ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Review Article*
Vol. 9, No. 4, December 2021, pp.1038-1055

Survey on encode biometric data for transmission in wireless communication networks

Mohammed Hussein Ali [1], Amer Ibrahim [2], Hasan Wahbah [3], Israa Al_Barazanchi [4]
[1] Mazaya University College/ Computer Engineering Technique, Thi-Qar, Iraq
[2,3] College of Computer and Information Technology, the American University in the Emirates
[4] College of Computing and Informatics, Universiti Tenaga Nasional (UNITEN), Malaysia
[4] Computer Engineering Techniques Department,Baghdad College of Economic Sciences University, Baghdad - Iraq

ABSTRACT

The aim of this research survey is to review an enhanced model supported by artificial intelligence to encode biometric data for transmission in wireless communication networks can be tricky as performance decreases with increasing size due to interference, especially if channels and network topology are not selected carefully beforehand. Additionally, network dissociations may occur easily if crucial links fail as redundancy is neglected for signal transmission. Therefore, we present several algorithms and its implementation which addresses this problem by finding a network topology and channel assignment that minimizes interference and thus allows a deployment to increase its throughput performance by utilizing more bandwidth in the local spectrum by reducing coverage as well as connectivity issues in multiple AI-based techniques. Our evaluation survey shows an increase in throughput performance of up to multiple times or more compared to a baseline scenario where an optimization has not taken place and only one channel for the whole network is used with AI-based techniques. Furthermore, our solution also provides a robust signal transmission which tackles the issue of network partition for coverage and for single link failures by using airborne wireless network. The highest end-to-end connectivity stands at 10 Mbps data rate with a maximum propagation distance of several kilometers. The transmission in wireless network coverage depicted with several signal transmission data rate with 10 Mbps as it has lowest coverage issue with moderate range of propagation distance using enhanced model to encode biometric data for transmission in wireless communication.

Keywords: Transmission, artificial intelligence, modelling, optimization, wireless, biometric, communication, encoding, decoding

Corresponding Author:

Mohammed Hussein Ali
Mazaya University College, Computer Engineering Technique
Thi-Qar, Iraq
E-mail: alamiry.83@gmail.com

1. Introduction

The transmission in Wireless Networks (WN) are normally used to evaluate one or more physical criterion in a vast area. A wireless network consists of hundreds of small nodes (sensors). These sensors measure the physical attributes of the area such as temperature, pressure, humidity, air pollution etc. They are widely used in different fields such as natural disasters monitoring like floods, earthquakes, and volcanic and other geological accidents as mentioned in [1]. As well, they are used in military, robotics, automated warehouses, chemical and medical applications. One of the most popular usages of the WN in the nature to measure temperature, pressure, humidity, and disasters in the mountains as mentioned in [2]. The researchers in [3] assume that each sensor is a small device with a limited energy source and memory, a system to send and receive the data to other nodes and some component to measure the characteristics of the area. The rise of smartphones and other devices that can use Wireless Network bring along applications that exhaust any way to reconnect to the internet in order to down an up-load personal data, advertisement or media with a high footprint in storage as mentioned in [4]. YouTube, WhatsApp, Facebook and similar apps move high quality scans and videos to and from end-users smart- phones. Since the number of smartphones in the field are constantly on the rise, this creates an additional strain for the backbone and access-links. As users prefer to use airborne wireless network instead of mobile internet-connections due to their costs and limitations with respect to available bandwidth, an airborne wireless network infrastructure like a WLAN needs careful planning as mentioned in [5]. Especially use cases like camping sites or large-scale deployments (widespread rural areas) with a lot of users put high requirements on the wireless network backbone. In this paper we consider python language-based simulation, a simulation which implements an easily deployable airborne wireless network with 3D-Plane for a set of APs in order to create a wireless infrastructure for a specific area.

A wireless access-point AP is a device which allows Wireless-Clients to connect to its 3D-Plane network. Typically, it serves as an entry point to a network-infrastructure and ultimately the internet like a common network switch, but APs can also be used in different ways. In the following we will describe the modes we use APs in:

Infrastructure-mode: Using this mode, the clients connect themselves to the APs in order to get access to the network behind the APs, like fileservers or the internet as mentioned in [6]. To do so one or more APs announce their services through small broad- casted packets called beacons, which include a Service Set Identifier (SSID), the name/identifier of the wireless network. Those are used to differentiate multiple wireless networks from each other if used in the same area. SSIDs, if received, are then used by the clients to establish a link to the AI based models.

Point-to-Point mode: This mode is defined by a static link between exactly two interfaces in contrast to infrastructure- and ad-hoc-mode, where this affiliation is not determined. It allows an AP to create a dedicated link to another AP using the same mode as mentioned in [7]. This link would consequently be shared only by these two APs, additionally the transmitted data is encrypted as mentioned in [8]. This mode is useful in scenarios where complex connection-constellations cannot be achieved by client-infrastructure-mode combinations solely. Alternatively, one could also use the ad-hoc mode, which was not available, as it was not implemented yet.

Client-mode: Here the AP behave the same as ordinary clients like laptops or smartphones. They search for wireless networks announced by APs in infrastructure mode and connect themselves to these. Often this mode is used to enable devices which lack 802.11-hardware to access a 3D-Plane through a wired link to those APs as mentioned in [9].

We will refer to airborne wireless network in its current form as 3D plane basic and the improved system, with the features of this requirements analysis realized, is called 3D plane extended. Up to now 3D plane basic automatically uses just one or a random set of channels for its backbone wireless connections. Additionally, the topology it creates often reassembles a tree-like structure, since the APs connect themselves to the first AP which comes into range and additionally there are no fallbacks, if a link fails. This results not only in severe bottlenecks for throughput, but also to prolonged downtimes, if a link happens to fail. Since after a disconnection it takes some time for the APs to automatically reconnect to the network, it nevertheless results in an unnecessarily long network-downtime for the attached clients. Especially clients that depend on an uplink connection severely suffer from this lack of alternative / backup links as mentioned in [10].

