computers

MDPI

Article

Challenges of IoT Identification and Multi-Level Protection in Integrated Data Transmission Networks Based on 5G/6G Technologies

Gennady Dik [1], Alexander Bogdanov [2,3], Nadezhda Shchegoleva [2,3], Aleksandr Dik [2,*] and Jasur Kiyamov [2]

[1] LLC "System Technologies", 198515 St. Petersburg, Russia
[2] Faculty of Applied Mathematics and Control Processes, Saint Petersburg State University, 199034 St. Petersburg, Russia
[3] Faculty of Digital Industrial Technologies,St. Petersburg State Marine Technical University, 190121 St. Petersburg, Russia
* Correspondence: st087383@student.spbu.ru

Abstract: This paper illustrates the main problematic issues of minimizing technological risks in the construction of an integrated architecture for the protection of a "smart habitat" (SH). We analyze the use of the IoT to identify both object hazards and the categorization of switching detection in information collection and processing centers. The article proposes wired and wireless data-transmission systems for the required level of efficiency as well as SH protection. Particular attention is paid to the organization of multi-level protection of promising 5G/6G cellular networks based on the analysis of the security threat landscape.

Keywords: infrastructure; wireless technologies; security; smart habitat; IoT; IT-system; 5G; 6G

Citation: Dik, G.; Bogdanov, A.; Shchegoleva, N.; Dik, A.; Kiyamov, J. Challenges of IoT Identification and Multi-Level Protection in Integrated Data Transmission Networks Based on 5G/6G Technologies. *Computers* **2022**, *11*, 178. https://doi.org/10.3390/computers11120178

Academic Editors: Osvaldo Gervasi and Bernady O. Apduhan

Received: 14 November 2022
Accepted: 2 December 2022
Published: 7 December 2022

1. Introduction

One of the significant factors in improving the quality of life of the population in modern conditions is the use of so-called "smart home" technology, which, for the purpose of further development, is evolving in a strategic direction of building the infrastructure of a habitat called a "smart habitat" [1]. The well-known technology "smart home" and then "smart city" (hereinafter referred to as technology) has long been used in the modern world; however, at the same time, the aspect of introducing these technologies in small summer countryside cottages and villages has gained increasing interest (Figure 1).

In these settlements (habitat fragments), there is also a need to automate life processes and ensure the personal and technical safety of residents. This raises the question of smart habitats (SHs) as a more universal and scalable application of an interconnected system of information and communication technologies with IoT [2], which simplifies the management of internal processes of the environment and makes the life of residents more comfortable and safe [3]. When considering the issue of constructing a SH, it is necessary to note two variants of approaches—the creation of a SH and the smart transformation of the habitat in the SH.

As for the issue of creating a SH, this process is a sustainable development of territories in accordance with the principles of new urbanism with the formation of innovative growth points for the region's economy with a new quality of life, while the process of smart transformation of the infrastructure of the habitat (hereinafter referred to as transformation) is the building of a sustainable and solidary system for the development of an area during the innovative and modernizing development of the existing infrastructure in accordance with the needs of modern society [4].

Within the framework of this article, we propose to consider the transformation process, which is of great interest in terms of upgrading the existing engineering infrastructure and IT infrastructure, as well as the risks associated with this process [5].

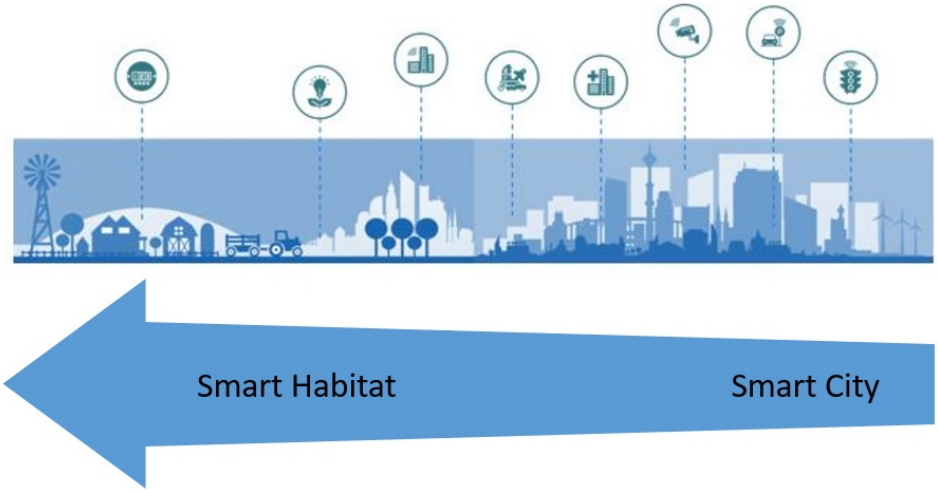

Figure 1. Smart habitats (SHs): integrated technology of a new standard of living.

The risks of the transformation considered include:

1. Technological risks:
   - the growth of waste volumes due to the rapid obsolescence of equipment and its disposal (E-waste);
   - an increase in the volume of data transmitted over networks ("information garbage", which doubles every one and a half to two years on average);
   - the manifestation of vulnerabilities in the software of smart home appliances and other IoT, which lead to a denial of service due to virus attacks ("hole in the teapot");
   - the hacking of personal (particularly medical) smart devices;
   - the presence of problems of leakage of personal data of residents, etc.
2. Legal and political risks:
   - the restriction of human rights and freedoms when using digital personal identification;
   - the existence of a threat of a one-time disconnection from all public services in the case of failures;
   - the use of personal data with criminal intent;
   - the possibility of disclosing personal data by various indirect methods (collection of incriminating evidence on the analysis of the media and social networks);
   - the growth of political, social and economic costs from cyberattacks and data leaks;
   - the development of virtual crime, etc.
3. Economic risks:
   - the development of cryptocurrency turnover makes the commodity-money exchange anonymous (ordering criminal acts, buying narcotic substances and weapons and paying for other asocial acts);
   - moving the shadow economy to the Internet (through anonymous networks, such as TOR).
4. Social risks:
   - depriving a part of the population from access to information and services (a "digital divide");
   - the presence of discrimination and the exclusion of certain categories of citizens from the process of consuming public goods when using smart technologies;
   - the problem of amateurism with the participation of the population in the management of a SH.

