International Journal of Embedded and Real-Time Communication Systems
Volume 13 • Issue 1

One Approach to Improving Smart Environment Communication via the Security Parameter

Narves Behlilovic, BH Telecom JSC Sarajevo, Bosnia and Herzegovina*
https://orcid.org/0000-0001-8540-7923

ABSTRACT

Improving smart environment communication remains a final unachievable destination. Continuous optimization in smart environment communication is mandatory because of an emerging number of connected devices. Carefully observing its parameters and demands leads to acknowledging existing challenges and boundaries regarding areas covered with signal and possibilities of approaching network architecture, limited battery resources in certain nodes of network architecture, privacy, and security of existing data transfer. One approach to dealing with these communication challenges and boundaries is focusing on important technical parameters respectively, signal processing speed, communication nodes distance, and communication channel security. The aim of this article is to point out these most important communication parameters in smart environments and how changing those can affect communication. Its original contribution is represented in establishing principles for governing security parameters by using permanent magnets in order to produce Faraday's rotation and thus manipulate the whole process of communication in a smart environment.

KEYWORDS

Ad Hoc Wireless Networks, Cellular Networks, Cryptography, Faraday's Rotation, Heterogeneous Network, Internet of Everything, Internet of Things, Physical Layer Security, Smart Grid

INTRODUCTION

Rapid development in communication extent, as well as in the number of subjects active participants, followed by a more complex use of network architectures for their processing, are activating additional topics for researchers. After a period when following and analyzing the quality of service (QoS) and quality of experience (QoE) parameters were sufficient performance measures in the communication process, in recent years, there has been an increasing interest in the Internet of things (IoT) creating additional space for advancement in transmitting data among connected subjects. After a short period of time, adding more subjects to communication resulted in the Internet of everything (IoE) as a new and even more complex smart environment. In this article, IoT and IoE will be addressed as a common IoE/IoT smart environment. Communication channels in IoE/IoT smart environment are currently being established using highly diverse communication technologies, including various advantages

DOI: 10.4018/IJERTCS.313042 *Corresponding Author

and disadvantages considering their parameters. With respect to existing approaches, it is reasonable to look towards new solutions due to an enormous number of connected devices requiring ever better performances, resulting in the necessity of proposing a completely new method or complementary method for that purpose.

Problem Description

These newly created environments for connecting devices and communicating information generated and still generate numerous research topics, such as:

- The possibility of harmonious functioning in heterogeneous network architecture, whether its heterogeneity is related exclusively to approached combined networks or related to the fact that some parts of the network are capable of dynamically reconfiguring over time or persisting static configuration.
- Achieving the desired data transfer security level, preserving the integrity of data transmitted, lowering electromagnetic pollution levels of media in use, and lowering distance between nodes in communication, as well as the inevitable process of their authentication and authorization.

An additional problem emerging while researching these phenomena is the fact that most of their parameters are not mutually independent, so formulating their mathematical correlations is demanding, involving different areas of mathematics. In order to achieve sufficient communication quality, the participant should fulfill these requests at a minimum:

- All participants in communication should undergo a process of authentication and authorization to limit their activities in real-time communication.
- Information integrity must be preserved in total. In a connected world with the automatic exchange of information and executing tasks, there is zero tolerance for failure in communication. Therefore, information integrity is considered a key element in automated environments.
- The confidentiality of information content must be ensured, with prescribed procedures, following the principles mentioned above. Thus, exchanged information security is requested, as well as the security of connected devices and communication processes.

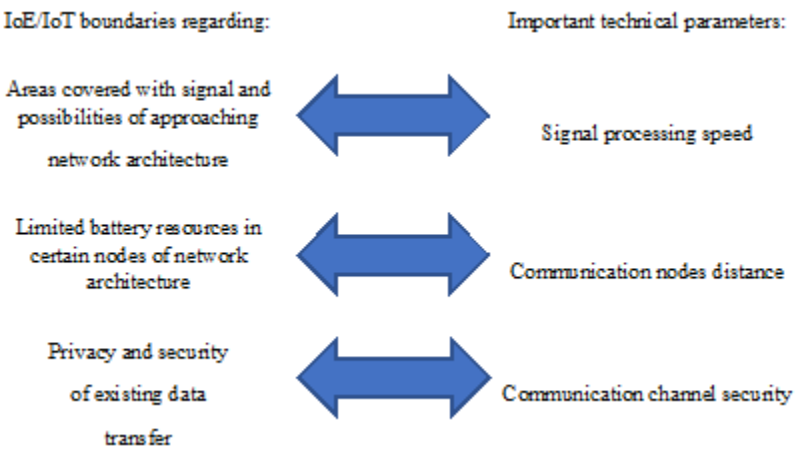
The research question in this article is:

How the parameter of security as a dominant technical parameter in a smart environment could be improved with Faraday's rotation, and what are the recommended values of B_{res} *as a result of interference between a magnetic field* B_0 *and electromagnetic waves of different frequency f in order to maximize the angle of rotation* ψ *value?*

Contribution

It is clear the search for new hardware solutions and more flexible network architectures with dominant, simple, and intelligent algorithms should be intensified. Accordingly, the advancement and development of new communication protocols should be expected. Thus, in front of researchers is a huge challenge in modeling complex communication systems, defining the identity of certain subjects in communication with relevant parameters, procedures for data processed integrity preservation, and maintaining desired connectivity among various devices, according to mutual IoE/IoT standards. After it has been stated that IoE/IoT has certain boundaries, it is reasonable to further analyze them in more detail.

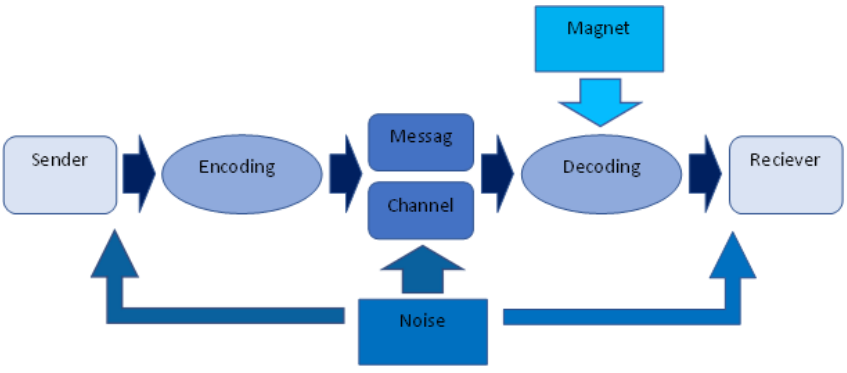
Figure 1. Challenges in smart environment communication



Significant parameters for improving the performance of smart environment communication are therefore signal processing speed, communication nodes distance, and communication channel security. It is possible to implement various communication channels with different characteristics, but it is impossible to guarantee performance. Existing "speed test" downloads and end-to-end latency measurements do not often reflect access network performance over an extended period of time, and they neglect various confounding factors (Sundaresan et al., 2011). Many would argue that available bandwidth is a key metric of access link speed. Unfortunately, the performance of available bandwidth estimation tools has rarely been tested from hosts connected to residential networks (Goga & Teixeira, 2012). When designing and implementing available bandwidth estimation algorithms and tools, one must be very aware of the system hardware issues (Jin & Tierney, 2003).

No matter the type of technology, the basic objective in reducing noise in communication channels is to minimize the probability of error. The probability of error can be minimized by maximizing the likelihood ratio, which, in terms of a physical operation, means improving the signal to noise. It is necessary to consider the way in which the signal-to-noise ratio is improved because there is an optimum way (Schwartz, 1956). Another approach would be maximizing the probability of error by adding noise into the communication channel and decreasing signal to noise ratio. This would protect the distant node or node in movement from unauthorized access and enable regular establishing of the communication channel with a node only when desired, in the absence of additional noise. The idea is presented in Figure 2.

Figure 2. Magnetic field interfering with electromagnetic wave



The possibility of magnetic field interference with microwaves is well known in wired communication, used in circulators and insulators as a part of fiber optical networks. The interference of a permanent magnetic field with electromagnetic waves or wireless technologies using certain frequencies results in Faraday's rotation as well. These aspects have received relatively limited attention in the literature so far; therefore, it is difficult to find related works in theory or practical experiments.

Scope of Work

The research and development target for this study are possible implementations of wireless network technologies in smart environments, analyzing their most important characteristics: technical parameters. This is performed first by listing known facts about wireless network technologies in Table 1 and plotting these values in Figures 3–8 using MATLAB software as a tool. After being visually represented and compared, the author was unable to find a clear mathematical correlation between the resulting values in graphs. However, it is obvious to conclude the parameter of security is a crucial one in establishing communication channels in IoE/IoT smart environment (Behlilovic, 2021). The novelty of this article in comparison with this paper is, therefore, subsequent analysis of security parameters. This parameter has been further discussed for its encryption techniques and their costs. In theory, every encryption technique is vulnerable. Thus, every communication channel is vulnerable as well. Minimizing exposure, to malicious activities, of receiving nodes in the communication channel is suggested by using a permanent magnet on its antenna. This interference has been analyzed using mathematical calculations, and the obtained results are presented as a formula, in which the final result depends on natural constants and different values of wavelength used for different communication protocols. The results for observed communication protocols combined with magnetic field are values presented in Table 3, with B_{res} values presented in Figure 10. This method can be used for communication protocols with modest performances, e.g., first exchanging initial information and subsequently initiating other communication protocols to establish a connection. Communication in a smart environment will therefore be improved by implementing new hardware on receiving side of the communication channel, at first upgrading its security parameter and, consequently, the other parameters as well.

This article is structured in a way such that after an introduction, the second section briefly reviews actual data transfer technologies. The first subsection of the third section concerns data transfer technologies in smart environments, while four of its subsubsections analyze the mutual correlation between listed wireless data transfer technologies, their technical parameters, and their basic characteristics. The last subsubsection compares characteristics of the frequency parameter with characteristics of other three important technical parameters (speed, distance, and security). The fourth section proposes a methodology for targeting the crucial security parameter of the communication channel by bringing the parameter of frequency into consideration, and in its subsection, presents an equation for the angle of rotation ψ. It is followed by the results in the fifth section and discussion in the sixth section, which is divided into three subsections, the first describing the new method, the second describing the existing method, and the third describing the proposed method.

REVIEW OF DATA TRANSFER TECHNOLOGIES

Communication between various devices makes it possible to provide unique and innovative services. Although this inter-device communication is a very powerful mechanism, it is also a complex and clumsy mechanism, leading to a lot of complexity in present-day systems. This not only makes networking difficult but also limits its ñexibility. Many standards exist today for connecting various devices. At the same time, every device has to support more than one standard to make it interoperable between different devices (Kumar et al., 2013). Often, as a result, there are problems with the scalability and flexibility of such solutions, resulting in their limitation in use. The reason can be found among

many different factors affecting connected devices working or increasing the complexity of such environments. The existing network management models reveal a wide variety of approaches to their construction, but there is no single model that allows network management at all levels of services, transport, and control. This is quite understandable by the difference in the principles of their level of operation and management, as a consequence of the difference in approaches to building models. (Kislyakov, 2022). An additional challenge is its development dynamics and continuous need for reconfiguration and optimization. Overcoming these challenges is inevitable in constantly raising the quality of implemented communication in the smart environment, because cities must now try to become smarter, to improve their management and systems to ensure they become more sustainable, which means that smart and sustainable city invests in human and social capital wisely, has citizens who participate in city governance, and has traditional and modern infrastructure that supports economic growth and high quality of life for its inhabitants (Peris-Ortiz et al., 2017). Similar challenges are more present in more urban environments, where approached factors have more influence. Growing and developing cities demands developing smart environments, and IoE/IoT represents the best way to make a city smart. Indeed, IoE/IoT can be applied in multiple scenarios (Hammi et al., 2018). Less urban environments can find benefits in implementing IoE/IoT solutions as well, depending on some different starting points. No matter the complexity of smart environments, there are their mutual areas of interest, which should be approached as fundamental in planning and developing smart environments. In order to approach them easier, it is possible to focus on certain segments. The development of an IoE/IoT smart environment depends on its focus and has the following three particular orientation visions: things, the Internet, and semantics (Singh et al., 2014). IoE/IoT users and consumers can be categorized into three groups:

- **Individuals:** Persons looking to improve their overall level of lifestyle.
- **Society:** A group of people (community) looking to find solutions for common tasks and issues.
- **Industry:** An economic or industry sector looking to satisfy customer needs and requirements.

