Journal Pre-proof

Intelligence and security in big 5G-oriented IoNT: An overview

Fadi Al-Turjman

PII: S0167-739X(19)30107-4
DOI: https://doi.org/10.1016/j.future.2019.08.009
Reference: FUTURE 5139

To appear in: *Future Generation Computer Systems*

Received date : 14 January 2019
Revised date : 7 June 2019
Accepted date : 6 August 2019

Please cite this article as: F. Al-Turjman, Intelligence and security in big 5G-oriented IoNT: An overview, *Future Generation Computer Systems* (2019), doi: https://doi.org/10.1016/j.future.2019.08.009.

Intelligence and Security in Big 5G-oriented IoNT: An Overview

Fadi Al-Turjman
Computer Engineering Dept., Antalya Bilim University, Antalya, Turkey
Fadi.alturjman@antalya.edu.tr

***Abstract*— Internet of Nano-Things (IoNT) overcomes critical difficulties and additionally open doors for wearable sensor based huge information examination. Conventional computing and/or communication systems do not offer enough flexibility and adaptability to deal with the gigantic amount of assorted information nowadays. This creates the need for legitimate components that can efficiently investigate and communicate the huge data while maintaining security and quality of service. In addition, while developing the ultra-wide Heterogeneous Networks (HetNets) associated with the ongoing Big Data project and 5G-based IoNT, it is required to resolve the emerging difficulties as well. Accordingly, these difficulties and other relevant design issues have been comprehensively reported in this survey. It mainly focuses on security issues and associated intelligence to be considered while managing these issues.**

***Index Terms* — IoNT, Security, Big Data, Design factors.**

I. Introduction

The Internet of Nano-Things (IoNT) has transformed the use of Internet in recent years with various nanotechnology applications [1]. Recent improvements in nanotechnology and design of nanoscale components (e.g. nano-sensors, nano-antenna, nano-routers, nano-interfaces, etc.) have given rise to a new class of applications and services in various domains and industries such as health [2] and agriculture [3], and have stimulated the evolution of a new nanonetworking paradigm [1][2][3]. IoNT is defined as an interconnection of nanoscale devices with the current communication technologies and the Internet [4]. Terahertz band communication is utilized through new developments in areas such as spectrum management and antenna design to obtain data from various objects. All these developments in turn result in the discovery of novel applications. For instance, environmental nano-sensors can provide information about allergens and pathogens in a given environment while on-body nano-sensors can collect electrocardiographic and other similar important signals [1]. By combining this information through IoNT, it would be much easier to monitor and diagnose a patient's conditions more accurately [1]. The IoNT paradigm is characterized by a very large number of nano-devices, gateways, and Internet communication protocols. It can lower the deployment cost and data processing complexity in several domains. However, it is really important to take into account critical properties for the IoNT such as security, privacy, reliability, confidentiality, and interoperability in the emerging big-5G oriented paradigms.

A. Comparison to other surveys

There have been a few surveys conducted in relation to the IoNT field. For example, in [5], authors have touched slightly the IoNT concept, focusing on the differences against two other similar paradigms, namely the Internet of Things (IoT) and the Internet of Everything (IoE). Authors have distinguished between IoT and IoE, which have wrongly considered the same. They briefly present scenarios for the possible future expansion of their applications without focusing a lot on the IoNT paradigm itself [5]. In [6], potential applications have been overviewed and authors conclude that IoNT is still in the nascent stage. Sooner it can be implemented in several other relevant applications [6]. So, the focus was mainly about the IoNT applications rather than relevant design aspects. In [7], the main objective was to overview the IoNT architecture. Authors have briefly mentioned a few challenges in IoNT for diverse areas. However, they ignored critical aspects such as security, privacy and cost issues. Another relevant survey has been proposed in [8]. This survey reviews the state of the art in electromagnetic communication between the nanoscale devices. Major challenges in terms of channel modeling, and encoding for nanonetworks have been discussed [8]. In [9] and [10], authors have focused only on the medical application of IoNT. In [9] for instance, authors provide a brief analysis of the IoNT performance in healthcare applications and services. In [10], the Internet of Bio-Nano Things (IoBNT) is introduced. Based on biological cells, and their functionalities in the biochemical domain, the IoBNT has been claimed as a potential intra-body sensing and actuation paradigm. It focuses mainly on environmental control of the toxic agents and pollution. Challenges that have been faced in developing efficient and safe techniques for the exchange of information, interaction, and networking within the biochemical domain are outlined. Nevertheless, both surveys [9] and [10] are restricted to healthcare applications only. In [11], authors have proposed a survey focusing mainly on molecular aspects of the IoNT. It considers nanonetworks for the short-range communication based on calcium signaling and molecular motors. Challenges, such as the development of network components, molecular communication theory, and the architectures, are presented and discussed briefly. In [12], authors have surveyed and extended relevant IoNT simulation tools. However, they focused again on nanonetworks operating in healthcare applications only, in addition to being a restricted survey for simulation tools only. Meanwhile, authors in [13] have restricted their survey to signal propagation models in nanocommunication networks. These studies and surveys have emphasized the demand for the nano-scale networking technology (i.e., IoNT) due to its importance in monitoring and fulfilling critical/vital missions in our daily life. However, it is essential first to secure this technology and apply the required intelligence while using its limited resources. Unlike the aforementioned surveys, this survey provides a comprehensive overview on various relevant studies in the

literature, while considering potential IoNT applications and market opportunities. We overview the agreed on IoNT architecture and its vital design issues. We focus mainly on intelligence and security issues in the IoNT, while being integrated with one of the vital communication paradigms, which is the 5G in the emerging big data era. Potential attacks/attackers have been outlined and overviewed. Promising solutions and a comprehensive categorization for these attacks have been discussed as well. Moreover, we spot the light on key open research issues, such as the need for IoNT-specific authentication/communication mechanisms, the development of more reliable components, and the need for a new secure IoNT architecture that pave the way for the deployment of nanonetworks everywhere in the emerging 5G/Big data era.

B. Paper scope and contributions

The aforementioned examples are just a few areas where IoNT and nano-sensing technology have made great enhancements. On top of all the studies presented, for efficient use of the new spectrum introduced for IoNT, it is necessary to investigate the challenges and opportunities introduced by the IoNT concept. In this survey article, we present an overview for the IoNT and focus on the strategies to be considered while dealing with the challenges introduced by the IoNT paradigm. Accordingly, our main contributions in this work can be summarized as follows:

- This article provides a critical overview of the IoNT in 5G/Big Data communication systems, while outlining the common network architecture, restrictions, and significant design factors.
- Related intelligence and cognition techniques are discussed and criticized.
- Security measures and requirements have been outlined for easy access.
- Expected and common attacks are overviewed in addition to classifying their attacker's types.
- Potential communication technologies have been overviewed and classified.
- Specific tools and assessment methods have been reported as well.
- Numerous security challenges facing the IoNT in 5G/Big Data communication systems are comprehensively discussed and outlined.

The rest of this article is organized as follows. The market opportunity relying on the 6V's in big data project is provided in Section II. Section III presents the common IoNT architecture. Significant design factors in IoNT are discussed in Section IV. In Section V, applied intelligence techniques have been reported and classified. Security requirements in the IoNT paradigm are discussed in Section VI. The physical layer discussions and the commonly utilized communication technologies are presented in Sections VII and VIII respectively. Section IX outlines critical restrictions caused by nano-communications in the IoNT paradigm. In Section X, useful assessment methods and benchmarking tools are overviewed. Classified attackers and security attacks are overviewed in Section XI. Section XII gives future research directions and discusses some open research issues. Finally, Section XIII concludes this survey article. For more readability, used abbreviations along with their brief definitions are provided in Table 1.

Table 1. The list of used abbreviations.

