One Approach in Improving Communication Quality of Smart Environment

Narves Behlilović
BH Telecom JSC
Sarajevo, Bosnia and Herzegovina
behlilovic.narves@gmail.com

***Abstract*—Being aware of diversity in implementation of different technologies in various smart environments, gives opportunity in finding possibility to classify given options in order to optimize resource usage and provide best user experience. Rapid development of technology enabled and caused bigger number of connected devices, resulting in dynamic environments where each participant can make decision on which level to be involved in it. Making that choice easier and getting most of it is crucial for optimization of such environments and also directs further efforts for improvement.**

Numerous papers considering above mentioned breakthroughs have been written lately, but were not considering possibility of defining principles that would help organize smart environments in order to follow certain hierarchy, according to various existing parameters. In this fast growing new world of connected devices, this approach is becoming a mandatory for their coexistence.

This paper is focusing technology characteristics, used for communication among connected devices in order to classify them according to those characteristics in respect to the needs of end users. Aim is to show potentials of continuous optimization in smart environments resulting in improvement of such environments and thus possibilities in welcoming new ideas.

I. Introduction

Rapid development in communication extent, as well as in number of subjects as active participants, followed by more complex use of network architectures for their processing, are activating additional topics for researchers. After a period when following and analyzing QoS (Quality of Service) and QoE (Quality of Experience) parameters were sufficient as performance measures in communication process, IoT (Internet of Things) created additional space for advancement in transmitting data among connected subjects. After short period of time, adding more subjects into communication resulted in IoE (Internet of Everything) as a new and even more complex smart environment. In this paper IoT and IoE will be addressed as a common IoE/IoT smart environment. These newly created environments for connecting devices and communicating information generated and still generate numerous research topics, such as:

- Possibility of harmonious functioning in heterogeneous network architecture, no matter if its heterogeneity is related exclusively to approached combined networks, or if its heterogeneity is related to the fact that some parts of network are capable of dynamically re-configuring over time or persisting static configuration.
- Achieving desired data transfer security level, completely preserving integrity of data transmitted, lowering electromagnetic pollution levels of media in use, lowering distance between nodes in communication, inevitable process of their authentication and authorization,...

Additional problem while researching mentioned phenomena is a fact that most of their functions are not mutually independent, so formulating their mathematical correlations is demanding involvement in very different areas of mathematics. In order to have sufficiently good communication, participant should fulfill these requests at least:

- All participants in communication should undergo 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 automatic exchange of information and executing tasks, there is zero tolerance for failure in communication. Therefore, information integrity is considered as a key element in automated environments;
- Confidentiality of information content, with prescribed procedures, following principles mentioned above. Thus, not only exchanged information security is requested, than security of connected devices and process of communication as well.

After main directions for technological development in period 2015.-2020. [1] have been publicly announced, many researches put in focus following problems:

- Scalability of configurations while forming network architectures, with ubiquitous coverage;
- Implementation of intelligence on making decisions in computer processing, to ease decision making procedure;
- Differences between indicators of presence for certain applications.

After it is stated that IoE/IoT has certain 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.

It is clear that search for new more flexible network architectures with dominant simple and intelligent algorithms should be intensified. Accordingly, 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 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. This paper is trying to make one step forward in that direction.

Paper is structured in a way that Section II is giving short review of actual technologies for data transfer with their basic characteristics. Subsequently, Section III is analyzing those technologies regarding their technical parameters (information signal processing speed, boundaries regarding distance, security of data transfer) which are considered peculiarly important by author. Section IV is trying to analyze existing correlation between observed parameters, assuming that protecting privacy and security has significant importance for maintaining desired quality of communication in observed smart environment.

II. Review of data transfer technologies

Communication between devices can be used as a powerful mechanism and at the same time it is very complex and can become problem for itself. Today there are many standards for connecting and communicating among devices, and every device must support several of them. Often as a result there are problems with scalability and flexibility of such solutions, resulting in their limitation in use [2]. The reason can be found among many different factors affecting connected devices working or raising complexity of such environments. Additional challenge is its development dynamics and continuous need for reconfiguration and optimization. Alike 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 [3]. Less urban environments can find benefit 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, that should be approached as a fundamental in planning and developing smart environments. In order to approach them easier it is possible to focus certain segments. Development of IoE/IoT smart environment depends on its focus and has following different orientation visions [4]: things, internet and semantic.