Obviously, the defined user groups have diverse areas of interest, and the number of domains may vary greatly according to the level of abstraction. Future IoE/IoT solutions are expected to be targeted at: the cost of devices, battery life, physical specifications, interoperability, data processing, context awareness, coverage, scalability and diversity, reliability, attack resistance, confidentiality, integrity, and availability (Pekar et al., 2020). The existence of numerous factors affecting the decision-making process in developing smart environments results in the need for a systematic approach to dealing with such problems. Some of these factors are important only in planning and are not affected by subsequent changes, while some of them are highly more dynamic in change, and their characteristics hardly can or cannot be predicted. As a good example, we can approach data transferred among communicating nodes inside a smart environment compared to data transferring to nodes outside a smart environment.

Today, data transfer is needed everywhere, and two different data types possess different characteristics and accordingly demand different approaches when it comes to enabling communication between nodes. On this topic, sufficiently good results can be achieved using different technologies and combining them in a correct manner. The aim of transferring data, processing information with as few errors and in as little time as possible, is often upgraded with procedures considering protecting those data and connecting devices from possible malicious third-party influence. Analyzing this subject and considering all these circumstances becomes too complex for more detailed observation, so it is recommended to approach network architecture and communication channels in smaller segments. This can be done in multiple ways. It is reasonable to start making classification considering environments in which data transfer is done, so communication channels are divided into non-moving (wired) and moving (wireless) communication channels. Processes and content created during communication should not be seeing such segmentation. Interworking these access networks with

wireline technologies is a significant step toward achieving a single telecommunications network foundation. Fixed-mobile convergence (FMC) addresses this network convergence together with service convergence and device convergence in order to provide convenience and simplicity for consumers and business users to get highly featured but lower-cost communications (Ergen, 2009). No matter the integration level of different approaches and technologies, planning and developing smart environments requires the classification of different solutions to maintaining communication. A similar approach should guarantee their implementation will fulfill expectations and use IoE/IoT resources in the most optimized way. This article will further focus on wireless communication channels and protocols, also called *mobile access network technologies* (MANTs).

The written history of wireless communication, including electrical and magnetic phenomena, started couple thousand years ago with the ancient Chinese, Greek, and Roman cultures (Sarkar et al., 2006). At the start of the 17th century, digital communication developed, as a founding layer for modern wireless communication. Although younger, wireless communication has many benefits compared to wired communication, it also faces certain boundaries. These boundaries are most obvious in the security of data transfer, while on the other side is the ease of communication channel implementation. Smart devices that are within the Wi-Fi range of one another can straightforwardly convey the information, whereas others require the aid of intermediate smart devices to route their packets of information. The link is created in real-time and makes the network completely dispersed; it can work anywhere without the assistance of an access point (Alam & Rababah, 2019).

MANTs are present in technical practice in many different options, developed over time in terms of the actual level of technological advancement and user requirements, with respect to the existing network infrastructure. Some of the most-used MANTs today for data transfer include: NFC, Li-Fi, Wi-Fi, RFID, Mi-Wi, Zig Bee, Bluetooth, Z Wave, LoRaWAN, Sigfox, Wi-Max, cellular, and satellite. These technologies have their unique properties, so it is rational to analyze and compare them further. The most obvious classification is the one considering the distance between the alerted node and the node where the alert has been processed. Data transfer between these two nodes should be protected and performed with speed and at a frequency according to industrial standards and best practices. Thinking similarly leads to further classification considering the distance, security, operating frequency, and signal processing speed between two nodes in communication, respectively, two ends of the communication channel.

TECHNICAL PARAMETERS OF DATA TRANSFER TECHNOLOGIES

In the previous section, some of the most important MANTs have been enumerated, while pointing out to elucidate in IoE/IoT environment, by analyzing data transfer, it is of special importance to consider the security levels of data in transmission, speed of signal processing, operating frequency, and length of distance between the first and last network nodes in the communication observed. Inside a smart environment are numerous nodes in communication demanding individual approach and consideration in the process of planning future IoE/IoT architecture. Considering more of such requests means, in other words, the future solutions will be more customized to actual requirements. IoE/IoT is interdisciplinary in nature, implying intelligent integration of several existing technologies (Newlin Rajkumar et al., 2014). Because of differences among single communication channels, it is recommended to pay attention to as many important characteristics as possible. Regarding differences among technologies, it is worthy to prepare a review on values of their characteristics: information signal processing speed, the distance between first and last network node in communication, and basic elements of data transfer security, meaning encryption key length and operating frequency. Having observed this before proposing network architecture makes it easier to compromise between operator potentials and end user needs. Acknowledging variable differences among mentioned technologies, it is reasonable to challenge them among each other and compare their performances and characteristics, as it is presented in Table 1.

Table 1. Mobile access networks characteristics

Technology		Speed	Distance	Security	Frequency
1	NFC	< 424 kbps	< 1 m	—	13.56 MHz
2	Li-Fi	< 10 Gbps	< 10 m	256 bit	200000 GHz
3	Wi-Fi	< 54 Mbps	< 50 m	192 bit	5 GHz
4	RFID	< 100 kbps	< 100 m	128 bit	928 MHz
5	Mi-Wi	< 250 kbps	< 100 m	64 bit	2.4 GHz
6	Zig Bee	< 250 kbps	< 100 m	128 bit	2.4 GHz
7	Bluetooth	< 2.1 Mbps	< 150 m	128 bit	2.45 GHz
8	Z Wave	< 100 kbps	< 200 m	128 bit	908 MHz
9	LoRaWAN	< 50 kbps	< 10 km	128 bit	915 MHz
10	Sigfox	< 1 kbps	< 50 km	128 bit	868 MHz
11	Wi-Max	< 100 Mbps	< 50 km	168 bit	5.8 GHz
12	Cellular	< 2.6 Gbps	< 200 km	256 bit	39 GHz
13	Satellite	< 1 Gbps	> 1000 km	384 bit	14 GHz

The process of planning and implementing mobile networks is facing many challenges in considering choosing parameters suitable at the moment. Among the mentioned parameters (speed of signal processing, distance between communicating nodes, number of bits representing encryption key length, and operating frequency), the decision-making process and choosing the best option for data transfer can be influenced by factors such as implementation cost, ease of implementation, media characteristics, electromagnetic pollution. The number of parameters, as variables affecting IoE/IoT smart environment, can hardly be counted or calculated. Therefore, it is only possible to set a list of priorities at a certain moment, which can easily change over time. Having observed two, three, or more parameters raises the level of mathematics needed in representing and calculating ratios among them. This article focuses on these mentioned parameters as fundamental ones in observing data transferred.

Dynamics of processes and changes in smart environment functioning puts in focus the data observed. Relevant data for considering communication protocol implementation and designing network architecture can be analyzed by its status as such: non-movement data, data in transport, and data in use.

One of the biggest challenges for network planners is developing a good understanding of what the competitive horizon and the current traffic patterns (activity levels, loads on different sections) look like (Mattison, 1997). Solving such problems can be significantly eased by using historical records on certain activities previously preserved in databases. The existence of such records does not need to be universally usable; for instance, certain data sets cannot be used in the same or similar circumstances. Therefore, it is recommended to use localized data sets, which best describe their surrounding smart environments.

Developing specialized data transfer models is subject to advanced computing algorithms, such that, among sufficient data inputs and data sets for algorithm training, it is necessary to adjust the model to existing circumstances. Planning mobile networks is, more and more, using help and models developed by artificial intelligence, thus leaving to computer algorithms an important part of a job that once was being done by teams of experts. The implementation of such solutions is expected to incorporate past experience and knowledge of the network in the system and thus facilitate their decisions. Moreover, they are expected—and in some cases have proved their ability—to enable faster decisions that are not any more blind, in terms of not knowing the expected results. In these terms,

learning capabilities will enhance the automation of network decisions with respect to their past and the time needed to reach them.

Moving from human-handled networks to cognitive ones requires cautious and stable steps. Despite the fact that learning is capable of enhancing network decisions, applying them can turn against the network in terms of complexity. Thus, caution is needed when choosing the learning technique that will develop each type of knowledge and the respective variables that will reveal the context where the network operates (Grace & Zhang, 2012). This part of the job remains, more or less, part of experts' interest in that domain, with an awareness that job amounts will decrease and change in the future with actual trends. Obvious is the need for developing optimized communication models and using artificial intelligence models to maximize the use of existing resources as well as to predict future scenarios for smart environment development.

Data Transfer Technologies in Smart Environments

Developing smart environments at the moment has very few standards and recommendations, which leaves a lot of free space in planning and goal implementation. Certainly, one of the reasons is its actuality, while still there are numerous options for achieving similar results. The first step is to identify the object. The identification equipment should be able to recognize the features of the objects and convert them to the electronic signals which are fit for transportation. The second step is to transport the data into the information center. The last step is intelligent processing. Based on the working flow and three-layer architecture of IoT, a new extent is a six-layer architecture from the point of technology (Zhang et al., 2012). The six layers of IoT are described below (Farooq et al., 2015):

- Coding layer
- Perception layer
- Network layer
- Middleware layer
- Application layer
- Business layer

Depending on the smart environment characteristics sought, mobile network parameters are being set in order to enable regular communication of all connected devices. The network environment is highly dynamic, counting not only the geographical positions of the nomadic nodes but also the overall situation and context of each node at a given moment in time, evolving user needs and requirements due to the ad-hoc selection of user activities, and availability of communication means (including the choice of a particular method of the network connection at a given place and time and choice of an access device; Wei et al., 2013). This approach guarantees long-term functioning smart environments and fulfilling its requirements according to all parameters. The importance of parameters involved can change over time and presents an additional dimension in planning IoE/IoT environment architecture.

The most modest performance is that of NFC. This data transfer technology enables various contactless ticketing, payment, and other similar applications, storing and managing valuable and private information (e.g., credit and debit card information). The most common users are mobile network operators, banking and payment services, semiconductor producers and electronic appliances, software developers, and other merchants, including transport operators and retailers (Coskun et al., 2013). A different conclusion would be made if, additionally, device pairing speed were considered, which would put NFC (less than 0.1s) ahead of ZigBee (0.5s) or Bluetooth (6s). Among the most used communication protocols in IoE/IoT smart home environments is Z Wave. This is a low-power MAC protocol that uses wireless home automation to connect 30–50 nodes and has been used for IoE/IoT communication, especially for smart homes and small commercial domains. This technology is

designed for small data packets at relatively low speeds, up to 100 kbps, and 30-meter point-to-point communication (Al-Sarawi et al., 2017).

Irrespective of the chosen and used data transfer technologies, as well as the required distance, it is important to focus on the security aspects of such solutions. The percentage rates of affecting the layers are as follows (Podder et al., 2021):

- Application layer (9%)
- Communication layer (18%)
- Device layer (42%)
- Network layer (27%)
- Transport layer (4%)

Challenges present in this domain can be approached from a few basic perspectives. The connected devices or machines are extremely valuable to cyber-attackers for several reasons (Abomhara & Køien 2015):

- Most IoE/IoT devices operate unattended by humans; thus, it is easy for an attacker to physically gain access to them.
- Most IoE/IoT components communicate over wireless networks where an attacker could obtain confidential information by eavesdropping.
- Most IoE/IoT components cannot support complex security schemes due to low power and computing resource capabilities.

