Chapter 7
Security Attacks and Countermeasures in 5G Enabled Internet of Things

A. K. M. Bahalul Haque, Tasfia Nausheen, Abdullah Al Mahfuj Shaan, and Saydul Akbar Murad

Abstract The use of previous generation networks like 4G was vastly used in the Internet of Things (IoT) devices. The constant need to grow and develop just so the network can fulfill the requirement of IoT devices is still going on. The exponential growth of the data services substantially challenged the security and the networks of IoT because they were run by the mobile internet requiring high bit rate, low latency, high availability, and performances within various networks. The IoT integrates several sensors and data to provide services and a communication standard. Fifth Generation Communication System (5G) enabled IoT devices to allow the seamless connectivity of billions of interconnected devices. Cellular connections have become a central part of the society that powers our daily lives. Numerous security issues have come to light because of the exponential expansion of 5G technologies and the adaptation of the slow counterpart of IoT devices. Network services without security and privacy pose a threat to the infrastructure and sometimes endanger human lives. Analyzing security threats and mitigation is a crucial and fundamental part of the IoT ecosystem. Authorization of data, confidentiality, trust, and privacy of 5G enabled IoT devices are the most challenging parts of the system. And to provide a solution to these, we need a robust system to handle cyberattacks and prevent vulnerabilities by countermeasures. This paper includes a comprehensive discussion of 5G, IoT fundamentals, the layered architecture of 5G IoT, security attacks and their mitigation, current research, and future directions for 5G enabled IoT infrastructure.

Keywords IoT · 5G · Security and privacy · 5G IoT networks · SDN · NOMA · WSN

A. K. M. Bahalul Haque (✉) · T. Nausheen · A. Al Mahfuj Shaan
Department of ECE, North South University, Dhaka, Bangladesh
e-mail: bahalul.haque@lut.fi

T. Nausheen
e-mail: tasfia.nausheen@northsouth.edu

A. Al Mahfuj Shaan
e-mail: abdullah.mahfuj@northsouth.edu

S. A. Murad
Faculty of Computing, Universiti Malaysia Pahang, Pekan, Malaysia

© The Author(s) 2023

B. Bhushan et al. (eds.), *5G and Beyond*, Springer Tracts in Electrical and Electronics Engineering, https://doi.org/10.1007/978-981-99-3668-7_7

Introduction

Fifth Generation Communication (5G) networks are constantly developing, and it is becoming a significant catalyst for the growth of Internet of Things (IoT) devices (I-Scoop 2018). Future applications of IoT related application are going to be integration of various other technologies. IoT integration with other technologies can facilitate seamless connections between heterogeneous devices and promote ubiquitous computing infrastructure throughout our daily life. However, multiple complex integration challenges have emerged because of the heterogeneity and fragmentation of the connectivity system that hampers IoT development (Rahimi et al. 2018a). Moreover, as the 5G technology is emerging, this is considered the pioneer of IoT development. As the application of IoT is becoming widespread and diverse, the security and vulnerability of 5G IoT networks are becoming a significant concern (Haque et al. 2021). The services 5G integrated IoT provides need to be secured against cyberattacks and data loss. Even though there are no discrete security systems for IoT devices, they mostly rely on detecting vulnerabilities and taking countermeasures (Li et al. 2018).

Security is an integral part of any infrastructure. The same is true for IoT and 5G integrated architecture. Therefore, it is crucial to address the issues of cyberattack vectors, analysis, prevention, and countermeasures of 5G IoT networks. IoT devices are interconnected, combining various types of sensors, actuators, embedded software, and operating systems to run the network (Gautam et al. 2019). The application vectors have also spread across from our day-to-day hose hold toward industrial implementation. IoT devices are generally equipped with low-power capacity, relatively smaller physical architecture, and closely attached wireless and ward links. Some of these attributes of IoT are used by the cyber attackers to exploit the network by probing, inserting malicious codes, and unauthorized access to the network.

Third Generation (3G) communication and Fourth Generation (4G) communication technology are widely used in different walks of lives and around our daily environment. However, both the 3G and 4G technologies are not completely optimized for the applications of IoT. 5G technology is drastically improving and their integrations with IoT have proven to be reliable and capable. For the last 20 years, many M2M technologies have been implemented like BLE (Rahimi et al. 2018a), ZigBee (Alam et al. 2015), RPMA (Girson 2018), SigFox (Chen et al. 2017), LoRa (Palanisamy et al. 2022), etc. There are many other technologies like these, and they bring in a new set of challenges for the 5G technology (Mehbodniya et al. 2022). However, they are required to meet the necessities of IoT applications as well (Singla et al. 2021).

Motivated by the factors mentioned above, in this paper, we have comprehensively analyzed the integration factors of 5G IoT and security threats and countermeasures (Dener 2014; Teniou and Bensaber 2018; Sinha et al. 2017). We have analyzed various security threats at different levels of 5G enabled IoT devices from existing literatures and comprehensively presented the countermeasures as well. We have also outlined the research challenges associated with 5G IoT, which were not limited

to reliability and communication issues. As 5G incorporates several technologies (Howe 2006; Rahimi et al. 2018b; Ahmad et al. 2018), it poses a significant impact on IoT applications. The paper's primary objective is to gain insights on the overview of the 5G network IoT devices, analyze the security issues, and develop solutions to prevent them from happening. The major contribution of this paper is listed as follows:

- This paper highlights the key features, architectural description, and extensive review of the 5G network.
- This paper provides an in-depth understanding, insights, and comprehensive description of IoT.
- This paper comprehensively discusses the integration trend, layered architectural analysis, and state-of-the-art technologies involved in 5G and IoT.
- This paper postulates various types of threats existing in 5G IoT networks.
- This paper also holistically analyzes the threat analysis and countermeasures of 5G IoT networks.
- Finally, this paper discusses the research gaps and future research directions of 5G IoT.

The paper was introduced in "Introduction" section; Second section includes the "Overview of 5G"; Section "Overview of IoT" provides a background on IoT; Section "5G Enabled IoT" contains the outline of the 5G and IoT integration; Section "5G Enabled IoT Architecture" includes the architectural description of 5G IoT integration; Section "Technologies in 5G Enabled IoT" introduces the technologies of 5G and IoT integration; threat analysis and countermeasures are comprehensively described in section "Threat Analysis in 5G IoT"; Eighth section demonstrates the "current Research for 5G and IoT"; Section "Future Research Directions and Challenges" demonstrate the current research trends and future research directions for 5G enabled IoT devices; and lastly, "Conclusion" section concludes the paper.