IoE/IoT users and consumers can be categorized [5] 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 very 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: cost of devices, battery life, physical specifications, interoperability, data processing, context awareness, coverage, scalability, reliability, attack resistance, confidentiality, integrity, and availability. Existence of numerous factors affecting decision-making process in developing smart environments, results in need for systematic approach in dealing such problems. Some of these factors are important just in planning and are not affected with subsequent changes, while some of them are highly more dynamic in change and their characteristics hardly can or can not be predicted. As a good example, we can approach data transferred among communicating nodes inside smart environment compared to data transferring to nodes outside smart environment.

Today is a fact that data transfer is needed everywhere, as well as fact that two different data types poses different characteristics and accordingly demand different approach 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 less 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 channel in smaller segments. This can be done in multiple and different ways. It is reasonable to start making classification considering environments in which data transfer is done, so communication channels are divided in non moving (wired) and moving (wireless) communication channels. Each of those segments is dominated by these two groups of technologies:

- Fixed access network technologies (abbr. FANT);
- Mobile access network technologies (abbr. MANT).

Processes and content created during communication should not be noticing such segmentation. Interworking of these access networks with wireline technologies is a significant step to achieve a single telecommunications network foundation. Fixed-mobile convergence (abbr. 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 [6]. No matter the integration level of different approaches and technologies, planning and developing smart environments requests classification of different solutions in maintaining communication. Alike approach should guaranty that their implementation will fulfill expectations and use IoE/IoT resources in most optimized way.

A. Fixed access network technologies - FANT (Wired)

FANT can be found as an implemented solution in variable environments. Its implementation developed over time in terms of actual level of technological advancement and user requirements, in respect to existing network infrastructure. Each dissimilarity has its own characteristics, resulting in certain advantages and disadvantages. At the moment dominant is the expansion of FTTx network access, while xDSL is still remaining significant in presence. Some of FANT technologies are: xDSL, Cable, Ethernet, FTTx, PLC.

While xDSL and FTTx network access are predominantly enabling communication between nodes in longer distance, cable and Ethernet along with PLC are used for implementation of communication channels in local environment and short distance. In technical practice it is common to combine multiple technologies when connecting two distant communicating nodes.

B. Mobile access network technologies'- MANT (Wireless)

History of wireless communication, including electrical and magnetic phenomena, starts couple thousands years ago with ancient Chinese, Greek and Roman culture. At the start of 18th century digital communication has begun its development, as a founding layer for modern wireless communication [7].

Although younger, wireless communication has many benefits compared to wired communication, but also faces certain boundaries. Boundaries are most obvious in security of data transfer, while on the other side is the ease of communication channel implementation. Smart devices that are in Wi-Fi range of one another can straightforwardly convey the information, whereas others required the aid of intermediate smart devices to route their packets of information. The link is created in the real time that makes the network completely dispersed and can work at wherever without the assistance of any access point [8].

MANT are present in technical practice in many different options, developed over time in terms of actual level of technological advancement and user requirements, in respect to existing network infrastructure. Some of most used MANT today for data transfer include: NFC, Li-Fi, Wi-Fi, RFID, Mi-Wi, ZigBee, Bluetooth, Z Wave, LoRaWAN, Sigfox, Wi-Max, Cellular, Satellite.

These technologies have their uniqueness, so it is rational to further analyze and compare them. The most obvious classification is the one considering distance among node that has been alerted and the node where that alert has been processed. Data transfer between these two nodes should be protected and performed in speed according to the industrial standards and best practices. Thinking alike leads to further classification considering distance, security and signal processing speed between two nodes in communication, respectively two ends of communication channel.

III. CHARACTERISTICS AND POSSIBILITIES OF DATA TRANSFER TECHNOLOGIES

In previous Section some of the most important FANT and MANT technologies have been enumerated, while at the end of it has been pointed that in IoE/IoT environment, by analyzing data transfer, it is of especial importance to consider security levels of data in transmission, speed of signal processing and length of distance between network nodes being first and last in communication observed.