It is obvious such problems cannot be eliminated, so it is only possible to work toward minimizing their effects. A serious approach and applying modern achievements can give satisfying results, dealing with this matter continually in time. The various threats to the security of IoT are front-end sensors and equipment, network, and the back-ends of IT systems. The privacy of users and their data protection have been identified as one of the important challenges which need to be addressed in the IoTs, thus, privacy in a device, privacy during communication, privacy in storage, and privacy at processing (Sathish Kumar & Patel, 2014). Such activities affecting the regular functioning of each segment mentioned result in disrupting the regular functioning of the entire smart environment.

Parameters of Speed and Security

In the current ongoing world of IoT devices, it is absolutely vital to have a safe, secure, and reliable cyberspace, free from all sorts of unethical activities like hacked systems, data breaches, and stolen data. For that goal to be accomplished, we need to have a modern, strong, and rigid cybersecurity system so that the information and data stay safe from threats and attacks (Tahsin et al., 2021). The security of the protocol lies in the strength of the cryptographic algorithms chosen by the peers (Bonetto et al., 2012). Developing and implementing modern cryptographic algorithms is raising the security level of protected content, but on the other side, mechanisms with opposite purposes are still being developed. The cryptographic algorithm's purpose is to make transferred information unusable for its potentially malicious user, but the malicious user's target may not always be the information being transferred. For tested IoE/IoT devices, send and receive rates were sufficient for identifying user behaviors and interactions. Though devices encrypted their traffic, encryption alone did not prevent privacy vulnerabilities (Apthorpe et al., 2017a). This kind of information can be used for various attacks on a smart environment and result in many problems in its regular functioning. Signal processing speed is positively affecting communication channel security, leaving less time for a potentially malicious user to plan activities.

Observing communication channel security, the focus of this article is only on encryption key length and, subsequently, different attacks aimed at encryption algorithms. Encryption attacks depend on destroying encryption technique and obtaining the private key (Deogirikar & Vidhate 2017):

- Side-channel attacks
- Cryptanalysis attacks
- Man-in-the-middle attacks

The importance of certain data set is determining the level of its protection using various security activities, while additional security bits are affecting speed of processing signal respectively data transfer. Advanced encryption techniques with more security bits mean more bits in overall communication and therefore affect the existing costs of the implemented communication channel. Communication channel security and the security of devices in communication depend on many factors, and only in the ideal case does it depend only on the number of bits creating key length and belonging to chosen encryption technique. A longer key length, properly combined with the chosen algorithm, will encrypt information transferred better and make it more difficult for a third party to access it. Some important factors for protecting communication include the amount of memory for encryption and decryption, speed of encryption and decryption, speed of generating a key, key length, number of keys, key management, the complexity of the encryption algorithm, and exposure to attacks.

Among today's widely used algorithms, it is noticeable in sum there have been no significant breakthroughs in the last 20 years, except for combining them or multiplying the same key, which does not result in a significant overall difference. One of the main reasons is hardware architecture limitation, affecting the capability to compute in a reasonable amount of time. This puts additional focus on optimizing the choice of traffic encryption techniques.

Smart environment traffic characteristics are furthermore different. Optimizing communication channels and protecting information transferred significantly depends on the possibility of differentiating and classifying traffic involved. Following activities to examine the characteristics of IoE/IoT devices from different viewpoints and highlight their dominant attributes, enabling us to distinguish an IoE/IoT device from a non-IoE/IoT device, such as a laptop or mobile phone, and identify a certain IoE/IoT device or its category (Sivanathan et al., 2017):

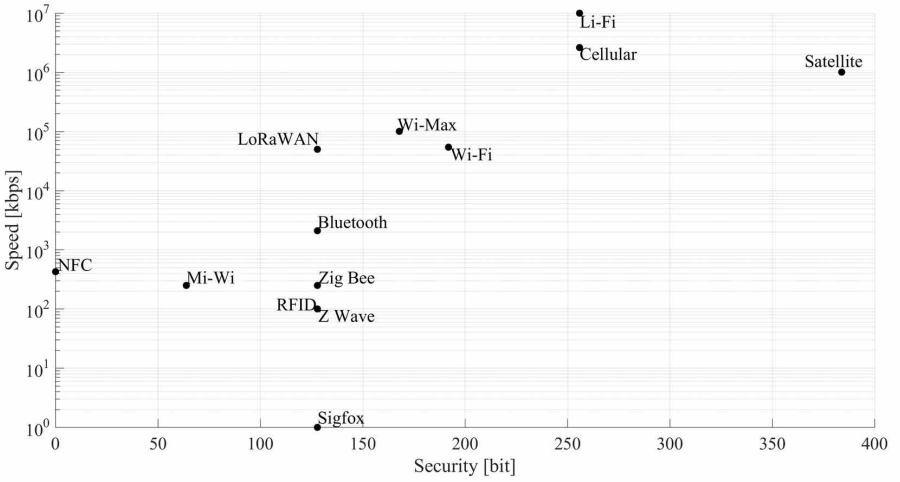
- Data traffic pattern
- Cloud servers
- Protocols
- DNS traffic
- NTP traffic

A similar approach allows different types of traffic, depending on their importance, to protect in different ways and, therefore, additionally optimize using existing resources. The existence of varieties and rising dynamics in data transfer are making the decision-making process more difficult and making it more obvious that thinking in that direction is necessary. However, studies focusing on characterizing IoE/IoT traffic—also referred to as *machine-to-machine (M2M) traffic*—are still in their infancy (Sivanathan et al., 2019), based on:

- Analysis of empirical traces
- Aggregated traffic model
- Use of machine learning

It is doubtless that involving resources of artificial intelligence can contribute in this case, but also questioning its purposefulness considering existing modest hardware and software resources, such as time for data signal processing and needed information security levels. These two parameters and corresponding values of communication protocols are shown in Figure 3.

Figure 3. Signal processing speed and communication channel security



Because of the big difference between starting and ending values of ordinate, it is represented using a logarithmic scale. The direct proportion of the two parameters can be discussed, albeit it is insufficient to maintain a clear correlation. The higher the signal processing speed is, the greater the number of encryption bits is. Unfortunately, this ratio also cannot provide a good foundation for creating a smart environment. These two parameters are equal for RFID and Z Wave and thus overlap themselves.

Parameters of Distance and Security

Smart environment implementation is a reasonable choice in many situations and most variable cases. To support real deployments, both short-range and long-range network technologies will be needed to fulfill the demands of varying network traffic types of IoE/IoT services (Pekar et al., 2018). Variety in technologies for establishing communication channels gives more opportunities and positively impacts the quality of a smart environment solution. A significant number of solutions are working only in shorter distances with lower average signal processing speed and data transfer, as a result of other factors and boundaries. In sensor-based applications, where sensors are the main end-devices (constrained in terms of memory, processing power, and battery), the proposed protocols must be lightweight, making a trade-off between power consumption and security (El-Hajj et al., 2019). Wireless sensor networks (WSNs) are geographically distributed autonomous sensors which are deployed either arbitrarily or using some predefined provision. It is used to monitor physical or environmental characteristics (Kumar et al., 2021). The presence of numerous sensors at shorter distances can negatively affect smart environment performances.

The characteristics of each node in communication and the need for interaction with other nodes determine its position in IoE/IoT environment, with position possibly being changed over time. In order to determine the distance between communication nodes, it is necessary to locate them first.

Traditional location technologies such as GPS cannot be used in wireless sensor networks (WSNs) directly, because of costly requirements of sophisticated equipment and high energy consumption, which have greatly constrained the application scale of WSNs (Chen et al., 2011). Many localization algorithms have been developed in WSNs, all of which can be roughly categorized as range-based localization or range-free localization. Range-based localization always has two phases: *ranging* and *position computation*. In the first phase, it uses a ranging method such as time of arrival (TOA), time difference of arrival (TDOA), angle of arrival (AOA), or received signal strength indicator (RSSI) to obtain the distance between two nodes—always a blind node at an unknown position and reference nodes (also called *beacon nodes*) with known positions (Huang et al., 2010). Calculating the distance between nodes can be time-consuming. Smart environments consisting of dynamically reconfiguring networks or networks in movement over time can experience more challenges compared to those consisting of networks persisting in a static configuration.

No matter the distance between nodes in communication, they need to be identified. IoE/IoT enables various devices and objects around us to be addressable, recognizable, and locatable, but at the same time, this opens the possibility of experiencing misuse or attack. There are four main types of attack in the IoE/IoT system: physical, software, network, and encryption attacks (Atlam & Wills, 2020). Experiencing IoE/IoT attacks represents a calculated risk; therefore, attention should be paid so that implementation is not more harmful than useful. Undergoing attacks on IoE/IoT infrastructure usually come in some patterns, and after a certain amount of time, it is possible to identify IoE/IoT attack models and the learning-based IoE/IoT security techniques, including the IoE/IoT authentication, access control, malware detection and secure offloading, which are shown to be promising to protect IoE/IoTs (Xiao et al., 2018). Among these two options, a balance should be achieved and maintained through time. A longer distance between nodes in communication leaves more space for malicious users and their potential to endanger safe communication principles.

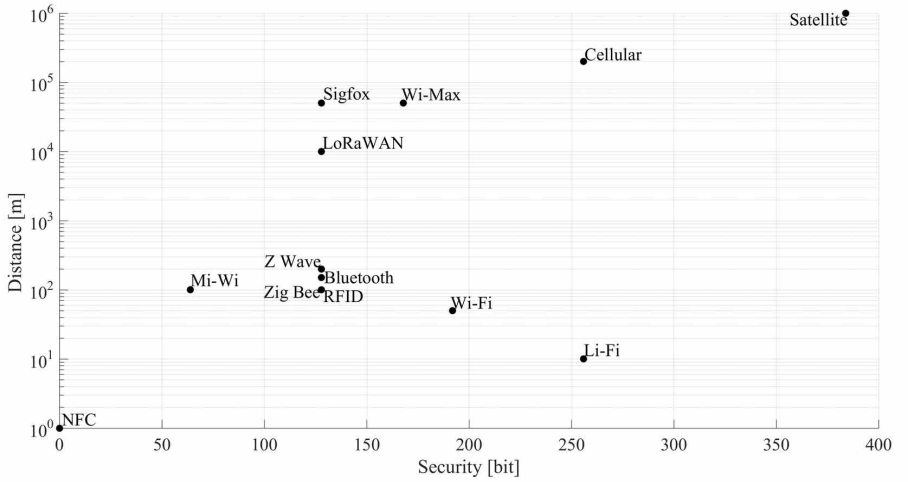
Different types of traffic between two ends of the communication channel, along with devices used for referring purposes, are not affected by their distance. Along with the rapid growth of IoE/IoT applications and devices, cyber-attacks will also be improved and pose a more serious threat to security and privacy than ever before (Zhou et al., 2019). For different traffic types and different device types, it is reasonable to ensure different types of encryption. Traffic shaping that adds 60 kbps bandwidth overhead is enough to mask non-audio/video devices like smart outlets, while traffic shaping that adds 320 kbps bandwidth overhead is enough to mask these data-intensive devices with a high level of performance (Apthorpe et al., 2017b). A larger number of encryption bits along with an adequate encryption algorithm enable a higher level of encryption for information in transfer. On the other hand, this is not always possible to achieve. Various technical difficulties, such as limited storage, power, and computational capabilities, hinder addressing IoE/IoT security requirements, enabling a myriad of vulnerable IoE/IoT devices to reside in the Internet space. Moreover, the insufficiency of IoE/IoT access controls and audit mechanisms enables attackers to generate IoE/IoT-centric malicious activities in a highly stealthy manner (Neshenko et al., 2019). The need for optimizing the use of existing resources is expressed once more, in order to provide the best possible solutions. The observed technologies are presented in Figure 4, according to their characteristics.