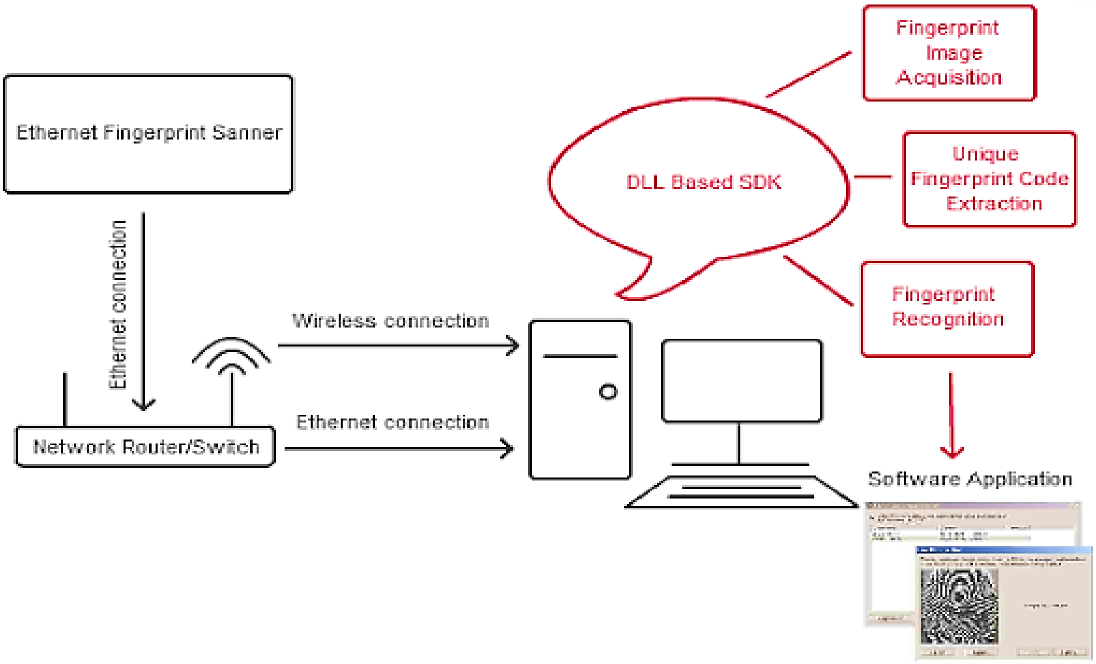
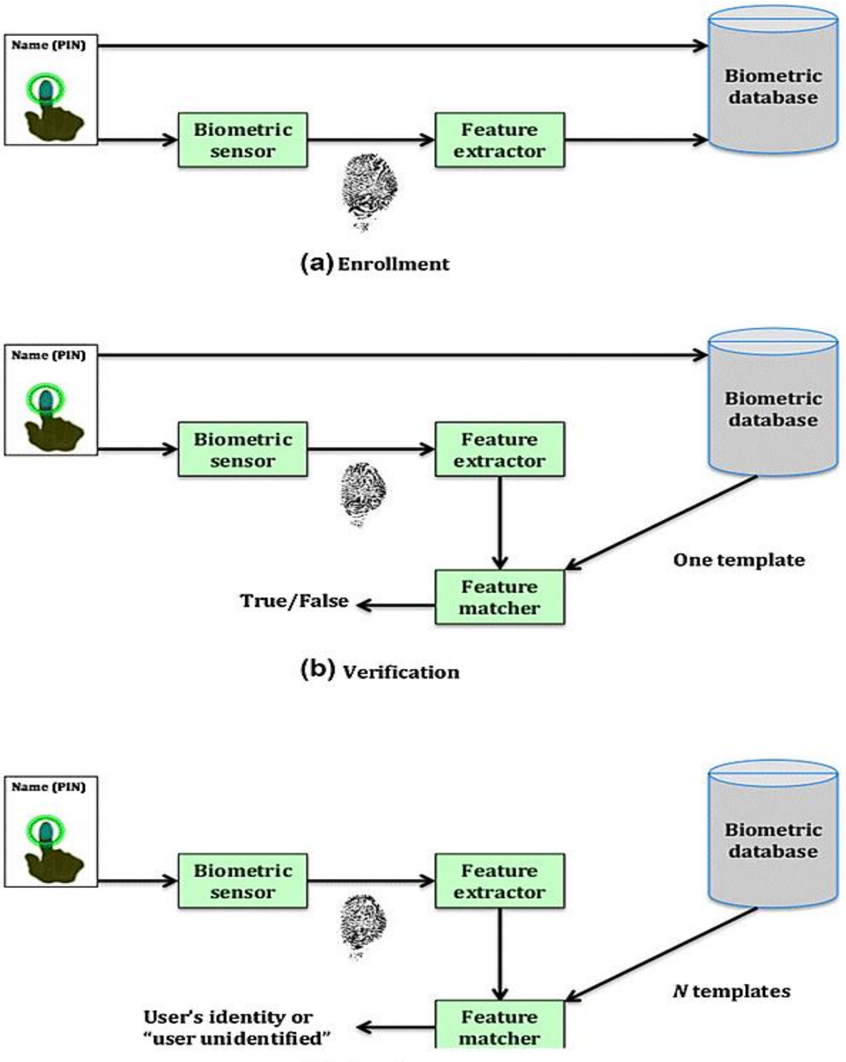


Figure 1. Aspects of biometric processing

The topics of wireless communication and verification are the applications considered here to demonstrate the benefits of the biometric decoding and analysis [10]. Since the systems, which are connected to the airborne wireless network, consume more data every day and with an increasing storage-footprint of new media like streaming High Definition (HD) biometric scans and generally downloading files of up to gigabytes, a wireless system is often solely defined by its capability of moving quantities of data over the air to the clients. This AI based algorithm for throughput is amplified by an increasing number of devices that take part in radio communication, thus it is also the key metric for quality in wireless communications as mentioned in [11]. Furthermore, not a single stream of data should be granted exclusive access to the radio, but multiple streams in parallel (gateway to clients) and across the network (clients to clients), as the common mesh / gateway / internet scenario does exist, but not exclusively (gateway to one client). Some use cases do only require local communication within the network. The wireless communications basic is due to its tree-like structure rather susceptible to network partition. As this may be just an inconvenience to users of devices like cellphones or laptops who are running non critical programs, keeping up a connection to certain parts of the network in an industrial environment gains importance. For example, where heavy machines depend on their uplink connections in order to continue proper operation. Hence wireless communication extended must provide the possibility to create and optionally use redundant connections in the network topology as mentioned in [12]. The failing scenario is defined as one link breaks while others are still usable. A resulting network topology should have the possibility of having the multiple-edge-connected attribute, as it may not be needed in all cases. The airborne wireless network extended must also be able to compute its solution on a central entity in contrast to a distributed fashion. Especially the wireless communications should not be used to compute such a solution as no additional tasks are to be assigned to them. Although not currently planned, a potential algorithm may be included in the Wireless-Plane in the simulation as mentioned in [13].



(c) Identification

Figure 2. Illustration of the biometric database task where the system is supposed to biometric patterns segments within a feature matching and feature extraction for enrolment, verification, and identification [14]

Reconfiguration of wireless communications and collection of data from the airborne wireless network will only be able through a central plan. That means the potential network-topology and channel assignment solution has to be set on the wireless communication and may not be broadcasted or otherwise distributed by or through the APs initially. Additionally, the management of certificates for security purposes is built up hierarchically and executed by the central wireless communication as mentioned in [14]. Especially since the support for doing things in a distributed fashion in the biometric encoding in wireless communications (multi-dimensional) is missing and would have to be implemented, makes distributed approaches undesirable in python language.

While setting up the test environment we also noticed that this effect of medium overload is no result of the size of our network. Whereas two unimpeded biometric scans were able to achieve a throughput of about 10Mbit in each direction, adding a third one would dramatically decrease overall throughput down to about 50kbit or less, growing worse with each newly added biometric scan in receive-range as mentioned in [15]. Even spreading the biometric scan further apart would not promise better results since the inherent problem of reusing the same channel for the forwarding and receiving link restricts the forwarding capabilities drastically. As the figures show, the outcome is dependent on the number of channels used as mentioned in [16]. A setup with only three distinct channels allowed yields still better results than a mono-channel-setup but is inferior to a setup where we can use even more channels as this gives us the possibility to use more collision domains which results in more available bandwidth and therefore increased throughput. In our example we used biometric scan with only two radios, which limits us in selecting separate modules for different connections. This means that an AP which already established two connections over its two modules would have to share one of its modules in order to apply a new link to a foreign biometric scan in order to maintain connectivity as mentioned in [17]. In conclusion: Instead of just using a lot of channels or just using a lot of communication-planes per biometric scan, a combination of both promises the best results. Each test run describes a 10 minutes' performance stress test for the network with throughput saturation in multiple planes. This should be enough time to notice any temporal effects and to get a picture of the lasting performance. To keep environmental conditions for each of the airborne wireless network systems as similar as possible we conducted the runs alternatively with respect to channel usage. So that a possible temporal interference in a certain band would affect both runs and not just favor a single system.

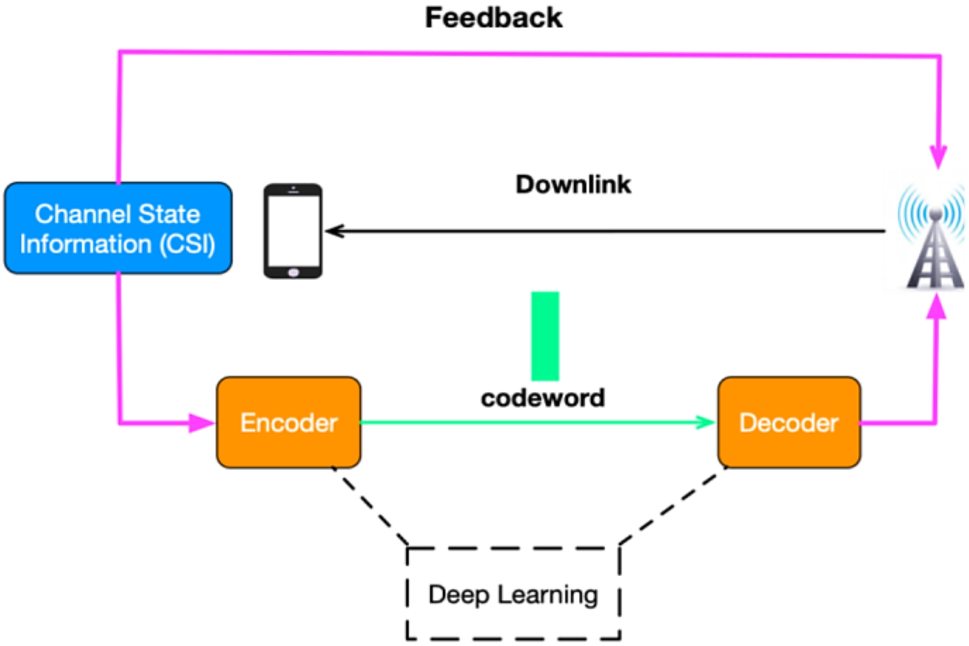


Figure 3. Illustration of a significant performance upgradation in case of AI-based deep learning environments transients which have some common properties of encoding/decoding [17]