Paying the greatest attention to minimizing technological risks, it is necessary to consider options for building integrated architecture for the automation of a SH as the

basis for the formation of an intellectual environment. This is proposed to include various types of infrastructures in this architectural solution in accordance with the following classification (Figure 2) [6].

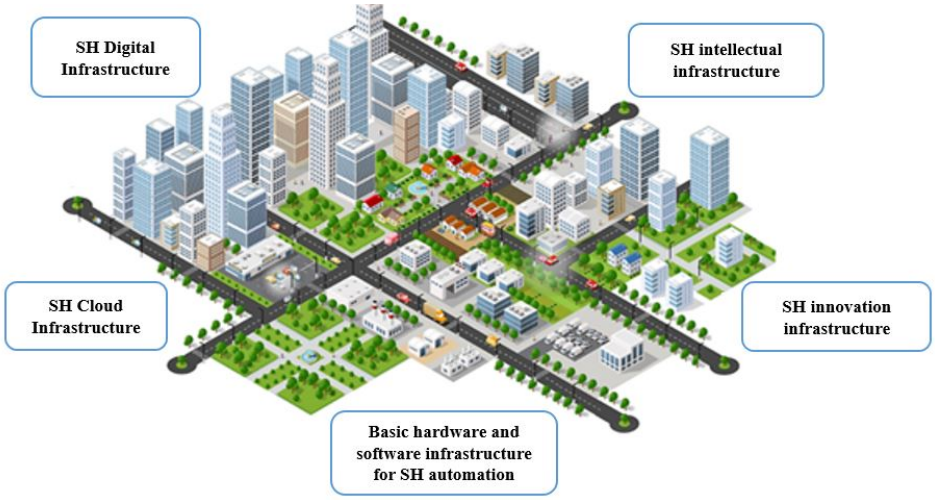

Figure 2. Types of integrated automation architecture for SH.

The central hardware–software infrastructure of SH automation is the basic hardware–software framework of the habitat, which functions in real time. This infrastructure includes a complex of information systems (automated control systems) and a structured telecommunications cable network (switching centers, wired and wireless communication systems, data processing centers, monitoring systems, various sensors, etc.). This allows the system to:

- receive, transmit, process and store relevant information about the life of the SH;
- provide the necessary backup and recovery capabilities as quickly as possible;
- ensure centralized and equal access of consumers to digital services and services of the environment.

The SH digital infrastructure is the digital basis of the habitat, which ensures not only its stable functioning but also information exchange between the participants of the automated (automatic) control system through a single information space, considering the differentiation of access rights to information at different levels. It should include a system of algorithms for organizing permits, methods, norms, rules, requirements and regulations for the operation of subsystems for the monitoring and life support of the SH [7].

The SH cloud infrastructure is a scheme in which various cloud infrastructure components, such as servers (required computing power), data stores (storage area network—SAN), operating systems (OS) and network resources are provided as a connected service [8].

SH users are provided with network access to cloud resources, including the platform, software and desktop (IaaS, PaaS, SaaS and DaaS).

The SH intellectual infrastructure consists of cyber-physical subsystems and complexes of modern protection tools (encryption, coding, etc.), as well as processing the received information using advanced analytics technologies to make the best management decisions. The main purpose of this infrastructure is to ensure the information security and confidentiality of the data circulating in it. The intellectual infrastructure includes a wide range of modern tools and interfaces that provide processing of various kinds of data and the provision of digital services and services as well as methods for automated processing and preparation of decision making, data recognition and decryption, "end-to-end" digital platforms (including cloud platforms), etc.

The SH innovation infrastructure is a set of industries; large, medium and small businesses; institutions; and organizations, which is designed to provide supply and demand

for digitalization within the city. This includes technology centers, engineering centers, an environment for the development of promising areas of research and development (including business incubators, technology transfer centers, venture financing and entrepreneurship support funds), the implementation of promising projects (including design enterprises), as well as a system for collecting and promoting innovative initiatives [9].

All of the infrastructures above create intersecting areas in the SH space, which, as a result of the functioning of the involved information systems, should achieve the most effective interaction, which is impossible without the use of data transmission facilities and networks (DTFNs). In this case, it seems possible to consider the DTFN complex as a scalable full-featured infrastructure hereinafter referred to as the network technology infrastructure (NTI). We propose to include elements of wired and wireless DTFNs with the necessary switching equipment as well as special software functioning in order to interact with all types of infrastructures as part of the SH automation architecture as part of the ICT.

At the same time, at the current moment in the modern world, there is no sufficient awareness of the principles of both the creation of SH and the transformation to a smart environment. In this case, there is no single approach, not only to the system for building the architecture of the SH automation (a complex of the listed infrastructures) but also to the issue of organizing NTI [1].

Within the framework of this article, we investigate the problems of forming a scalable NTI in order to rationally deploy IoT SH to support a large number of devices (the case of the Internet of Things (IoT) of various levels—from meters, sensors and various monitoring devices to real-time terminal devices). At the same time, special attention should be paid to the problem of organizing independent levels of IoT information exchange and NTI control devices as well as—directly related to this process—the issues of the security threat landscape [10].

The authors claim that the dominant contribution to the creation of NTI considers the following issues:

1. Analysis of modern IoT for identification and further categorization to develop options for switching to local centers for collecting and processing information.
2. Analysis of existing wired and wireless DTFNs in order to organize a "network of networks" to maintain the required level of efficiency and safety of SH operation.
3. Identification of information-security issues in NTI based on the analysis of the landscape threat in 5G/6G networks.
4. Organizations of hybrid protection of 5G and 6G networks.