Because of the big difference between starting and ending values of ordinate, it is again represented using a logarithmic scale. Considering the observed values, it is not possible to make a mutual correlation of these parameters, except as it is done in the graphic. This ratio results in difficulties in planning a smart environment, as in the previously mentioned case. Single data transfer technology can often use different encryption key lengths, despite this is not always possible. Parameter values for Zig Bee and RFID are identical, and therefore, they overlap in the graph.

Comparing Parameters of Speed, Distance, and Security

The variety of traffic types in a smart environment results in the use of various communication protocols in order to transfer data. Different criteria are used to compare the communication protocols.

Figure 4. Communication nodes distance and communication channel security



Such criteria include network, topology, power, range, cryptography, spreading, modulation type, coexistence with mechanism, and power consumption (Al-Sarawi et al., 2017). Many attacks generally exploit weaknesses in specific devices, thereby gaining access to their systems and consequently making secure devices weak. This security gap further motivates comprehensive security solutions that consist of research that is efficient in applied cryptography for data and system security, non-cryptographic security techniques as well as frameworks that assist developers in coming up with safe systems on devices that are heterogeneous (Hussein, 2019). Choosing critical characteristics can provide better choices when selecting a communication protocol, paying attention to the type of traffic. In a general-purpose network, most activity will be generated by smartphones or laptops (Shahid et al., 2018).

The most modest in entitled parameters are WSNs, but even as such, they can be useful in certain domains if not too demanding with some other parameters. WSNs may consist of many different types of sensors, including seismic, magnetic, thermal, visual, infrared, acoustic, and radar, which are able to monitor a wide variety of ambient conditions including: temperature, humidity, pressure, speed, direction, movement, light, soil makeup, noise levels, the presence or absence of certain kinds of objects, and mechanical stress levels on attached objects. As a result, a wide range of applications is possible. The major challenge for the proliferation of WSNs is energy (Akyildiz & Vuran, 2010). Therefore, WSN networks are not useful in situations requiring substantial and variable resources, also meaning more investments in smart environment infrastructure.

More complexity in observed parameters can be noticed approaching cellular and ad-hoc networks. This type of network is capable of supporting much more complex devices and communication. Unlike a cellular network, an ad hoc network is a collection of wireless mobile nodes (or routers) dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably (Kumar et al., 2013). Both types find wide applications depending on their detailed characteristics. On the other side, the complexity of smart environments is sufficiently big to recognize both types and the benefits of their use. Some important differences between cellular and ad-hoc wireless network characteristics are listed in Table 2.

When choosing technologies, companies make decisions based on costs, benefits, and performance reports. Securing data and digital services is a cost that businesses need to pay in the digital era, and protecting IoE/IoT devices will increase that cost as more security risks need to be taken into account

Table 2. Cellular and wireless ad-hoc networks characteristics

Cellular Networks	Ad-Hoc Wireless Networks
Infrastructure network	Infrastructure-less network
Fixed, pre-located cell sites and base station	No base station and rapid deployment
Static backbone network topology	Highly dynamic network topologies with multi-hop
Relatively caring environment and stable connectivity	Hostile environment (noise, losses) and irregular connectivity
Detailed planning before base station can be installed	Ad-hoc network automatically forms and adapts to changes
High setup costs	Cost-effective
More setup time	Less setup time

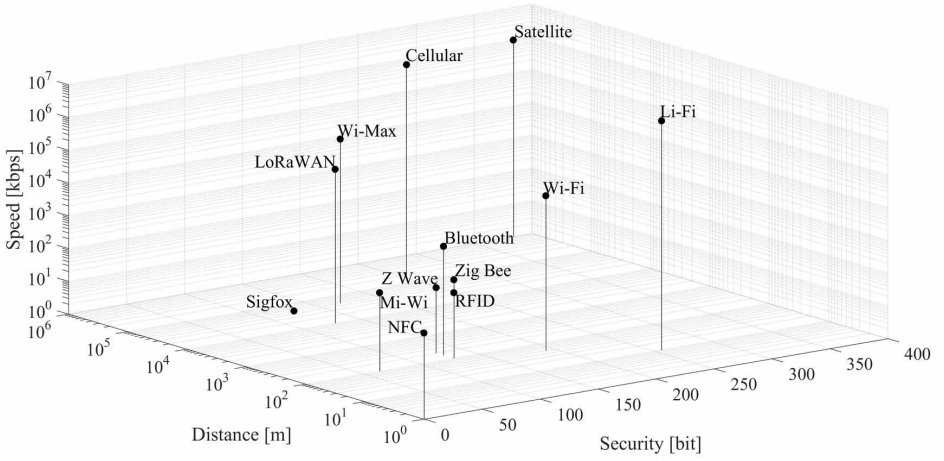
(Zamfiroiu et al., 2020). It is obvious as evidence the presence of smart environments is increasing, so it is reasonable in its very beginning to pay attention to its long-term planning process. This way, it is possible to ensure the long-term development of IoE/IoT environments and their continual upgrades.

Numerous challenges are facing smart environment implementation, and this article mentions only the technical aspects. The main challenge of smart grid implementation is the communication of heterogeneous distributed elements (Tightiz & Yang, 2020). Their communication can usually be implemented through numerous nodes in communication and the use of numerous communication protocols. All mentioned technologies are capable of coexisting and functioning in heterogeneous networks. The basic concept behind heterogeneous networks is the seamless integration and interoperation of different wireless access technologies in order to increase the system performance and energy efficiency both at the operator's and the user's side. To that end, the development of low-power micro-base-stations (e.g., femto-size, pico-size, and Wi-Fi) inside the coverage area of macro base stations (e.g., LTE and WiMAX) contributes in both directions: The traffic load balancing to different base stations implies better resource allocation and utilization and the use of low power short radio links leads to enhanced energy efficiency in the network (Rodriguez, 2015). Everything mentioned contributes to better-optimized the functioning of smart environments but also requests continual monitoring, coordinating, and upgrading. Different technologies functioning in the same network and overlying their frequency spectrum involve meeting some additional requirements. The most important requirement for functional heterogeneous mobile networks, such as WLAN, LTE, and WiMAX, is efficient handoff mechanisms to guarantee seamless connectivity (Nithyanandan & Parthiban, 2012). Having all these different technologies and their various parameters on one network requires advanced levels of mathematics in order to understand it.

After considering the characteristics of three parameters, individually and paired, it is reasonable to put their values in a three-dimensional graph, as has been done in Figure 5.

Showing these three parameters together, the resulting graph becomes more complex and gives better insight into possibilities of choice. At the same time, it is not enabling the establishment of solid mutual correlations, as discussed regarding the previous two figures. Parameter values for communication node distance and signal processing speed are noticeably grouped in two groups each, especially if logarithmic scales are considered. Communication channel security is represented only with the most commonly used values for each communication protocol and, therefore, shows very few options for consideration, which might change in the future, with the presence of advanced quantum cryptography algorithms. The starting point in establishing communication between nodes is the character of data transmitted. Determining that can be significantly eased by using high-quality databases and artificial intelligence models previously trained with those data sets. An analogous approach can result in the meaningful preservation of time and other important disposable resources.

Figure 5. Signal processing speed, communication nodes distance, and communication channel security



The importance of particular data is determining the level of security, thus the encryption algorithm, and finally, the number of bits for encryption of information during its transfer. Afterward, it is important to resolve the distance between nodes in communication and possibly patterns of their allocation or relocation. Subsequently, attention should be given to the signal processing speed, which can be affected by the previous two parameters, maximizing the security level of data protection and respecting the distance between ends of the communication channel. After these three fundamental parameters, all the others should follow (such as frequency and mobility).

The communication protocols addressed here were developed over long periods of time, and they did not follow systematic approaches needed for the smart environments of the future. Working on continuous improvement of this smart environment segment with a systematic approach remains the final unachievable destination.

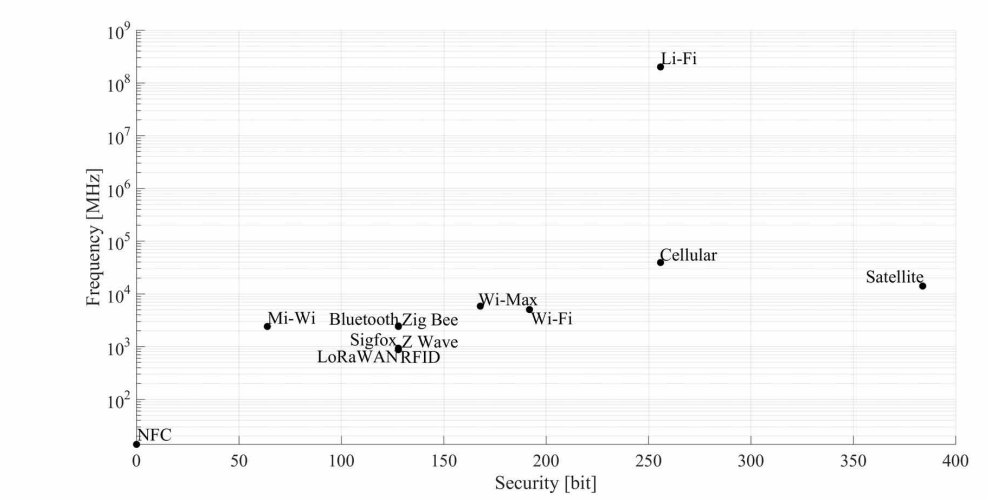
Parameters of Frequency and Security

The smart grid infrastructure is said to be smart in operation only when it is full proof from all kinds of cyber-attacks (Pal et al., 2021). Establishing a communication channel starts with determining the character of data, followed by deciding which level of security is needed for data transfer and afterward securing it with one or multiple encryption algorithms. Security is the main concern across the people, data, process, and things and needs to be ubiquitous as the IoE. Therefore, the security solutions must protect the devices, applications, networks, data, users, and things that make up the IoE and these systems work collaboratively and smartly with each other and perform the desired task (Rajiv, 2021). Security has traditionally been implemented at the higher, logical layers of communication networks, rather than at the level of the physical transmission medium (Poor & Schaefer, 2016). This approach should be enhanced and complemented beyond encryption algorithms only. Recent advances in quantum computing pose a serious threat to the currently used cryptographic schemes with their unlimited computational capacity. Therefore, it is evident that the conventional methods of secure wireless communication are becoming less reliable (Sanenga et al., 2020). So far, all encryption algorithms have been broken—or eventually will be, and thus, communication could have been compromised or will be in the future. At this moment, it is impossible to guarantee security with the encryption algorithms presently used and claimed to be unbreakable when securing communication between distant nodes. Therefore, it is not serious about guaranteeing that any algorithm completely

protects information in transfer. It would be reasonable to discuss it with terms such as *highest possible* and *best effort*, because one's limitation in understanding those principles does not have to affect others and stop them from being more advanced in thinking or faster in processing. The most secure communication would be one that does not exist, but in this context, it might be obscure or even considered a paradox.

With careful management and implementation, physical layer security can be used as an additional level of protection on top of the existing security schemes (Wu et al., 2018). When trying to govern created and protected communication channels and disable the possibility of being impacted by another entity, it could be an advancement to incorporate elements that cannot be affected by a foreign entity because of ubiquitous laws of nature. Everything encrypted by a human can also be decrypted by a human, but decryption in complete is impossible if encryption is done not by a human but by nature itself. Even though it might be weird when trying to govern something invisible, final results can be predicted correctly if the nature of that invisible is well known. Radiation of electromagnetic spectrum follows the same principles of electromagnetic wave propagation, while differentiating only in its frequency (Cindro, 1985). Combining values of frequency and number of security bits for previously mentioned communication technologies results in intersecting points, represented in Figure 6.