2. Wireless communication consensus algorithms

Wireless network transmission requires in-depth knowledge about all protocols flowing across the network. Capture software must therefore implement many complex parsers in order to interpret the collected data the right way. Keeping up with the increasing amount of data that must be processed can be challenging, and

requires effective implementations and algorithms as mentioned in [18]. Real time data processing is necessary, to ensure a fast uncovering of an ongoing or past biometric scan and to prevent or lighten economic damage. New vulnerabilities appear every day and are quickly exploited with so called zero-day biometric scans. Signature based detection strategies suffer from the inability to detect previously unknown threats as mentioned in [19]. However, although having been a popular area of research over the last 20 years, machine learning techniques are rarely seen in commonly available tools. High amounts of false positives and the lack of proper training and evaluation data are well known problems of biometric based wireless communication as mentioned in [20]. Traffic patterns change a lot and so does the software stack inside network environments. To reflect this, modern datasets must be used for the evaluation of biometric based wireless communication strategies. Network wireless communication greatly helps in identifying network breaches, tracing them back to the responsible parties and then taking action to isolate and retrieve any damage that occurred as mentioned in [21]. The biometric scan recognition and event monitoring capabilities of wireless communication systems also have a deterrent effect on biometric scanners, who face a greater risk of being discovered and prosecuted. The presence of a wireless communication might convince a biometric scanner to search for another target, that is easier to penetrate. Being blocked by the monitor or by an analyst due to an alert, creates unwanted attention for the intruder and slows down his operations as mentioned in [22]. However, in order to benefit from wireless communication, there is a need for a reliable and extensive data source in order to make accurate predictions.
Preventative techniques like authentication and access control can fail, wireless communication provides a second line of defense and serves as the base for incident response after a system was compromised as mentioned in [23]. After gaining a foothold on a network, time passes for the biometric scanner to perform reconnaissance and identify assets of interest. Although the initial infection might not be detected, it is possible to prevent further damage when detecting the lateral movement of the biometric scanner as mentioned in [24].

Wireless communication plays a critical role in uncovering such behavior and greatly aids in reconstructing it for further forensic investigation. Only one third of organizations discovered the transmission themselves. Their latest report from 2018 states a median detection time of 99 days in 2016 and 101 days in 2017 as mentioned in [25]. Even though the decreasing detection time is a positive development, it is still too high. 100 days are a lot of time for a biometric scanner to identify assets of interest and take action. Besides that, even the most sophisticated and secure systems are still vulnerable to insiders, who misuse their privileges. When inspecting vulnerability visualizations, an alarming trend becomes visible: the overall number of reported vulnerabilities each year is growing and the vast amount of them is scored as medium or high severity as mentioned in [26]. Wireless communication is a key component for network defense and information security, it helps identifying attempts to compromise information systems and protect their availability, integrity, and confidentiality. Security information and event management (SIEM) systems often struggle with organizing the huge amount of data and provide interoperability between various data formats and input sources as mentioned in [27]. Data fed into a SIEM can be divided into 4 categories: network traffic, host data from the monitored endpoints, logs generated by various systems and threat intelligence feeds as mentioned in [28].

Network data is the most valuable of these information’s, since every biometric scan must go through the network and thus leaves traces, even if a biometric scanner tries to hide or obfuscate his presence. On the contrary for example, host data is not always reliable, because a compromised machine can be manipulated by a biometric scanner as mentioned in [29]. A recent study from the American Consumer Institute Center for Citizen Research has shown that 83% of routers contain vulnerable code. Infrequent updates cause the devices to be vulnerable for a long period of time, even after the vulnerabilities have been published in [30]. Although recent claims about hardware biometric scans by implants in the supply chain of the server manufacturer super micro have not been proven at the time of this writing, they describe a possible scenario that should be considered when securing a network environment. Network security monitoring can detect malicious attempts to contact the outside world, from both compromised software or hardware components, and allows to search the gathered data for indicators of compromise afterwards, to determine if there were other attempts in the past as mentioned in [31]. In order to infiltrate assets or information, the data has to be transferred to a server that is controlled by the intruder. This makes network data a very powerful piece of evidence. A recent study on the history of Remote Access Tools (RATs) shows that the development of Trojans has not stopped, instead it seems to be increasing. The study analyzed the 300 most important RATs of the last 20 years as mentioned in [32]. It shows the importance of behavior-based detection strategies, since signatures can only identify known malicious programs, and new malware variants appear frequently

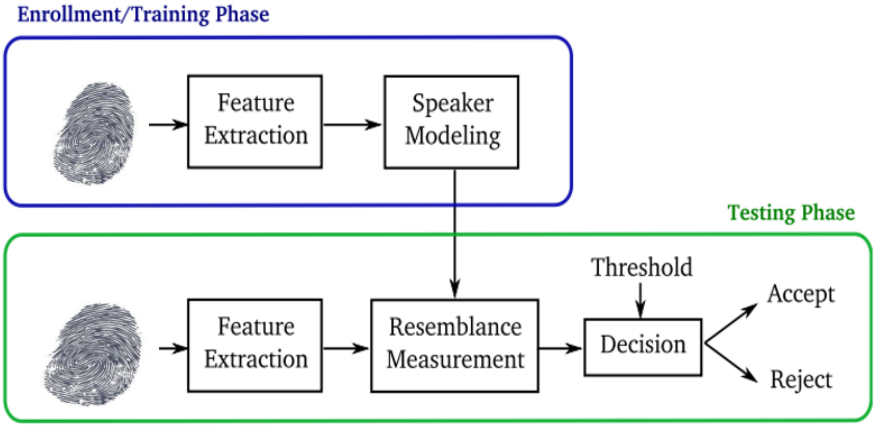


Figure 4. The wireless analysis based on during a speaker change point, the difference between two consecutive utterances is faded and the change point is missed before deciding for encoding the data [32]

Feature collection for the purpose of network wireless communication faces several problems. First, the increasing volume of data that has to be processed: high resolution video streaming, large file transfers and video conferences are common scenarios in corporate environments and generate huge amounts of network packets that have to be processed as mentioned in [33]. Another problem are biometric scans against the monitoring system, which can result in crashes and therefore loss of audit data, or in the worst case even to remote compromise of the network monitor. Current solutions for collecting features from traffic are written in low level system programming languages. This increases the biometric scan surface tremendously since these languages do not provide automated memory management as mentioned in [34]. This can lead to memory corruption vulnerabilities that enable denial of service or remote code execution biometric scans. Even if the state of an implementation is considered audited and secure, future updates to protocol specifications or new protocols will require continuous modifications, which can possibly (re-) introduce exploitable security vulnerabilities. Furthermore, the collection sensor should not be dependent on a specific architecture and be functional across all major platforms, to qualify for a widespread area of applications. The output data format should be consumable by as many systems as possible, to enable easy and quick integration into an existing network monitoring stack. The most used data format for big data analysis and machine learning are comma separated values (CSV), which do not preserve data types or provide structure to the data. Deployment and configuration of existing solutions is complex and time intensive for large environments as mentioned in [35]. A growing share of internet traffic is encrypted, denying access to content, and requiring analysis strategies that do not rely on clear text packet payloads for classification. The current state of tooling is insufficient to meet requirements for convenient and effective experiments because most of those tools were not designed specifically with a research task in mind. There might be fundamental differences in architecture or in client behavior as mentioned in [36]. Collecting network traffic during a penetration test inside the network and using this as a dataset to verify the deployed countermeasures work as expected, would create a much more realistic scenario and therefore more meaningful results. Currently, no publicly available tooling exists to accomplish this kind of independent verification in an effective and reproducible manner.