2. Analysis of Modern IoT for Identification and Further Categorization

The period of late 2008–early 2009 is widely known for the fact that, at that time, there was a gradual—but inevitable for the modern development of society—transition from the "Internet of People" to the "Internet of Things", i.e., the number of objects connected to the network exceeded the number of people [11]. Thus, most of the manufactured appliances, such as refrigerators, washing machines and coffee makers, began to have their own processor, own IP address, own computer interface and subsequent connection to the Internet.

Such devices do not require an update associated with going to the store and buying a more modern model. Moreover, they learn the owner's preferences and tastes and also update their firmware by tracking changes on the manufacturer's server. They can also order missing products (by learning the average consumption rates) or necessary components for their functioning, etc.

IoT is a set of different devices and sensors connected by wired and wireless communication channels and connected to the Internet in order to better integrate the real and virtual worlds, and communication is performed between people and devices. It is assumed that, with the development of IoT technology, "things" will become active participants in business, information and social processes, where they will be able to interact and commu-

nicate with each other, exchanging information about the environment and reacting and influencing the processes occurring in the world around them without human intervention.

The interaction under consideration is impossible without the active and comprehensive use of DTFN, which ultimately leads to the fact that it is advisable to consider IoT as a "network of networks", where compact, loosely connected networks form larger and then global networks. We note not only the variety of primary data collection devices (gas, water, heat, electricity meters, fire alarm sensors, etc.) but also the need for centralized transmission to the server through base stations and the processing of incoming information. The information received can be displayed in a personal account on a computer or smartphone; however, it should be possible at any time to receive or send data from devices.

According to Rob Van Kranenburg (Founder of the European IoT Council), the "Internet of Things" is a "four-layer pie" [12]:

- Level 1 is associated with the identification of each object (a Body Area Network—BAN);
- Level 2 is a set of services to serve the needs of the consumer (can be considered as a network of owned "things", a particular example is a "smart home") (a Local Area Network—LAN);
- Level 3 is associated with the urbanization of urban life, i.e., this is the concept of a "smart city", where all the information that concerns the inhabitants of this city is pulled together to a specific residential area, to your house and neighboring houses and then to SH (a Wide Area Network—WAN);
- Level 4 is a sensory planet (a Very Wide Area Network—VWAN).

It should be noted that this definition of levels involves initially defining (identifying) an object and then involving it in an ever-expanding circle of network connections. At the same time, the Internet of Things is inherently a continuous flow of data in space, passing through different networks around us, which leads to the emergence of the so-called "web of things" [13]. At the same time, the performance of this "web" is possible if the following two conditions are met (in contrast to the levels of the four-layer pie:

1. The mandatory identification of each specific object from the IoT (the first level).
2. The continuous switching of the growing volume of information and objects in the network, which, in turn, will also be combined in the network (interrelation from the second to the fourth level of the four-layer pie).

To fulfill the first condition, it is recommended to categorize the IoT in accordance with Table 1 (the use of IoT in the military sphere is out of the scope of the article) according to the generally recognized use cases of the web of things (Figure 3) [14].

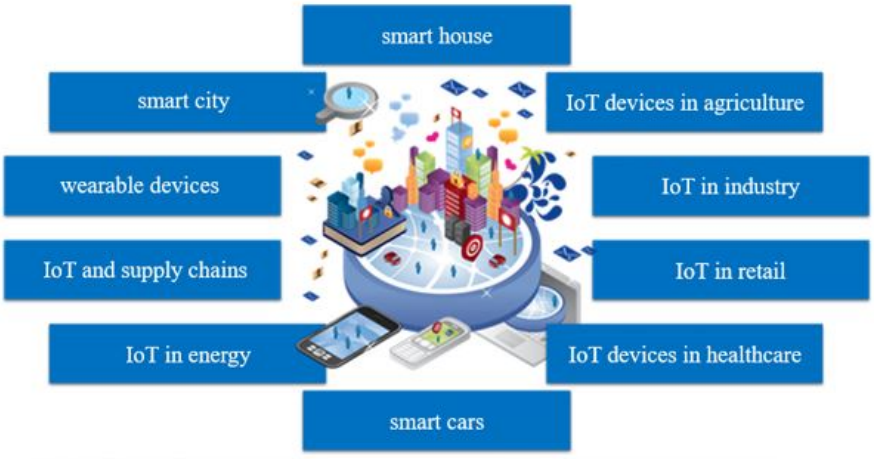

Figure 3. Web of things.

Table 1. Categorizing the Internet of Things by purpose.

The Main Branches and Directions of Vitality	Scope of Application
IT and means of communication	Modern types of communications and communications (5G/6G); cloud services; providing remote access; billing in telecommunications.
Engineering and dispatching	Intelligent planning and control systems production, quality management, etc.; intelligent warning systems (city services, etc.); smart technologies for emergency and urban services.
Trade	New forms of mutual settlements; remote banking technologies; using big data to conduct targeted marketing campaigns; using q-code; electronic services and service delivery portals.
Smart transport	Intelligent control systems/traffic restrictions; video mapping; smart city navigation systems; intelligent public management systems transport; systems for collecting fees, fees, duties, taxes, etc.
Industry [15]	Intelligent technologies for enterprise resource planning (ERP solutions), finding bottlenecks and auditing; green technologies; systems that reduce emissions of CO_2 and harmful substances; monitoring and notification of emergencies; robotization of production.
Healthcare	Intelligent technologies for diagnosis patients based on big data analysis; IoT to control the distribution of drugs, etc.; bionics—new biomaterials and cell technologies in transplantology; telemedicine; color QR codes according to images of faces and a device for implementation [16].
Consumer sector and home	Ensuring energy efficiency (classes, BREAM/LEED); modern automated control systems in the management of buildings and structures; home systems for individual analysis resource and energy consumption.
Power industry [17]	Management information system for resource and energy saving in production; electricity supply and demand management—smart energy market; micro grid—ensuring energy autonomous objects.
Construction	Building information modeling and structures; smart houses; energy-passive and active houses; green houses; technologies that ensure the mobility of personnel and their ability to perform more tasks per unit of time.
Agriculture	Smart devices and monitoring applications patients' conditions; satellite monitoring systems for animals (where they are and whether they got lost during the walk); intelligent systems for managing financial and economic activities.
Logistics	Big data in the management of logistics companies; satellite monitoring systems for transport routes.