Figure 6. Frequency and communication channel security



Replacing the parameter of speed in Figure 5 with the parameter of frequency would result in Figure 7.

If the parameter of speed replaces the parameter of distance in Figure 7, the result is shown in Figure 8.

Because of the big difference between starting and ending values of ordinate, it is again represented using a logarithmic scale in Figures 6–8. The direct proportion between parameters in Figure 6 can be discussed, albeit it is again insufficient to maintain a clear correlation. The higher frequency, the bigger the number of encryption bits, with the exception of satellite communication. Groups of six, or more precisely, groups of two and four parameter values, are close or overlapping (Bluetooth and Zig Bee on one side, and on the other side LoRaWAN, RFID, Z Wave, and Sigfox). Adding parameter of distance results in Figure 7, where intersecting values of parameters are set in two groups (or three if NFC is considered), divided by their

Figure 7. Frequency, communication nodes distance, and communication channel security

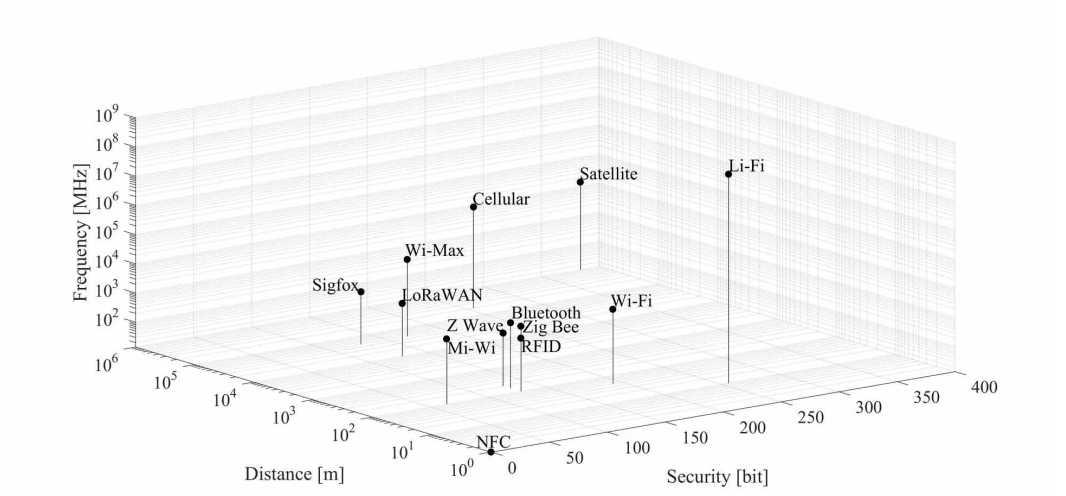
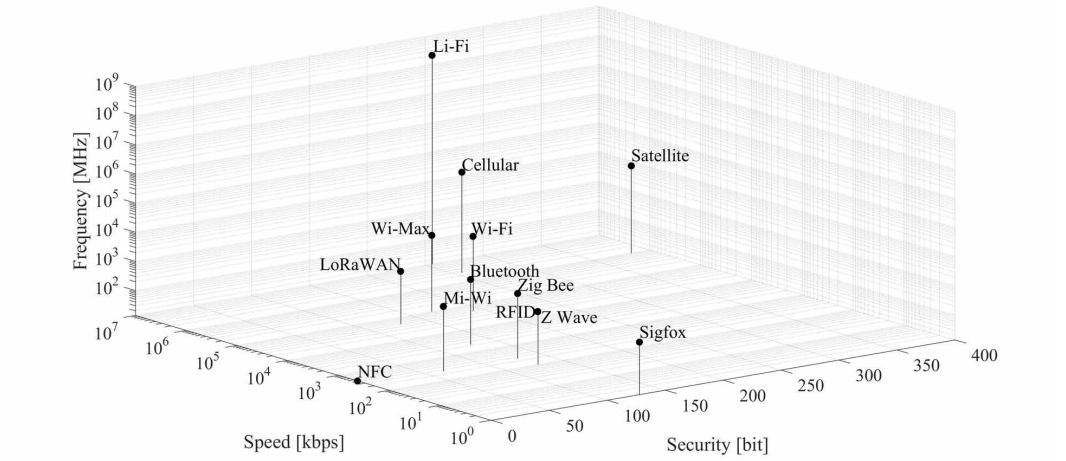


Figure 8. Frequency, signal processing speed, and communication channel security

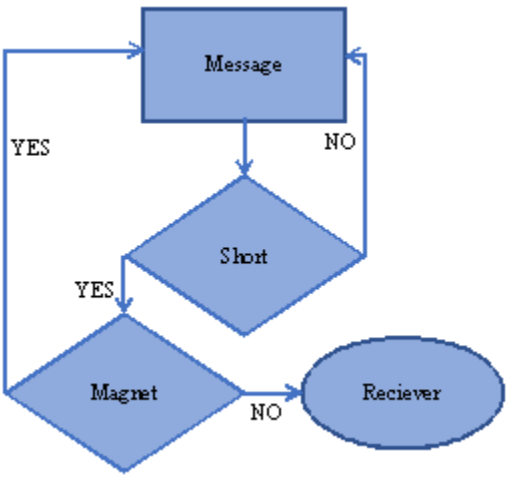


distance parameter. Considering both groups, a noticeable increase in frequency is followed by an increase in the number of security bits and vice versa, as in Figure 6. The parameter of distance does not provide any obvious correlation with the other two parameters. Replacing the parameter of distance with the parameter of speed results in Figure 8. Higher values of signal processing speed are followed by values of both frequency and security bits. The same conclusion can be made if two other parameters were taken as a starting point. Although it cannot be expressed with a simple formula, there is an obvious correlation between the parameters observed. Changing one of them would affect the values of the other two parameters represented above.

METHODOLOGY

Wireless networks provide flexible, ubiquitous user communications but, at the same time, provide the same access to an attacker or eavesdropper trying to intercept private messages. Hence, security has become a primary concern in wireless networks, and there has been a resurgence of interest in physical layer forms of secrecy based on Shannon's original information-theoretic formulation and Wyner's consideration of the wiretap formulation of such (Goeckel et al., 2014). Depending on frequency is the design of devices on both sides of the communication channel, transmitting and receiving. In radiocommunication, a common name for a device that transmits or receives electromagnetic waves is *antenna* (Haznadar & Štih, 1998). At the receiving side of the communication channel, the main function of an antenna is to capture electromagnetic waves propagating through space and prepare them as a signal fed to the input of the first stage of the radio frequency amplifier. The reality is if the signal of interest is not captured and available for processing at the input of the first stage of the RF amplifier, then signal processing techniques cannot recreate that signal (Sarkar et al., 2018). Disturbing electromagnetic wave paths to the antenna results in compromising the information being transferred or at least slowing signal processing speed. Protecting implemented wireless communication channel by disturbing its synchronization in periods when there is no need for active communication can improve its security parameters and guard it against attacks performed by malicious users. This can be achieved by blocking or by degrading the quality of electromagnetic waves from receiving antennas and augmenting conventional cryptographic methods. The hypothesis in this article concerns the possibility of affecting data in transport, electromagnetic waves with Faraday's rotation, caused by using a permanent magnet on the receiving node in a communication channel. The mathematical model reflecting the hypothesis is presented and explained in the following subsection. The proposed method is described in Figure 9.

Figure 9. Proposed method with magnet for possible Faraday's rotation



The level of signal degradation is proportional to additional noise created with implemented permanent magnet and its magnetic field. Future research directions include new and more effective smart beamforming and artificial noise techniques (Cepheli & Kurt, 2013).

Faraday's Rotation and the Angle of Rotation

In the second half of the 19th century, scientists were highly interested in electromagnetic field phenomena. The academic community did not have an explanation for the nature of light as much as it is explained today. Therefore, intersecting these two areas led to many experiments being conducted and results documented. Michael Faraday's thoughts and experiments had special attention, and he is still remembered as one of the leading experimenters in the history of physics (Ilic et al., 2012).

Arguably the most important and far-reaching implication of Maxwell's equations is the idea that electric and magnetic effects can be transmitted from one point to another through the intervening space, whether that be empty or filled with matter (Inan & Inan, 1999). Not only is intervening space important here but also everything affecting space, its emptiness or fulfillment. Therefore, it is reasonable to calculate with materials whose characteristics can be involved in this process, affecting the signal-to-noise ratio. A magnetic field affects different materials through different surroundings in a variable way, due to structural and magnetic characteristics (Mills Purcell, 1965). This can lead to numerous calculations, considering variable combinations of surroundings and materials.

No matter their values and the electromagnetic wave characteristics mentioned in previous sections, all of them obey the same laws and thus can be observed with a unique mathematical approach. Observing wave propagation through ionized gas in the direction and influence of the magnetic field, which is assumed to be homogeneous and constant in time, it can be concluded there is Faraday's rotation (Popovic, 1980). The resulting angle is called the angle of rotation (Faraday's rotation) and grows along the z-axis:

$$\psi = \omega\sqrt{\mu_0}\left(\sqrt{\varepsilon_r} - \sqrt{\varepsilon_l}\right)\frac{z}{2} = \pi f\sqrt{\mu_0}\left(\sqrt{\varepsilon_r} - \sqrt{\varepsilon_l}\right)z = \pi\frac{c}{\lambda}\sqrt{\mu_0}\left(\sqrt{\varepsilon_r} - \sqrt{\varepsilon_l}\right)z \tag{1}$$

where ε_r and ε_l are representing permeabilities for right and left wave polarization, while z is the plane of polarization.

RESULTS

By definition, the Faraday's angle is positive for counterclockwise rotation when the magnetic flux density vector has the same direction as the wave vector and for clockwise rotation when these vectors are in the opposite direction. Therefore, the Faraday's effect is truly a nonreciprocal effect, and the Faraday's angle will double after the light is reflected and goes back along the same path (Mihailovic & Petricevic, 2021). As it has been previously shown, Faraday's effect depends on multiple constants and variables. Adding more complexity to Equation 1 by supplementing these constants and changing variables is possible in order to achieve certain calculations, according to necessities in smart environment communication. However, it is also possible to simplify this equation in order to determine starting points in those calculations.

Observing previous Equation 1, and if some of its values can be assumed as in the following expression:

$$\varepsilon_r \simeq \varepsilon_l \simeq \varepsilon_0 \tag{2}$$

Using Equation 2, then $\sqrt{\varepsilon_r}$ and $\sqrt{\varepsilon_l}$ can be further developed with binomial expansion, leading Equation 1 to resulting equation (Popovic, 1980):

$$\psi \simeq \sqrt{\varepsilon_0 \cdot \mu_0} \cdot \frac{Q^2}{2 \cdot m \cdot \varepsilon_0} \cdot \frac{\omega_0}{\omega^2 - \omega_0^2} \cdot N \cdot z \tag{3}$$

In order to answer the research question, it is reasonable to approach electromagnetic waves of different frequencies *f* with the magnetic field of different strength *B* and write down the results of their interference. The resulting values of Equation 3, using previously observed electromagnetic waves values and corresponding values of the magnetic field are presented in Table 3.