Inside smart environment there are numerous nodes in communication demanding individual approach and consideration in process of planning future IoE/IoT architecture. Considering more of such requests means that future solution will be more customized to actual requirements. IoE/IoT is interdisciplinary in nature, implying intelligent integration of several existing technologies [9]. Because of various differences among single communication channels, it is recommended to pay attention on as much as possible important characteristics. Regarding differences among technologies, it is worthy to prepare a review on values of their characteristics: information signal processing speed, distance between first and last network node in communication and basic elements of data transfer security meaning encryption key length. Having this observed 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. For comparing only signal processing speed both FANT and MANT characteristics are presented in Table I, though further focus in this paper is put exclusively on wireless communication technologies.

TABLE I. FANT AND MANT CHARACTERISTICS

Technology		**Speed [bps]**	**Distance [m]**	**Security [bit]**
Wired (FANT)				
1	xDSL	<1Gbps	-	-
2	Cable	<400\<30Mbps	-	-
3	Ethernet	<1Gbps	-	-
4	FTTx	<1Gbps	-	-
5	PLC	<3Mbps	-	-
Wireless (MANT)				
1	NFC	<424kbps	<1m	-
2	Li-Fi	<10Gbps	<10m	256
3	Wi-Fi	<54Mbps	<50m	192
4	RFID	<100kbps	<100m	128
5	Mi-Wi	<250kbps	<100m	64
6	Zig Bee	<250kbps	<100m	128
7	Bluetooth	<2,1Mbps	<150m	128
8	Z Wave	<100kbps	<200m	128
9	LoRaWAN	<50kbps	<10km	128
10	Sigfox	<1kbps	<50km	128
11	Wi-Max	<100Mbps	<50km	168
12	Cellular	<2,6Gbps	<200km	256
13	Satelitte	<1Gbps	>1000km	384

Process of planning and implementing mobile networks is facing many challenges considering choosing parameters that are suitable at the moment. Among mentioned parameters (speed of signal processing, distance between communicating nodes, number of bits representing encryption key length) important role in decision-making process and choosing the best option for data transfer, can be influenced with implementation cost, ease of implementation, media characteristics, electromagnetic pollution,... Number of parameters, as variables affecting IoE/IoT smart environment, can hardly be counted or calculated. Therefore it is only possible to set list of priorities at the 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 paper focuses three mentioned parameters as fundamental ones in observing data transferred.

Dynamic in smart environments functioning puts in focus its 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, data in use.

One of the biggest challenges in planning communication network capacity is understanding and developing data transfer patterns, respectively traffic (level of activity through time, load balancing capacity,...). Solving such problems can be significantly eased by using historical records on certain activities, previously preserved in databases [10]. Existence of such records does not need to be universally usable, in respect that certain data sets can not be used in the same or alike circumstances. Therefore, it is recommended to use localized data sets, which are best describing their surrounding smart environment.

Developing specialized data transfer models is subject to advanced computing algorithms, that among sufficient data inputs and data sets for algorithm training, need adjusting model to existing circumstances. Planning mobile networks is, more and more, using help and models developed by artificial intelligence, thus leaving to computer algorithms important part of job that once was being done by teams of experts.

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 which 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 for reaching them.

Moving from human handled networks to cognitive ones needs 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 [11]. This part of job, more or less, remains part of expert interest in that domain, still being aware that job amount will decrease in future with actual trends. Obvious is the need for developing optimized communication models and using artificial intelligence models to maximize use of existing resources as well as to predict future scenarios for smart environment development.

IV. Comparing Parameters of Data Transfer Technologies

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 alike results. The main architecture of IoE/IoT [12] is: coding layer, perception layer, network layer, middleware layer, application layer, business layer.

Depending on approached smart environment characteristics, mobile networks parameters are being set in order to enable normal communication of all connected devices. The network environment is highly dynamic, counting not only geographical positions of the nomadic nodes [13], but also 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 network connection at a given place and time and choice of an access device). This approach guaranties long term functioning smart environment and fulfilling its requirements according to all parameters. Importance of parameters involved can change over time and that gives additional dimension in planning IoE/IoT environment architecture.

Irrespective of chosen and used data transfer technologies, as well as required distance, it is important to focus on security aspects of such solution. Challenges that are present in this domain can be approached in few basic perspectives [14]:

- 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 can not support complex security schemes due to low power and computing resource capabilities.

It is obvious that existence of such problems can not be eliminated, so it is only possible to work toward minimization of theirs effect. Serious approach and applying modern achievements can give satisfying result, requesting dealing with this matter continually in time. Malicious activities towards devices can be threatening front-end sensors and equipment, network and back-end of ICT systems. This can result in problems with privacy in device, privacy during communication, privacy in storage and privacy at processing [15]. Such activities affecting normal functioning of each segment mentioned result in disrupting normal functioning of entire smart environment.