Overview of 5G

In telecommunications, the mobile network that has been launched is 5G which is available in different cities all over the world. After the launch of 5G, it has come to attention that it is far more significantly enhanced than 4G LTE, especially in 3 aspects. In the advanced 5G core network, a support network function virtualization and network slicing are present, which is actually, Software Defined Networking (SDN) (Bosshart et al. 2014; Lin et al. 2018; Chuang et al. 2018). The SDN in a network decouples the data, as well as the control planes, and these control planes are the ones who play a role in issuing instructions for the SDN switches in the data plane, and this control plane is present in the SDN controller.

Programmability, centralized policy management, and a global network state are a few of the advantages of SDN to the 5G system. Still, the benefits have to be properly looked at in the 5G core network. For this very reason, it is a must to maintain security

within the communication channel to prevent potential attacks and safely guard the privacy and security of the data. In today's time, 5G, the state-of-the-art technology, can create new interfaces for regularly used devices and networking components. One of the essential roles of a 5G connection is to build connections between huge numbers of users so that it can provide more competent and faster communications. The design of 5G was done in a way where it can provide better coverage, bandwidth, reliability, and latency because these are what make 5G better than any other mobile network that was launched before 5G. However, even being better than other mobile networks, like any other, there are security issues, and there are several issues that look into these 5G security issues.

Ferrag et al. (2018) show 5G authentication and privacy-preserving surveys. Prasad et al. (2018) show privacy surveys, replay, bidding down, attacks on control, and user planes. But there was, this study in Basin et al. (2018) gives a formal analysis of the authentication of 5G. Jover and Marojevic 2019 showed a few unrealistic assumptions made by 5G specifications, which caused the adversarial attacks because of the vulnerability in the 5G systems until other optional security features were added. And potential security attacks or threats were shown by Teniou and Bensaber (2018) which measures are to be taken for the security of 5G. It also indicates that IPsec, a security protocol, is used primarily on LTE and to make IPsec more secured for the communication of 5G, IPsec tunneling can be done by authentication integration, integrity, and encryption.

As the mobile communication network is actually on the way to completing the 5G network cycle, it is becoming capable of supporting novel usage scenarios with stringent performance requirements. But 5G is not just stuck to seamless broadband connectivity only. It is already on the verge of advancement toward the vision of IoT. It has been prepared in order to be able to enable a wide range of machine-type applications. In today's world, wireless media is the way to have most communications that are actually open to various attackers. For this reason, efficient security operations must include and have (Sinha et al. 2017).

Overview of IoT

Nowadays, the advancement of technology, the IoT, is a significant paradigm shift in mobile service providers and the manufacturer of electronic devices. It helps to contemplate their business models and innovation context. IoT helps create an interconnection of billions of devices via the internet and has a tremendous growth rate. IoT is a network of devices consisting of sensors and actuators and helps to enable multiple applications and services by exchanging data between each other. The end-user does need compute-intensive operations, and along with it, there is a need for huge storage and real-time communication, and it is thought to be not an efficient way by the cloud service providers. And one of the essential features of all is the authentication of legitimate IoT devices (Howe 2006). And the authentication is

addressed with the help of certificates given by a specific Certificate Authority (CA) but is one of such which offers a lightweight solution.

Smart city, among a large number of applications, is an integral field of IoT that is increasing the number of smart services within IoT systems (Rahimi et al. 2018b; Ahmad et al. 2018). The IoT application focuses on cities that are always composed of and controlled by computing units (Bosshart et al. 2014). Different definitions are given to smart cities like intelligent and digital cities (Lin et al. 2025). Smart cities focus on improving the service quality of the people and taking advantage of resources or decreasing the costs of public administration (Chuang et al. 2018). Smart lighting or smart traffic, and many other services are seen to grow exponentially (Ferrag et al. 2018). But with efficiency and advanced technology comes security. Security is the most crucial and the most significant feature of any smart device with an IoT architecture. Data confidentiality, authorization, trust, and client privacy are security challenges IoT systems face nowadays. So, to challenge these security problems, secured taxonomy is applied in order to handle cyberattacks and all other vulnerabilities using forensic techniques (Prasad et al. 2018).

Without efficient and strong security, IoT devices can create trouble rather than making life of people easier and more efficient because these devices end up endangering the privacy and safety of the people. There might be no trusted security, but the advancement and growth in the IoT systems and their services depend on recognizing potential security breaches and not being able to defy them. Security breaches occur due to various communication technologies being used in different layers of the wireless sensor network. The security and privacy issues were looked at with more details of the three-layer IoT architectures (Basin et al. 2018), and those defects were further investigated in Jover and Marojevic (2019).

5G Enabled IoT

Various types of research from the academic and industrial point of view focusing on 5G and IoT have been conducted (Ahmad et al. 2017; Liyanage et al. 2018; Bhushan and Sahoo 2017). Currently, advances are seen in theory, applications, and standardizations, especially in the implementations of the technologies related to 5G. The most crucial focus is to offer them a place to grow within IoT scenarios. And in the past few years, various work has been done on 5G and IoT as well (Ahmad et al. 2017). On 5G, a wireless research project was initiated by CISCO, Intel, Verizon combinedly to launch a novel set, "Neuroscience-Based Algorithms," and for the requirement of the human eye, adaptive video quality was launched where a hint was shown that it even has wireless networks which would include built-in human intelligence (Liyanage et al. 2018).

5G played a crucial role in the advancement of IoT because of 5G, billions of smart devices could create an inter-connection and interact and share data without the help of any users (Bhushan and Sahoo 2017). But recently, different application domains are making it more complicated for IoT to recognize devices that meet the

application needs requirements (Bhushan and Sahoo 2017). IoT system which exists vastly uses fixed application domain like

- BLE
- ZigBee, etc.

There are other technologies like

- WiFi
- LP-WA networks
- Cellular communications, e.g., MTC using 3GPP and so.

IoT is constantly evolving quickly but with evolved proposals and new application domains. But IoT is growing and becoming more efficient to make people's lives more efficient and fast paced and trying to make more efficient inter-connection networks between smart devices. But with the growth of Industry IoT (IIoT), new challenges and obstacles are also coming in the way, like, the need for new advanced addition to the existing business models and products and solutions for the betterment (Ta-Shma et al. 2018). And there are technical challenges in Industry IoT:

- Reliabilities
- Timeless
- Connection robustness, and so on.