Table 1. Performance evaluation of artificial intelligence-based techniques under noisy conditions including different transients and transmission mechanism for wireless communication [37, 38]

Compared System	Non-Connected	Connected	Wireless
Baseline	69.92%	71.23%	79.9%
PCA (Euclidean)	57.6%	56.2%	68.1%
PCA (Cosine)	56.8%	56.1%	67%
SVM	42.6%	43.9%	49.2%
CNN	28.9%	27.2%	37.6%
RNN-LTSM	18.6%	19.3%	26.6%

Researchers in [40] presents several network traffic flow capture formats, tools, and techniques to visualize, filter and analyze network flow data. Researchers in [41] covers the general practice of network security monitoring and incident response and provides lots of background knowledge on network topologies and sensor placement. Common tools are explained, and their usage is demonstrated. Researchers in [42] present several feature selection algorithms among classification techniques to identify network anomalies and vulnerabilities at various layers. They also cover the assessment of network biometric detection systems, present different tools and discuss research challenges.

Researchers in [43] presents techniques for experimental data analysis, traffic behavior analysis, data collection using sensors and network mapping using python. He also deals with application identification and provides various ways to visualize network data. Researchers in [44] describes requirements for a network transmission detection system and explained the structure and functionality of the bro network monitor. Although this paper is more than 20 years old at the time of this writing, it contains fundamental aspects of network security monitoring, and inspired this research project with its philosophy of separating mechanism from policy.

Researchers in [45] reduce the different features widely adopted from the KDD dataset, to only 16 features, while still achieving similar detection results as with the full feature set. They used several filter algorithms including Weight by Maximum Relevance (WMR), Stepwise Regression and Stability Selection. For validation the Bayes Classifier was used, besides Support Vector Machines (SVM). This research paper served as a motivation for questioning the need for overly complex extracted features and served as a hint to conduct experiments with a more basic feature set.

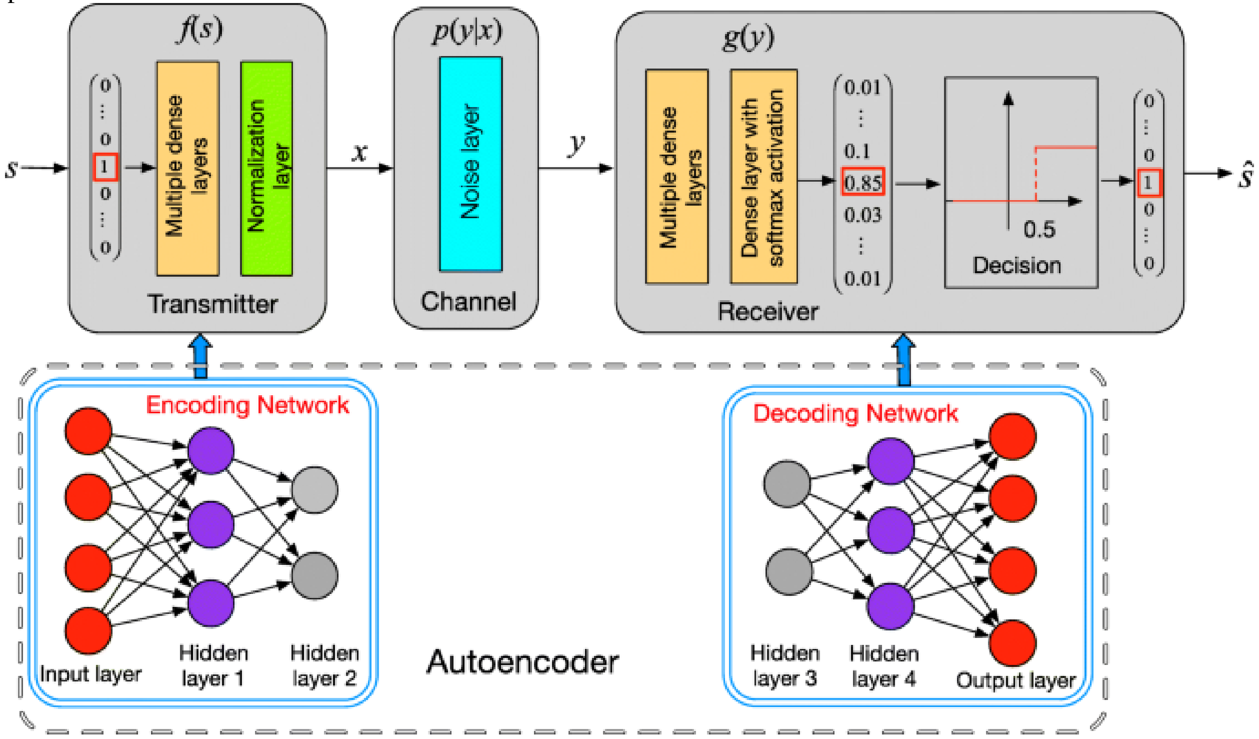


Figure 5. Reconfiguration of AI-based neural network and collection of data for wireless communication network will only be able through a central plan with multi-layer neural network [45]

With the evolution of multi-core processors and their decreasing cost, more and more systems are equipped with this technology. When designing a monitoring system, availability of several processing cores should be considered from the beginning. The term concurrency refers to the process of splitting a big problem into many small sub-problems, which unveils opportunities to execute independent operations in parallel as mentioned in [46]. Concurrency describes programming as the composition of independently executing processes. Parallelism refers to programming as the simultaneous execution of, possibly related, computations. While concurrency could also be expressed as dealing with lots of things at once, parallelism can be described as doing lots of things at once. While concurrency refers to structure, parallelism refers to execution. Although not identical, both are related. To enable concurrency, independent executions must be coordinated through communication. Since receiving network packets always happens sequentially, no matter if reading them from a dump file or live from the network card, parallelizing their decoding process is an option to utilize the power of multi-core systems, and speed up the overall processing. Many systems haven't been designed with concurrent processing in mind from the ground up as mentioned in [47].

Live capture from a network interface should be supported, to allow operation and monitoring in real time. Since dumping the collected data to disk is not always an option due to disk space constraints, e.g. on embedded devices, capture to disk should be optional and an alternate data collection mechanism should be provided. Uncovering successful breaches in real time and raising alerts, puts pressure on biometric scanners to move quicker in a compromised network. This increases the possibility for mistakes and leaves less time for cleaning up traces, which is beneficial for damage reduction, incident response and digital forensics as mentioned in [48]. A system that is too slow might generate alerts with a high delay, thus giving biometric scanners more time to accomplish their goals. Identifying attempted breaches in real time gives network security operators valuable information about targeted systems and used techniques and helps to put counter measures into place. Python is a statically typed and compiled imperative systems programming language released by python software foundation in 1991. It is syntactically like the Go programming language, but adopted lots of ideas from other languages, in order to improve readability and productivity. Commonly used for network programming and backend implementation, Python is known for its extremely fast compile time and generation of statically linked binaries, which are independent of any libraries on the execution environment. Python is currently available in version 3.8 and provides a built-in model for concurrent execution and coordination of asynchronous processes, which was inspired by the Communicating Sequential Processes (CSP) paper. An asynchronous process is called a go routine, which should not be confused with an operating system (OS) thread. WSN in python are multiplexed onto threads of the OS as required as mentioned in [49]. In case a WSN blocks, the corresponding OS thread blocks as well, but no other block is affected. WSNs are less computationally expensive compared to a thread and allocate resources dynamically as needed. For synchronization and messaging, python offers channels as a lightweight way to communicate between WSN. This design decision was inspired by the idea of sharing memory by communicating, instead of communicating by sharing memory.