Term	Abbreviation
IoNT	Internet of Nano-Things
5G	5th Generation of cellular networks
BAN	Body Area Network
Wi-Fi	Wireless Fidelity
GSM	Global System for Mobile Communications
ML	Machine Learning
IoT	Internet of Things
GW	Gateway
NMI	Nano- to Micro- Interface
SPA	Shortest Path Approach
NNA	Nearest Neighbor Approach
E3A	Enhanced Energy Efficient Approach
THz	Terahertz
TEG	ThermoElectric Generator
MIMO	Multiple Input Multiple Output
EM	Electro-Magnetic
LoS	Line of Sight
HDFS	Hadoop distribution file system
MAC	Medium Access Control
YARN	Yet Another Resource Negotiator
RDD	Resilient Distributed Datasets
DoS	Denial of Service
HetNets	Heterogeneous Networks
QoS	Quality of Service
SVM	Support Vector Machine
SPP	Surface Plasmon Polariton
AGNRs	Armchair Graphene Nanoribbons
MITM	Man-in-the-Middle
PLS	Physical Layer Security
URLLC	Ultra-Reliability and Low-Latency Communication
NAN	Neighborhood Area Network
HAN	Human Area Network
NB-IoT	Narrow Band IoT

II. IoNT Market Opportunity in 5G/Big Data Era

The number of connected devices is expected to rapidly increase in the coming years. In order to provide efficient interaction between these devices, intelligent communication paradigms are required. These intelligent paradigms are able to effectively process data of varying sizes and complexities in order to satisfy the rapidly growing Big data project. Keeping in mind, Big data is mainly defined by six dimensions commonly called the 6 V's:

- **Volume** refers to the amount of data that is generated. It encompasses the available data that are out there and need to be assessed for relevance.
- **Velocity** indicates the speed at which data are being generated. Data can be generated and may require to be processed in real-time. Also, data source can be online or offline. As a result, data processing can be classified as batch and stream processing. Batch processing typically works on stored data while stream processing aims to analyze the data in real-time as it is generated.
- **Variety** refers to the issue of data being in incompatible formats and disparate. It may take significant amount of time to preprocess data that comes in from different sources and in many forms. Data can be structured into a model with predefined columns, data types and so on,

whereas unstructured data such as documents, emails, videos etc. may not have a defined form.

- **Veracity** refers to the uncertainty of data. Uncertainty can be in the form of bias, noise and abnormality. It may be because of poor data quality. Identifying the relevance of data and ensuring data cleansing is required to only store valuable parts and dispose the rest. The main challenge while streaming high-velocity data is the limited time to verify that the data is suitable, can be used for the intended purpose and applicable to the analytic model.
- **Variability** dimension of big data derives from the lack of consistency or fixed patterns in data. It is different from variety in the sense that variability refers to establishing if the contextualizing structure of the data is regular and dependable even in conditions of high level of unpredictability.
- **Value** deals with the worthiness of data to store and invest in infrastructure, either on premises or in the cloud. It refers to aim, business outcome or scenario that the solution has to address. Sometimes, data processing needs to also consider ethical and privacy issues.

According to a market research analysis, it is estimated that the global IoNT will grow at a significant growth rate over 24% from 2016 to 2020 [16]. Significant investments in research and development have notable growth in the IoNT market. For instance, a 480,000,000 USD has been invested in nanomedicine research projects in 2014 [16]. Several other segments including transportation, utilities, etc. have a significant market share in the IoNT as well [16]. It is worth mentioning that this market share has been recognized by key vendors such as Alcatel-Lucent, Cisco, IBM, Intel, and Qualcomm. The increasing utilization of nanotechnology in the aforementioned 6Vs, is one of the most important factors leading to the growth of IoNT market on a global scale. Nevertheless, interoperability concerns and the absence of the realistic testbeds can significantly degrade the success of the IoNT in the market.

III. IoNT Architecture in 5G/Big Data

Understanding the architecture of IoNT helps us to obtain a clear insight about the required security functionalities. Majority of the reported studies in the literature [1]-[4] have agreed on the following common components of the IoNT architecture presented in Fig. 1:

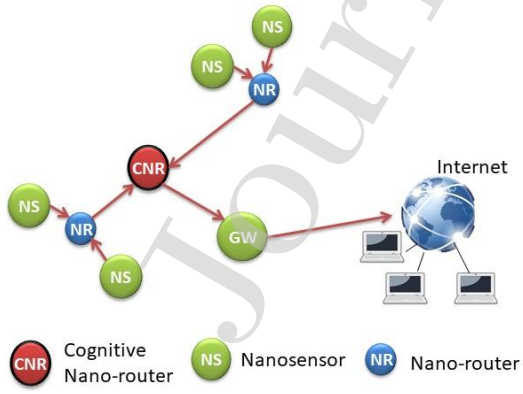

Fig. 1 Network architecture and main components in the IoNT.

Nano-nodes: These are the end-points such as nano-sensors and nano-actuators, which are able to perform simple computation and processing tasks. Due to their limited communication capabilities, reduced energy, and limited memory, they can only transmit over very short distances.

Nano-routers: Compared to the nano-nodes, nano-routers have better computation/communication capabilities in order to collect and relay information from the nano-nodes.

Interface devices (GW): Information forwarded by nano-routers is aggregated by nano-to-micro interface devices. These devices can handle information from microscale to nanoscale devices, and vise versa. Nano-micro interfaces can be considered as hybrid devices, which are able to communicate in nanoscale using nano-communication technologies. In addition, they can also use classical communication models in micro/macro communication networks and act as the gateway (GW) to the Internet.

The IoNT architecture can also be intelligently customized according to the targeted application in order to achieve specific goals. For example, in [14], the nano-routers forward the collected data to cognitive relay nodes that is usually connected to the Internet for remote processing. These cognitive nodes act and make decision based on the nano-network conditions in order to save considerable amount of energy in the entire system. Authors have compared the performance of such intelligent/cognitive IoNT routing against two typical routing approaches, namely the shortest path approach (SPA) and the nearest neighbor approach (NNA), while varying the time period during which a data request might occur as shown in Fig. 2. Obviously, there was a significant improvement in terms of the network lifetime. Moreover, there was a noticeable improvement in terms of number retransmission due to failure in packet reception rates. It was shown that intelligence in IoNT can lead dramatic decrements in these failure rates as depicted in Fig. 3.

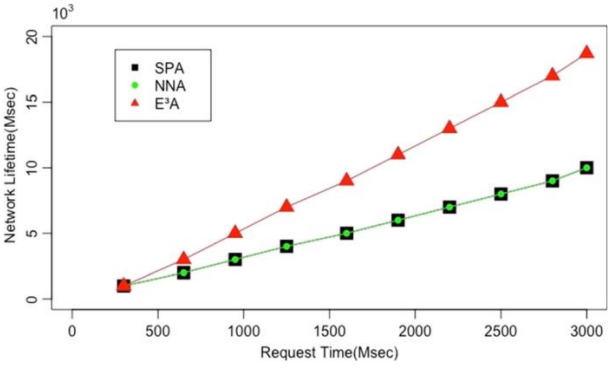

Fig. 2. Comparison of network lifetime vs. the request time [14].

As for the general big data infrastructure, it includes both the big data analytics and the Internet-based components, which are required for the best performance in terms of security, high accuracy and low latency. The main components can be summarized as follows: 1) Data management tools (infrastructure), 2) Data registration, classification, prediction, and visualization, 3) Data analytics, and 4) Collaborative data gathering and sourcing as depicted in Fig. 4.

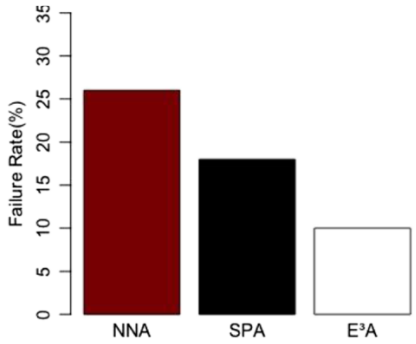

Fig. 3. Comparison of the failure rates in transmissions [14].

IV. IoNT Design Factors

5th generation of cellular network (5G) is expected to be available in the market soon. One of the main objectives specified is to have ubiquitous communication anytime and anywhere between anyone and anything. In this section, the most important design factors of the IoNT paradigm that will significantly affect the performance in terms of security, energy efficiency, and quality of service (QoS), are discussed [29].