There are most used communication techniques within the IoT connectivity and are, 3GPP and LTE (Rathore et al. 2016), which are offered to the IoT systems also like (Zanella et al. 2014),

- Wide coverage
- Low Deployment costs
- High-security level
- Access to dedicated spectrum
- Management simplicity.

However, MTC communication cannot bear the cellular networks present because those present cellular networks are the primary key in IoT, which is one of the problems. But this isn't a problem when instead of MTC communication, the 5G network is used because the present cellular networks are making it faster in terms of data rate, and it occurs because of low latency and the better version of MTC communication with respect to current 4G (LTE) and which results in more efficient IoT applications and devices.

5G Enabled IoT Architecture

More efficient and advanced architecture is needed, which will help achieve more sustainable and efficient new technologies. More scalable architectures of IoT devices will be better than the present 5G IoT architecture (Jin et al. 2014). The advantage of using new technology during the development is that it makes the architecture

- More simple
- Convenient for scalability
- Analysis
- Modularity
- Efficiency
- Agility
- Accessibility to high-demand services
- Eight layers interconnected along with data exchange capability, two-way, this architecture has been designed, explained below (Jin et al. 2014).

L1 Physical Device Layer

The general layer of the architecture of the IoT includes

- Wireless sensors
- Actuators
- Controller

L2 Communication Layer

The two sub-layers discussed below.

Device to Device Communication Sub-Layer: 5G enhances D2D communication in this sub-layer and is an important participant that provides connectivity for devices with Machine-Type Communication (MTC) (Mohammadi et al. 2018).

Connectivity Sub-Layer: Cell phones, tablets, etc., are the devices connected to the BSs communication centers within the sub-layer. These devices proceed with data analysis and are then sent to the storage units through centers with an Intranet connection (Millr 2015; Conti et al. 2018). Those are specified with

- High Reliability
- Performance
- Agility.

L3 Fog Computing Layer

Within this layer, in order to make decisions, edge processing is applied on the data by the nodes (Kumar and Patel 2014).

L4 Data Storage Layer

Physical devices send the information of edge processing to the data storage units here in this layer (Zhao and Ge 2013). And here, large amounts of data are handled and the traffic of the future devices and applications but not without the data security, which is the key of this layer.

L5 Management Service Layer

Here in this layer, there are three sub-layers, and these are

Network Management Sub-Layer: Communication purposes occur between devices and data centers in this layer. 5G IoT or ZigBee are communication protocols where the network type is consistent with the technology present in this layer: Wireless Network Functionality Virtualization (WNFV). IoT networks are managed, and network reconfiguration is enabled because of the Wireless Software Defined Network (WSDN) (Xu et al. 2014) technology. Because of this technology, traditional network monitoring for performance enhancement is unnecessary.

Cloud Computing Sub-Layer: The data from a layer from Fog Computing Layer can be reprocessed in this sub-layer, and then the processed information is generated in the final step.

Data Analytics Sub-Layer: For generating values for decision-making in this layer, new learning algorithms of data analytics can be implemented to the last sub-layer information (Millr 2015; Conti et al. 2018). Since the information from the IoT networks is collected, it starts turning more dominant and expanding with time.

L6 Application Layer

Business related people make the most of use of this layer because they need to plan with the correct data, and it also helps in revolutionization, which are (Kumar and Patel 2014).

- Vertical markets and business need by control applications
- Vertical and mobile applications
- Business intelligence and analytics.

L7 Process and Collaboration Layer

Collaborations and communications are permitted in these layers within IoT devices and services. That occurs because the data and information cannot be utilized with a single entity since they come from the previous layers (Rahimi et al. 2018a).

L8 Security Layer

This is the protection layer for all the other previous layers, and this protection is done without impacting the different previous layers' functionality. Also, the security taxonomy for blocking and foreseeing the dangers of cyberattacks is protected here in this layer.

The Fig. 7.1 added below shows a brief overview of the 5G IoT architecture.

Technologies in 5G Enabled IoT

In the last decade, much research has been done on 5G enabled IoT (Mohammadi et al. 2018). To build the state-of-the-art IoT and 5G systems, extensive research is done by academics and industry (Millr 2015; Conti et al. 2018; Kumar and Patel 2014). 5G enabled IoT devices can significantly impact the interconnections of IoT devices. Heterogeneous networks currently are unable to satisfy the needs of the application of IoT devices (Zhao and Ge 2013). Popular IoT systems include BLE, ZigBee, WiFi, LP-WA, etc. (Hošek 2016). The current systems focus on improving our regular life, making a better-quality life, and engaging interconnections between smart homes, smart cities, agriculture, and healthcare (Mohammadi et al. 2018; Millr 2015; Conti et al. 2018). 3G and LTE networks are currently the most used connectivity technologies that offer low cost and wide coverage. However, these

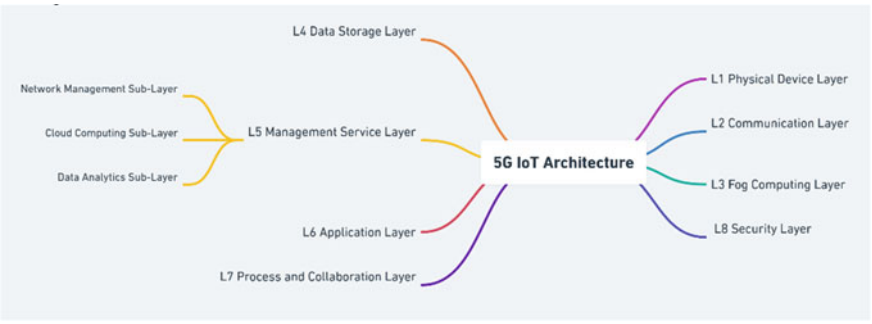

Fig. 7.1 5G IoT architecture

Table 7.1 Technologies in 5G enabled IoT

Technology	Use cases
Heterogeneous networks (HetNet)	Enables on demand transmission rate for 5G IoT (Millr 2015; Conti et al. 2018)
Direct device to device (D2D)	D2D was proposed to create communications between short ranges. power efficient, optimized power and communication load occur here and are expected to provide an efficient spectrum (Millr 2015; Conti et al. 2018)
Spectrum sharing	To enable the technology in covering the traffic load imbalance, spectrum management is the key. Massive MIMO is centerpieces of spectrum sharing (Mohammadi et al. 2018; Millr 2015)
Zigbee	It's a power optimized and cost efficient mesh network widely used in WSNs and primarily used in Industrial IoT applications (Millr 2015; Conti et al. 2018)
Other technologies	Other enabling technologies include machine-type communication (MTC), mmWave, SDN, NFV, and NB-IoT

present networks cannot manage to support MTC, which is the key to enabling the factor in IoT devices (Jin et al. 2014; Mohammadi et al. 2018).

