti programmal [27].

A Hamász drónműveletei kevésbé láthatóak, bár ez talán nem is annyira a szervezet szándékain múlott, sokkal inkább azzal magyarázható, hogy a ténylegesen végrehajtott és sikerre vitt műveleteik száma alacsony. Az izraeli védelmi minisztérium szerint ugyanis a 2016 és 2018 közötti időszakban 352 drónalkatrészt és százhetvenöt komplett drónt foglaltak le a kerem-shalomi és az erezi határátkelőhelyen Egy másik körülmény, mely arra utal, hogy a Hamász drónprogramja jóval szélesebb körű volt annál, mint ami napvilágra került: a szervezet 2016 végén elismerte, hogy elhunyt Mohammed Zawari, a drónprogramjának felügyelője [45]. A huti lázadók – ellentétben a Hamász és a Hezbollah terroristáival – kifejezetten nagy és látványos célpontokat kerestek maguknak, erre különösen jó példát jelentenek a nyolcezernél is több résztvevős katonai parádé vagy éppen a repülőterek elleni támadások. [28].

Az Iszlám Állam drónprogramja alapjaiban eltér a többi tárgyalt terrorszervezetétől. Döntően a kereskedelemben olcsón beszerezhető eszközök módosításával állították fel drón-flottájukat, ebből pedig következik az is, hogy az általuk használt gépek kevésbé voltak „technikásak", nem a legfejlettebb technológiát, hanem az egyszerűen, könnyen cserélhető alkatrészekből álló megoldásokat keresték. A legfőbb különbséget azonban a kreatív felhasználás jelentette, továbbá az, hogy az ISIL igyekezett a lehető legnagyobb nyilvánosságot biztosítani a drónokkal végrehajtott támadásainak. Elfogadva Archambault és Veilleux-Lepage (2020) érvelését, mindennek hátterében egy, a katonai, harcászati sikereknél szofisztikáltabb célt fedezhetünk fel: az Iszlám Állam tudatosan tette a drónműveleteket, illetve az ezek során készült felvételeket a vizuális propagandája meghatározó elemévé. Az ellenséges országok felett repülő drónok képe a szemlélőben azt az érzetet volt hivatott erősíteni, hogy az Iszlám Állam egy szuverén, a fennhatósága alatt álló területek felett tényleges ellenőrzést gyakorló állam. [29]

Bunker (2015) vélekedése szerint a drónműveletek, egy az ISIL által előre nem feltétlenül látott következménnyel jártak. „Valahányszor egy állam vagy csoport új technológiát alkalmaz a háborúban" – mutatnak rá Mueller és társai (2008) – „gyakran keményebb választ kap az ellenfelektől, mert a háború fokozódásának tekintik". Bunker (2015) úgy véli, az ISIL esetében pontosan ez történt: a fokozódó drónműveletek a szövetséges erőket a korábbinál is intenzívebb válaszlépésre sarkallták, és célzottan bombázni kezdték azokat a helyszíneket, melyeket az Iszlám Állam a drónok építésére, fejlesztésére használt, illetve, amelyeket a drónműveletek céljából igénybe vett. Egy egyszerű megfigyelés alátámasztani látszik e megállapítást: a drónhasználat azokban az években volt igazán intenzív, amikor az Iszlám Államnak még nem kellett szembenéznie számottevő fenyegetéssel, ám visszaesett a használat, midőn a szövetséges erők erőteljesebbé tették az ISIL elleni fellépést. Ekkor már nemcsak meggyengült a szervezet, de veszített a presztízséből is: ahhoz pedig, hogy erősítse az imázsát, már nem bizonyult elegendőnek a végtelen sivatagok felett repülő drónok képe, sem a bizonytalan kimenetelű drónműveletek lehetősége – erőszakos, határozott üzenetet közvetítő támadásokra volt szükség, látványos öngyilkos merényletekre, nagy pusztítással járó merényletekre, civil lakosok elleni kegyetlen mészárlásra, vagyis olyan akciókra, melyek egyfelől félelmet keltenek, másfelől tekintélyt ébresztenek és felkeltik a potenciális új tagok érdeklődését [7, 30, 31].

A fenti áttekintés alapján megállapíthatjuk, hogy a dróntámadásoknak elsődlegesen nem a katonai, harcászati veszteség okozása a célja, és reálisan szemlélve nem is lehetne az, hiszen a drónműveletek jóval kevésbé halálosak, mint a terrorizmus egyéb formái. A terroristák választása rendszerint akkor esik a drónokra, amikor nehezen megközelíthető helyen akarnak támadni vagy amikor valamilyen látványos, a közvélemény figyelmét felkeltő akcióra van szükségük. A dróntámadások azonban jellemzően propagandacélokat szolgálnak: csak az a terrorszervezet él ezzel az eszközzel, mely már elért a stratégiai érettség egy bizonyos szintjére, a drónhasználat révén pedig azt kívánja demonstrálni, hogy rendelkezik annyi tudással és tapasztalattal, hogy képes alkalmazni ezt az újfajta technológiát. A visszaszorulóban lévő ISIL példája ugyanakkor rávilágít arra, hogy a dróntámadás kétélű fegyver: sok benne a bizonytalansági tényező, számos olyan körülmény felmerülhet, mely meghiúsítja a műveletet, márpedig „a sikertelen dróntámadás káros nyilvánosságot eredményez".