A. mm-Waves

Antennas and graphene transceivers are employed popularly in the IoNT paradigms [25]. However, although this provides potentially good data rates with frequency in the range of 0.1 to 10 THz, because of the very low wavelength, the practical range has been reduced to around 10 mm [26]. Where the vision of the emerging millimeter-waves (mm-Waves) communications has appeared to unleash wavelengths between 1 to 10 mm spectrum with the potential of over 100 GHz of a new spectrum suitable for wearable devices and its IoNT applications. In fact, the use of mm-Waves has several advantages, especially from the perspective of security and privacy issues. In [30] for instance, the Anntenna Subset Modulation (ASM), was used to secure data exchanged in mm-Waves. ASM accomplishes intelligent symbol discovery at a selected direction, while experiencing high errors in the other directions. In [31], security was investigated in correspondence to experienced delays, while utilizing analog beamforming with phase shifters in order to diminish the framework cost. In [32], a new mm-Waves technique, called Silent Antenna Hopping (SAH) was proposed in order to additionally improve the attainable security. SAH guarantees scrambling the constellation points of the signal amplitude/phase in the undesired directions, while maintaining a clear constellation in the selected/desired direction. Hence, data exchanged in a specific direction can be successfully secured.

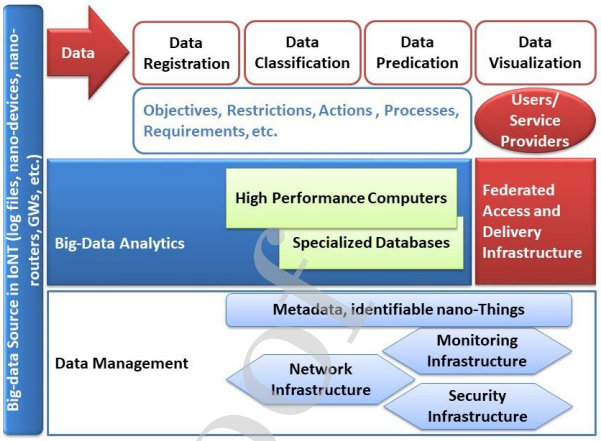

Fig. 4. Big-Data infrastructure and components.

B. Energy harvesting

Energy harvesting is a crucial factor in the IoNT paradigm. For example, in the case of nanoscale batteries, they cannot store much energy for long duration. Thus, the IoNT-specific solutions/implementations should be energy efficient to extend the overall network lifetime. Recent studies have emphasized the demand for energy scavenging methods as well. For example, energy can be extracted from temperature differences using thermoelectric generators (TEGs) and results can be visualized on handheld devices such as PDAs and/or smartphones [19]. A simplified system architecture has been shown in Fig. 5.

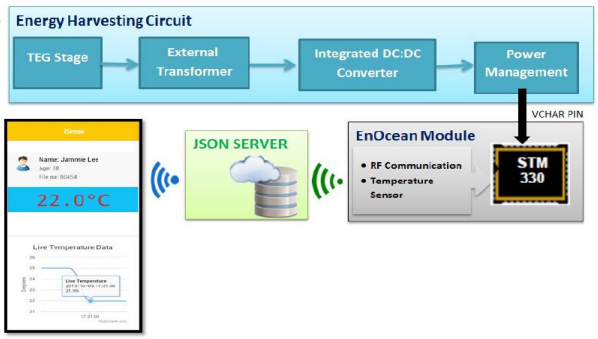

Fig. 5. System architecture for energy harvesting using TEGs [19].

In Fig. 6, the output voltage of the TEG is between 0 – 0.6 V and the maximum achievable power was around 250 µW. Obviously, any increment in the temperature difference can lead noticeable increment in the output voltage, and thus, the generated power [20]. Energy harvesting has been considered as the preliminary design factor for the assessment of the proposed algorithm in [21], as well. Authors in [22] propose a routing algorithm for multi-hop data transmission, which is enabled by the latest developments in the physical layer coding while harvesting more energy. Energy harvesting and security are assessed as the preliminary design metrics in the proposed algorithm in [23]. In [24], a routing scheme for energy harvesting in terahertz band was proposed. The routing scheme assumes a hierarchical cluster-based architecture. Packet transmission from the source to the cluster-head or nano-controller can be direct or multi-hop based on the probability of saving energy through transmission, optimizing throughput and minimizing nano-sensors load.

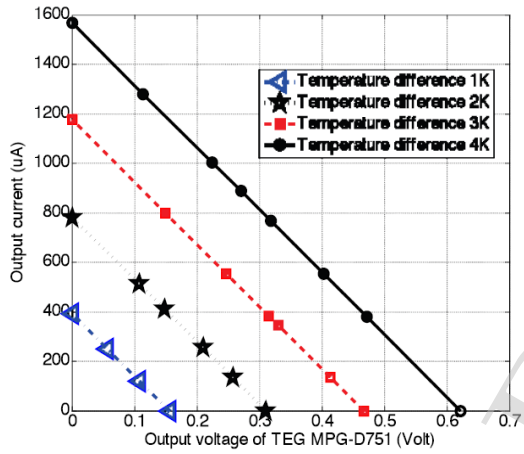

Fig. 6. Simulation results for a commercial TEG [20].

In [25], an in-depth overview of nano-sensor technology and electromagnetic communication among nano-sensors is provided by considering energy-harvesting, security and terahertz channel modelling.

C. Quality of Service (QoS)

QoS features such as capacity enhancement and channel bonding where the channel can be coupled with an adjacent channel that have same frequency band to enhance data transmission rate, symmetrical streaming and enhanced uploading speeds have been examined in the literature. Considering the necessary IoNT high data rate, the emerging 5G technology can make a good communication medium in smart NANs and HANs where most of data congestions occur. Hence, QoS metrics such as jitter, bandwidth, delay, latency shall be well maintained in IoNT. Accordingly, QoS-aware routing protocols has been proposed in the literature to support numerous IoNT big data applications [33]. Cluster based routing protocols, which helps to minimize the distance between cluster heads and the cluster sensors while focusing on surveillance and safety applications with balanced energy distribution has been proposed in [34]. A QoS-aware energy management approach has been proposed in [35]. However, the finite battery capacity is a significant problem that needs further investigations, especially in biomedical applications. Since the majority components of the aforementioned IoNT architecture are communicating via mm-Waves (or the Terahertz band), significant restrictions including the LoS and signal attenuation issues can evolve. Hence, intelligence and learning techniques can play a key role in improving the QoS.

Table 2. Considered design factors in secured IoNT.

Ref.	mm-Waves	Energy-harvesting	Security	QoS
[21]	X	X	X	X
[22]	X	X	X	X
[23]	X	X	X	-
[25]	X	X	X	-
[26]	X	X	X	-
[27]	-	X	X	-

A summary of the aforementioned design factors is presented in Table 2.

V. Intelligence and IoNT

The IoNT instrumented and interconnected paradigms make the best use of information obtained from sensors and systems at the different scales in case an intelligent approach has been employed. It is typical in any IoNT paradigm to observe the employment of Artificial Intelligence (AI), especially the Machine Learning (ML) techniques, while offering the best life style to citizens in order to enhance usage of the available network resources. Besides using ML method to optimize the performance and the operation of the IoNT network, it can also be used to understand and find insights on the collected data. For instance, ML can be used in healthcare systems to understand the patient disease evolution, enhance the general health monitoring, diagnose any health issue, or predict any health breaks ahead. ML techniques can be classified in general into three main categories. This classification is mainly based on the kind of the data and the objective of the desired IoNT network task. The three categories are as follow.

1) Supervised learning

This is the well-established, and the most used technique. It uses the data to make accurate predictions and learn the mapping between the input and its corresponding outputs, while receiving the learning process feedback to identify/correlate things based on the most similar features. Approaches in this category, are used to predict an outcome, or classify the input into a set of desired classes. Most common approaches in this category can be the regression algorithms, the support vector machine (SVM), and the neural network approach. In order to introduce the training employed in these techniques, usually a function that can best approximate the relation between the input and output data is defined. This function can be linear, nonlinear, polynomial, fully connected neural network, etc. Then a cost function is set to tell the learner how much it is far from the best answer, so it acts as a feedback signal. In turn, at each iteration this signal is used to update the parameters of the function. Finally, this function is used to predict the future input or classify the unseen data.

2) Unsupervised learning

Unlike supervised learning that use labelled data, unsupervised learning has no labels and no feedback signal. This technique is mostly used to find the hidden structure of

the data, and move it into similar groups. So, they are mainly used in pattern recognition and descriptive modelling. These types of algorithms are promising to achieve the general artificial intelligence, but they usually lack behind the supervised learning in terms of accuracy and delay. K-means, and autoencoder are the most popular unsupervised algorithms.