The novelty of this approach can be emphasized by analyzing the values presented above, with assumed values for $N = 1$ and $z = 1$, so several conclusions can be made. Among the most interesting facts is that, in 11 out of 13 communication protocols, changing the strength of the magnetic field values listed in the table results in an alternation of the sign in front of the final result. These values are highlighted in the middle rows of Table 3. Thus, it is interesting to calculate the strength of the magnetic field B_{res} when alternation is actually happening, where $\omega_0^2 \approx \omega^2$ and ψ is at its maximum value. Maximizing ψ is important because, no matter the sign, it maximizes influence on the process of communication. With possible multiple and frequent alternations of the sign, this influence would be even more obvious and, therefore, would affect processes in communication channels the most,

Table 3. Resulting values for ψ with listed values of B_0 and *f* and assumed values for *N* = 1 and *z* = 1

Angle of Rotation (ψ)		Frequency *f* (Hz)				
		NFC	Sigfox	Z Wave	LoRaWAN	RFID
		13.56 MHz	868 MHz	908 MHz	915 MHz	928 MHz
Magnetic Field B_0 (T)	1 µT	1.28611E-16	3.13873E-20	2.86829E-20	2.82457E-20	2.74598E-20
	5 µT	6.43118E-16	1.56937E-19	1.43414E-19	1.41228E-19	1.37299E-19
	10 µT	1.28665E-15	3.13873E-19	2.86829E-19	2.82457E-19	2.74598E-19
	50 µT	6.49975E-15	1.56937E-18	1.43415E-18	1.41229E-18	1.373E-18
	100 µT	1.34335E-14	3.13877E-18	2.86831E-18	2.82459E-18	2.74601E-18
	500 µT	-9.83589E-13	1.56978E-17	1.43448E-17	1.41261E-17	1.3733E-17
	1 mT	-3.94326E-14	3.142E-17	2.87101E-17	2.82721E-17	2.74849E-17
	5 mT	-6.09308E-15	1.61126E-16	1.46905E-16	1.44612E-16	1.40495E-16
	10 mT	-3.02504E-15	3.50306E-16	3.16952E-16	3.11622E-16	3.02085E-16
	50 mT	-6.03645E-16	-9.80817E-16	-1.04223E-15	-1.05409E-15	-1.0771E-15
	100 mT	-3.01801E-16	-3.33899E-16	-3.37282E-16	-3.37897E-16	-3.39058E-16
	500 mT	-6.03589E-17	-6.05919E-17	-6.0614E-17	-6.06179E-17	-6.06254E-17
	1 T	-3.01794E-17	-3.02085E-17	-3.02112E-17	-3.02117E-17	-3.02126E-17
Magnetic field B_{res} [T]		0.000484416	0.031008317	0.032437272	0.032687339	0.033151749

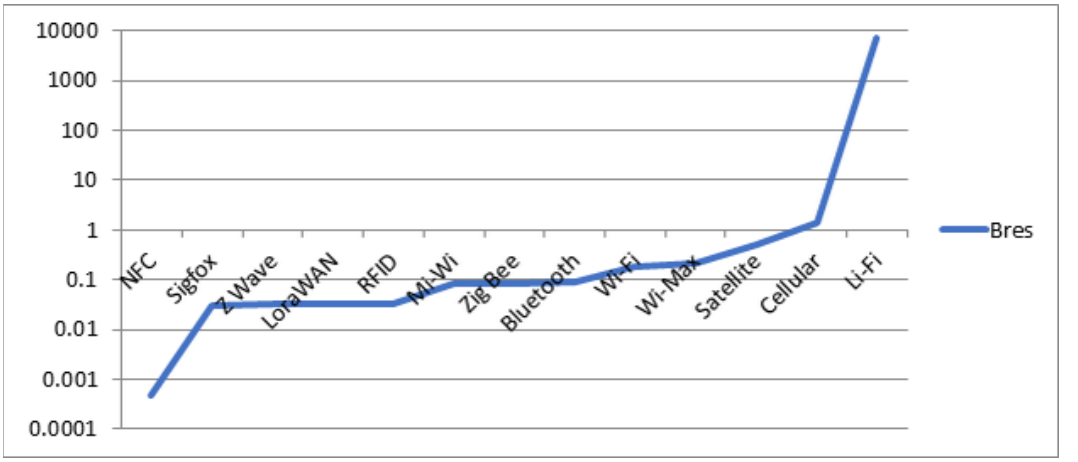
continued on following page

Table 3. Continued

Angle of Rotation (ψ)		Frequency f (Hz)				
		Mi-Wi	**Zig Bee**	**Bluetooth**	**Wi-Fi**	**Wi-Max**
		2.4 GHz	**2.4 GHz**	**2.45 GHz**	**5 GHz**	**5.8 GHz**
Magnetic Field B_0 (T)	1 µT	4.10555E-21	4.10555E-21	3.93969E-21	9.45919E-22	7.02972E-22
	5 µT	2.05278E-20	2.05278E-20	1.96984E-20	4.7296E-21	3.51486E-21
	10 µT	4.10555E-20	4.10555E-20	3.93969E-20	9.45919E-21	7.02972E-21
	50 µT	2.05278E-19	2.05278E-19	1.96984E-19	4.7296E-20	3.51486E-20
	100 µT	4.10556E-19	4.10556E-19	3.93969E-19	9.45919E-20	7.02972E-20
	500 µT	2.05285E-18	2.05285E-18	1.96991E-18	4.72963E-19	3.51488E-19
	1 mT	4.10611E-18	4.10611E-18	3.9402E-18	9.45949E-19	7.02988E-19
	5 mT	2.05978E-17	2.05978E-17	1.97629E-17	4.7333E-18	3.51691E-18
	10 mT	4.16217E-17	4.16217E-17	3.9918E-17	9.48893E-18	7.04613E-18
	50 mT	3.11072E-16	3.11072E-16	2.92416E-16	5.13171E-17	3.7322E-17
	100 mT	-1.13923E-15	-1.13923E-15	-1.28992E-15	1.37775E-16	9.16439E-17
	500 mT	-6.21874E-17	-6.21874E-17	-6.22668E-17	-6.91887E-17	-7.28729E-17
	1 T	-3.04029E-17	-3.04029E-17	-3.04124E-17	-3.1174E-17	-3.15332E-17
Magnetic Field B_{res} (T)		0.085737282	0.085737282	0.087523475	0.178619338	0.207198432
Angle of Rotation (ψ)		Frequency f (Hz)				
		Satellite	**Cellular**	**Li-Fi**		
		14 GHz	**39 GHz**	**200000 GHz**		
Magnetic Field Bo (T)	1 µT	1.20653E-22	1.55477E-23	5.91199E-31		
	5 µT	6.03265E-22	7.77383E-23	2.956E-30		
	10 µT	1.20653E-21	1.55477E-22	5.91199E-30		
	50 µT	6.03265E-21	7.77383E-22	2.956E-29		
	100 µT	1.20653E-20	1.55477E-21	5.91199E-29		
	500 µT	6.03265E-20	7.77383E-21	2.956E-28		
	1 mT	1.20653E-19	1.55477E-20	5.91199E-28		
	5 mT	6.03325E-19	7.77393E-20	2.956E-27		
	10 mT	1.20701E-18	1.55485E-19	5.91199E-27		
	50 mT	6.09355E-18	7.78385E-19	2.956E-26		
	100 mT	1.25677E-17	1.56282E-18	5.91199E-26		
	500 mT	1.12473E-13	8.92306E-18	2.956E-25		
	1 T	-4.02464E-17	3.20685E-17	5.91199E-25		
Magnetic Field B_{res} (T)		0.500134145	1.393230833	7144.773504		

manipulate and govern them. This key finding of the article can strongly support its previous hypothesis concerning the possibility of affecting data in transport, electromagnetic waves with Faraday's rotation, caused by using a permanent magnet on the receiving node in a communication channel. The resulting values for angle v ψ , located on both sides of the B_{res} values, are following predictable progression or regression, especially for higher frequency communication protocols. There is an obvious disturbance in these predictabilities around the values of B_{res} for all observed communication protocols, and it is more obvious and in larger value range with cases of lower frequency. Observing these values with the same time limitations, higher frequencies allow these protocols to be more complex in terms of their various other parameters and their modulation type. This further puts focus on low-frequency communication protocols as the area of interest for Faraday's rotation. The resulting B_{res} values for different communication protocols, highlighted in the bottom rows of Table 3, are presented in Figure 10.

Figure 10. Different B_{res} values for different communication protocols



These results suggest the starting values for frequency f and magnetic field B_0 should be chosen according to potentials and expectations for communication channels regarding three important technical parameters (signal processing speed, communication nodes distance, and communication channel security). Different values for N and z can also be selected in order to give a contribution to manipulating and governing communication channel characteristics and the whole communication process.

DISCUSSION

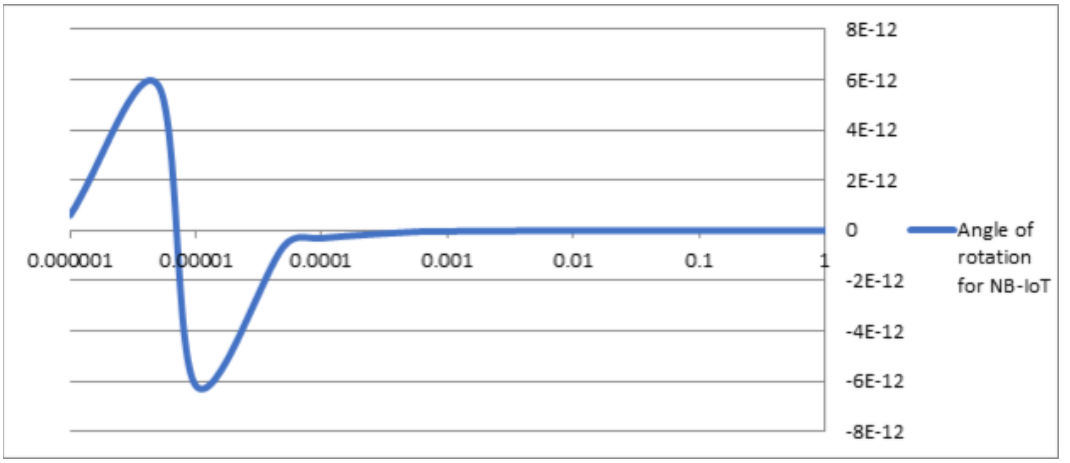
Approaching electromagnetic waves with appropriate permanent magnetic fields can result in important changes to their nature and can be further exploited. Faraday's rotation is directly affecting the electromagnetic wave's phase velocity, which is defined as a product of wavelength and frequency, that is among amplitude recognized by receiving antenna for the purpose of signal decoding. Potential application scenarios for Faraday's rotation in smart environments are numerous, because it is applicable with various frequencies representing communication technologies with different characteristics, therefore can be useful to improve existing security

standards and overall communication. Some similar effects might be achieved with a Faraday cage or Faraday shielding, but they would surely be significantly less governable and not scalable at all. Moreover, it can be bypassed using low-frequency magnetic fields, as has been discussed in Guri (2021) and Guri et al. (2019). When it comes to the number of bit rates, it is also important to notice that the loss of intelligibility is not as severe for high-bit-rate coders as for low-bit-rate coders (Martin et al., 2004). In any case considered, good antenna design is necessary to maintain good signal strength and to improve high-speed Internet from weak Internet speed in required applications (Saravanan & Sudhakar, 2020).

New Method

In the previous section, approaching different frequency values resulted in presenting a wide range of corresponding B_{res} values. There is a direct proportion manifesting in higher frequency communication protocols demanding higher values of B_{res} which are not desirable in smart environments with modest resources. On the contrary, there are lower frequency communication protocols demanding lower values for B_{res} which can be easily implemented in smart environments. Lower frequency communication protocols are the founding layer for implementing principles for governing security parameters by using permanent magnets in order to produce Faraday's rotation and decrease the signal-to-noise ratio. Among presented values, nor Table 3 nor Figure 10 present results for NB-IoT, a widely popular wireless technology standard in IoE/IoT smart environments that is fast-growing in presence. Its operating frequency of 200 kHz would result in a B_{res} value of 7.14477 μT. This value is clearly visible in Figure 11, which presents intersecting points of approached magnetic field B_0 values and resulting angle of rotation ψ values for NB-IoT frequency.

Figure 11. Angle of rotation values for different values of the magnetic field approaching NB-IoT



All things considered, numerous pairings could be made, and all further calculations should be done following various other parameters in planning smart environments.