Several 5G enabled IoT technologies have been developed in the last few years, and some are developing. Some of these are described in Table 7.1.

Threat Analysis in 5G IoT

As security in IoT is emerging as one of the significant factors in security schemes, it is essential to analyze and mitigate the attacks. In this section, categorization of various attacks and countermeasures to emphasize the contribution to this paper are done.

Eavesdropping

The attackers of eavesdropping try to intercept some of the confidential information but detecting the legitimacy of the transmitters or receivers is challenging to locate or trace since the attackers do not transmit any signals (Xu et al. 2014; Kaplan 2018).

Interception

The attackers can easily detect the authentication of the communication since they snoop within the nearby wireless environment. With this technique the attacker can

capture the information about the network. The network information can include the configuration, sensory data transfer protocol, etc. Eavesdropping through interception is one of the most effective and oldest techniques to exploit the security (Hošek 2016; Liyanage et al. 2018).

Traffic Analysis

Cryptographic algorithms may encrypt the critical information in legitimate communication. In this case, attackers intercept the transmitted signal. Still, they cannot obtain significant content, but traffic analysis can come in handy for the tracking of communication patterns in order to realize other forms of attacks (Wang et al. 2019).

Contaminating

In this type of attack the attackers try to gain illicit access to the network and contaminate the channel estimation stage as well (Astely et al. 2013; Palattella et al. 2016). This sort of attack can be categorized into two types of contamination according to different channel.

Spoofing

Attackers inject fake identity information to destroy or join communications. The attacker is able to establish a fake communication channel between two or more legitimate points. In this way, unknowingly, two legitimate parties communicate with each other through a fake entity (Liyanage et al. 2018).

Here, malicious nodes can copy other nodes, claim fake identities, and generate a random number of different identities only using hardware devices (Li et al. 2021; Lin et al. 2019). Sybil types of attacks make the system generate false reports, and that can make users get spam and lose privacy (Wang et al. 2021).

Jamming

Here the target of the attackers is to block legitimate communication using noise (Haque and Bhushan 2021), and an adversary can send continuous signals by decreasing signal to noise ratio (Xu et al. 2014) through the channel only to hamper communication. It can also prompt DoS attacks at the physical layer (Kaplan 2018). There are three types of signal jamming, in general, such as pilot jamming, proactive jamming, and reactive jamming (Hošek 2016).

Pilot jamming is launched when a channel is trained (Hasan and Hossain 2013; Ge et al. 2014; Ahmad et al. 2020) and aims to create an illegitimate connection without the exact pilot sequences. An adversary can launch the attack when he knows the pilot length and sequence. Pilot jamming is also very efficient as only the signals need to be corrupted (Millr 2015; Conti et al. 2018; Haque et al. 2020).

Physical Layer Security

5G and IoT are the fundamental paradigms of today's time, and for the security of wireless communication, physical layer security is becoming a growing prospect. PLS protects the confidentiality of data by exploiting the intrinsic randomness of the communication medium (Padmavathi and Shanmugapriya 2009; Shiu et al. 2011). This technique plays an aid in improving 5G IoT security from two main aspects,

The network latency on the Internet of Vehicles (IoV) and Unmanned Aerial Vehicles (UAV) can be reduced. The vehicles can randomly join and leave the network, making the UAV highly dynamic (Steinmetzer et al. 2018). PLS will offer an efficient and quickest authentication by exploring radio frequency (RF) fingerprint otherwise, roaming in different networks will lower communication performance. Different schemes in PLS can be additional protection that cooperates with the existing security architecture to provide better protection for 5G IoT devices.

Random wireless channel use cases are done to generate keys in PLS schemes that can release the burden (Zhou et al. 2012) in 5G IoT networks; it becomes difficult or rather challenging to achieve effective key distribution and management. Reinforcing communication security can be done without encryption and decryption using information theory.

Massive MiMo

Core 5G technology received considerable attention in IoT research (Nitsche et al. 2014; Ylmaz and Arslan 2015). It helps in providing numerous communication superiority based on the beamforming technology like an array that gains channel hardening and nearly orthogonal channels (Ylmaz and Arslan 2015). In the meantime, MiMo techniques for PLS are also discussed in Zeng et al. (2010), Newsome et al. (2004).

Passive eavesdropping (Xiao et al. 2009) and also the active attacks in massive MiMo were investigated by many authors. The analysis showed that PLS against passive eavesdropping could increase pilot contamination attacks (Zhang et al. 2014), and it is fatal for MiMo communication since an active attacker can send the same pilot sequence.

NoMa

IoT with NoMa and non-orthogonal resources can improve spectral efficiency and also reduce low transmission latency and signaling cost (Mpitziopoulos et al. 2009), and it can also be used where the number of sensors is huge, like in smart farming and intelligent manufacturing (Bhushan and Sahoo 2020). Allocating two users to a single orthogonal resource block for user pairing is a technique for balancing complexity and efficiency (Clancy 2011). The capacity to superpose numerous signals into an orthogonal resource is achieved via superposed coding technology.

MmWave

A 5G technology that can improve network transmission (Mpitziopoulos et al. 2009; Yang et al. 2018) helps the devices connect to higher bandwidth communication channels (Wood et al. 2007). Characteristics like blocking effect, highly directional transmissions are new in mmWave (Wood et al. 2007). The new characteristics of mmWave channels can help in improving the efficiency of traditional PLS techniques (Wang et al. 2018; Hamamreh et al. 2018; Arsh et al. 2021). Because of the tiny wavelengths of mmWave, dozens to hundreds of antenna elements may be put in an array on a small physical platform, which significantly aids the application of MiMo and the integration of different 5G technologies (Zeng 2015; Lu et al. 2014, 2018; Araujo et al. 2016).