3) Reinforcement learning (semi-supervised)

This technique resembles to high extend the way humans can learn through their daily life tasks. Reinforcement learning, is neither fully supervised, nor unsupervised, it is kind of a hybrid approach, which gather the advantages of both.

Online IoNT big data is supposed to be generated and processed almost instantaneously. The change in the structure of data, and its type can be a key challenge for the learning technique and needs to be addressed with advanced adaptive algorithms. Typically, developing and deploying learning techniques can take time, but most of this time is spent on understanding and preprocessing the data. Efficient learning can only be possible when usable and valuable data is available at training stages. Some issues such as data redundancy, inconsistency, noise, heterogeneity, transformation, labeling for (semi-)supervised learning, data imbalance and feature selection need to be addressed during the data pre-processing stage. In the following, we further elaborate on these issues.

- **Data redundancy** and duplication means that at least more than one instances of data represent the same value. Redundancy does not create additional value and creates problems for techniques such as pairwise similarity comparison.
- **Data noise** indicates the parts of the data that needs to be cleaned from missing and incorrect values. Data sparsity and outliers create noise in machine learning models. Manual or human-wise methods are not scalable and inefficient.
- **Data heterogeneity** means different data types, different file/data formats, and variability among samples.
- **Data discretization** is the process of converting quantitative data to qualitative data. This process is required for some algorithms like Naive Bayes and Decision Trees.
- **Data labeling** is required for supervised, semi-supervised learning, transfer learning and active learning. Online crowd-generated repositories can be source for free annotated data.
- **Imbalanced data** is common for the cases of rare events such as credit card fraud detection. Special care is required for leaning from imbalanced data and typically, data sampling is performed.
- **Feature selection** is the identification of data properties, which have the most influential effect. Feature engineering requires prior domain knowledge and feature selection process is labor intensive.

VI. Security and Privacy Requirements

This section is mainly focusing on privacy and security requirements for IoNT in 5G/Big-Data applications.

A. Confidentiality and Authentication

To ensure the confidentiality of data transmission between the IoNT hubs, encryption-based techniques are generally collaborating towards a reliable storage in the 5G-oriented Big-Data. Authentication also is an essential requirement of the emerging 5G-oriented networks and it is of utmost importance to allow only authentic users for service/data access in heterogeneous systems such as those found in the IoNT era. Thus, IoNT devices are supposed to intelligently verify the system user and their connected gadgets. However, current identification and authentication methods are not sufficient for the emerging 5G-oriented IoNT applications where transparency and reliability are key elements.

B. Privacy

In IoNT some common attacks, such as the malware in smart devices and mobile applications, are hacking the Big Data servers, capturing information in wireless communications and leading to sensitive data leakage. And this can significantly threaten the user privacy in in IoNT applications. Specific data can be used in hacking the IoNT user privacy such as, repurposed data, published data and leaked data. To stay away from unauthorized hackers, effective countermeasures such as anonymous and encryption techniques in addition to privacy protection mechanisms must be applied.

C. Time-Criticality

Considering the mobility factor in a typical wearable IoNT networks, strict constraints shall be expected. Especially, when we are dealing with time-sensitive data, which cannot tolerate any mistake and could have disastrous influences, if it has not been met in a timely manner.

D. Availability

Generally, availability implies that devices should be accessible whenever it is required. Applications and smart devices should continue functioning even while they are prone to attacks. Thus, smart devices must have the ability to recognize any unusual behavior and have the capacity to stop the system attack. Security components in these devices should have solid defense and adaptive techniques to intelligent attacks. However, existing techniques, for example, the firewalls can control the data traffic in the high-level IoNT network but it cannot assure an integrated protection mechanism with the endpoints devices due to their limited computational capacity.

E. Trust

The primary element in any secure IoNT system is the trust factor. With a significant count of independent devices/nodes in the IoNT network, in addition to the presence of human factors, it is highly expected that misbehaviors may occur. In IoNT, users are increasingly concerned about their privacy and must trust the service provider. Accordingly, IoNT networks and service providers, must be mutually controlled by a considerable third party authority that guarantees the trust issue.

F. Intrusion Detection and Predication

Mainly, there are three approaches used in intrusion detection: 1) the anomaly detection, 2) the specification detection, and 3) the misuse detection. However, these approaches need more development in order to cope with the limited IoNT capabilities. Thus, lightweight intrusion detection strategies must be developed and further investigated. On the other hand, prediction of the intrusion in advance can be a better alternative. Because, once we recognized the possibility of attacks, and verified the insufficient protection, dramatic costs can be saved. For example, in [36], a hybrid-biometric approach based on fingerprinting has been developed to enhance traditional intrusion detection mechanisms. It measures the inter-layer data response processing time, and then analyze network traffic to filter abnormal packets. It shows significant improvements in mobile environments and industrial control networks. Thus, it is very important to develop smart applications that achieve security levels via automatic prediction for the varying attacks.

G. Non-repudiation

IoNT users/service providers causing illegal actions must be reliably identified/reported. This is of utmost importance not to allow unauthorized network users to select which message to broadcast or deny for a certain illegal reason.

In order to satisfy the aforementioned security requirements, significant actions have been taken over the planned 5G/Big-Data paradigm while configuring every node in the cluster. These security actions (activities) includes: 1) Scanning and Identification, 2) Authorization and Authentication Review, 3) Cluster Configuration and Deployment Control, and 4) Big Data Security Planning. In Table 3, we overview the intended deliverables out of these actions.

Table 3. Intended IoNT deliverables out of security actions in 5G/Big-Data.

Security Actions	Satisfied security requirement	Deliverables
Scanning and Identification	• Confidentiality and Authentication • Availability • Non-repudiation	• Vulnerability scanning • Foot printing • Manual penetration testing • Manual verification
Authorization and Authentication Review	• Confidentiality and Authentication • Privacy • Trust • Availability	• Review authorization policies • Review exception management and Error handling • Review management and cluster authentication • Review session and users • Identify configuration and privilege issues
Cluster Configuration and Deployment Control	• Intrusion Detection and Predication • Time-Criticality • Confidentiality and Authentication • Availability	• Understand control and data flow • Review the cluster configuration and patch Management process • Identify architectural issues in Big-Data implementation • Review monitoring, logging and backup processes.
Big Data Security Planning	• Intrusion Detection and Predication • Time-Criticality • Confidentiality and Authentication • Availability	• Uncover operational Big-Data risks • Share related expertise on privacy and data risk • Gain understanding for personalized programs and global operations

Apparently, authentication and authorization actions can play a key role in securing any IoNT paradigm, especially in relevant mobile environments. Authentication methods in such environments can be categorized as follows:

- Encrypted password: In this method, an encrypted text (i.e., the password) can be automatically remembered in the utilized mobile environment (e.g., web pages, mobile browser, etc.) over the interface node in the afore-described architecture.
- Proxy-based method: It locates a man-in-the-middle between the nano-/wearable devices and the server over the Cloud in order to authenticate the data access.
- Single Sign-On: This type of the authentication methods enables web/server sites to authenticate a user/device by redirecting them to a trusted identity server, which can attest the identities.
- Graphical passwords: This scheme attempts to leverage humans' ability in remembering images, which have been assigned as passwords. It is believed to consume exceeded memories in comparison to the simple text password method.
- Cognitive authentication: In this method, the user deliver a proof that he knows the secret without exposing the secret itself (e.g., mapping the grid digits with a 4-digit path pattern).
- Hardware tokens: In this type, an external hardware such as a flash memory for example, is used to validate and/or verify the user/device identity.
- Mobile-Phone method: Here the mobile phone is utilized to verify a user via a randomly generated code that is exchanged using the 5G cellular network based on a preregistered cell-phone number.
- Biometric methods: Those methods are utilizing unique human body feature(s) as a mean of authentication, while eliminating the need to carry/memorize anything.