This tabular presentation of IoT categorization makes it possible to determine the types, quantity and necessary requirements for the planned terminal devices (gas, water,

heat, electricity meters, fire, medical, game, transport and other sensors, video cameras, etc.). This definition at each level of categories will allow the identification of IoT devices (in accordance with the protocol TCP/IP ver 6 of the transport layer of the OSI network model) [18].

As a conclusion on the issue of identifying and categorizing IoT, there is a mandatory provision of IoT to industries regarding the field of use, scope, etc., as well as a strict definition of the characteristics and purpose for combining into a single information space using DTFNs.

3. Analysis of Existing Wired and Wireless DTFNs in Order to Organize a "Network of Networks" in SH

According to the second condition of functioning of the so-called "web of things", it is necessary to ensure the interaction of the involved IoT. To this end, it is planned to fully use the DTFN complex as a platform for NTI, where compact loosely connected networks (BANs) form larger (from LANs to WANs) and then global networks (VWANs or Global Area Networks (GANs)) [19].

Wired and wireless data-transmission systems (DTS) are used as the standard for DTFNs. Modern wired DTS include the following communication lines

1. Shielded copper twisted pair (UTP, FTP, STP and other types and categories) or "Ethernet".
2. Fiber optic communication lines (fiber optic cable—FOC) is a type of communication in which information is transmitted through optical dielectric waveguides, known as "optical fiber".

In addition to these two widely used DTS, other communication lines based on the RS-232, RS-432, Modbus and other protocols have found applications in practice.

The basics of building networks based on wired DTS, as well as their main advantages and disadvantages, are widely covered in the scientific and technical literature and are beyond the scope of this article. At the same time, when transforming to SH, one should consider both the construction of new wired backbones and the availability, characteristics and capabilities of existing wired DTFNs.

Along with wired DTS, a wireless method of building networks has become widespread, a feature of which is the possibility of organizing communication in a variant inaccessible to wired DTS. In various IoT projects, IoT connections can be based on technologies, such as Bluetooth, Wi-Fi, Lora WAN, ZigBee, Z-wave, 3G, LTE, 5G, 6G and others (Figure 4) [20].

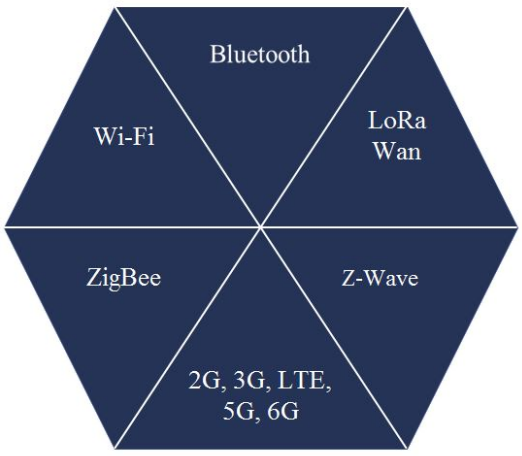

Figure 4. Wireless DTS.

In order to understand the further use of wireless DTS, we consider the main features of these networks [12].

ZigBee is an open wireless communication standard for data acquisition and control systems. ZigBee technology allows the creation of self-organizing and self-healing wireless networks with automatic message relaying and with support for battery and mobile nodes. ZigBee networks provide guaranteed packet delivery at relatively low data rates and protection of the transmitted information [21].

Wi-Fi is a wireless LAN technology with devices based on the IEEE 802.11 standards. This technology connects devices with wireless adapters to a local/corporate network or connects them to the Internet. Some versions of the 802.11 standards group are capable of transfer rates up to 600 Mbps or more [22].

Bluetooth is a technology for wireless data transmission. Bluetooth radio communication is performed in the ISM band, which is used in various household appliances and wireless networks (license-free band 2.4–2.4835 GHz). Bluetooth uses a frequency-hopping spectrum-spreading technique. The FHSS method is easy to implement and provides resistance to broadband interference [23].

LoRaWan is a technology that works as follows—the base station listens to the air in a given frequency range, and, when it hears a request from any of the devices, it responds to it at the frequency of circulation. The channel width in this case is 125 kHz, and the maximum speed is slightly over 5 kilobits/s (quite small). This IoT standard is not suitable for watching streaming video but is the fastest and most guaranteed way to send a small message from a sensor to the base station [24].

Z-Wave is a widely used radio communication protocol for home automation. A characteristic feature of Z-Wave is standardization from the physical layer to the application layer, i.e., the protocol covers all levels of OSI classification, which makes it possible to ensure the compatibility of devices from different manufacturers when creating heterogeneous networks [25].

A comparison of the main parameters of the considered networks is presented in Table 2 [26].

Table 2. Comparison table of the main parameters of wireless DTS.

Wireless Technology	ZigBee	Wi-Fi	Bluetooth LE	LoRaWan	Z-Wave
frequency range	2.4–2.483 GHz	2.4–2.483 GHz	2.4–2.483 GHz	2.4–2.483 GHz	868.42 MHz, 908.42 MHz, 921.42 MHz, 919.8 MHz, 865.2 MHz, 868.20 MHz, 951–956 MHz, 922–926 MHz.
Bandwidth, kbp/s	250	11,000	1024	250	42
Protocol stack size, Kb	32–64	1000 and more	250 and more	20 and more	32
Maximum number of nodes in the network	65,536	10	7	500	232
Action range, m (average value)	10–100	20–300	10–100	10–110	40–120
Current consumption, active mA/sleep mkA	30/1	450/-	15/10	20/1	22/1

At the same time, special attention is paid to wireless DTS—cellular networks of 3G, LTE, 5G and 6G standards due to the distinctive features of the implementation of this method of constructing DTFNs [27].