Trust Mechanism in WSN

This mechanism in WSN has been emerging as a significant factor when it comes to security schemes, and so, it is really a necessity to analyze how these attacks can be resisted with the help of trust schemes (Zhou et al. 2012; Goyal et al. 2021; Zhu et al. 2014; Kapetanovic et al. 2015). Recently these mechanisms have been remodeled to filter the fake nodes in a sensor network. This approach was first introduced in E-commerce to choose dependable transaction objects, and many researchers in different fields have since developed it (Zhou et al. 2012). Because the evaluation of trust is entirely based on past behaviors of participants or indirectly mixed with the reputation of other recommenders, this mechanism has the potential to be more efficient, but higher standards are required to develop an effective trust framework in WSNs because of

- Limitations of energy
- Limited Storage Space
- Wireless communication's inherent vulnerabilities.

Crowdsourcing Analysis

In 5G networks, crowdsourcing is a potent tool against hackers. The major goal of this analysis is to present the problem to a participatory community that is eager to solve the problem and then anticipate a reward (Zhou et al. 2012). This concept has been used in the IoT in a variety of ways by users and their IoT devices for a variety of reasons. (Ding et al. 2017) However, there hasn't been enough discussion of how these features can help mitigate the impact of cyberattacks in truly complex networks, which are particularly vulnerable due to the wide range of technologies at various levels of abstraction, as in the case of 5G networks (Li et al. 2018; Gautam et al. 2019; Rahimi et al. 2018a). The concept of crowdsourcing connects both the 5G and the IoT network world naturally

- Participant's interests are defined (users and providers)
- Motivating mutual cooperation to stop cyberattacks

Commercial Purposes

The 5G business model requires infrastructure sharing among service providers, and in this case it is very important to use crowdsourcing analysis between the service providers to identify attacks (Millr 2015; Conti et al. 2018). It is essential to use security mechanisms to mitigate potential attacks and ensure privacy and confidentiality. Malware Information and Sharing Platform also uses a similar system to develop countermeasures for threats (Ding et al. 2018).

Removing Physical Attacks

Data coming from mobile phones are used in crowdsourcing analysis, and it is used to provide a warning system. Software and physical attacks are very different and require more research (Ding et al. 2016). A novel way of solving problems like finding the attacker's location is to expand the security controls at the edge of the user's IoT device, and crowdsourcing analysis can be implemented to identify potential attacks (Rappaport et al. 2013).

Social Media

Social media like WhatsApp, Twitter, and Facebook are the biggest platforms for crowdsourcing (Niu et al. 2015). Social media is a gateway for crowdsourcing, and it can be done in two ways: 1. by the traditional method, which involves humans but focuses on the attacks on the systems of the whole infrastructure, or 2. the other is done by extracting relevant information and identifying attack patterns (Heath et al. 2016).

Attacks at the Architecture Level

Today's world is becoming more interconnected, and smart cities are the key. In smart cities, various IoT devices are integrated, and nodes in smart cities are vulnerable to security threats like DoS attacks and manipulation of data (Wang and Wang 2016).

L1 Physical Device Layer

Various threats and attacks can damage the sensor nodes in the architecture (Gautam et al. 2019). Some attacks in the L1 are described below.

- **Unauthorized Access to Tags**: Attackers can easily access tags in RFID due to the lack of proper authentication techniques.
- **Tag Cloning**: RFID tags can be cloned in the physical layer, and reverse engineering can extract relevant information.
- **Sleep Deprivation Attack**: Unstoppable sending of control information is done in this attack and it keeps the nodes constantly in a working state in the network.

L2 Communication Layer

- **DoS Attack**: DoS attacks engage the user to overflow the victim's system with a large amount of network traffic.
- **Sybil Attack**: This attack deceives the victim to do one task multiple times as it shows pseudonymous identities in the node.
- **Replay Attack**: During eavesdropping, a valid data packet is collected from the network and every time the user connects to the network, and the attackers collect resources from them.
- **Sinkhole Attack**: The flow of data is attracted from other nodes residing nearby by using another compromised node.

L3 Fog Computing Layer

Fake gateways and attackers replace edge devices to collect data from these edges (Zhou et al. 2012).

L4 Data Storage Layer

Data privacy, confidentiality, and integrity are concerned with any IoT data storage system.

L5 Management Layer

The attackers attack the server, database, and other services in this layer.

- **VM Manipulation**: VMs run in the host system, and the adversary controls it. This can be attacked, and the range of these attacks is from extracting information and manipulating data in the VM (Xu et al. 2014).
- **Flooding Attacks in Cloud**: This attack is done in the sub-layer of the cloud, and the attackers frequently send service requests (Xu et al. 2014).
- **Cloud Malware Injection**: Malicious services can be inserted into the cloud and used to manipulate the system, and sensitive data could retrieve sensitive data.

L6 Application Layer

Attacks in this layer are mainly to access the data of users.

- **Code Injection**: Attackers insert worms and other malicious codes to exploit the errors in the program and gain system control.
- **Buffer Overflow**: Attackers use programs to violate the data buffer or codes to overflow the entire system.
- **Permission Manipulation**: This attack mainly leads to the illegitimate administration of data and violates user privacy.

Current Research for 5G and IoT

This section discusses the current research topics and solutions that can also be introduced to future research directions.

The number of research done on mobility is minimal, and it is a fascinating subject matter in terms of mobility in physical layer attacks on both user and attacker sides. The attacker may use the mobility feature to find the best area of attack and try to avoid detection. Mobility can also be used to counter this attack. But users might also have to consider the performance if mobility is implemented and investigating the 5G IoT mobility system is a current research topic (Mohammadi et al. 2018).

mmWave and NOMA are new features currently available in 5G technology. Few studies show exploitations of these new features to achieve physical layer attacks. And schemes for these new features are yet to be found (Millr 2015).

Trust models for securing data are another field where data sensing and aggregation are focused. The wide range of data types and privacy safety increases the obstacles and brings in newer problems (Haque et al. 2021; Li et al. 2018; Gautam et al. 2019). Current threats and attacks in the WSN can be identified with trust models, and also trusted models can be used to plan the attack itself. And currently, the analysis of existing and potential threats is the objective (Mohammadi et al. 2018; Conti et al. 2018; Conti et al. 2018).

Future Research Directions and Challenges

Even though 5G satisfies the requirements for IoT security, it also opens up newer sets of challenges like architecture security of IoT and verified communications between devices. In this section, we have reviewed future research areas for 5G IoT security.

Characteristics Synthesis

The 5G framework is a synthesis of many technologies (Mohammadi et al. 2018). A combination of MIMO, mmWave, and NOMA increases the spectrum efficiency. An IoT environment with low-cost and low-power different virtual channel models can help build a powerful Access Point. It can help distinguish between multiple users which can help prevent attacks like pilot contamination attacks. Researching the field of synthesis characteristics of 5G IoT can be a boost to novel solutions.