3. Encoding biometric data in wireless network

The implemented solution in [50] is referred to as secure, because parsing the wireless network traffic is implemented in a memory-safe language for biometric scans classification. It is scalable because wireless network can increase throughput with more processing cores and can be used in a distributed monitoring setup. Python programming can take advantage of multi-core architectures as well as GPUs, to accelerate the computations for the Deep Convolutional Neural Network. Results from the series of experiments show that classification of labeled audit records is possible with a high accuracy, while only using a reduced feature subset compared to previous research in the area as mentioned in [51]. Wireless network is meant to be a useful technique in the process of feature collection, selection, and generation for research on biometric-based intrusion detection strategies. By providing the generated data in separate files, wireless network enables other applications that consume its output to implement a concurrent design as well. Choosing a platform neutral format for serialized structured data, greatly in- creases accessibility of the generated audit records for experiments across all major programming languages. The landscape of interesting libraries and techniques is constantly evolving, and so are the possibilities and options for experiments. Implementing the framework in python helps in reducing syntactic complexity, increases performance compared to implementations in scripting languages, and provides memory safety as mentioned in [52]. The fact that memory safety is a big problem for today's intrusion detection frameworks has been recognized by this advance research, which have begun to port parts of their protocol decoding logic to achieve an accuracy of 93.41% for detecting all the intrusions within the WSN that use a parser generation framework to accomplish safe protocol parsing. Although, these countermeasures are a good step forward, they only reduce the attack surface partially, since the remaining parts of the frameworks are still written in a language that is affected by this category of vulnerabilities. A key takeaway from the series of experiments is the absence of many computationally expensive extracted features, while still achieving very high classification results as mentioned in [53]. Questioning the need for those features comes with the possibility to improve the performance of network monitoring systems. The fewer data is needed for classification of malicious behavior, the more efficient implementations for feature collection and extraction can become. By publishing the developed tooling, the experiments are made reproducible for other researchers, which will hopefully lead to more academic publications and novel research in the area. However, the problem is not and will never be solved simply by deploying an intrusion detection system - there is always the need for an analyst that monitors the alerts and events and takes appropriate action. It is important to keep in mind, that network monitoring systems can be evaded as well and may even provide an increased attack surface to the system or network they were supposed to protect. To counter this development, frequent updates to defensive strategies and tools are necessary as mentioned in [54].

Researchers in [55] provides the possible sources of variation include the smoothening techniques, filter status, topography, filter properties, smoothening conditions, segmentation methods and other classification influences. Due to such local variations, the task of accurately differentiating between several field biometric filter can become ambiguous. This makes it difficult to create robust biometric processing algorithms that recognize all kinds of field instances without overfitting to the specific scene. In addition to the variation within a single scene, satellite scans can show even stronger intra-class variations as mentioned in [56]. This applies to scans from different filter regions, from different dates or growing seasons, or under different atmospheric and illumination conditions. Also, in view of increasing public availability of high-quality fusion biometric datasets, the use of additional and more heterogeneous ground truth and fusion biometric data (e.g. from multiple study areas in parallel) could improve the general model accuracy, robustness and transferability. Additional data augmentation (e.g. random scaling, distortions, color offset or jitter, introduction of biometric noise) might also help mitigate overfitting and increase the robustness to different fusion settings as well as biometric lightning conditions. In the proceeding discussion, the biometric scan will serve as a guideline to discuss the most poignant results obtained with CNN's with indication of some remarkable new elements. To give an indication of the performance of these models, the top-5 error rate in the wireless communication of the nets is presented. It has to be noted that the submitted nets, training and testing schemes offer a myriad of other hyper-parameters, which were tuned to achieve these results (e.g. a 7-network ensemble of CNN-architectures) as mentioned in [57].

The researchers in [58] focuses on compiling the delineate details and classifies wireless communication retrieval with edge smoothing using artificial bee colony algorithm and convolutional neural network while distinguishing between biometric instances of the same class. Instance segmentation lies at the intersection of edge detection (predicting the bounding box and class of a variable number of scans, but not segmenting them) and semantic segmentation (labeling each biometric pixel with a semantic category label, but not distinguishing between edges of the same category). With semantic segmentation it would be possible to find single instances of CNN algorithm on fields if they were surrounded by areas of different biometric classes. These datasets usually biometric scan from manual tracing of field boundaries as mentioned in [59]. However, manual tracing of biometric edge smoothening is heavily dependent on the used transmission and supplementary data. It also is a highly subjective task, inevitably leading to inaccuracies and ambiguities depending on the priorities of the operator. The ground truth dataset can be complemented by existing property parcel information that could be indistinguishable based on the biometric alone. Furthermore, a single field biometric edge smoothening can potentially show several subfields due to unreported land use changes within the growing season.

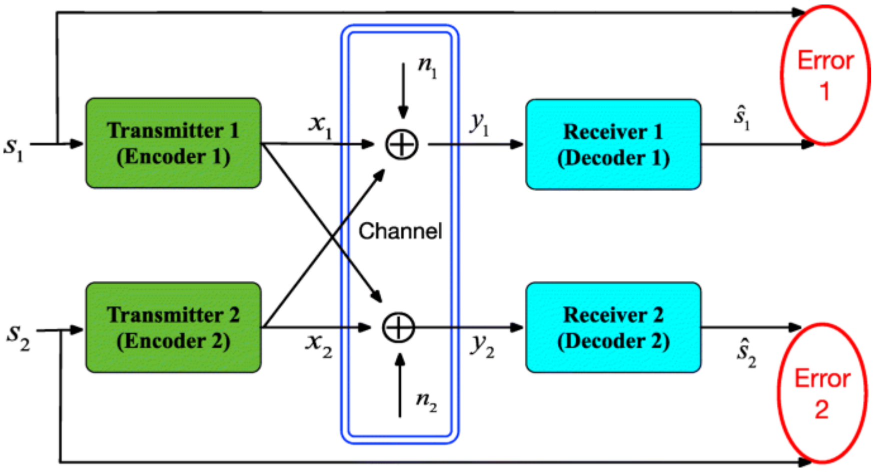


Figure 6. A system performance based on features extraction techniques where maximum window size steps in larger sliding window for encoding and decoding with respect to the transmitter/receiver [59].

Results in [60] show that accurate classification of biometric scan with CNN is possible within wireless communication network, with a feature set consisting mainly of collected and only a handful of generated features. Furthermore, classification achieved better results when applied to specific protocols, compared to classification of summary structures such as flows and connections. The time needed to encode the data to a numeric feature vector, heavily depends on the strategy used for encoding alphanumeric values (strings). Encoding strings as indices performed better in the encoding phase but required more time for training the deep neural network, compared to encoding them as dummy variables as mentioned in [61]. Using biometric scan descriptions instead of biometric scan classes as labels delivered comparable results and should be subject to further experiments. Since there might be several alerts for the same audit records, a strategy for handling this must be chosen. Collecting all classifications and merging them into a final label has shown great results and should be further investigated in combination with using specific biometric scan descriptions instead of biometric scan in wireless transmission as mentioned in [62].

4. Artificial intelligence technique comparison

The research on wireless communication network and application layer data for several types of biometric data classification is presented in [63]. Moreover, the previous works on the application layer data in the paper titled "A Model for Biometric Data in Wireless Communication Network" used only a 2-node clustering algorithm for comparison whereas we are comparing with 10-node wireless communication network with clusters and evaluating the accuracy. Furthermore, the research worked on application layer data. However, the data was collected from open-source repository and it was synthetic data set. Our data is non-synthetic and attained from an open-source repository dedicated for wireless communication network-based systems. Another important addition to our research is the analysis of the time taken by each algorithm to execute itself as we have seen that our own algorithm took the least execution time for the execution. As we discussed earlier in literature review that in wireless communication network, the difficulties were discovering calculations which can deal with huge datasets. Numerous calculations can deal with huge dataset with higher measurements as mentioned in [64].

The researchers in [65] saw support wireless sensor calculation with a massive precision of 99.21% and the least execution time which is exceptionally high accuracy as it works on multiple classes and does not have any classification of biometric scans in real-time, whereas it classifies the 'Worms' in a wireless communication network. Moreover, this research portrays the procedure of interruption identification and classification with the assistance of a few techniques which are somewhat sure in deciding the classification procedure and characterizing them to accomplish higher precision utilizing logistic processing with the clusters situated in WSN network with low execution time. This WSN technique classifies the real-time biometric scans in a wireless sensor-based network.

Anyway, in the research [66], the random clusters are processed for transmissions and accomplished a level of 97.72% so as to detect and classify the biometric scan on a wireless based system with an execution time of practically low. In this research, we accommodate to detect and classify the transmissions and real-time biometric scan types with higher accuracy in detailed comparison with other work and contribution of detecting and classifying the biometric scans in a wireless based network as mentioned in [67].