Irodalomjegyzék

[1] Braun, Thomas – Fleiss, Alexander: Miniature Menace: The Threat of Weaponized Drone Use by Violent Non-state Actors. https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2344151/miniature-menace-the-threat-of-weaponized-drone-use-by-violent-non-state-actors/. Letöltve: 2021.03.10.

[2] Archambault, Emil – Veilleux-Lepage, Yannick: Drone imagery in Islamic State propaganda: flying like a state. International Affairs, Volume 96, Issue 4, July 2020, Pages 955–973, https://doi.org/10.1093/ia/iiaa014 Letöltve: 2021.03.10.

[3] Krajnc Zoltán: Drónok, hibrid fenyegetés, terrorizmus a légtérből: a légi hadviselés privatizálása. Hadmérnök XIII. évfolyam 4. szám, 2018. december. 358–369. http://hadmernok.hu/184_29_kranjc.pdf Letöltve: 2021.03.12.

[4] Serbakov Márton Tibor: A terroristák drónhasználata. Nemzetbiztonsági Szemle 7. évfolyam (2019) 4. szám 30–43. https://folyoirat.ludovika.hu/index.php/nbsz/article/view/829 Letöltve: 2021.03.12.

[5] Hirklikk.hu: Drónos terrorveszély a világban – az Országgyűlést is védik ellenük. 2019.08.05. https://hirklikk.hu/kozelet/dronos-terrorveszely-a-vilagban-az-orszaggylest-is-vedik-ellenuk/353318. Letöltve: 2021.03.12.

[6] Trautmann Balázs: Drónvadászat. https://honvedelem.hu/hatter/haditechnika/dronvadaszat.html. Letöltve: 2021.03.12.

[7] Bunker, Robert J.: Terrorist and Insurgent unmanned aerial vehicles: Use, potential and military implications. Strategic Studies Institute, US Army War College (2015). Elérhető: http://www.jstor.com/stable/resrep11741. Letöltve: 2021.03.15.

[8] Smithson, Amy E.: Rethinking the Lessons of Tokyo. In: Ataxia: The Chemical and Biological Terrorism Threat and the US Response. Washington, DC, Henry L. Stimson Center, 2000.

https://www.stimson.org/2000/ataxia-chemical-and-biological-terrorism-threat-and-us-response/. Letöltve: 2021.03.20

[9] Romaniuk, Scott N. – Burgers, Tobias, J.: Entering the Era of 'Unmanned Terrorism'. Terrorism Monitor Volume: 15 Issue: 1. January 13, 2017. Elérhető: https://jamestown.org/program/entering-era-unmanned-terrorism/ Letöltve: 2021.03.20

[10] Miasnikov, Eugene: Terrorists Develop Unmanned Aerial Vehicles. On „Mirsad 1" Fight Over Israel. December 6, 2004. Elérhető: http://www.armscontrol.ru/UAV/mirsad1.htm Letöltve: 2021.03.21

[11] G4s.com: Corporate Risk Services: Drones: Threat from Above. 2017. Elérhető: https://www.g4s.com/-/media/g4s/canada/files/whitepapers/usa/drones_threat_from_above.ashx?la=en&la=en Letöltve: 2021.03.21

[12] Fernandez, Belen: Meet Ayoub: The Muslim drone. 18 Oct 2012.: https://www.aljazeera.com/opinions/2012/10/18/meet-ayoub-the-muslim-drone Letöltve: 2021.03.21

[13] Sterman, Adiv: Hezbollah Drones Wreak Havoc on Syrian Rebel Bases. The Times of Israel, 21 Sept. 2014. www.timesofisrael.com/hezbollah-drones-wreak-havoc-on-syrian-rebel-bases Letöltve: 2021.03.21

[14] United States v. Chandia, 675 F.3d 329 (4th Cir. 2012).: https://casetext.com/case/united-states-v-chandia Letöltve: 2021.03.23

[15] Hall, John: ISIS Propaganda, Call of Duty-Style: Latest Footage Shows Drone's View of Battle-Ravaged Streets of Kobane before Swooping in to Show Gun Battles on the Ground. Daily Mail, December 12, 2014. www.dailymail.co.uk/news/article-2871389/ISIS-propaganda-Call-Duty-style-Latestfootage-shows-drone-s-view-battle-ravaged-streets-Kobane-swoopinggun-battles-ground.html Letöltve: 2021.03.27