Signal Revoking

Detection of any active attack in the network is the primary step toward any kind of countermeasure. It is expected for IoT devices to maintain secure communication even if it is under any attack. And it is very challenging to eliminate the attacks even while maintaining contact. Waveform designs (Wang et al. 2018) can be an additional functionality, and they could be used to recognize if the signals are coming from the same user. Afterward, a filter mechanism might be developed to filter eavesdroppers in the network using this technology.

Location Awareness

Location awareness can be a positive factor for removing threats and preventing threats, as 5G location services can accurately provide location data (Jaitly et al. 2017). Location awareness could help mitigate threats in the network, and there are many prospective characteristics of the 5G network to attain location awareness (Goyal et al. 2021). And to achieve more efficient communication, location information is an exciting research direction.

Technical Challenges

Many works have been made to mitigate any challenges for the 5G enabled network. But there are still many technical challenges. There are design-related issues at the architecture level that includes Scalability and network management, which is a major issue in managing the state of the information (Fuentes et al. 2013).

Interoperability and heterogeneity allow devices to connect seamlessly, and it is a major concern as it is used to collect information about smart networks or applications (Zeng 2015).

Wireless Software Defined Network

Even though WSDN solves the scalability issue in the 5G network, many cases need to be resolved in SDN. It needs to provide flexibility and separation of control and data plane, which is the most challenging part of SDNs.

Security Assurance and Privacy Analysis

Next-generation 5G enabled IoT devices, security, and privacy needs to be added to the network and device levels as they will address many different complex applications, including smart cities and intelligent networks. 5G is a diverse system, and security system is very complicated, and security assurance must be considered at the device and network levels during the design process.

Standardization Issues

As 5G is being developed, it has also enabled to provide many IoT solutions. And the calibration of IoT will make the implementation of 5G IoT even easier. Lack of consistency and standardization (Li et al. 2018; Gautam et al. 2019; Rahimi et al. 2018a) has made it a big hurdle and challenge for closing the gap between humans and environment control. IoT as a service (Haque et al. 2021) might one day be a possible result.

Conclusion

This paper focuses on various security attacks and their countermeasures, the impact of 5G enabled IoT, and possible solutions for mitigating threats in a 5G enabled network. We have reviewed 5G and IoT characteristics and physical layer threats. We also categorized various types of threats with different kinds of attacking purposes. The open issues for 5G enabled IoT were also discussed, and current and future research trends were also introduced in the last section of the paper. The development of 5G enabled IoT devices will open many more gates for the future, bringing in possible data privacy and security issues. And it is essential to acknowledge what is associated with 5G enabled IoT and its security and different solutions under the wide spectrum of the 5G network. The paper's main aim was to provide a comprehensive insight into the 5G enabled IoT and threat analysis and discuss the future research areas. We hope this paper will help further research on the future of 5G enabled devices.

References

Ahmad I, Kumar T, Liyanage M, Okwuibe J, Ylianttila M, Gurtovk A (2017) 5G security: analysis of threats and solutions. In: 2017 IEEE conference on standards for communications and networking (CSCN)

Ahmad I, Kumar T, Liyanage M, Okwuibe J, Ylianttila M, Gurtov A (2018) Overview of 5G security challenges and solutions. IEEE Commun Stand Mag 2(1):36–43

Ahmad A, Bhushan B, Sharma N, Kaushik I, Arora S (2020) Importunity & evolution of IoT for 5G. In: 2020 IEEE 9th international conference on communication systems and network technologies (CSNT). https://doi.org/10.1109/csnt48778.2020.9115768

Alam KM, Saini M, El Saddik A (2015) Toward social internet of vehicles: concept, architecture, and applications. IEEE Access 3:343–357

Araujo DC, Maksymyuk T, de Almeida AL, Maciel T, Mota JC, Jo M (2016) Massive MIMO: survey and future research topics. IET Commun 10(15):1938–1946

Arsh M, Bhushan B, Uppal M (2021) Internet of Things (IoT) toward 5G network: design requirements, integration trends, and future research directions. Adv Intell Syst Comput 887–899.https://doi.org/10.1007/978-981-15-9927-9_85

Astely D, Dahlman E, Fodor G et al (2013) LTE release 12 and beyond [accepted from open call]. IEEE Commun Mag 51(7):154160

Bahalul Haque AKM, Arifuzzaman BM, Abu Noman Siddik S, Kalam A, Sadia Shahjahan T, Saleena TS, Alam M, Rabiul Islam M, Ahmmed, F (2022) Semantic Web in Healthcare: A Systematic Literature Review of Application, Research Gap, and Future Research Avenues. Int J Clin Pract 20221–27. https://doi.org/10.1155/2022/6807484

Basin D, Dreier J, Hirschi L, Radomirović S, Sasse R, Stettler V (2018) A formal analysis of 5G authentication. In: 2018 ACM SIGSAC conference on computer and communications security. Toronto, Canada, pp 1383–1396

Bhushan B, Sahoo G (2017) A comprehensive survey of secure and energy efficient routing protocols and data collection approaches in wireless sensor networks. In: 2017 international conference on signal processing and communication (ICSPC). https://doi.org/10.1109/cspc.2017.8305856

Bhushan B, Sahoo G (2020) Requirements, protocols, and security challenges in wireless sensor networks: an industrial perspective. In: Handbook of computer networks and cyber security, pp 683–713.https://doi.org/10.1007/978-3-030-22277-2_27

Bosshart P, Daly D, Gibb G, Izzard M, McKeown N, Rexford J, Schlesinger C, Talayco D, Vahdat A, Varghese G, Walker D (2014) P4: programming protocol-independent packet processors. SIGCOMM Comput Commun Rev 44(3):87–95

Chen X, Ng DWK, Gerstacker WH, Chen H-H (2017) A survey on multiple-antenna techniques for physical layer security. IEEE Commun Surv Tutor 19(2):1027–1053

Chuang C-C, Yu Y-J, Pang A-C (2018) Flow-aware routing and forwarding for SDN scalability in wireless data centers. IEEE Trans Netw Serv Manage 15(4):1676–1691

Clancy TC (2011) Efficient OFDM denial: pilot jamming and pilot nulling. In: 2011 IEEE international conference on communications (ICC). IEEE, pp 1–5