Table 2. The comparison between existing technique for encoding biometric data in wireless communication and transmission in terms of accuracy

TITLE	TYPE OF DEFECT	PROPOSE SOLUTION	TOOL OR PROGRAM	ACCURACY	REMARK
Optimizing Efficient Energy Transmission on a SWIPT Interference Channel Under Linear/Nonlinear EH Models.[68]	The wireless communication system is found to be defective from normal samples.	The samples were labeled by expert who categorized the wireless communication by the likelihood of a defect within each sample. The labeled sample can be used for development of deep learning and machine learning methods for automatic detection of different defects, like cracks, fracture interconnects, quality and for the purpose of predicting the efficiency loss.	Linear/Nonlinear EH Models	88.42 %	The accuracy extracted is insufficient and the defects are not classified

TITLE	TYPE OF DEFECT	PROPOSE SOLUTION	TOOL OR PROGRAM	ACCU RACY	REMARK
Learning to Optimize: Training Deep Neural Networks for Interference Management [69]	Utilizing the wireless communication detection system using artificial neural network, any power loss due to damaged samples, shadows etc. is detected and reported immediately which increases the efficiency of the wireless communication power stations and decreases the long-term maintenance and support costs.	Using counterfeit neural system innovation, the sun-based board shortcoming recognition framework is equipped for seeing wireless communication situation in the sky and evaluating the comparing yield intensity of a wireless communication-based board dependent on the calculations inferred by the recurrent neural system which has been prepared on sun-based information at a few time interims.	Deep Neural Networks (DNN)	97.65 %	The data set is collected for only one and it considered small
Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems [70]	The point of this work is the location of sun oriented wireless communication boards in low-quality samples. It is imperative to get the geospatial information, (for example, nation, postal division, and road and home number) of introduced sunlight-based boards, since they are associated straightforwardly to the neighborhood control	A Convolutional Neural Network was utilized. For preparing and testing dataset comprises of 3347 low-quality speaking samples was utilized	Scikit-Learn and TensorFlow	This paper does not specify the exact accuracy	The intricately structured profound convolutional neural systems (CNN) proposed by the authors can naturally extricate amazing highlights with less early information about the wireless communication for imperfection recognition. New framework for convolutional neural networks
Wireless information transfer with opportunistic energy harvesting [71]	Micro crack wireless communication defect, large-scale defect, defect and low resolution.	The authors introduce a Deep Learning based classification pipeline operating on the wireless communication. This includes biometric preprocessing for distortion correction, segmentation and perspective correction as well as a deep convolutional neural network for wireless communication defect classification with special emphasis on dealing with highly imbalanced dataset.	For the fully automated R-CNN based classification of objects, researchers developed a pipeline which processes the object detection modules. Detection of a communication module containing 6 × 12 mm. Since the objects contain the intrinsic distortions caused by the camera	97.59 %	The work not specified how the accuracy is performed for each used technique

TITLE	TYPE OF DEFECT	PROPOSE SOLUTION	TOOL OR PROGRAM	ACCURACY	REMARK
			lens, a first intrinsic calibration step is needed to correct the objects measurement distortions. This is done offline by using a calibration pattern and a standard calibration method		
Joint Power and Time Allocation in Full-Duplex Wireless Powered Communication Networks [72]	Detect defects in wireless communication	The elaborately designed Full-Duplex Wireless Powered Communication for real time detection	Full-Duplex Wireless Powered Communication	99.8%	The intricately structured profound Full-Duplex Wireless Powered Communication proposed by the authors can naturally extricate amazing highlights with less early information about the pictures for imperfection recognition. New framework for convolutional neural networks
Deep-Learning-Based Channel Estimation for Wireless Energy Transfer [73]	The wireless communication classification and localization	Although our method is simple, the convolutional neural network combined with class activation mapping technique makes chip biometric classification and defect regions localization possible in one single forward-pass. In this section, we revisit convolutional neural network and class activation mapping, the major techniques of our method	Long Term Short Memory (LTSM)	This paper does not specify the exact accuracy	Only classify two types of defects Not all defects can be detected

TITLE	TYPE OF DEFECT	PROPOSE SOLUTION	TOOL OR PROGRAM	ACCURACY	REMARK
Learning-Based Wireless Powered Secure Transmission [74]	Naturally wireless communication extricate amazing highlights for speakers.	The effectiveness and the suitability of the proposed approach.	The authors use especially trained DCNN for cells degradations. The framework is comprehensively evaluated on the “Wireless communication Dataset”, a proprietary dataset collected for this work.	This paper does not specify the exact accuracy	Approaches used on small dataset speaking samples.
Transmit Power Control Using Deep Neural Network for Underlay Device-to-Device Communication [75]	Programmed location of such deformities in a solitary detection of a wireless communication.	The methodologies vary in their equipment prerequisites, which are directed by their particular application situations. The more equipment proficient methodology depends close by created highlights that are ordered in a detect the biometric scans. To acquire a solid exhibition, we examine and look at different preparing variations. The more equipment requesting approach utilizes a start to finish profound Deep Neural Network (DNN)	Deep Neural Network (DNN)	88.42 % DNN	From the previous work on the classification of wireless communication, the following challenges are identified: 1-The highest accuracy achieved in the literature is 88% using deep learning. This result was obtained used a pre-trained deep learning model. Here, we aim to build our model for improving accuracy. 2-Preprocessing techniques, feature extraction methods, and types of models used in the literature are limited. There is room for improving these essential processing techniques to achieve better accuracy. 3-The data contains four classes, and through an in-depth investigation of the speaking samples, it can be concluded that the data classes can be further rebuilt

The goal of each biometric scan patch-wise illumination estimation experiment is to obtain a set of features for each biometric that describes its sequence. This set of features is called the biometric profile. Biometric profiles can be analyzed and compared to each other. In a patch-wise illumination estimation experiment for example, illumination estimation of scans that were treated can be compared against profiles of scans in the control set to quantify important matrix changes using CNN. For example, biometric patches can reveal a biometric sequence state or can be used for classification in biometric states such as phases of the biometric cycle or hematopoietic differentiation. Patch-wise illumination estimation using CNN can be of very different kinds. Examples include expression profiles that quantify the transcription of genes and morphological profiles that quantify the shape of the biometric and its compartments. Patch-wise illumination estimation is an important tool in morphological profiling and captures the scans used to obtain morphological biometric profiles. In this experiment, the original datasets were used, without adding any further effects on them. Moreover, in order to produce the proposed biometric, a combination of all of the used quality measure were implemented together.

5. Conclusion

In this research survey, we assumed on reviewing several scientific research articles terming artificial intelligence-based techniques and encoding the biometric data during the transmission in wireless communication. The implemented solution is referred to as secure, because parsing the network traffic is implemented in a memory-safe language. It is scalable because wireless communication can increase throughput with more processing cores and can be used in a distributed monitoring setup. Python programming can take advantage of multi-core architectures as well as GPUs, in order to accelerate the computations for the artificial intelligence techniques. Results from the series of experiments show that classification of labeled audit records is possible with a high accuracy, while only using a reduced feature subset compared to previous research in the area. Wireless communication is meant to be a useful technique in the process of feature collection, selection, and generation for research on biometric-based intrusion detection strategies. By providing the generated data in separate files, wireless communication enables other applications that consume its output to implement a concurrent design as well. Choosing a platform neutral format for serialized structured data, greatly increases accessibility of the generated audit records for experiments across all major programming languages. The landscape of interesting libraries and techniques is constantly evolving, and so are the possibilities and options for experiments. Implementing the framework in python helps in reducing syntactic complexity, increases performance compared to implementations in scripting languages, and provides memory safety. The fact that memory safety is a big problem for today’s intrusion detection frameworks has been recognized by this advance research, which have begun to port parts of their protocol decoding logic to achieve an accuracy for detecting all the intrusions within the wireless communication that use a parser generation framework to accomplish safe protocol parsing. Although, these countermeasures are a good step forward, they only reduce the attack surface partially, since the remaining parts of the frameworks are still written in a language that is affected by this category of vulnerabilities. A key takeaway from the series of experiments is the absence of many computationally expensive extracted features, while still achieving very high classification results.

References

[1] D. Wang, Y. Si, W. Yang, G. Zhang and J. Li, "A novel electrocardiogram biometric identification method based on temporal-frequency autoencoding", Electronics, vol. 8, no. 6, pp. 667, Jun. 2019.

[2] A. Iula and M. Micucci, "Experimental validation of a reliable palm-print recognition system based on 2d ultrasound images", Electronics (Switzerland), vol. 8, no. 12, 2019.

[3] B. Ammour, L. Boubchir, T. Bouden and M. Ramdani, "Face–iris multimodal biometric identification system", Electron., vol. 9, no. 1, 2020.