A. Signal processing speed and communication nodes distance

Considering these two parameters, the most modest performances are those 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 card, debit information). Most common users are mobile network operators, banking and payment services, semiconductor producers and electronic appliances, software developers, other merchants including transport operators and retailers [16]. Different conclusion would be made if additionally devices pairing speed was considered, which puts NFC (less than 0,1s) ahead of ZigBee (0,5s) or Bluetooth (6s). Among 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 home and small commercial domains. This technology is designed for small data packets at relatively low speeds up to 100 kbps and 30 meter [17]. Variety in technologies usable for communication channel establishment, gives more opportunities and positive impact on quality of smart environment solution. Significantly bigger number of solutions is working only in shorter distance with smaller average signal processing speed and data transfer, as a result of other factors and boundaries. In sensor-based applications, where sensors (constrained in terms of memory, processing power, battery, etc.) are the main end-devices, the proposed protocols must be lightweight, making a trade-off between power consumption and security [18]. Presence of numerous sensors in shorter distance can negatively affect smart environment performances.

Characteristics of each node in communication and the need of interaction with other nodes, determine its position in IoE/IoT environment, with that position possibly being changed over time. In order to determine distance between communication nodes it is needed to locate them first. Traditional location technique such as GPS cannot be used in WSNs (Wireless Sensor Network) directly, as its costly requirement of sophisticated equipment and high energy consumption, which have greatly constrained the application scale of WSNs [19]. Many localization algorithms have been developed in WSNs, all of which can be roughly categorized into one of the follows: range-based localization and range-free localization. Range-based localization always has two phases to go: ranging and position computation. In the first phase it utilize some ranging method such as TOA (abbr. Time of Arrival), TDOA (abbr. Time Difference of Arrival), AOA (abbr. Angle of Arrival) and RSSI (abbr. Received Signal Strength Indicator) to obtain the distance between two nodes (always blind node whose position unknown and reference nodes also called beacon nodes whose position pre-known) [20]. Calculating distance between nodes can be time-consuming. Smart environments that consists of dynamically re-configuring networks or networks in movement over time, can experience more challenges compared to those consisting of networks persisting in static configuration.

Having observed mentioned parameters, it is possible to graphically represent communication protocols, as in Fig 1.

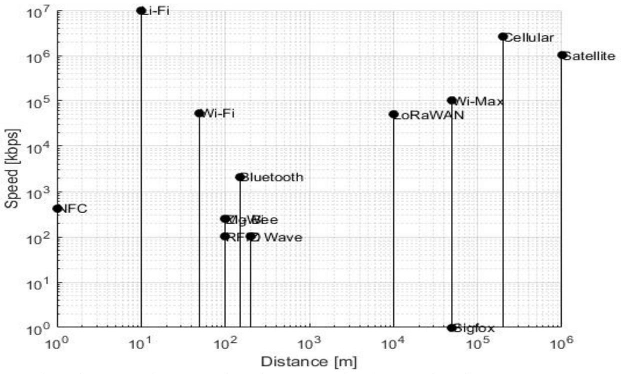

Fig. 1. Signal processing speed and communication nodes distance

Considering big differences between starting and ending values of parameters, both are represented using logarithm scale. Observing their values, visible correlation can not be represented in other way than graphically. Impossibility in representing these parameters and their values otherwise is an additional problem when it comes to establishing principles in functioning of smart environment. Eight protocols support distances up to 200m, while the others serve up to 10 km or longer. Zig Bee and Mi-Wi values are similar and overlapping.

B. *Signal processing speed and communication channel security*

The security of the protocol lies on the strength of the cryptographic algorithms chosen by the peers [21]. Developing and implementing modern cryptographic algorithms is raising the security level of protected content, but at the other side mechanisms with opposite purpose are still being developed. Cryptographic algorithm purpose is to make transferred information unusable for its potentially malicious user, but malicious users goal must not always be 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 [22]. This kind of information can be used for various attacks on smart environment and result with many problems in its normal functioning. Signal processing speed is positively affecting communication channel security, leaving less time for planned activities to potential malicious user.