At the same time, the question arises—if there exist ready-made and run-in solutions, such as WiFi and LTE, why not use them? Why LoRaWAN and later 5G/6G?

There are several reasons. Imagine a house with 400 apartments, each of them having two water meters and an electric meter. Let us say this is a modern house, and each meter transmits readings to the Internet.

Volume. There will be 1200 user meters for one residential building of 400 apartments. They will have penny traffic; however, if they are all located, for example, at an LTE base station, then there will no longer be room for people at this base station. Furthermore, this is one building, and base stations are typically meant for a district or even larger area.

Consumption. If the electricity meter can still be powered, then pulling the cable to the water meter is not convenient. In this case, the radio module of this meter must be battery operated. However, even a good WiFi and LTE battery will be eaten up in a few days (the desired replacement of batteries is once a year at most).

Other priorities. We do not need a 5 Mbps communication channel to transmit once a day how much water has run into each apartment. A few bits is sufficient. We are limited by the power of the transmitter, and it is necessary that this does not eat the battery. Thus, we can use the "more energy per bit—higher probability of reception" rule in such a way that the communication channel at the minimum speed and with the minimum power is guaranteed to cover the required distance even if the signal is below the noise level.

Thus, when transforming during the creation of NTI, an integrated approach to the issue of choosing a DTS is expedient. In this situation, an important role is given to 5G/6G cellular networks, which are expected to provide global coverage of the entire Earth's surface so that users and connected IoT can access the Internet anywhere and anytime [24]. Wireless terrestrial networks need to be combined with air and water off-Earth access nodes. Such communication nodes will include satellites, drones, high-altitude platforms (HAP), surface signal broadcast stations, etc. The seamless 3-D (land, sea and sky) coverage built in this way will form a global integrated communication network, where all terrestrial and non-terrestrial networks will be comprehensively integrated at the system level, thereby, providing the convergence of services, wireless interfaces, various types of networks and connected user devices (Figure 5).

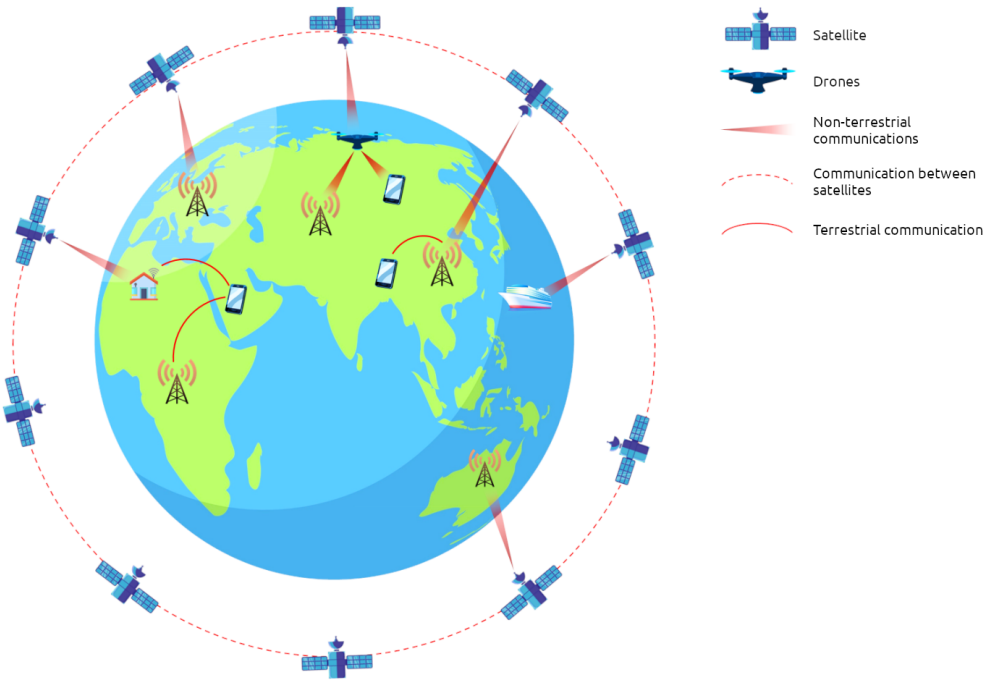

Figure 5. A converged multilayer heterogeneous network.

It should be noted that such a network construction will allow users and connected IoT to be in a single information space, regardless of their mode of movement or location. In addition, the failure of a network fragment will not significantly affect the performance of NTI SHs.

In addition, such a network construction creates the necessary conditions for organizing the following vital processes for SHs:

1. First responder communications and disaster relief. This option is essential in response scenarios as it provides not only disaster forecasting but also warnings, emergency response and emergency communications. This duplication of terrestrial networks with non-terrestrial networks will ensure continuity of service and support for emergency management. It is also planned to support voice and data transmission using a video system for the purpose of operational communications with a control point.
2. High-precision positioning and navigation, which will provide high-quality Vehicle-to-Everything (V2X) services for vehicles, both in the urban environment and accurate positioning and vehicle navigation services in remote and hard-to-reach areas.
3. Monitoring of the earth's surface in real time. In this case, optical filming using visible light and partially infrared cameras, as well as radio-frequency scanning, will avoid the limitations of transmitting and receiving communication channels.

Cellular communication with the introduction of networks of the 5G and then the promising 6G will significantly expand the capabilities of NTI, considering three main scenarios for its use, namely:

1. Enhanced mobile broadband (eMBB): up to 25 Gbps peak data rate. Applications: 4K, 8K, 3D live streaming; Augmented Reality (AR)/Virtual Reality (VR) services; cloud gaming; and other high-traffic services.
2. Ultra-Reliable and Low-Latency Communication (URLLC): Reducing data transfer delays to 1 ms and always having a connection. Applications: unmanned vehicles (V2X) and remote technologies (automation of production lines and robotic surgery).
3. Mass machine-to-machine communication (enhanced Mobile BroadBand-MTC): support up to 1 million connections to the base station per 1 square kilometer with data transfer rates up to tens of gigabits per second. Applications: development of consumer and industrial IoT (power supply, manufacturing, smart city, SH, etc.) (Figure 6).