Existing Method

On the other side is the noise reduction preprocessor for optimal enhancement algorithms for the various parameters found, operating in the frequency domain. Their role in the communication system is the opposite of the method proposed in this article. In this scenario, higher security standards for

communication channels do not rely on human intervention. Anomaly detection systems are based on machine learning, data mining, or statistical algorithms. These systems use a "normal behavior" model for detecting unexpected behavior. These approaches fall under two categories: *supervised methods*, which make use of pre-existing knowledge, and *unsupervised methods*, which do not make use of this knowledge (Shon & Moon, 2007). Supervised learning methods imply the presence of a database that consists of a certain number of different samples, each of which is characterized by its own set of features and the corresponding class. This database is divided into a training and test sequence. The training sequence is used to build a classifier or regressor model, and the test sequence is used to evaluate it. During testing, the algorithm's efficiency is checked by comparing the predicted values and the true classes. Supervised learning methods are fast and accurate but can only predict classes known to the model initially. For unsupervised learning methods, class values are not defined, which complicates the task and reduces prediction accuracy, but it is possible to detect new classes (Deart et al., 2022). Implementing such resources can be expensive and demanding in previously analyzed technical parameters and difficult to achieve in IoE/IoT smart environment. Clearly, future networks will have to support explosive growth in traffic volume and connected devices, to provide exceptional capabilities for accessing and sharing information. The unprecedented scale and degree of uncertainty will amplify the complexity of traffic engineering tasks, such as congestion control, traffic prediction, classification, and routing, as well as the exposure to faults and security attacks. Although machine learning solutions have shown promising results in addressing many traffic engineering challenges, their scalability needs to be evaluated with the envisioned volume of data, number of devices, and applications. On the other hand, existing machine learning approaches for fault and security management focus mostly on single-tenant and single-layer networks. To develop the fault and security management framework for future networks, existing machine learning approaches should be extended or re-architected to take into account the notion of multi-tenancy in multi-layer networks (Boutaba et al. 2018). Adding more advanced technological achievements into network and communication channels does not automatically make it better. All improvements need to respect starting and very basic principles, and only after integrating some additional value if possible. Critical infrastructures such as wireless network systems demand dependability, which addresses attributes of availability, reliability, maintainability, and survivability (ARMS). Given a variety of reliability and maintainability attribute scenarios for wireless infrastructure, the resulting impacts on network availability and survivability are determined (Snow et al., 2005).

Proposed Method

However, both of these scenarios are looking towards the same final objective: secure communication channels. What is surely different is the approach, and therefore they differ in implementation cost and ease of implementation in the first place. The passive attacks lay a foundation for later launching an active attacks either against the wireless network resources or end-users nodes (Khan et al., 2008). Cryptographic power costs are high, and such operations shall be restricted in time. The use of cryptographic algorithms in network protocols, especially multi-hop protocols, introduces an important overhead due to the network interface costs during waiting times. The problem is not so in computationally cryptographic costs but the total protocol completion time that involves notorious energy consumption (Rifa-Pous & Herrera-Joancomartí, 2011). Embedded systems are generally prone to security risks, since they are often in the possession of potential adversaries in large amounts. In the context of wireless technology some special threats evolve or are of particular importance. For example, copying a mechanical key premises physical access to the key or at least to the door lock. In contrast, circumventing a contactless system may be possible from a distance and without leaving any physical traces (Kasper et al., 2012). An important fact to observe is communication nodes are becoming more and more mobile or even constantly in movement, and thus it is wise to implement only simple and modest solutions. The proposed method considers receiving node of the communication

channel (see Figures 2 and 9), which is more often in movement (i.e., drones). Existing (active security) methods and algorithms would not be completely replaced with the proposed (passive security) method but complemented at the receiving node of the communication channel. This approach could be, for example, used only for the initial process of authentication and authorization but, once configured properly, could secure receiving node of the communication channel in a way no known algorithm can do at this moment, implementing security advancements at its physical layer, or even below, it might be said at the zero-layer. Thus, passive security method would be protecting communication channel even if inactive. Communication nodes secured on this level of security using a permanent magnet and Faraday's rotation can be useful predominately in one-time or part-time communication channels over permanent communication channels. Those communication channels would be preferably short-ranged ones, with the potential to establish long-ranged communication channels if needed or once security tests passed (i.e., AAA). Short-ranged communication channels for this purpose can be found in both the licensed and non-licensed spectrums. The presence of appropriate Faraday's angle ψ, as a result of Faraday's rotation (also Faraday's effect), affects characteristics of the communication channel as long as the magnetic field B_{res} is influencing electromagnetic waves of frequency *f*. The magnetic field caused by permanent magnets lasts for decades, with some natural magnets losing 1% over the course of 10 years and some sintered (i.e., Nd-Fe-B) magnets losing less than 1% of their strength over 100 years. For this purpose, sintered permanent magnets would be a more reasonable choice, since they can be produced and optimized according to certain needs in existing smart environments or, more precisely, on receiving nodes of the communication channel. The backmost factors in Equation 3, N and z, are also important in dimensioning conditions in the approached interference, since they can also be easily designed according to existing circumstances.

These principles can serve as a founding layer for implementing communication channels in smart environments, being aware of existing boundaries mirroring three important technical parameters (signal processing speed, communication nodes distance, communication channel security), and observing security parameter as the most crucial among them.

CONCLUSION

The number of variable connected devices and implemented communication channels is rising constantly and rapidly in all smart environments of our everyday life. Among implementing new technology achievements, inevitable is the optimization of ongoing processes and managing resources more efficient and more effective, along with the important role of standardization. On close analysis of three important technical parameters (signal processing speed, communication nodes distance, and communication channel security), the security parameter is noted as a crucial starting point, having the consequence in its further analysis.

Securing communication channels is mandatory in smart environments, and along with technical measures, it should also be approached with non-technical elements, such as policies regulating time schedules for communication or addressing only predetermined destinations. Keeping in mind security issues and battery limitations of devices in smart environments, it is reasonable to look toward those resources operating only by their nature that do not and cannot be turned off or on, like natural permanent magnets. Magnetic field interference with electromagnetic waves can therefore create a whole new paradigm in securing information transfer between nodes that can also be in movement. The base of improvement is Faraday's rotation, apropos magnetic field B_{res} interfering with an electromagnetic wave of a certain frequency *f* (i.e., communication protocols).

All things considered, as a key finding of this article, it should be noted the most significant results are achieved among lower frequency communication protocols, such as NFC and possibly

NB-IoT. For NB-IoT frequency of 200 kHz, B_{res} value is 7,14477 μT. The B_{res} value further progresses according to Figure 10, resulting in 484,416 μT for NFC, resulting in around 30 mT for SigFox, ZWave, LoRaWAN, RFID, and resulting in around 90 mT for Mi-Wi, ZigBee, and Bluetooth. Permanent magnets with resulting values for similar frequencies can easily be deployed in communication channels. This approach or model would enhance development of passive security component, complement existing security procedures and improve the physical layer security of communication channels, it might be said on its "zero-layer security".

Further studies need to be carried out in order to establish whether existing communication protocols (frequencies and modulations) can serve smart environments or should another be scrutinized. Future work would also be considering implementation algorithms and applications for chosen solutions. Implementing such a solution would unladen and enhance other resources and new ideas for continually and sustainably growing smart environments and their devices while (re) creating and growing their new world.

ACKNOWLEDGMENT

Thanks to all the reviewers for devoting their time and reading this article, and thanks to all the contributors to this article, mentioned in the References section.

CONFLICT OF INTEREST

The author of this publication declares there is no conflict of interest.

FUNDING AGENCY

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

Abomhara, M., & Køien, G. M. (2015). Cyber security and the Internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65–88. doi:10.13052/jcsm2245-1439.414

Akyildiz, I. F., & Vuran, M. C. (2010). *Wireless sensor networks* (1st ed.). Wiley. doi:10.1002/9780470515181

Al-Sarawi, S., Anbar, M., Alieyan, K., & Alzubaidi, M. (2017). Internet of things (IoT) communication protocols: Review. *8th International Conference on Information Technology (ICIT)*, 685–690. doi:10.1109/ICITECH.2017.8079928

Alam, T., & Rababah, B. (2019). Convergence of MANET in communication among smart devices in IoT. *International Journal of Wireless and Microwave Technologies*, *9*(2), 1–10. doi:10.5815/ijwmt.2019.02.01

Apthorpe, N., Reisman, D., & Feamster, N. (2017a). *A smart home is no castle: Privacy vulnerabilities of encrypted IoT traffic*. https://arxiv.org/abs/1705.06805

Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. (2017b). *Spying on the smart home: privacy attacks and defenses on encrypted IoT traffic*. https://arxiv.org/abs/1708.05044

Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety and ethics, digital twin technologies and smart cities. *Springer Nature*, 1–27.

Behlilovic, N. (2021). One approach in improving communication quality of smart environment. *Proceedings of the 28th FRUCT Conference*, 545–553.

Bonetto, R., Bui, N., Lakkundi, V., Olivereau, A., Serbanati, A., & Rossi, M. (2012). Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples. *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 1–7. doi:10.1109/WoWMoM.2012.6263790

Boutaba, R., Salahuddin, M. A., Limam, N., Ayoubi, S., Shahriar, N., Estrada-Solano, F., & Caicedo, O. M. (2018). A comprehensive survey on machine learning for networking: Evolution, applications and research opportunities. *Journal of Internet Services and Applications*, *9*(1), 1–99. doi:10.1186/s13174-018-0087-2

Cepheli, Ö., & Kurt, G. K. (2013). Physical layer security in wireless communication networks. In D. Rawat, B. Bista, & G. Yan (Eds.), *Security, privacy, trust and resource management in mobile and wireless communications* (pp. 61–81). IGI Global.

Chen, Z., Xia, F., Huang, T., Bu, F., & Wang, H. (2011). A localization method for the Internet of things. *The Journal of Supercomputing*, *63*(3), 657–674. doi:10.1007/s11227-011-0693-2

Cindro, N. (1985). *Fizika 2: Elektricitet i magnetizam* [Physics 2: Electricity, and magnetism]. Školska knjiga.

Coskun, V., Ozdenizci, B., & Ok, K. (2013). A survey on near field communication (NFC) technology. *Wireless Personal Communications*, *71*(3), 2259–2294. doi:10.1007/s11277-012-0935-5

Deart, V., Mankov, V., & Krasnova, I. (2022). Traffic flows forecasting based on machine learning. *International Journal of Embedded and Real-Time Communication Systems*, *13*(1), 1–19. doi:10.4018/IJERTCS.289198

Deogirikar, J., & Vidhate, A. (2017). Security attacks in IoT: A survey. *International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, 32–37.

El-Hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019). A survey of Internet of things (IoT) authentication schemes. *International Conference on Information Technology (ICIT)*, 202–207. doi:10.3390/s19051141

Ergen, M. (2009). *Mobile broadband: Including WiMAX and LTE* (1st ed.). Springer. doi:10.1007/978-0-387-68192-4

Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on Internet of things (IoT). *International Journal of Computers and Applications*, *113*(1).

Goeckel, D., Capar, C., & Towsley, D. (2014). Physical layer secrecy in large multihop wireless networks. In X. Zhou, L. Song, & Y. Zhang (Eds.), *Physical layer security in wireless communications* (1st ed., pp. 271–285). CRC Press.