Observing communication channel security, focus of this paper is just encryption key length and subsequently different attacks aiming encryption algorithms. Encryption attacks [23] depend on destroying encryption technique and obtain the private key:

- Side-channel attacks;
- Cryptanalysis attacks;
- Man in the Middle attacks.

Importance of certain data set is determining the level of security activities for its protection, which is affecting speed of processing signal respectively data transfer. Parameter of security is much more complex than two parameters previously approached. Communication channel security and security of devices in communication depends on many factors, and only in ideal case it depends only on number of bits that create key length belonging to chosen encryption technique. The bigger the key length is, properly combined with chosen algorithm, will better encrypt information transferred and make it more difficult to access by third party. Some of important factors for protecting communication are amount of memory for encryption and decryption, speed of encryption, speed of generating key, key length, number of keys, key management, complexity of encryption algorithm, exposure to attacks,... Mostly used encryption algorithms for communication protocols, including those observed in this paper, can be found in Table II.

TABLE II. ENCRYPTION ALGORITHMS

Algorhitm	Invented by	Key length	Year invented
DES	IBM	56	1975
AES	Vincent Rijmen, Joan Daemen	256	2000
RSA	Ron Rivest, Adi Shamir, Leonard Adleman	1024	1978
IDEA	James Massey, Xuejia Lai	128	1991
OPGP	Phil Zimmermann	512	1991
3DES	IBM	168	1998
Blowfish	Bruce Schneier	256	1993
Twofish	Bruce Schneier	256	1998

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

Smart environment traffic characteristics are very different. Optimizing communication channel and protecting information transferred depend a lot on possibility of differentiating and classifying traffic involved. Following activities to examine characteristics of IoE/IoT devices from different viewpoints and highlight their dominant attributes, enables 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 [24]:

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

Alike approach allows different types of traffic, depending on their importance, to protect in different ways and therefore additionally optimize using existing resources. Existence of varieties and raising dynamics in data transfer are making decision-making process more difficult and making more obvious that thinking in that direction is necessary. However, studies focusing on characterizing IoE/IoT traffic (also referred to as machine-to-machine (abbr. M2M) traffic) are still in their infancy [25], being 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 it is questioning its purposefulness considering existing 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 Fig2.

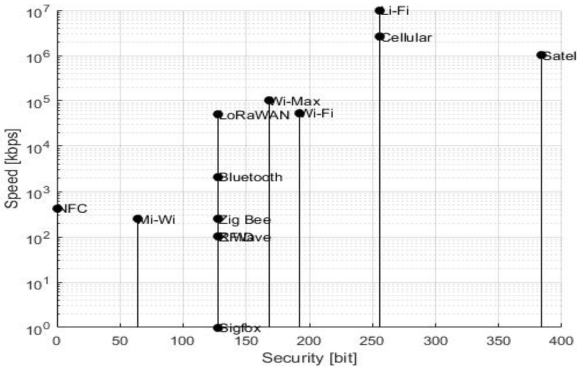

Fig. 2. Signal processing speed and communication channel security

Because of the big difference between starting and ending values of ordinate, it is represented using logarithm scale. Unlike previous graphic, direct proportion of two parameters can be discussed, albeit it is insufficient to maintain clear correlation. The longer distance is, the bigger number of encryption bits is. Unfortunately this ratio also can not provide good fundamental for creating smart environment. These two parameters are equal for RFID and Z Wave and thus overlap themselves.

C. Communication nodes distance and communication channel security

Smart environment implementation is 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 [26].

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 possibility to experience misuse or attack. There are four main types of attacks in the IoE/IoT system: physical, software, network and encryption attacks [27]. Experiencing IoE/IoT attacks is representing some kind of calculated risk, therefore attention should be paid so implementation should not be 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 [28]. Among these two options balance should be achieved and maintained through time. Longer distance between nodes in communication leaves more space for malicious users and their potential intents to endanger safe communication principles.

Different types of traffic between two ends of communication channel along with devices used in that purpose are not affected by their distance. Along with the rapid growth of IoE/IoT application and devices, cyber attacks will also be improved and pose a more serious threat to security and privacy than ever before [29]. For different traffic types and different device types it is reasonable to ensure different type 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 [30].

Bigger number of encryption bits along with adequate encryption algorithm enable higher level of encryption for information in transfer, but it is not always possible to achieve that. 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 enable attackers to generate IoE/IoT-centric malicious activities in a highly stealthy manner [31]. Need for optimizing use of existing resources is expressed once more, in order to provide the best possible solutions.