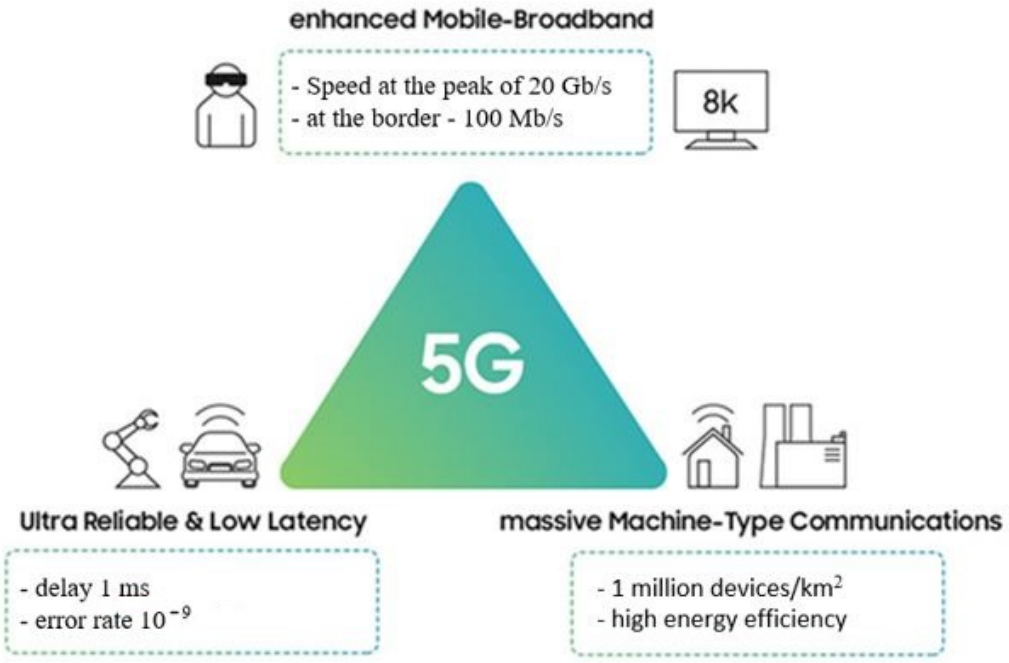

Figure 6. Main scenarios for using 5G/6G networks.

As a conclusion regarding the consideration of various ways of organizing DTFN, it should be emphasized that it is necessary to combine the possible ways of using DTS

depending on the chosen NTI option, which is particularly important at the stage of building a transformation to a SH.

4. Identification of Problematic Issues of Information Security in NTI Based on the Analysis of the Security Threat Landscape for SHs

Based on the fact that the issues of organizing the protection of wired and wireless DTFNs have been repeatedly covered in the scientific and technical literature, this article focuses on the issue of information security in 5G/6G networks (as in the latest network technologies).

Despite the positioning of the fifth and sixth generation SFSs as secure, the analysis below allows us to highlight a number of protection issues [28]:

1. A significantly increased attack surface. This circumstance is primarily due to the ever-increasing number of IoT devices, which, in turn, leads to a proportional increase in entry points for organizing targeted attacks. In addition, according to the concept of converged architecture, WiFi radio access networks, 4G-LTE, etc. must also connect to a single core 5G/6G network, making the connected devices less resistant to outside hacking. This will give hackers more IoT devices to collect and use for DDoS attacks, which will cause an increase in the frequency of such attacks. As a result, risks are possible: a large number of connections and high bandwidth increases the attack surface, while the number of IoT devices that are less resistant to hacking is growing.
2. The architecture of the core network (network core or 5G Core) is based on cloud technologies and the virtualization of network functions—software-defined networks (SDNs) and virtualization of network functions (NFV), allowing the creation of many independent segments, thus, supporting services with different sets of characteristics. In addition, segmentation will allow operators to provide network infrastructure as a separate service. At the same time, the network infrastructure used will depend on 5G/6G, much more than on their predecessors, and a protection breach in any area could become critical; thus, the consequences could be catastrophic. Thus, the risks should include the fact that such a construction of a network infrastructure leads to more serious consequences in case of failures and cyber-attacks when considering the scale of use.
3. Ample opportunities are opening for more aggressive conduct of various types of so-called “espionage”. It is known than any IoT device with the ability to capture video or audio information (the presence of cameras and microphones) can be used by cybercriminals or software or hardware manufacturers for them to view and listen to uninformed users. In this case, the risks are clear.
4. An analysis conducted by an international team of protection researchers from Purdue University and Iowa State University (USA) found almost a dozen vulnerabilities in the 5G mobile communication standard [29]. The exploitation of the vulnerabilities allowed for several attacks, such as location tracking, the transmission of false alarms and the complete disconnection of the phone’s 5G connection from the network. A group of researchers was able to track and fix the location of the device in real time. Moreover, experts were able to intercept the phone’s paging channel to broadcast fake emergency alerts, which, according to the research team, could cause “artificial chaos”. It should also be considered that a new kind of security threat can exploit vulnerabilities in all AKE protocols, including 5G protocols, and invade the privacy of mobile device users, causing more serious damage than before. Such “snoop activity monitoring” attacks use fake base station attacks that attackers have used to target vulnerable AKE protocols and protection leaks in 3G and 4G networks, as well as an encryption vulnerability for sequence numbers (SQNs).