[4] I. Nakanishi and T. Maruoka, "Biometrics using electroencephalograms stimulated by personal ultrasound and multidimensional nonlinear features", Electronics, vol. 9, no. 24, pp. 1-18, 2020.

[5] F. HERAVI, et al. Impact of Aging on Three-Dimensional Facial Verification. Electronics, 8.10: 1170, 2019.

[6] I. Al Barazanchi et al., “Proposed a New Framework Scheme for the PATH LOSS in Wireless Body Area Network,” Iraqi J. Comput. Sci. Math., vol. 3, no. 1, pp. 11–21, 2022.

[7] B. FANG, et al. Classification of genetically identical left and right irises using a convolutional neural network. Electronics, 8.10: 1109, 2019.

[8] I. Al Barazanchi, S. A. Sahy, and Z. A. Jaaz, “Traffic Management with Deployment of Li-Fi Technology Traffic Management with Deployment of Li-Fi Technology,” J. Phys. Conf. Ser., vol. 1804, no. 012141, 2021, doi: 10.1088/1742-6596/1804/1/012141.

[9] S. DE LA PEÑA, A. POLO, C. ROBLES-ALGARÍN . Implementation of a portable electromyographic prototype for the detection of muscle fatigue. Electronics, 8.6: 619, 2019.

[10] Available Online: http://www.biometricsys.de/ethernet-fingerprint-scanner-efis121poe.html.

[11] M. GIL-MARTÍN, Manuel, J. MONTERO, R. SAN-SEGUND. Parkinson’s disease detection from drawing movements using convolutional neural networks. Electronics, 8.8: 907, 2019.

[12] L. Ma, Z. Li, Z. Birech, S. Li, Y. Yang, W. Zhang, et al., "Multi-channel optoelectronic measurement system for soil nutrients analysis", Electronics, pp. 8-451, 2019.

[13] S. Mekruksavanich and A. Jitpattanakul, "Smartwatch-based Human Activity Recognition Using Hybrid LSTM Network," 2020 IEEE SENSORS, 2020, pp. 1-4, doi: 10.1109/SENSORS47125.2020.9278630.

[14] I. Abdulshaheed, H. R., Yaseen, Z. T., Salman, A. M., & Al_Barazanchi, “An Evaluation study of WiMAX and WiFi on Vehicular Ad-Hoc Networks (VANETs),” IOP Conf. Ser. Mater. Sci. Eng. Pap., vol. 3, no. 12, pp. 1–7, 2020, doi: 10.1088/1757-899X/870/1/012122.

[15] A. Mahfouz, T. M. Mahmoud and A. S. Eldin, "A survey on behavioral biometric authentication on smartphones", J. Inf. Security Appl., vol. 37, pp. 28-37, Dec. 2017.

[16] S. Mekruksavanich and A. Jitpattanakul, "Convolutional neural network and data augmentation for behavioral-based biometric user identification" in ICT Systems and Sustainability, Singapore:Springer Singapore, pp. 753-761, 2021.

[17] O. D. Lara and M. A. Labrador, "A Survey on Human Activity Recognition using Wearable Sensors," in IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1192-1209, Third Quarter 2013, doi: 10.1109/SURV.2012.110112.00192.

[18] N. Hnoohom, S. Mekruksavanich and A. Jitpattanakul, "Human Activity Recognition Using Triaxial Acceleration Data from Smartphone and Ensemble Learning," 2017 13th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), 2017, pp. 408-412, doi: 10.1109/SITIS.2017.73.

[19] A. Chrungoo, S. Manimaran and B. Ravindran, "Activity recognition for natural human robot interaction", Proc. Int. Conf. Social Robot., pp. 84-94, 2014.

[20] D. Gehrig et al., "Combined intention, activity, and motion recognition for a humanoid household robot," 2011 IEEE/RSJ International Conference on Intelligent Robots and Systems, 2011, pp. 4819-4825, doi: 10.1109/IROS.2011.6095118.

[21] B. Yousefi and C. K. Loo, "Biologically-Inspired Computational Neural Mechanism for Human Action/activity Recognition: A Review", Electronics, vol. 8, no. 10, pp. 1169, 2019.

[22] S. Mekruksavanich and A. Jitpattanakul, "Exercise Activity Recognition with Surface Electromyography Sensor using Machine Learning Approach," 2020 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), 2020, pp. 75-78, doi: 10.1109/ECTIDAMTNCON48261.2020.9090711..

[23] S. S. Oleiwi, G. N. Mohammed, and I. Al-barazanchi, “Mitigation of packet loss with end-to-end delay in wireless body area network applications,” Int. J. Electr. Comput. Eng., vol. 12, no. 1, pp. 460–470, 2022, doi: 10.11591/ijece.v12i1.pp460-470.

[24] R. Damaševičius, R. Maskeliūnas, A. Venčkauskas and M. Woźniak, "Smartphone user identity verification using gait characteristics", Symmetry, vol. 8, no. 10, pp. 100, 2016.

[25] T. Rault, A. Bouabdallah, Y. Challal and F. Marin, "A survey of energy-efficient context recognition systems using wearable sensors for healthcare applications", Pervasive Mobile Comput., vol. 37, pp. 23-44, Jun. 2017.

[26] J. Wang, Y. Chen, S. Hao, X. Peng and L. Hu, "Deep learning for sensor-based activity recognition: A survey", Pattern Recognit. Lett., vol. 119, pp. 3-11, Mar. 2019.

[27] W. Jiang and Z. Yin, "Human activity recognition using wearable sensors by deep convolutional neural networks", Proc. of the 23rd ACM Int'l Conf. on Multimedia (MM‘15). ACM, pp. 1307-1310, 2015..

[28] L. Zhang, X. Wu and D. Luo, "Recognizing Human Activities from Raw Accelerometer Data Using Deep Neural Networks," 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), 2015, pp. 865-870, doi: 10.1109/ICMLA.2015.48.

[29] F. J. Ordóñez and D. Roggen, "Deep convolutional and LSTM recurrent neural networks for multimodal wearable activity recognition", Sensors, vol. 16, no. 1, pp. 115, 2016.

[30] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition", Proc. Int'l Conf. Learning Representations (ICLR), 2015.

[31] R. Chavarriaga, H. Sagha, A. Calatroni, S. T. Digumarti, G. Tröster, J. d. R. Millán, et al., "The opportunity challenge: A benchmark database for on-body sensor-based activity recognition", Pattern Recognition Letters, vol. 34, no. 15, pp. 2033-2042, 2013.

[32] I. PIRES, et al. Improving Human Activity Monitoring by Imputation of Missing Sensory Data: Experimental Study. Future Internet, 12.9: 155, 2020.

[33] K. Xia, J. Huang and H. Wang, "LSTM-CNN Architecture for Human Activity Recognition," in IEEE Access, vol. 8, pp. 56855-56866, 2020, doi: 10.1109/ACCESS.2020.2982225..

[34] H. Cho and S. Yoon, "Divide and conquer-based 1d cnn human activity recognition using test data sharpening", Sensors, vol. 18, no. 4, pp. 1055, 2018..

[35] L. Basora, X. Olive and T. Dubot, "Recent Advances in Anomaly Detection Methods Applied to Aviation", Aerospace, vol. 6, no. 11, pp. 117, 2019..

[36] R. MORI . Anomaly Detection and Cause Analysis During Landing Approach Using Recurrent Neural Network. Journal of Aerospace Information Systems, 1-7, 2021.

[37] Z. Menter, W. Tee and R. Dave, "A Study of Machine Learning Based Pattern Recognition in IoT Devices", 3rd International conference of Communications and Computing Technologies 2021 Algorithms for Intelligent Systems LNNS, India, 27–28 February 2021.

[38] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system", Simul. Model. Pract. Theory, vol. 101, May 2019.

[39] J. MASON, et al. An Investigation of Biometric Authentication in the Healthcare Environment. Array, 8: 100042, 2020.

[40] D. Gunn, Z. Liu, R. Dave, X. Yuan and K. Roy, "Touch-Based Active Cloud Authentication Using Traditional Machine Learning and LSTM on a Distributed Tensorflow Framework", International Journal of Computational Intelligence and Applications(IJCIA), 2019.

[41] I. Al Barazanchi, H. R. Abdulshaheed, M. Safiah, and B. Sidek, “A Survey : Issues and challenges of communication technologies in WBAN,” Sustain. Eng. Innov., vol. 1, no. 2, pp. 84–97, 2020.