Conti M, Dehghantanha A, Franke K, Watson S (2018) Internet of things security and forensics: challenges and opportunities. Futur Gener Comput Syst 78:544–546

de Fuentes JM, González-Manzano L, González-Tablas AI, Blasco J (2013) WEVAN—a mechanism for evidence creation and verification in VANETs. J Syst Architect 59(10):985–995

Dener M (2014) Security analysis in wireless sensor networks. Int J Distrib Sens Netw 10(10):303501

Ding Z, Fan P, Poor HV (2016) Impact of user pairing on 5G nonorthogonal multiple-access downlink transmissions. IEEE Trans Veh Technol 65(8):6010–6023

Ding ZG, Lei XF, Karagiannidis GK, Schober R, Yuan JH, Bhargava VK (2017) A survey on non-orthogonal multiple access for 5G networks: research challenges and future trends. IEEE J Sel Areas Commun 35(10):2181–2195

Ding Z-G, Xu M, Chen Y, Peng M-G, Poor HV (2018) Embracing non-orthogonal multiple access in future wireless networks. Front Inf Technol Electron Eng 19(3):322–339

Ferrag MA, Maglarasc L, Argyrioud A, Kosmanosd D, Janickec H (2018) Security for 4G and 5G cellular networks: a survey of existing authentication and privacy-preserving schemes. J Netw Comput Appl 101:55–82

Gautam S, Malik A, Singh N, Kumar S (2019) Recent advances and countermeasures against various attacks in IoT environment. In: 2019 2nd international conference on signal processing and communication (ICSPC). IEEE, pp 315–319

Ge X, Cheng H, Guizani M, Han T (2014) 5G wireless backhaul networks: challenges and research advances. IEEE Netw 28(6):611

Girson A (2018) IoT has a security problem will 5G solve it? https://www.wirelessweek.com/article/2017/03/iot-has-securityproblem-will-5g-solve-it. Accessed 15 Jan 2018

Goyal S, Sharma N, Kaushik I, Bhushan B, Kumar N (2021) A green 6G network era: architecture and propitious technologies. Data Anal Manag 59–75.https://doi.org/10.1007/978-981-15-8335-3_7

Hamamreh JM, Furqan HM, Arslan H (2018) Classifications and applications of physical layer security techniques for confidentiality: a comprehensive survey. IEEE Commun Surv Tutor 21(2):1773–1828

Haque AB, Bhushan B (2021) Security attacks and countermeasures in wireless sensor networks. In: Integration of WSNs into internet of things. CRC Press, pp 17–43

Haque AKMB, Shurid S, Juha AT, Sadique MS, Asaduzzaman AS (2020) A novel design of gesture and voice controlled solar-powered smart wheel chair with obstacle detection. In: 2020 IEEE international conference on informatics, IoT, and enabling technologies (ICIoT). https://doi.org/10.1109/iciot48696.2020.9089652

Haque AKMB, Bhushan B, Dhiman G (2021) Conceptualizing smart city applications: requirements, architecture, security issues, and emerging trends. Expert Syst 1–23. https://doi.org/10.1111/exsy.12753

Hasan M, Hossain E (2013) Random access for machine-to-machine communication in LTE-advanced networks: issues and approaches. IEEE Commun Mag 51:86–93

Heath RW, Gonzalez-Prelcic N, Rangan S, Roh W, Sayeed AM (2016) An overview of signal processing techniques for millimeter wave MIMO systems. IEEE J Sel Topics Signal Process 10(3):436–453

Hošek J (2016) Enabling technologies and user perception within integrated 5G-IoT ecosystem. Brno, Czech Republic, VysokéUčeníTechnické v Brně, Nakladatelství VUTIUM

Howe J (2006) The rise of crowdsourcing. Wired Mag 14(6):1–4. Accessed 10 Feb 2022

I-Scoop, 5G and IoT in 2018 and beyond: the mobile broadband future of IoT. https://www.i-scoop.eu/internetof-things-guide/5g-iot/. Accessed 14 Jan 2018

Jaitly S, Malhotra H, Bhushan B (2017) Security vulnerabilities and countermeasures against jamming attacks in Wireless Sensor Networks: a survey. In: 2017 international conference on computer, communications and electronics (Comptelix). https://doi.org/10.1109/comptelix.2017.8004033

Jin J, Gubbi J, Marusic S, Palaniswami M (2014) An information framework for creating a smart city through internet of things. IEEE Internet Things J 1(2):112–121

Jover RP, Marojevic V (2019) Security and protocol exploit analysis of the 5G specifications. IEEE Access (99):1–1

Kapetanovic D, Zheng G, Rusek F (2015) Physical layer security for massive MIMO: an overview on passive eavesdropping and active attacks. IEEE Commun Mag 53(6):21–27

Kaplan K (2018) Will 5G wireless networks make every internet thing faster and smarter? https://qz.com/179794/will-5g-wireless-networks-make-every-internet-thing-faster-and-smarter/. Accessed 14 Jan 2018

Kumar JS, Patel DR (2014) A survey on internet of things: security and privacy issues. Int J Comput Appl 90(11)

Li S, Da Xu L, Zhao S (2018) 5G internet of things: a survey. J Ind Inf Integr 10:1–9

Li W, Wang N, Jiao L, Zeng K (2021) Physical layer spoofing attack detection in MmWave massive MIMO 5G networks. IEEE Access 9:60419–60432

Lin Y-B, Wang S-Y, Huang C-C, Wu C-M (2018) SDN approach for aggregation/disaggregation of sensor data. Sensors 18(7):2025

Lin YB, Huang TJ, Tsai SC (2019) Enhancing 5G/IoT transport security through content permutation. IEEE Access 7:94293–94299

Liyanage M, Ahmad I, Abro AB, Gurtov A, Ylianttila M (eds) (2018) A comprehensive guide to 5G security. Wiley, Hoboken, p 231

Lu L, Li GY, Swindlehurst AL, Ashikhmin A, Zhang R (2014) An overview of massive MIMO: benefits and challenges. IEEE J Sel Topics Signal Process 8(5):742–758

Lu X, Xiao L, Dai C (2018) UAV-aided 5G communications with deep reinforcement learning against jamming. arXiv preprint: 1805.06628

Mehbodniya A, Bhatia S, Mashat A, Elangovan M (2022) Proportional fairness based energy efficient routing in wireless sensor network. Comput Syst Sci Eng

Millr M (2015) The internet of things: how smart TVs, smart cars, smart homes, and smart cities are changing the world. Pearson Education