   Although the AKE protocols used in 5G/6G networks have improved protection against base station spoof attacks, researchers have shown that relay attacks can break the SQN security of cellular networks, thereby, rendering it useless. These attacks are much more dangerous than the previous attacks due to having an important feature:

previously, a user could avoid an intrusion by leaving the attack zone; however, now hackers can continue to monitor a user's activity even if the user leaves the range of a fake base station using a new fake attack. In this case, the risks include attacks, such as "monitoring subscriber activity", which, in addition to physical tracking of the subscriber or certain devices, create prerequisites for the protection of encryption protocols.

5. 5G networks, and then 6G, involve the active use of edge-computing technology—mobile edge computing (MEC). These can be, in particular, corporate applications running on the network of operators: intelligent services, financial services and multimedia. In this case, the operator's 5G/6G networks are integrated into the corporate infrastructure. At the same time, one of the advantages of 5G/6G networks is a significantly low latency, which can be "successfully" used in the same DDoS attacks [11], because hackers will be able to strike faster—in seconds, not minutes. To confirm the theory, the researchers created a malicious base radio and, using the 5GReasoner tool, successfully performed several attacks on a smartphone connected to 5G. In one of the scenarios, a DoS attack on a phone resulted in a complete cut of the connection from the cellular network [29]. Thus, the risks include new opportunities for penetration into corporate networks, placement of MEC equipment outside the protected perimeter of the organization and the fact that the speed of a malicious attack becomes significantly higher.
6. The centralized network management infrastructure (Operations and Maintenance—O&M) used in 5G and then 6G networks is complicated by the need to simultaneously support a large number of service segments. In this case, risks can be attributed to the more serious consequences of misuse of resources and/or O&M configuration errors.

5. 5G/6G Network Protection Organization

Based on the analysis of possible protection issues of 5G/6G networks, we propose several levels of protection [29].

The first level is protection at the level of implementing technical solutions, building network infrastructure and equipment placement options:

1. The use of a powerful firewall between users and the outside world, multi-level isolation and integrity protection of SDN and VNF components—hypervisor, virtual machines, OS, controllers and containers.
2. MEC application authentication, using an additional authentication factor when accessing the corporate network, whitelisting devices and services ands authorizing API requests.
3. Providing high availability of virtual machines for fast recovery after attacks.
4. A trusted hardware environment—a secure device boot and the application of Trusted Execution Environment (TEE) technology.
5. Real-time attack detection on network nodes and virtual infrastructure elements using artificial intelligence algorithms.

The second level is protection at the level of network infrastructure management:

1. Secure management of not only user data but also service, technical, analytical and other types of information involved in solving SH problems (the so-called attack on a subscriber and an attack on a mobile operator), using encryption, anonymization, depersonalization, etc.
2. Centralized management of identified vulnerabilities, as well as policies and levels of information security, the use of information during the ongoing analysis of big data to detect anomalies and quickly respond to attacks.
3. Comprehensive use of counterfeit base station detection tools based on the real-time monitoring of operation and maintenance events.
4. The application of multi-factor authentication algorithms and organization of access control to segments by O&M.

The third level is protection at the level of standards:

1. Separating the layers of the data transmission and reception protocol into three planes: the User Plane, Control Plane and Management Plane. Each separate plane has its own entire isolation, encryption and integrity control.
2. Using encryption methods for subscriber and technological traffic with an increase in the length of the encryption key from 128 to 256 bits.
3. Using a single subscriber authentication mechanism for various types of wireless communications.
4. Supporting flexible protection policies for segments.
5. Using unified standards.

At the same time, a comprehensive approach is needed to protect networks of all NTI standards used to ensure information security at all levels presented. The approach includes administrative and technical issues ranging from constant network auditing to continuous security system improvements. Furthermore, here, the protection issues of all types of network traffic used are the most acute, which, having great potential, opens up wide opportunities for cyber-attacks, invasion of privacy, and the serious disruption of not only IoT but also the entire SH as a whole. It should be borne in mind that, when transforming to SH, we are dealing with an already built DTFN (to varying degrees—from the initial state to fully implemented).

The concepts of "smart home", "smart city", "smart environment", etc. begin to cover a wide range of options for using networks of all standards as webs that transform all aspects of the life of the planet's population, transforming it into a so-called "smart life".

Organically integrated into one converged, multi-layered, heterogeneous network, eventually covering the entire globe, NTI will provide users with a consistent experience. At the same time, ensuring the global delivery of mobile services will be an important aspect of the development of the 6G network.

6. Conclusions

In conclusion, the proposed transformation to SHs is aimed at ensuring sustainable economic development, effective municipal management and the large-scale implementation of IoT usage opportunities from unmanned vehicles to the use of virtual/augmented reality, etc. However, the analysis of IoT requires the mandatory identification of IoT and the comprehensive integration of all types of DTFN (wired and wireless advanced standards 5G/6G) as well as compliance with strict information and communication technology requirements. At the same time, as a prerequisite, it is recommended to strictly follow a set of measures related to three levels of protection—namely, at the level of implementation of technical and infrastructure solutions, at the level of network infrastructure management and at the level of standards.

Author Contributions: Conceptualization, G.D. and A.D.; Resources, J.K.; Writing–original draft, G.D. and A.D.; Writing–review & editing, G.D., A.B. and A.D.; Supervision, N.S.; Project administration, A.B. All authors have read and agreed to the published version of the manuscript.

Funding: The research was partially funded by the Ministry of Science and Higher Education of the Russian Federation as part of the World-Class Research Center program: Advanced Digital Technologies (contract No. 075-15-2022-312 dated 20 April 2022).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Streitz, N. Beyond 'Smart-Only' Cities: Redefining the 'Smart-Everything' Paradigm. *J. Ambient. Intell. Humaniz. Comput.* **2019**, *10*, 791–812. [CrossRef]
2. The International Telecommunication Union (ITU). Available online: https://www.itu.int/en/mediacentre/backgrounders/Pages/smart-sustainable-cities.aspx (accessed on 8 November 2022).