[16] Alexander, David: U.S. Has Flown 2,320 Strikes against Islamic State at a Cost of $1.83 Billion: Official, Reuters, March 19, 2015. www.reuters.com/article/2015/03/19/us-mideast-crisis-usa-idUSKBN0MF2HC20150319 Letöltve: 2021.03.27

[17] Hambling, David: ISIS is Reportedly Packing Drones with Explosives Now, Popular Mechanics, December 16, 2015. http://www.popularmechanics.com/military/weapons/a18577/isis-packing-drones-with-explosive Letöltve: 2021.03.27

[18] [18] Sterman, Adiv: Hezbollah Drones Wreak Havoc on Syrian Rebel Bases. The Times of Israel, 21 Sept. 2014. www.timesofisrael.com/hezbollah-drones-wreak-havoc-on-syrian-rebel-bases Letöltve: 2021.03.27

[19] [19] France24.com: Exclusive: IS Group's Armoured Drones Attack from the Skies in Battle for Raqqa. France 24, 26 June 2017. www.france24.com/en/20170626-syria-exclusive-raqqa-drones-islamic-state-group-battle Letöltve: 2021.03.27

[20] [20] Utterback, Mitch: How ISIS is turning commercial drones into weapons in the battle for Mosul. 2017. Elérhető: www.foxnews.com/tech/how-isis-is-turningcommercial-drones-into-weapons-in-the-battle-for-mosul Letöltve: 2021.03.27

[21] [34] Abc.net.au: Syria: footage shows Islamic State drone blowing up stadium ammo dump. ABC News, 25 Oct. 2017. https://www.abc.net.au/news/2017-10-25/footage-shows-is-drone-attack-on-syrian-government-stadium/9085750 Letöltve: 2021.03.28

[22] Tadjdeh, Yasmin: Islamic state militants in Syria now have drone capabilities. National Defense, 28 Aug. 2014. http://www.nationaldefensemagazine.org/articles/2014/8/28/islamic-state-militants-in-syria-now-have-drone-capabilities Letöltve: 2021.03.28

[23] Al Jazeera: Yemen: Houthis launch drone attacks on Saudi airports, airbase . 5 Aug 2019. Elérhető: https://www.aljazeera.com/news/2019/8/5/yemen-houthis-launch-drone-attacks-on-saudi-airports-airbase Letöltve: 2021.03.28

[24] Timesofisrael.com: IDF names Iranian general as mastermind of thwarted drone attack plot. 27 August 2019. Elérhető: www.timesofisrael.com/idf-names-iranian-general-as-mastermind-of-thwarted-drone-attack-plot Letöltve: 2021.04.03

[25] Axe, David: Great, Mexican Drug Cartels Now Have Weaponized Drones. Vice, 25 October 2017. https://www.vice.com/en_us/article/j5jmb4/mexican-drug-cartels-have-weaponized-drones Letöltve: 2021.04.03

[26] Koettl, Christoph – Marcolini, Barbara: A Closer Look at the Drone Attack on Maduro in Venezuela. New York Times, 10 August 2018. www.nytimes.com/2018/08/10/world/americas/venezuela-video-analysis.html Letöltve: 2021.04.03

[27] Woods, Chris: Sudden justice: America's secret drone wars. New York, Oxford University Press, 2015. https://global.oup.com/academic/product/sudden-justice-9780190202590?cc=hu&lang=en& Letöltve: 2021.04.03

[28] Fishman, Alex: The new explosive drone threat from Gaza. Ynetnews, 7 July 2018. https://www.ynetnews.com/articles/0,7340,L-5318598,00.html Letöltve: 2021.04.04

[29] Rassler, Don: Remotely piloted innovation: terrorism, drones and supportive technology. West Point, NY, Combating Terrorism Center at West Point, Oct. 2016. https://css.ethz.ch/en/services/digital-library/publications/publication.html/1b5ae13e-bbff-4c4c-a5e0-def2189d56d4 Letöltve: 2021.04.04

[30] Beninati, Joseph A.: Examining the Cyber Operations of ISIS. Order No. 10108064, Utica College, 2016, Ann Arbor: ProQuest, Web, 18 December 2019. Elérhető: https://hssonline.org/wp-content/uploads/2017/08/ISISdiss77-10-4444-COMPLETE-2-08.29.2017.pdf Letöltve: 2021.04.04

[31] Galehan, Jordan N.: Gender and the Enactment of Suicide Bombings by Boko Haram. Order No. 13901011, Southern Illinois University at Carbondale, 2019, Ann Arbor: ProQuest, Web, 18 December 2019. https://opensiuc.lib.siu.edu/cgi/viewcontent.cgi?article=2713&context=dissertations Letöltve: 2021.04.04