All these methods can vary in their efficiency/appropriateness in the targeted IoNT paradigm based on three important features. These features can be relevant to either security, usability, and/or deployability levels. Authors in [37] have investigated the above-listed authentication methods in terms of these three main features and a detailed analysis and assessment have been provided. It was concluded that most of these methods perform better than encrypted text passwords in terms of security levels. Nevertheless, they might do worse in terms of the other two features; deployability and usability,

which can have critical influences on the IoNT paradigm in this study. Therefore, we are in need for other alternatives that can better perform under mobile circumstances. In [38], authors present a solution to usability/security tradeoff problem using a mobile phone as a hand-held authentication token, and a security proxy, which allows the system to be used with unmodified third-party web services. The main objective is to create a system that is both secure and highly usable. Authors in [39], utilize the motion-sensor behavior for active and continuous smartphone authentication across various operational scenarios. For each sample of sensor behavior, kinematic information sequences are extracted and analyzed to provide accurate categorization for users' actions. A Markov-based decision procedure, using one-class learning techniques, is developed and applied to the feature space for authentication. It was shown that motion-sensor behavior exhibits sufficient discriminability and stability for active and continuous authentication scenarios.

VII. IoNT Physical Layer & 5G/Big Data

The communication in nano-networks can utilize nano-mechanical, acoustic, electromagnetic and chemical or molecular communication. Comparison for the existing communication technologies can be seen in Table 3. The physical signaling is performed at the terahertz (THz) levels. Therefore, due to the necessary antenna sizes, special modulation techniques are required. On the other hand, research studies on use of graphene-based plasmonic materials for antennas to overcome signaling difficulties look promising. For example, in [15], the authors propose a graphene-based plasmonic nano-antenna for communication between nano-devices. They reveal that by utilizing the high wave compression mode of Surface Plasmon Polariton (SPP) waves in Armchair Graphene Nanoribbons (AGNRs), graphene-based nano-antennas can operate at much lower frequencies than traditional metallic antennas of the same size. The large bandwidth in terahertz band communication enables very high speed communication which is envisaged in 5G wireless communication systems [17]. Moreover, the terahertz band offers great amount of spectrum resources, which in turn reveal the potential to support data rates of up to even 1 Tbps [4]. In addition, MIMO techniques can be incorporated in the terahertz band communication in order to increase the data throughput and improve the reliability of the systems [17][18]. The frequency spectrum of terahertz band is already investigated in studies such as [27] for 5G communication systems. Existing studies investigate ways of efficient spectrum allocation through pushing the carrier frequencies into the terahertz band quite extensively. Various antenna designs are proposed for small cells and small coverage areas for this frequency spectrum [27]. QoS related challenges are different when compared to traditional microwave spectrum using larger range cellular infrastructures. To start with, the interference structure in terahertz spectrum using systems can be principally different to what is so far observed at lower frequencies. This structure causes various limitations, which include the need for line-of-sight (LoS) links since reflections will deflect the waves and molecular absorption would significantly affect the signal strength. Therefore, the following challenges are quite important for terahertz spectrum management in 5G communication systems: 1) Implementations of antennas with high directivity to transmit/receive gigantic amounts of data, 2) Solutions for molecular absorption caused by the short wavelength, and 3) Solution for the blockage of high-frequency radiation.

VIII. IoNT Communication Technologies

In this section, we emphasize the different secure communication techniques in the aforementioned IoNT architecture. These techniques can be divided based on the communicating component/device into: *A) Nanosensor to nanosensor/Interface, and B) Interface to Internet communication techniques.*

A. Nanosenor to nanosensor/Interface (GW)

At the nano-scale, there is a common agreement in the literature that millimeter-Waves (mm-Waves) and/or Terahertz (THz) communication technique is the most appropriate technology. It provides a communication method between nanosensors themselves and from the nanosensor to the Interface node (or GW) of the nanonetwork. mm-Waves have been used in the medical filed to transmit patients' vital signs (e.g., the heart rate, pulse, blood pressure, etc.). Several mm-Waves' bands, such as the IEEE 802.15.3c and IEEE 802.11ad, have been opened for the commercial use [40][41][42]. It has emerged as an effective solution for high data transfer rate (Terabits/s). Moreover, it is also efficient in terms of energy consumption. This technology can significantly expand the range of services, which can be provided to public IoNT users and service providers. It has negligible transmission delay, very low collision rates and provides high security levels in real-time communications. Bluetooth Low Energy (BLE) is another short-range communication alternative that can be utilized in IoNT systems since it has a reasonable scope of 1 to 10m. It follows the IEEE 802.15.1 standard to exchange information at a rate of 700kbps/2.4GHz. It is well-known by its low energy consumption.

B. Interface to Internet

Several communication technologies can be used in connecting the nanonetwork interface to the Internet. In the following, we list the most common technologies.

1) ZigBee

Zigbee is the most popu;ar low energy technology that can connect an interface node to the Internet. It operates at frequency equal to 2.4 MHz. Interoperability and compatibility of the connected Zigbee-based devices were the key challenge in the past. However, recently released Zigbee versions aim to have a better operability, regardless of their manufacturer.

2) Wi-Fi

Wireless Fidelity (Wi-Fi) is the most famous and secure communication technology that is largely used nowadays. It has a robust authentication procedure, which can guarantee a secure BAN application. It considers the IEEE 802.11b/g/n standard with transmission frequencies equal to 2.4 and 5 GHz, and a rate of 54 Mbps. The communication range of the Wi-Fi technology is much wider than Zigbee. It also provides higher transmission rates.

3) NB-IoT

Narrow Band IoT (NB-IoT) technology plays an important role in IoNT. This technology consists of 3G, 4G, 5G, LTE, an LTE-A modes that provide the capability of big data transmissions. It rates from 14.4 kbps (for 3G) to 100 Mbps (for 4G) and at a licensed frequency bands 824 MHz and 1900 MHz, respectively. Where the forthcoming 5G technology is expected to operate at rates equal to 20 Gbps, and would definitely have higher coverage range. Moreover, 5G can efficiently handle the interface between the gateway and the Internet [43]. The distinctive feature of 5G is its intrinsic flexibility, which allows supporting several IoNT applications in an optimized way, either using low-band spectrum below 1 GHz, mid-band frequencies from 1 GHz to 6 GHz, or using the high-band spectrum above the 6 GHz [43]. With that being said, NB-IoT technology can be considered the most promising technology in the near future. A summary of the aforementioned communication technologies is presented in Table 4.

Table 4. Summary of the reviewed communication technologies.

Reference	Nanosensor to Nanosensor /Interface	Interface to Internet
[44]	mm-Wave	-
[45]	-	Zigbee
[46]	-	Zigbee
[47]	mm-Wave	-
[48]	BLE	-
[49]	-	Wi-Fi
[50]	-	NB-IoT

- Indicates that the communication technology is not mentioned in the referenced work.

IX. Restrictions in Secured IoNT

Any secured IoNT paradigm has a number of restrictions that can be classified into primary vs. secondary restrictions. Primary restrictions are the most important constraints, which must be satisfied in order to achieve an efficiently secured IoNT paradigm. Energy consumption is one of the primary constraints that has to be satisfied in order to implement a secured IoNT. In IoNT, the full nano-device energy is usually sufficient for transmitting at most one packet. Hence, any retransmission can be very expensive in terms of energy and time (until the nano-device recharge itself). Another primary constraint the deployment of the IoNT components. Several attempts have proposed in the literature to satisfy this constrain. For instance, in [21], the authors assume a grid deployment that has been mapped into a radial deployment for efficient and secured nanonetworks. Radiation exposure must be also considered carefully, especially in the biomedical applications of the IoNT paradigm. Electro-Magnetic Fields (EMFs) at different spectrums can negatively affect the human body in different ways. For example, the spectrum between 1 MHz to 10 GHz frequency can penetrate through tissues and produce absorbable heat. Therefore, the shared spectrum RF emissions must be considered carefully to avoid such undesired side effects. Meanwhile, the secondary restrictions can be tolerated in specific scenarios. For instance, cost is one of the secondary constraints in any well-secured IoNT network. Nevertheless, it is still of interest to both users and service providers. Typically, the use of 5G technology in connecting the IoNT components to the Internet for extensive data analytics can lower the cost, while facilitating quick setup and integration of new nano-devices [15].

X. Assessment & Tools

The emerging 5G/Big-Data project does not only deal with the massive amount of manipulated data, but also with its usage. With the IoNT, any item or device, even in the nano-scale, can be associated with the Internet, and thus, generate gigantic data amounts. Therefore, sophisticated assessment methods and benchmarking tools are of utmost importance in this era. In the following, we list the common ones.

A. Hadoop

Hadoop platform is used for a wide assortment of techniques that have been created to record, arrange, and test massive amounts of data. Hadoop is including open source devices, methods, and libraries for big data analysis and models. Majority of the other tools/techniques are connected with Apache Hadoop including the HDFS, MapReduce, Mahout, spark, and Hive tools.