Observed technologies are presented in Fig 3, according to their characteristics.

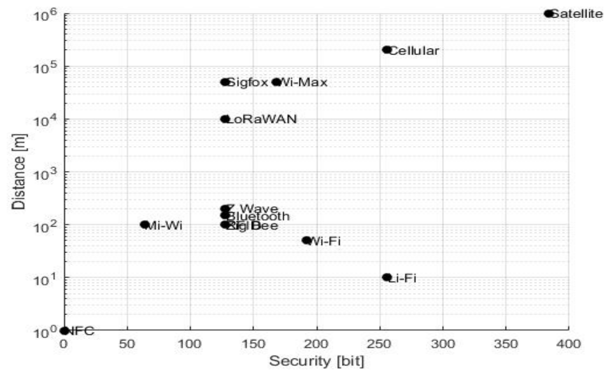

Fig. 3. Communication nodes distance and communication channel security

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

D. Signal processing speed, communication nodes distance and communication channel security

Varieties of traffic types in smart environment are resulting in use of variable communication protocols in order to transfer data. Different criteria are used to compare between the communication protocols. Such criteria include network, topology, power, range, cryptography, spreading, modulation type, coexistence with mechanism and power consumption [17]. Choosing critical characteristics can provide better choice while selecting communication protocol, paying attention on type of traffic. In a general-purpose network most activity will be generated by smartphones or laptops [32]. The most modest in entitled parameters are Wireless Sensor Networks, but even as such they can be very 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 that include the following: 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 are possible. The major challenge for the proliferation of WSNs is energy [33]. Therefore, WSN networks are not useful a lot in situations when needing substantious and variable resources, meaning also more investments in smart environment infrastructure.

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

Some important differences between cellular networks and ad-hoc wireless networks characteristics are listed in Table III bellow.

TABLE III. CELLULAR AND WIRELESS AD-HOC NETWORKS CHARACTERISTICS

Cellular networks	**Ad-hoc wireless networks**
Infrastructure network	Infrastructure-less network
Fixed, prelocated 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

When choosing technologies, companies make decisions based on costs, benefits and performance reports. Securing data and digital services is a cost that business 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 [34]. It is obvious that presence of smart environments is increasing, so it is reasonable on its very beginning to pay attention on its long term planning process. This way it is possible to ensure long term development of IoE/IoT environments and its continual upgrades.

Numerous challenges are facing smart environments implementation and this paper is mentioning only those of technical aspect. The main challenge of smart grid implementation is the communication of heterogeneous distributed elements [35]. Their communication usually can be implemented through numerous nodes in communication and 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 the energy efficiency both at the operator and the user side. To that end, the development of low power micro base stations (femto, pico, WiFi) inside the coverage area of a macro base stations (LTE, 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 [36]. Everything mentioned contributes better optimized functioning of smart environments, but also requests continual monitoring, coordinating and upgrading. Different technologies functioning in the same network and overlying their frequency spectrum, demands 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 [37]. Having all these different technologies in one network and their various parameters over time, opens advanced chapters of mathematics in order to understand it.

After considering characteristics of three parameters individually and in pairs, it is reasonable to put their values in three dimensional graph, as it has been done in Fig4.

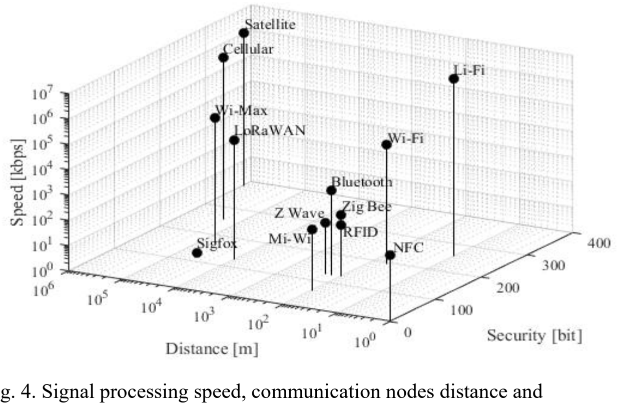

Fig. 4. Signal processing speed, communication nodes distance and communication channel security

Observing these three parameters together, resulting graph is becoming more complex and gives better insight in possibilities of choice. At the same time it is not enabling establishment of solid mutual correlations, as it was stated just after previous three graphics. Parameter values for communication nodes distance and signal processing speed are noticeably grouped in two groups each, especially if used logarithmic scales are considered. Communication channel security is represented only with most commonly used values for each communication protocol and therefore shows very few options for consideration, which might change in future with presence of advanced quantum cryptography algorithms.