[42] S. Jia et al., "Biometric Recognition Through Eye Movements Using a Recurrent Neural Network," 2018 IEEE International Conference on Big Knowledge (ICBK), 2018, pp. 57-64, doi: 10.1109/ICBK.2018.00016..

[43] N. Siddiqui, L. Pryor, R. Dave. An examination of user authentication schemes using machine learning methods. In Proceedings of the 3rd International Conference on Communication and Computational Technologies, Algorithms for Intelligent Systems, Jaipur, India, 27–28 February 2021.

[44] S. Li and W. Deng, "Deep Facial Expression Recognition: A Survey," in IEEE Transactions on Affective Computing, doi: 10.1109/TAFFC.2020.2981446.

[45] X. Li, D. Song, P. Zhang, G. Yu, Y. Hou and B. Hu, "Emotion recognition from multi-channel EEG data through Convolutional Recurrent Neural Network," 2016 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), 2016, pp. 352-359, doi: 10.1109/BIBM.2016.7822545.

[46] R. Benjamin, , A. Trias Antonioj and S. Jim, "A. Network traffic anomaly detection using recurrent neural networks", Chinese Journal of Network & Information Security., 2018.

[47] P. Fernandez-Lopez, J. Liu-Jimenez, K. Kiyokawa, Y. Wu and R. Sanchez-Reillo, "Recurrent neural network for inertial gait user recognition in smartphones", Sensors, vol. 19, no. 18, pp. 4054, Sep. 2019.

[48] B.-H. Kim and J.-Y. Pyun, "ECG identification for personal authentication using LSTM-based deep recurrent neural networks", Sensors, vol. 20, no. 11, pp. 3069, May 2020.

[49] R. Salloum and C. . -C. J. Kuo, "ECG-based biometrics using recurrent neural networks," 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2017, pp. 2062-2066, doi: 10.1109/ICASSP.2017.7952519.

[50] Y. Sun, et al. Smartphone user authentication based on holding position and touch-typing biometrics. Comput. Mater. Continua, 3.61: 1365-1375, 2019.

[51] S. Fu, D. Qin, D. Qiao and G. T. Amariucai, "RUMBA-Mouse: Rapid User Mouse-Behavior Authentication Using a CNN-RNN Approach," 2020 IEEE Conference on Communications and Network Security (CNS), 2020, pp. 1-9, doi: 10.1109/CNS48642.2020.9162287.

[52] A. Ferhatovic, et al. Implementation of Long Short-Term Memory (LSTM) For User Authentication Based On Keystroke Dynamics. Southeast Europe Journal of Soft Computing, 9. 1. 2020.

[53] I. Al Barazanchi, “An Analysis of the Requirements for Efficient Protocols in WBAN,” J. Telecommun. Electron. Comput. Eng., vol. 6, no. July, p. 43, 2014.

[54] X. Lu, Z. Shengfei and Y. Shengwei, "Continuous authentication by free-text keystroke based on CNN plus RNN", Pro-cedia Computer Science, vol. 147, pp. 314-318, 01 2019.

[55] R. Tolosana, R. Vera-Rodriguez, J. Fierrez and J. Ortega-Garcia, "Biometric Signature Verification Using Recurrent Neural Networks," 2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR), 2017, pp. 652-657, doi: 10.1109/ICDAR.2017.112.

[56] R. Tolosana, R. Vera-Rodriguez and J. Fierrez, "BioTouchPass: Handwritten Passwords for Touchscreen Biometrics," in IEEE Transactions on Mobile Computing, vol. 19, no. 7, pp. 1532-1543, 1 July 2020, doi: 10.1109/TMC.2019.2911506.

[57] S. Rajan, P. Chenniappan, S. Devaraj and N. Madian, "Novel deep learning model for facial expression recognition based on maximum boosted CNN and LSTM", The Institution of Engineering and Technology, vol. 14, no. 7, pp. 1373-1381, 2020.

[58] N. Jain, S. Kumar, A. Kumar, P. Shamsolmoali and M. Zareapoor, "Hybrid deep neural networks for face emotion recognition", Pattern Recognit. Lett., vol. 115, pp. 101-106, Nov. 2018.

[59] W. J. Baddar, S. Lee and Y. M. Ro, "On-the-Fly Facial Expression Prediction using LSTM Encoded Appearance-Suppressed Dynamics," in IEEE Transactions on Affective Computing, doi: 10.1109/TAFFC.2019.2957465.

[60] S. Chen and Q. Jin, "Multi-modal dimensional emotion recognition using recurrent neural networks", Proc. 5th Int. Workshop Audio/Visual Emotion Challenge, pp. 49-56, 2015.

[61] L. Chao, J. Tao, M. Li and Z. Wen, "Long short term memory recurrent neural network based multimodal dimensional emotion recognition", Proceedings of the 5th International Workshop on Audio/Visual Emotion Challenge, pp. 65-72, 2015.

[62] H. Wang, G. Zhou, X. Wang,. Video emotion recognition using local enhanced motion history image and CNN-RNN networks. Biom. Recognit. 2018.

[63] K. Huang, et al. An efficient algorithm of facial expression recognition by TSG-RNN network. In MultiMedia Modeling Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2019.

[64] D. Nguyen, R. Vadaine, G. Hajduch, R. Garello and R. Fablet, "GeoTrackNet--A Maritime Anomaly Detector Using Probabilistic Neural Network Representation of AIS Tracks and A Contrario Detection," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2021.3055614.

[65] T. Ergen and S. S. Kozat, "Unsupervised Anomaly Detection With LSTM Neural Networks," in IEEE Transactions on Neural Networks and Learning Systems, vol. 31, no. 8, pp. 3127-3141, Aug. 2020, doi: 10.1109/TNNLS.2019.2935975.

[66] F. Muharemi, D. Logofătu and F. Leon, "Machine learning approaches for anomaly detection of water quality on a real-world data set", J. Inf. Telecommun., vol. 3, no. 3, pp. 294-307, 2019.

[67] L. Bontemps, V. L. Cao, J. McDermott and N.-A. Le-Khac, "Collective anomaly detection based on long short term memory recurrent neural network", Proc. Int. Conf. Future Data Secur. Eng., pp. 141-152, 2016.

[68] P. V. Tuan and I. Koo, "Optimizing Efficient Energy Transmission on a SWIPT Interference Channel Under Linear/Nonlinear EH Models," in IEEE Systems Journal, vol. 14, no. 1, pp. 457-468, March 2020, doi: 10.1109/JSYST.2019. 2924265.

[69] H. Sun, X. Chen, Q. Shi, M. Hong, X. Fu and N. D. Sidiropoulos, "Learning to Optimize: Training Deep Neural Networks for Interference Management," in IEEE Transactions on Signal Processing, vol. 66, no. 20, pp. 5438-5453, 15 Oct.15, 2018, doi: 10.1109/TSP.2018.2866382..

[70] A. Géron, Hands-on Learning wiith SciKit-Learn and TensorFlow, O'Reilly, 2017.

[71] L. Liu, R. Zhang and K. Chua, "Wireless Information Transfer with Opportunistic Energy Harvesting," in IEEE Transactions on Wireless Communications, vol. 12, no. 1, pp. 288-300, January 2013, doi: 10.1109/TWC.2012.113012.120500.

[72] Y. Cheng, P. Fu, Y. Chang, B. Li and X. Yuan, "Joint power and time allocation in full-duplex wireless powered communication networks", Mobile Information Systems 2016.

[73] J. Kang, C. Chun and I. Kim, "Deep-Learning-Based Channel Estimation for Wireless Energy Transfer," in IEEE Communications Letters, vol. 22, no. 11, pp. 2310-2313, Nov. 2018, doi: 10.1109/LCOMM.2018.2871442.

[74] I. Al Barazanchi, Y. Niu, S. Nazeri, W. Hashim, and A. A. Alkahtani, "A survey on short-range WBAN communication ; technical overview of several standard wireless technologies," Period. Eng. Nat. Sci., vol. 9, no. 4, pp. 877–885, 2021.

[75] W. Lee, M. Kim and D. -H. Cho, "Transmit Power Control Using Deep Neural Network for Underlay Device-to-Device Communication," in IEEE Wireless Communications Letters, vol. 8, no. 1, pp. 141-144, Feb. 2019, doi: 10.1109/LWC.2018.2864099.