1) HDFS

Hadoop distribution file system (HDFS) was developed for big data processing. It can support several users frequently and simultaneously. It is a file system that sits at the bottom of Hadoop architecture made up of data and name nodes with a built-in fault-tolerance by keeping copies of nodes in each other.

2) MapReduce

MapReduce is the most powerful tool in distributed and parallel applications functioning under the umbrella of 5G/Big-Data paradigm. It depends mainly on conquer and divide techniques. This data processing engine with two parts; mapping raw data into key/value pairs and processing, and reducing by combining and summarizing the results in parallel.

3) YARN

Yet Another Resource Negotiator (YARN) is a resource manager, which allows separation between infrastructure and the programming model.

4) Common

A set of common utilities like compression codecs, I/O utilities and error detection.

B. Spark

Apache Spark is also a cluster-computing environment and uses ideas similar to MapReduce model, but improves speed by using in-memory computations. Its response time is significantly faster than MapReduce in processing tasks stored in memory and Hadoop at disk operations. It stores data in memory and provides fault tolerance without replication with abstraction called Resilient Distributed Datasets (RDD). RDD can be understood as read-only distributed shared memory. The RDD was extended to include DataFrames. This allows grouping of collection of data by columns hence it can be thought as RDD with schema. Learning process is through in-memory caching of intermediate results. Spark is easy to

program and supports integration with Java, Python, Scala and R programming languages. It supports multiple data sources, including Cassandra, HBase, or any Hadoop data source. Besides its effective features, Spark has some inefficiencies in terms of stream processing and bottlenecks can occur because of data transfer across nodes using network [28].

C. *Mahout*

It offers wide selection of robust algorithms. Mahout is good for batch processing (not streaming). There is a lack of active user community and documentation. It is commonly claimed to be difficult to set up an existing Hadoop cluster. Configuration problems may occur. Algorithms focus on classification, clustering and collaborative filtering. Extensibility is good but strong java knowledge is required. Mahout is best known for collaborative filtering (recommendation engines) offers similarity measures like Pearson correlation, Euclidean distance, Cosine similarity, Tanimoto coefficient, log-likelihood, and others.

D. Hive

Storage layer also includes data integration tools such as Hive, which allows running standard SQL queries on data stored in the HDFS and NoSQL databases using HiveQL, an extension of ANSI SQL. This is a powerful and simple way to query the system, which then is distributed across MapReduce/TEZ commands, and then runs on top of Hadoop YARN. Metadata for tables and partitions is kept in the Hive Metastore. HIVE provides interactive way of working with big data on a cluster and way easier than writing MapReduce code in Java. It is highly optimized and extensible. Hive is good for online transaction processing and stores data de-normalized as flat text files. No record level updates, inserts or delete are allowed because of not existing relational database underneath.

E. *Sqoop*

Sqoop is another tool that is used to import and export data between relational databases and Hadoop ecosystems. This is useful when HDFS is used as an enterprise data warehouse-preprocessing engine. The idea behind Sqoop that it leverages map tasks of MapReduce framework. It enjoys the following features: 1) Connections with all main RDBMS, 2) Kerberos security integration, 3) Data transfer from RDBMS to Hive or Hbase and vice versa.

F. Apache Hbase

Hbase is a column-oriented NoSQL database utilized in Hadoop, in which client can store substantial quantities of code lines and sections. Hbase has the function, which will perform write/read activities. It additionally supports record level updates, which is not conceivable using HDFS. Hbase gives parallel data capacity by means of the hidden data file frameworks over the cloud servers. Hbase is an open-source code to handle data in petabytes in thousands of nodes. It enjoys the following features: 1) Compatible with Java API for client access, 2) Bloom Filters and Block cache for real-time queries, 3) Linear and modular scalability, 4) Strictly consistent reads and writes, 5) Extensible JIRB shell, 5) Supports exporting metrics via Hadoop, and 6) Convenient classes for backing the MapReduce tasks and Hbase tables.

XI. Security Attackers and Attacks

In this section, we provide a general classification of possible attackers and attacks reported in the literature. We take into consideration the attacks that are expected to be committed in the IoNT against the exchanged messages.

A. Attacker Types

Understanding the nature of the attacker is important for classifying the types of attacks that IoNT might be subjected to in the 5G-Big-Data era. Existing attacker's types can be classified as follows.

- **Active/Passive:** In this category the active attacker generates the messages, however, in the passive one, the attacker is just eavesdropping (spying) the wireless channel.
- **Insider/Outsider:** An authenticated member of the network who can broadcast and receive messages from other members is an insider attacker. Meanwhile, the outsider is considered as a foreign object by the network members and as an intruder. Associated interactions are limited with security protocols.
- **Local/Global:** An attacker can be limited in scope, even if he controls several nodes, which makes him local and limiting his impact on the globe. The global attacker can control several entities that are scattered across the network, thus allowing him to be active on a larger scope.
- **Malicious/Rational:** A malicious attacker is not in search of any kind of personal benefits from the attacks. His aim is to harm the integrity of the network and create havoc. On the other hand, the attacker who seeks personal profit is rational and do not overextend his resources for any intangible gain.

B. Attacks

In the following, we overview the majority of the expected attacks' types in IoNT. These attackes can be either intentional or unintentional (simple and easy to set-up).

1. Intentional Attacks

Misbehaving nodes in IoNT can intentionally deny forwarding messages that it receives from another node in the network, purposefully misinterpret/modify messages, or inject fake information. In the following, we list samples of these intentional attacks.

- **Masquerade:** It is masking the attacker identity to appear like another IoNT node by using false identities, such as public keys.
- **Location Tracking:** The observer can monitor the trajectories of a group of nodes and can use this information for malicious and mundane purposes.
- **Cheating with nano-sensor information:** Attackers alter their perceived location to escape liability. It can be used notably in criminal cases.
- **Denial of Service (DoS):** The attacker breaks down the network by using malicious nodes to forge a significant number of bogus identities, such as IP addresses, with the objective of disrupting the proper functioning of data and information transformation.
- **hijacking:** It means the hacker hijacks the IoNT device and use it according to his own purpose and will. Usually,

it takes only one device to infect the whole network devices. To prevent device hijacking, regular device updates must be performed in addition to strong authentication methods [51].

- **Wormhole:** Typically, this is accomplished by tunnelling messages between two remote nodes of the network. This can occur by using mobile technologies such as the forthcoming 5G. It allows attackers to spread misleading but properly signed messages at the destination area.
- **Man-in-the-Middle (MITM):** In this one, malicious nodes eavesdrop the communication between the IoNT devices and inject false information. Reasonable solutions are strong cryptography, secure authentication and data integrity verifications.
- **Malware and Spam:** Attacks, like spam and viruses, can lead to severe disruptions in IoNT operations. They are typically the work of malicious insiders rather than outsiders who have access to network devices when they are performing software updates.
- **Sybil:** The perpetrator creates multiple identities in an effort to simulate multiple nodes. This type of attacks is significantly hazardous in the constraint dense IoNT networks since a member can also potentially claim to be in a different region at the same time causing substantial security risks and causing chaos in the network.
- **Impersonation (**spoofing**) Attack:** This a case of an impersonation attack, where a malicious node transmits a message on behalf of another member to create chaos in the network. This type of attacks is the reason behind the paramount identity keys distribution in order to identify the origin of the broadcasted messages.
- **Illusion Attack:** It produces an illusion to the members in IoNT when an attacker broadcasts warning messages that do not correspond to the current actual conditions.

2. Unintentional Attacks

Misbehaving nodes in IoNT might unintentionally deny forwarding messages, or unintentionally modify messages. In the following, we list samples of these unintentional attacks.

- **False information:** It transmits erroneous information and data in the network, which might affect the behaviour of other nodes. It can be both intentional and unintentional.
- **Black Hole:** is a network member that has some nodes (gadgets) that refuse to broadcast or forward data packets to the next hop. This attack can be avoided by keeping redundant paths between the sender and destination.
- **Timing:** An attack is labelled as Timing whenever a malicious node receives a time-critical emergency message and do not forward it to their neighbouring members on time in an effort to create a fake delay in transmission and response.