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. Analogous approach can result in meaningful preservation in time and other important disposable resources. Importance of particular data is determining the level of security, thus encryption algorithm and finally number of bits for encryption of information during its transfer. Afterward is important to resolve distance between nodes in communication and possibly patterns of their allocation or relocation. Subsequently, interest should be put in signal processing speed, which can be affected by previous two parameters, maximizing security level of data protection and respecting the distance between ends of communication channel. After these three fundamental parameters, all the others should follow.

Approached communication protocols have been developed during longer period of time and their development was not followed by systematic approach needed for smart environments of the future. Working on continuous improvement of this smart environment segment, with systematic approach, remains final unachievable destination.

V. Conclusion

Presence of variable connected devices is raising constantly and rapidly in all segments of life. Customers can be found among many smart environments in everyday life, such as: transport, building, city, life-style, retail, agriculture, factory, supply chain, emergency, healthcare, user interaction, culture, tourism, energy,… Advanced smart environments are confronting their participants to more and more challenging offers, changing their routines in a radical way. Along with implementing new technology achievements, inevitable is optimization of ongoing processes and managing resources more efficient and more effective. Important role of standardization in all possible aspects, should improve results by each iteration. Communication technologies could be further quantified, linking values to certain levels in smart environment. Additional effort should be put in precisely defining those levels to maximize its potentials, thus enabling unladen resources for continually welcoming new ideas.

This paper intent is to enlighten approach in which results are enabling the best possible performance and allocating optimal resources for all connected devices in order for sustainably creating and growing their new world.

ACKNOWLEDGMENT

Thanks to all the reviewers for devoting their time and reading this paper and thanks to all the contributors for this paper, that are mentioned bellow in References.

REFERENCES

[1] A. Spender, “Top 10 Strategic technology trends for 2015“, *Gartner,* 2015.

[2] S.S. Kumar, T.G. Basavaraju, C. Puttamadappa, *Ad Hoc Mobile Wireless Networks Principles, Protocols, and Applications.* CRC Press, 2nd Edition, 2013.

[3] B. Hammi, R. Khatoun, S. Zeadally, A. Fayad, L. Khoukhi, “Internet of things (IoT) technologies for smart cities“, *IET Networks,* vol. 7, No. 1, pp. 1-13, 2018.

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

[5] A. Pekar, J. Mocnej, W.K.G. Seah, I. Zolotova, “Application domain-based overview of IoT network traffic characteristics“, *ACM Computing Surveys (CSUR),* vol. 53, pp. 1-33, 2020.

[6] M. Ergen, *Mobile Broadband - Including WiMAX and LTE.* Springer, 1st Edition, 2009.

[7] T.K. Sarkar, R. Mailloux, A.A. Oliner, M. Salazar Palma, D.L. Sengupta, *History of Wireless.* Wiley-IEEE Press, 1st Edition, 2006.

[8] T. Alam, B. Rababah, “Convergence of MANET in communication among smart devices in IoT“, *International Journal of Wireless and Microwave Technologies (IJWMT),* vol. 9, No. 2, pp. 1-10, 2019.

[9] M. Newlin Rajkumar, C. Chatrapathi, V.Venkatesakumar, “Internet of things: A vision, technical issues, applications and security“, *IPASJ International Journal of Computer Science (IIJCS),* vol. 2, Issue 8, 2014.

[10] R. Mattison, *Data Warehousing and Data Mining for Telecommunications.* Artech House Publishers, 1997.

[11] D. Grace, H. Zhang, *Cognitive Communications: Distributed Artificial Intelligence (DAI), Regulatory Policy & Economics, Implementation.* Wiley, 1st Edition, 2012.

[12] M.U. Farooq, M. Waseem, S. Mazhar, A. Khairi, T. Kamal, “A review on internet of things (IoT)“, *International Journal of Computer Applications,* vol. 113, No. 1, 2015.

[13] Hung-Yu Wei, J. Rykowski, S. Dixit, *WiFi, WiMAX and LTE Multi-hop Mesh Networks Basic Communication Protocols and Application Areas.* Wiley, 1st Edition, 2013.