3. Bogdanov, A.; Shchegoleva, N.; Dik, G.; Khvatov, V.; Dik, A. "Smart Habitat": Features of Building It Infrastructure, Main Problems of Building Data Networks Using 5G (6G) Technologies. In *Computational Science and Its Applications—ICCSA 2022 Workshops*; Lecture Notes in Computer Science; Gervasi, O., Murgante, B., Misra, S., Rocha, A.M.A.C., Garau, C., Eds.; Springer: Cham, Switzerland, 2022; Volume 13380, pp. 628–639.
4. Trindade, E.P. Sustainable Development of Smart Cities: A Systematic Review of the Literature. *J. Open Innov. Technol. Mark. Complex.* **2017**, *3*, 11. [CrossRef]
5. Drozhzhinov, V.I.; Kupriyanovskii, V.P.; Namiot, D.E.; Sinyagov, S.A.; Kharitonov, A.A. Smart cities: Models, tools, rankings and standards. *Int. J. Open Inf. Technol.* **2017**, *5*, 19–48
6. Argunova, M. The "Smart City" Model as a Manifestation of the New Technological Mode. *Sci. Sch.* **2016**, *3*, 14–23.
7. Mityagin, S.; Karsakov, A.; Bukhanovsky, A.; Vasiliev, V. "Smart St. Petersburg": An integrated approach to the implementation of information technologies for managing a metropolis. *Control. Eng. Russ.* **2019**, *1*, 19–25.
8. Popov, E.V.; Semyachkov, K.A. Optimization of the urban environment digitalization processes. *Probl. Territ. Dev.* **2019**, *5*, 53–63. [CrossRef]
9. Recupero, D.R. An Innovative, Open, Interoperable Citizen Engagement Cloud Platform for SmartGovernment and Users' Interaction. *J. Knowl. Econ.* **2016**, *7*, 388–412. [CrossRef]
10. Anti-Malware. Available online: https://www.anti-malware.ru/analytics/Threats_Analysis/smart-cities-threats-opportunities (accessed on 6 November 2022).
11. Kupriyanovskiy, V.P. On Standardization of Smart Cities, Internet of Things and Big Data. The Considerations on the Practical Use in Russia. *Int. J. Open Inf. Technol.* **2016**, *2*, 34–40. (In Russian)
12. Postscapes. Available online: https://www.postscapes.com/iot-voices/interviews/iot-interview-series-5-questions-rob-van-kranenburg-internet-things-council (accessed on 5 November 2022).
13. IETF Journal. Available online: https://www.ietfjournal.org/the-internet-of-things-unchecked/ (accessed on 27 November 2022).
14. Gupta, A. Big Data & Analytics for Societal Impact: Recent Research and Trends. *Inf. Syst. Front.* **2018**, *20*, 185–194.
15. Boyes, H.; Hallaq, B.; Conningham, J.; Watson, T. The industrial internet of things (IIoT): An analysis framework. *Comput. Ind.* **2018**, *101*, 1–12. [CrossRef]
16. Shchegoleva, N.; Zalutskaya, N.; Dambaeva, A.; Kiyamov, J.; Dik, A. New Technologies for Storing and Transferring Personal Data. In *Computational Science and Its Applications—ICCSA 2022 Workshops*; Lecture Notes in Computer Science; Gervasi, O., Murgante, B., Misra, S., Rocha, A.M.A.C., Garau, C., Eds.; Springer: Cham, Switzerland, 2022; Volume 13380. [CrossRef]
17. Cnews. Available online: https://www.cnews.ru/articles/2020-04-21_cherez_tri_goda_na_kazhdogo_rossiyanina (accessed on 27 November 2022).
18. Jakovlevich, C.V. *Internet of Things as a Global Infrastructure for the Information Society*; Modern Management Technology: Kirov, Russia 2017; Volume 6, p. 7803, ISSN 2226-9339. Available online: https://sovman.ru/article/7803/ (accessed on 5 November 2022).
19. Minerva, R.; Biru, A.; Rotondi, D. Towards a Definition of the Internet of Things (IoT). 2015. Available online: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf (accessed on 27 November 2022).
20. Derevyashkin, V.M.; Virkunin, A.O.; Maksimov, A.S.; Rozhentsev, V.L. Analysis of radio access technologies for the implementation of the smart house system. *Mod. Probl. Telecommun.* **2018**, *1*, 526–529.
21. Roberto Sandre. Thread and ZigBee for Home and Building Automation Systems Engineer. Texas Instruments. 2018. Available online: https://www.ti.com/lit/wp/sway012/sway012.pdf (accessed on 5 November 2022).
22. Control Engineering Russia. Available online: https://controleng.ru/besprovodny-e-tehnologii/putivoditel-iot-3-wi-fi/ (accessed on 5 November 2022).
23. Bluetooth. Available online: https://www.bluetooth.com/learn-about-bluetooth/tech-overview (accessed on 5 November 2022).
24. Olsson, J. 6LoWPAN Demystified. Texas Instruments. 2014. Available online: https://www.ti.com/lit/wp/swry013/swry013.pdf (accessed on 5 November 2022).
25. Wltd. Available online: https://wltd.org/posts/thedifferences-between-z-wave-versions-made-easy (accessed on 5 November 2022).
26. Letfullin, I.R. *Standards and Technologies of Short-Range Wireless Communication Networks*; Trudy MAI: Moscow, Russia, 2022; p. 124. [CrossRef]
27. Onizawa, T.; Tatsuda, T.; Kita, N.; Yamashita, F. Recent research and developments focusing on fixed wireless and satellite communication systems. *IEICE Tech. Rep.* **2019**, *32*, 53–58.
28. Nakamura, T. 5G Evolution and 6G. In Proceedings of the 2020 International Symposium on VLSI Design, Automation and Test (VLSI-DAT), Hsinchu, Taiwan, 10–13 August 2020; p. 1. [CrossRef]
29. Securitylab. Available online: https://www.securitylab.ru/news/502542.php (accessed on 6 November 2022).