It is worth mentioning that among the many design requirements for ultra-reliability and low-latency communication (URLLC) 5G-services, communication security comes as one of the key priorities to fulfill [52]. In order to satisfy this priority, novel security algorithms are needed to meet the aforementioned security and privacy requirements. Among these requirements, preserving data confidentiality by allowing data access to only authorized network users, comes first. Because data confidentiality in IoNT can be considered as the first line of defense against not only eavesdropping, but also many other attacks such as DoS, MITM, hijacking, spoofing, and illusion. Moreover, devices in IoNT are usually energy-constrained, processing-restricted due to limited CPU and memory, and delay-sensitive. This makes cryptography-based techniques infeasible in the emerging big 5G-oreinted IoNT. Therefore, the use of Physical Layer Security (PLS) approaches for securing IoNT can help a lot. Because, regardless of the computational power and processing complexity the attackers may have, it will be so difficult to decrypt the employed security algorithms [53][54]. In [55] for instance, both maximum ratio transmitting beamforming and the artificial noise beamforming have been examined. It was concluded that the achievable security level is closely affected by attackers density in the network as well as the spatially resolvable paths of both source and destination channels in mm-Waves systems.

XII. Open Research Issues

Several challenges and open research issues are still understudy in the literature and needs careful attention. One of them is the terahertz channel modelling. The IoNT in 5G/big data era need to transmit very large amount of data in a timely and reliable manner. Therefore, the impact of molecular absorption on the path-loss and noise should be accurately analyzed. This can help in identifying the most appropriate transmission window in terms of achievable rates, security, and channel capacity. Another important challenge is related to the utilized MAC protocols. The terahertz band supports very high bit rates and has a specific relation between the available transmission window, the bandwidth for each window, and the transmission distance. Therefore, research into transmission schemes would be beneficial in order to develop novel transmission techniques using the relation between the transmission bandwidth and the transmission distance.

IoNT paradigms are planned to be integrated with cell-phones, household-appliances, sensors, vehicles, and various other edge devices. Since these devices come with application specific control and monitoring procedures, which are integrated with the Internet, security and related issues will continue to be significant open research problems. Especially, in medical applications, attackers can exploit private biological data gathered by both in-body planted and wearable sensors and cause severe influences. Thus, novel authentication schemes, as well as, guaranteed data integrity in IoNT are essential things for the secured personal information. Due to potential security attacks mentioned in this study, it is also necessary to develop novel intrusion detection mechanisms at the nano-level. Existing security mechanisms, which employ strict key managements, are not sufficient for a large-scale IoNT paradigm that can be used in the emerging big 5G-oriented networks. While new security related protocols can be recommended, the performance and energy efficiency should also be taken into account carefully.

Moreover, handheld gadgets are usually little light physical gadgets, which are hard to anchor. They can be stolen or broken. This may affect secrecy, yet in addition the information accessibility. Besides, many hazard partners, life partners, and

relatives can be physically accessed to their connected sensors and/or related accounts.

XIII. Concluding Remarks

The evolving IoNT project is rapidly growing and aiming to advance the quality of life of people. The enhancements in the IoNT and nanotechnology will have a great impact on advanced development in various fields such as healthcare, agriculture, environmental monitoring, and next generation cellular systems, to just name a few. In this survey article, we provided an overview of the IoNT considering the architecture and main security and intelligence issues in the field. We also presented potential communication technologies per the different components employed in the common IoNT architecture. We discussed challenges regarding mm-Waves spectrum management in 5G/Big data systems. Moreover, we spot the light on several open research issues such as radiation exposure and other critical design factors in the IoNT paradigm.

References

[1] S. Balasubramaniam and J. Kangasharju, "Realizing the internet of nano things: challenges, solutions, and applications", *Computer*, 46(2), 2013, pp.62-68.

[2] M. Stelzner, F. Dressler and S. Fischer, "Function Centric Nano-Networking: Addressing nano machines in a medical application scenario", *Nano Communication Networks*, 2017.

[3] K. Bhargava, S. Ivanov and W. Donnelly, "Internet of Nano Things for Dairy Farming", In *Proceedings of the Second Annual International Conference on Nanoscale Computing and Communication*, September 2015, p. 24.

[4] I.F. Akyildiz, S. Nie, S.C. Lin and M. Chandrasekaran, "5G roadmap: 10 key enabling technologies", *Computer Networks*, 106, 2016, pp.17-48.

[5] M. Miraz ; M. Ali ; P. Excell ; R. Picking, "A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)", In proc. Of the IEEE Int. conf. on Internet Technologies and Applications (ITA), Wrexham, UK, Sept. 2015, pp. 219-224.

[6] P. Kethineni, Applications of internet of nano things: A survey, In proc. Of the IEEE International Conference for Convergence in Technology (I2CT) Mumbai, India, April, 2017, pp. 371 – 375

[7] A. Nayyar, V. Puri, D. Le, Internet of Nano Things (IoNT): Next Evolutionary Step in Nanotechnology, Nanoscience and Nanotechnology, Vol. 7 No. 1, 2017, pp. 4-8. doi: 10.5923/j.nn.20170701.02

[8] I. Akyildiz, J. Jornet, (2010). The Internet of Nano-Things. IEEE Wireless Communications. 17. 58 - 63. 10.1109/MWC.2010.5675779.

[9] N. Abu Ali, M. Abu-Elkheir, (2015). Internet of nano-things healthcare applications: Requirements, opportunities, and challenges. 9-14. 10.1109/WiMOB.2015.7347934.

[10] I. Akyildiz, M. Pierobon, S. Balasubramaniam and Y. Koucheryavy, "The internet of Bio-Nano things, "IEEE Communications Magazine, vol. 53, no. 3, pp. 32-40, 2015.

[11] I. Akyildiz, F. Brunetti, C. Blázquez, (2008). Nanonetworks: A new communication paradigm. Computer Networks. 52. 2260-2279. 10.1016/j.comnet.2008.04.001.

[12] G. Piro, L. Grieco, G. Boggia and P. Camarda, "Nano-Sim: Simulating Electromagnetic-based Nanonetworks in the Network Simulator 3," in Proceedings of the 6th International ICST Conference on Simulation Tools and Techniques, Cannes, France, 2013.

[13] I. Akyildiz, J. Jornet and M. Pierobon, "Propagation models for nanocommunication networks," in Proceedings of the Fourth European Conference on Antennas and Propagation (EuCAP), 2010.

[14] F. Al-Turjman, "A Cognitive Routing Protocol for Bio-Inspired Networking in the Internet of Nano-Things (IoNT)", *Mobile Networks and Applications*, 2017, pp.1-15.

[15] J.M. Jornet and I.F. Akyildiz, "Graphene-based plasmonic nano-antenna for terahertz band communication in nanonetworks", *IEEE Journal on selected areas in communications*, 31(12), 2013, pp.685-694.

[16] Global Internet of Nano Things Market 2016-2020, https://www.technavio.com/report/global-it-professional-services-internet-nano-things-market, 2016, Accessed on 14 May 2018.

[17] N. Khalid and O.B. Akan, "Experimental throughput analysis of low-THz MIMO communication channel in 5G wireless networks". *IEEE Wireless Communications Letters*, 5(6), 2016, pp.616-619.

[18] F. Al-Turjman, and S. Alturjman, "Context-sensitive Access in Industrial Internet of Things (IIoT) Healthcare Applications", *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2736-2744, 2018.

[19] R. Kanan, and R. Bensalem, "Energy harvesting for wearable wireless health care systems," IEEE Wireless Communications and Networking Conference, pp.1-6, April 2016.

[20] Mypelt simulation tool., www.micropelt.com/products/mypelt.php

[21] C. Liaskos, A. Tsioliaridou, S. Ioannidis, N. Kantartzis and A. Pitsillides, "A deployable routing system for nanonetworks", In *IEEE International Conference on Communications (ICC)*, May. 2016, pp. 1-6.

[22] R. Zhou, Z. Li, C. Wu and C. Williamson, "Buddy Routing: A Routing Paradigm for NanoNets Based on Physical Layer Network Coding", In *21st IEEE International Conference on Computer Communications and Networks (ICCCN)*, July. 2012, pp. 1-7.

[23] H. Yu, B. Ng and W.K. Seah, "Forwarding schemes for EM-based wireless nanosensor networks in the terahertz band", In *Proceedings of the Second Annual International Conference on Nanoscale Computing and Communication*, September. 2015, p. 17.