Goga, O., & Teixeira, R. (2012). Speed measurements of residential Internet access. In *International Conference on Passive and Active Network Measurement* (pp. 168–178). Springer. doi:10.1007/978-3-642-28537-0_17

Grace, D., & Zhang, H. (2012). *Cognitive communications: Distributed artificial intelligence (DAI), regulatory policy & economics, implementation* (1st ed.). Wiley. doi:10.1002/9781118360316

Guri, M. (2021). Magneto: Covert channel between air-gapped systems and nearby smartphones via CPU-generated magnetic fields. *Future Generation Computer Systems*, *115*, 115–125. doi:10.1016/j.future.2020.08.045

Guri, M., Zadov, B., & Elovici, Y. (2019). Odini: Escaping sensitive data from Faraday-caged, air-gapped computers via magnetic fields. *IEEE Transactions on Information Forensics and Security*, *15*, 1190–1203. doi:10.1109/TIFS.2019.2938404

Hammi, B., Khatoun, R., Zeadally, S., Fayad, A., & Khoukhi, L. (2018). Internet of things (IoT) technologies for smart cities. *IET Networks*, *7*(1), 1–13. doi:10.1049/iet-net.2017.0163

Haznadar, Z., & Štih, Ž. (1998). *Elektromagnetizam* [Electromagnetism]. Mikroštampa.

Huang, T., Chen, Z., Xia, F., Jin, C., & Li, L. (2010). A practical localization algorithm based on wireless sensor networks. *IEEE/ACM Int'l Conference on Green Computing and Communications and Int'l Conference on Cyber, Physical and Social Computing*, 50–54. doi:10.1109/GreenCom-CPSCom.2010.41

Hussein, A. H. (2019). Internet of things (IOT): Research challenges and future applications. *International Journal of Advanced Computer Science and Applications*, *10*(6). Advance online publication. doi:10.14569/IJACSA.2019.0100611

Ilic, G., Osmokrovic, P., Stankovic, D. (2012). *Primenjena magnetika* [Applied Magnetics]. Akademska misao.

Inan, U., & Inan, A. (1999). *Engineering electromagnetics* (1st ed.). Addison Wesley.

Jin, G., & Tierney, B. L. (2003). System capability effects on algorithms for network bandwidth measurement. *Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement*, 27–38. doi:10.1145/948205.948210

Kasper, T., Oswald, D., & Paar, C. (2012). Security of Wireless Embedded Devices in the Real World. In ISSE 2011 Securing Electronic Business Processes (pp. 174-189). Vieweg+ Teubner Verlag.

Khan, S., Mast, N., Loo, K. K., & Silahuddin, A. (2008). Passive security threats and consequences in IEEE 802.11 wireless mesh networks. *International Journal of Digital Content Technology and its Application, 2*(3), 4-8.

Kislyakov, S. V. (2022). A digital twin model of the smart city communication infrastructure. *International Journal of Embedded and Real-Time Communication Systems*, *13*(1), 1–16. doi:10.4018/IJERTCS.304803

Kumar, M., Kumar, D., & Akhtar, M. A. K. (2021). A modified GA-based load balanced clustering algorithm for WSN: MGALBC. *International Journal of Embedded and Real-Time Communication Systems*, *12*(1), 44–63. doi:10.4018/IJERTCS.20210101.oa3

Kumar, S. S., Basavaraju, T. G., & Puttamadappa, C. (2013). *Ad hoc mobile wireless networks principles, protocols, and applications* (2nd ed.). CRC Press.

Martin, R., Malah, D., Cox, R. V., & Accardi, A. J. (2004). A noise reduction preprocessor for mobile voice communication. *EURASIP Journal on Advances in Signal Processing*, *2004*(8), 1–13. doi:10.1155/S1110865704312138

Mattison, R. (1997). *Data warehousing and data mining for telecommunications*. Artech House Publishers.

Mihailovic, P., & Petricevic, S. (2021). Fiber optic sensors based on the Faraday effect. *Sensors (Basel)*, *21*(19), 6564. doi:10.3390/s21196564 PMID:34640884

Mills Purcell, E. (1965). *Electricity and magnetism* (1st ed., Vol. 2). McGraw Hill.

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Communications Surveys and Tutorials*, *21*(3), 2702–2733. doi:10.1109/COMST.2019.2910750

Newlin Rajkumar, M., Chatrapathi, C., & Venkatesakumar, V. (2014). Internet of things: A vision, technical issues, applications and security. *IPASJ International Journal of Computer Science*, *2*(8).

Nithyanandan, L., & Parthiban, I. (2012). Vertical handoff in WLAN-WIMAX-LTE heterogeneous network through gateway relocation. *International Journal of Wireless and Mobile Networks*, *4*(4), 203–215. doi:10.5121/ijwmn.2012.4415

Pal, R., Chavhan, S., Gupta, D., Khanna, A., Padmanaban, S., Khan, B., & Rodrigues, J. J. (2021). A comprehensive review on IoT-based infrastructure for smart grid applications. *IET Renewable Power Generation*, *15*(16), 3761–3776. doi:10.1049/rpg2.12272

Pekar, A., Mocnej, J., Seah, W. K. G., & Zolotova, I. (2018). *Network traffic characteristics of the IoT application use cases* (Technical Report ECSTR18-01). School of Engineering and Computer Science, Victoria University of Wellington.

Pekar, A., Mocnej, J., Seah, W. K. G., & Zolotova, I. (2020). Application domain-based overview of IoT network traffic characteristics. *ACM Computing Surveys*, *53*(4), 1–33. doi:10.1145/3399669

Peris-Ortiz, M., Bennet, D. R., & Perez-Bustamante Yabar, D. (2017). Preface. In M. Peris-Ortiz, D. R. Bennet, & D. Perez-Bustamante Yabar (Eds.), *Sustainable smart cities* (p. ix). Springer. doi:10.1007/978-3-319-40895-8

Podder, P., Mondal, M., Bharati, S., & Paul, P. K. (2021). *Review on the security threats of Internet of things*. arXiv preprint arXiv:2101.05614.

Poor, H. V., & Schaefer, R. F. (2017). Wireless physical layer security. *Proceedings of the National Academy of Sciences of the United States of America*, *114*(1), 19–26. doi:10.1073/pnas.1618130114 PMID:28028211

Popovic, B. (1980). *Elektromagnetika* [Electromagnetics]. Građevinska knjiga.

Rajiv, K., Sreekumar, N., & Gurjeet, K. (2021). Future of Internet of everything (IOE). *IRJCS: International Research Journal of Computer Science*, *8*, 84–92.

Rifa-Pous, H., & Herrera-Joancomartí, J. (2011). Computational and energy costs of cryptographic algorithms on handheld devices. *Future Internet*, *3*(1), 31–48. doi:10.3390/fi3010031

Rodriguez, J. (2015). *Fundamentals of 5G mobile networks* (1st ed.). Wiley. doi:10.1002/9781118867464

Sanenga, A., Mapunda, G. A., Jacob, T. M. L., Marata, L., Basutli, B., & Chuma, J. M. (2020). An overview of key technologies in physical layer security. *Entropy (Basel, Switzerland)*, *22*(11), 1–34. doi:10.3390/e22111261 PMID:33287029

Saravanan, S., & Sudhakar, P. (2020). Analysis of mobile Internet speed, signal strength and FMDH antenna design for improved Internet speed. *The Journal of Supercomputing*, *76*(6), 4449–4475. doi:10.1007/s11227-018-2382-x

Sarkar, T. K., Mailloux, R., Oliner, A. A., Salazar Palma, M., & Sengupta, D. L. (2006). *History of wireless* (1st ed.). Wiley – IEEE Press. doi:10.1002/0471783021

Sarkar, T. K., Salazar Palma, M., & Abdallah, M. N. (2018). *The physics and mathematics of electromagnetic wave propagation in cellular wireless communication* (1st ed.). Wiley – IEEE Press. doi:10.1002/9781119393146

Sathish Kumar, J., & Patel, D. R. (2014). A survey on Internet of things: Security and privacy issues. *International Journal of Computers and Applications*, *90*(11).

Schwartz, L. S. (1956). Principles of noise reduction in communication channels. *Transactions of the American Institute of Electrical Engineers, Part I: Communication and Electronics*, *75*(1), 44–50. doi:10.1109/TCE.1956.6372480

Shahid, M. R., Blanc, G., Zhang, Z., & Debar, H. (2018). IoT devices recognition through network traffic analysis. *IEEE International Conference on Big Data*, 5187–5192. doi:10.1109/BigData.2018.8622243

Shon, T., & Moon, J. (2007). A hybrid machine learning approach to network anomaly detection. *Information Sciences*, *177*(18), 3799–3821. doi:10.1016/j.ins.2007.03.025

Singh, D., Tripathi, G., & Jara, A. J. (2014). *A survey of Internet-of-things: Future vision, architecture, challenges and services* [Conference presentation]. IEEE World Forum on Internet of Things (WF-IoT).

Sivanathan, A., Gharakheili, H. H., Loi, F., Radford, A., Wijenayake, C., Vishwanath, A., & Sivaraman, V. (2019). Classifying IoT devices in smart environments using network traffic characteristics. *IEEE Transactions on Mobile Computing*, *18*(8), 1745–1759. doi:10.1109/TMC.2018.2866249

Sivanathan, A., Sherratt, D., Gharakheili, H. H., Radfordy, A., Wijenayake, C., Vishwanathz, A., & Sivaraman, V. (2017). Characterizing and classifying IoT traffic in smart cities and campuses. *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 559–564. doi:10.1109/INFCOMW.2017.8116438

Snow, A., Rastogi, P., & Weckman, G. (2005). Assessing dependability of wireless networks using neural networks. *2005 IEEE Military Communications Conference*, 2809–2815. doi:10.1109/MILCOM.2005.1606090

Sundaresan, S., de Donato, W., Feamster, N., Teixeira, R., Crawford, S., & Pescapè, A. (2011). Broadband Internet performance: A view from the gateway. *Computer Communication Review*, *41*(4), 134–145. doi:10.1145/2043164.2018452

Tahsin, M. S., Aziz, M. Y., Kabbo, T. A., Tahsin, T., Zumme, N. H., & Hossain, M. I. (2021). Data security model using deep learning and edge computing for Internet of things (IoT) in smart city. *19th OITS International Conference on Information Technology*, 381–386. doi:10.1109/OCIT53463.2021.00081

Tightiz, L., & Yang, H. (2020). A comprehensive review on IoT protocols, features in smart grid communication. *Energies*, *13*(11), 2762. doi:10.3390/en13112762

Wei, H.-Y., Rykowski, J., & Dixit, S. (2013). *Wi-Fi, WiMAX and LTE multi-hop mesh networks basic communication protocols and application areas* (1st ed.). Wiley.

Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K., & Gao, X. (2018). A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE Journal on Selected Areas in Communications*, *36*(4), 679–695. doi:10.1109/JSAC.2018.2825560

Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). *IoT security techniques based on machine learning*. https://arxiv.org/abs/1801.06275

Zamfiroiu, A., Iancu, B., Boja, C., Georgescu, T. M., Cartas, C., Popa, M., & Toma, C. V. (2020). IoT communication security issues for companies: Challenges, protocols and the web of data. *Proceedings of the International Conference on Business Excellence, 14*, 1109–1120. doi:10.2478/picbe-2020-0104

Zhang, M., Sun, F., & Cheng, X. (2012). Architecture of Internet of things and its key technology integration based on RFID. *IEEE Fifth International Symposium on Computational Intelligence and Design*, 294–297. doi:10.1109/ISCID.2012.81

Zhou, W., Zhang, Y., & Liu, P. (2019). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, *6*(2), 1606–1616. doi:10.1109/JIOT.2018.2847733

Narves Behlilović received his Dipl. Ing. (2009.) and ME (2014.) degrees in telecommunications from the Faculty of Electrical Engineering in Sarajevo, where he is currently a PhD candidate at the Department of Telecommunications Engineering. He also holds an MBA (2011.) degree from Cotrugli Business School. In 2008 he was hired by an insurance company for its IT department, and afterwards he worked for an IT consulting company. At the moment, he is working in the Executive Directorate for Business Development in BH Telecom JSC, Sarajevo, Bosnia and Herzegovina. His interests include security and optimization of information systems and business processes as part of developing and implementing new and sustainable business models.