[14] M. Abomhara, G.M. Køien, “Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks“, *Journal of Cyber Security and Mobility,* vol. 4, Issue 1, pp. 65-88, 2015.

[15] J. Sathish Kumar, D.R. Patel, “A survey on internet of things: Security and privacy issues“, *International Journal of Computer Applications,* vol. 90, No. 11, 2014.

[16] V. Coskun, B. Ozdenizci, K. Ok, “A survey on near field communication (NFC) technology“, *Wireless personal communications,* vol. 71, pp. 2259-2294, 2013.

[17] S. Al-Sarawi, M. Anbar, K. Alieyan, M. Alzubaidi, “Internet of things (IoT) communication protocols: review“, *8th International Conference on Information Technology (ICIT),* pp. 685-690, 2017.

[18] M. El-hajj, A. Fadlallah, M. Chamoun, A. Serhrouchni, “A survey of internet of things (IoT) authentication schemes“, *International Conference on Information Technology (ICIT),* pp. 202-207, 2019.

[19] Z. Chen, F. Xia, T. Huang, F. Bu, H. Wang, “A localization method for the internet of things“, *The Journal of Supercomputing,* vol. 63, pp. 657-674, 2011.

[20] T. Huang, Z. Chen, F. Xia, C. Jin, L. Li, “A practical localization algorithm based on wireless sensor networks“, *IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing,* pp. 50-54, 2010.

[21] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, M. Rossi, “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),* pp. 1-7, 2012.

[22] N. Apthorpe, D. Reisman, N. Feamster, “A smart home is no castle: Privacy vulnerabilities of encrypted IoT traffic“, *ArXiv, abs/1705.06805,* 2017.

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

[24] A. Sivanathan, D. Sherratt, H.H. Gharakheili, A. Radfordy, C. Wijenayake, A. Vishwanathz, V. Sivaraman, “Characterizing and classifying IoT traffic in smart cities and campuses“, *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS),* pp. 559-564, 2017.

[25] A. Sivanathan, H.H. Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath, V. Sivaraman, “Classifying IoT devices in smart environments using network traffic characteristics“, *IEEE Transactions on Mobile Computing,* vol. 18, No. 8, pp. 1745-1759, 2019.

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

[27] H.F. Atlam, G.B. Wills, “IoT security, privacy, safety and ethics, digital twin technologies and smart cities“, *Springer Nature,* pp. 1-27, 2020.

[28] L. Xiao, X. Wan, X. Lu, Y. Zhang, D. Wu, “IoT security techniques based on machine learning“, *ArXiv, abs/1801.06275.,* 2018.

[29] W. Zhou, Y. Zhang, P. Liu, “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,* vol. 6, No. 2, pp. 1606-1616, 2019.

[30] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, N. Feamster, “Spying on the smart home: privacy attacks and defenses on encrypted IoT traffic“, *ArXiv, abs/1708.05044,* 2017.

[31] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, “Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations“, *IEEE Communications Surveys & Tutorials,* vol. 21, No. 3, pp. 2702-2733, 2019.

[32] M.R. Shahid, G. Blanc, Z. Zhang, H. Debar, “IoT devices recognition through network traffic analysis“, *IEEE International Conference on Big Data (Big Data),* pp. 5187-5192, 2018.

[33] I.F. Akyildiz, M.C. Vuran, *Wireless Sensor Networks.* Wiley, 1st Edition, 2010.

[34] A. Zamfiroiu, B. Iancu, C. Boja, T.M. Georgescu, C. Cartas, M. Popa, C.V. Toma, “IoT communication security issues for companies: Challenges, protocols and the web of data“, *Proceedings of the International Conference on Business Excellence, Sciendo,* vol. 14, pp. 1109-1120, 2020.

[35] L. Tightiz, H. Yang, “A comprehensive review on IoT protocols, features in smart grid communication“, *Energies,* vol. 13, Page 2762, 2020.

[36] J. Rodriguez, *Fundamentals of 5G Mobile Networks.* Wiley, 1st Edition, 2015.

[37] L. Nithyanandan, I. Parthiban, “Vertical handoff in WLAN-WIMAX-LTE heterogeneous network through gateway relocation“, *International Journal of Wireless & Mobile Networks (IJWMN),* vol. 4, No. 4, 2012.