[24] M. Pierobon, J.M. Jornet, N. Akkari, S. Almasri and I.F. Akyildiz, "A routing framework for energy harvesting wireless nanosensor networks in the Terahertz Band", *Wireless networks*, *20*(5), 2014, pp.1169-1183.

[25] I.F. Akyildiz and J.M. Jornet, "Electromagnetic wireless nanosensor networks", *Nano Communication Networks*, *1*(1), 2010, pp.3-19.

[26] H. Yu, B. Ng and W.K. Seah, "On-Demand Probabilistic Polling for Nanonetworks Under Dynamic IoT Backhaul Network Conditions", *IEEE Internet of Things Journal*, *4*(6), 2017, pp.2217-2227.

[27] M.T. Barros, R. Mullins and S. Balasubramaniam, "Integrated Terahertz communication with reflectors for 5G small-cell networks". *IEEE Transactions on Vehicular Technology*, *66*(7), 2017, pp.5647-5657.

[28] F. Al-Turjman, "5G-enabled Devices and Smart-Spaces in Social-IoT: An Overview", *Elsevier Future Generation Computer Systems*, 2017. DOI: 10.1016/j.future.2017.11.035

[29] F. Al-Turjman, "QoS–aware Data Delivery Framework for Safety-inspired Multimedia in Integrated Vehicular-IoT", Elsevier Computer Communications Journal, vol. 121, pp. 33-43, 2018.

[30] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," IEEE Trans. Commun., vol. 61, no. 8, pp. 3231–3245, 2013.

[31] L. Wang, M. Elkashlan, T. Q. Duong, and R. W. Heath, "Secure communication in cellular networks: The benefits of millimeter wave mobile broadband," in 2014 IEEE 15th Int. Work. Sig. Process. Advances Wireless Commun. (SPAWC), June 2014, pp. 115–119.

[32] N. N. Alotaibi and K. A. Hamdi, "Silent antenna hopping transmission technique for secure millimeter-wave wireless communication," in 2015 IEEE Glob. Commun. Conf. (GLOBECOM), Dec 2015, pp. 1–6.

[33] Samina, E., Bechir, H. A survey on energy-efficient routing techniques with QoS assurances for wireless multimedia sensor networks. IEEE Communications Surveys & Tutorials, 14(2) (2012) 265-278

[34] Duc, C. H., Parikshit, Y., Rajesh, K., Sanjib, K. P. Real-time implementation of a harmony search algorithm-based clustering protocol for energy-efficient wireless sensor networks. IEEE Transactions on Industrial Informatics, 10(1) (2014) 774-83

[35] E. Ibarra, A. Antonopoulos, E. Kartsakli, J. Rodrigues, and C. Verikoukis, "QoS-aware energy management in body sensor nodes powered by human energy harvesting," IEEE Sensors Journal, vol. 16, no. 2 pp. 542-549, January 2016.

[36] C. Shen, C. Liu, H. Tan, Z. Wang, D. Xu, X. Su, "Hybrid-Augmented Device Fingerprinting for Intrusion Detection in Industrial Control System Networks". IEEE Wireless Commun. vol. 25, no. 6, pp. 26-31, 2018.

[37] J. Bonneau, C. Herley, P. C. van Oorschot, F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes", University of Cambridge Computer Laboratory, Tech Report 817, 2012, www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.html.

[38] M. Wu, S. Garfinkel, R. Miller, (2019). Secure web authentication with mobile phones.

[39] C. Shen, Y. Li, Y. Chen, X. Guan and R. A. Maxion, "Performance Analysis of Multi-Motion Sensor Behavior for Active Smartphone Authentication," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp. 48-62, Jan. 2018.

[40] IEEE 802.15 WPAN Millimeter Wave Alternative PHY Task Group 3c (TG3c).
[41] R. Fisher, "60Ghz WPAN Standardization within IEEE 802.15.3c," 2007 International Symposium on Signals, Systems and Electronics.
[42] A. Hirata, R. Yamaguchi, Y. Sato, T. Mochida, and K. Shimizu, "Multiplexed Transmission of Uncompressed HDTV Signals Using 120-GHz-band Millimeter-wave Wireless Communications System," NTT Technical Review, Vol. 4, No. 3, pp. 64–70, 2006.
[43] A Morgado, KMS Huq, S. Mumtaz, J. Rodriguez, "A survey of 5G technologies: regulatory, standardization and industrial perspectives", Digital Communications and Networks 4 (2), 87-97, 2018.
[44] IEEE802.15.6, IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks, no. February. 2012.
[45] M. Ghamari, B. Janko, R. S. Sherratt, W. Harwin, R. Piechockic, and C. Soltanpur, "A survey on wireless body area networks for ehealthcare systems in residential environments," Sensors (Switzerland), vol. 16, no. 6, pp. 1–33, 2016.
[46] E. Ezhilarasan and M. Dinakaran, "A Review on Mobile Technologies: 3G, 4G and 5G," in 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), 2017, pp. 369–373.
[47] P. Klaynin, W. Wongseree, A. Leelasantitham, and S. Kiattisin, "An electrocardiogram classification method based on neural network," in The 6th 2013 Biomedical Engineering International Conference, 2013, pp. 1–4.
[48] R. Saini, N. Bindal, and P. Bansal, "Classification of heart diseases from ECG signals using wavelet transform and kNN classifier," in International Conference on Computing, Communication & Automation, 2015, pp. 1208–1215.
[49] L. N. Sharma, S. Dandapat, and R. K. Tripathy, "A new way of quantifying diagnostic information from multilead electrocardiogram for cardiac disease classification," Healthc. Technol. Lett., vol. 1, no. 4, pp. 98–103, Oct. 2014.
[50] N. Gawande and A. Barhatte, "Heart diseases classification using convolutional neural network," in 2017 2nd International Conference on Communication and Electronics Systems (ICCES), 2017, pp. 17–20.
[51] "Here Is How to Fend Off a Hijacking of Home Devices," [Online]. Available: https://www.nytimes.com/2017/02/01/technology/personaltech/stop-hijacking-home-devices.html. [Accessed 20 12 2018].
[52] S. A. Alabady, F. Al-Turjman, and S. Din, "A novel security model for cooperative virtual networks in the IoT era," International Journal of Parallel Programming, Jul 2018.
[53] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," IEEE Communications Surveys Tutorials, pp. 1–1, 2018.
[54] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret key generation using channel quantization with SVD for reciprocal MIMO channels," in 2016 Int. Symp. Wirel. Commun. Syst. IEEE, sep 2016, pp. 597–602.
[55] Y. R. Ramadan and H. Minn, "Artificial noise aided hybrid precoding design for secure mmwave MISO systems with partial channel knowledge," IEEE Sig. Proc. Lett., vol. 24, no. 11, pp. 1729–1733, Nov 2017.

Prof. Dr. Fadi Al-Turjman received his Ph.D. degree in computer science from Queen's University, Canada, in 2011. He is a Professor with Antalya Bilim University, Turkey. He is a leading authority in the areas of smart/cognitive, wireless and mobile networks' architectures, protocols, deployments, and performance evaluation. His record spans over 200 publications in journals, conferences, patents, books, and book chapters, in addition to numerous keynotes and plenary talks at flagship venues. He has authored/edited more than 12 published books about cognition, security, and wireless sensor networks' deployments in smart environments with Taylor & Francis, and the Springer (Top tier publishers in the area). He was a recipient of several recognitions and best papers' awards at top international conferences. He led a number of international symposia and workshops in flag-ship IEEE conferences. He is serving as the Lead Guest Editor in several journals, including the IET Wireless Sensor Systems and Sensors, MDPI sensors and the Elsevier Internet of Things.

Highlights

- This article provides a critical overview of the IoNT considering the main application areas, architecture, limitations, and design factors.
- Related intelligence and cognition techniques are discussed and criticized.
- Security measures and requirements have been outlined for easy access.
- Expected and common attacks are overviewed in addition to classifying their attacker's types.
- Specific tools and assessment methods have reported as well.
- Potential enabling technologies from the physical layer up to various routing protocols that can be employed for the IoNT as well as the interaction with the cloud-based infrastructures and Machine Learning (ML) techniques are presented.
- Various challenges regarding terahertz spectrum management in 5G/Big Data communication systems are comprehensively discussed.