Mohammadi M, Al-Fuqaha A, Guizani M, Oh J-S (2018) Semisupervised deep reinforcement learning in support of IoT and smart city services. IEEE Internet Things J 5(2):624–635

Mpitziopoulos A, Gavalas D, Konstantopoulos C, Pantziou G (2009) A survey on jamming attacks and countermeasures in WSNS. IEEE Commun Surv Tutor 11(4)

Newsome J, Shi E, Song D, Perrig A (2004) The sybil attack in sensor networks: analysis & defenses. In: Third international symposium on information processing in sensor networks, 2004. IPSN 2004. IEEE, pp 259–268

Nitsche T, Cordeiro C, Flores AB, Knightly EW, Perahia E, Widmer JC (2014) IEEE 802.11 ad: directional 60 GHz communication for multi-gigabit-per-second wi-fi. IEEE Commun Mag 52(12):132–141

Niu Y, Li Y, Jin D, Su L, Vasilakos AV (2015) A survey of millimeter wave communications (mmWave) for 5G: opportunities and challenges. Wirel Netw 21(8):2657–2676

Padmavathi DG, Shanmugapriya M (2009) A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576
Palanisamy T, Alghazzawi D, Bhatia S, Malibari AA (2022) Improved energy based multi-sensor object detection in wireless sensor networks. Intell Autom Soft Comput
Palattella M, Dohler M, Grieco A et al (2016) Internet of things in the 5G era: enablers, architecture and business models. IEEE J Sel Areas Commun 34(3):2016
Prasad AR, Arumugam S, Sheeba B, Zugenmaier A (2018) 3GPP 5G security. J ICT 6(1&2):137–158
Rahimi H, Zibaeenejad A, Safavi AA (2018a) A novel IoT architecture based on 5G-IoT and next generation technologies. Presented at IEEE IEMCON conference, Vancouver, BC, Canada, Nov 2018a. https://arxiv.org/abs/1807.03065
Rahimi H, Zibaeenejad A, Rajabzadeh P, Safavi AA (2018b) On the security of the 5G-IoT architecture. In: Proceedings of the international conference on smart cities and internet of things, pp 1–8
Rappaport TS, Sun S, Mayzus R, Zhao H, Azar Y, Wang K, Wong GN, Schulz JK, Samimi M, Gutierrez F (2013) Millimeter wave mobile communications for 5G cellular: it will work! IEEE Access 1:335–349
Rathore MM, Ahmad A, Paul A, Rho S (2016) Urban planning and building smart cities based on the internet of things using big data analytics. Comput Netw 101:63–80
Shiu Y-S, Chang SY, Wu H-C, Huang SC-H, Chen H-H (2011) Physical layer security in wireless networks: a tutorial. IEEE Wirel Commun 18(2)
Singla R, Kaur N, Koundal D, Lashari SA, Bhatia S (2021) Optimized energy efficient secure routing protocol for wireless body area network. IEEE Access
Sinha P, Jha VK, Rai AK, Bhushan B (2017) Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: a survey. In: 2017 international conference on signal processing and communication (ICSPC). https://doi.org/10.1109/cspc.2017.8305855
Steinmetzer D, Ahmad S, Anagnostopoulos N, Hollick M, Katzenbeisser S (2018) Authenticating the sector sweep to protect against beam-stealing attacks in IEEE 802.11 ad networks. In: Proceedings of the 2nd ACM workshop on millimeter wave networks and sensing systems, conference proceedings. ACM, pp 3–8
Ta-Shma P, Akbar A, Gerson-Golan G, Hadash G, Carrez F, Moessner K (2018) An ingestion and analytics architecture for IoT applied to smart city use cases. IEEE Internet Things J 5(2):765–774
Teniou A, Bensaber B (2018) Efficient and dynamic elliptic curve qu-vanstone implicit certificates distribution scheme for vehicular cloud networks. Secur Privacy 1(1):e11
Wang C, Wang H-M (2016) Physical layer security in millimeter wave cellular networks. IEEE Trans Wirel Commun 15(8):5569–5585
Wang D, Bai B, Zhao W, Han Z (2018) A survey of optimization approaches for wireless physical layer security. IEEE Commun Surv Tutor 21(2):1878–1911
Wang N, Jiao L, Zeng K (2018) Pilot contamination attack detection for NOMA in mm-wave and massive MIMO 5G communication. In: 2018 IEEE conference on communications and network security (CNS), conference proceedings. IEEE, pp 1–9
Wang N, Wang P, Alipour-Fanid A, Jiao L, Zeng K (2019) Physical-layer security of 5G wireless networks for IoT: challenges and opportunities. IEEE Internet Things J 6(5):8169–8181
Wang N, Jiao L, Wang P, Li W, Zeng K (2021) Exploiting beam features for spoofing attack detection in mmwave 60-GHz IEEE 802.11 ad networks. IEEE Trans Wirel Commun 20(5):3321–3335
Wood AD, Stankovic JA, Zhou G (2007) DEEJAM: defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks. In: 4th annual IEEE communications society conference on sensor, mesh and ad hoc communications and networks, 2007. SECON'07, conference proceedings. IEEE, pp 60–69
Xiao L, Greenstein LJ, Mandayam NB, Trappe W (2009) Channel-based detection of sybil attacks in wireless networks. IEEE Trans Inf Forensics Secur 4(3):492–503

Xu LD, He W, Li S (2014) Internet of things in industries: a survey. IEEE Trans Ind Inform 10(4):2233–2243
Yang H, Shi M, Xia Y, Zhang P (2018) Security research on wireless networked control systems subject to jamming attacks. IEEE Trans Cybern 49(6):2022–2031
Ylmaz MH, Arslan H (2015) A survey: spoofing attacks in physical layer security. In: 2015 IEEE 40th conference proceedings on local computer networks conference workshops (LCN workshops). IEEE, pp 812–817
Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M (2014) Internet of things for smart cities. IEEE Internet Things J 1(1):22–32
Zeng K (2015) Physical layer key generation in wireless networks: challenges and opportunities. IEEE Commun Mag 53(6):33–39
Zeng K, Govindan K, Mohapatra P (2010) Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]. IEEE Wirel Commun 17(5)
Zhang K, Liang X, Lu R, Shen X (2014) Sybil attacks and their defenses in the internet of things. IEEE Internet Things J 1(5):372–383
Zhao K, Ge L (2013) A survey on the internet of things security. In: 2013 9th international conference on computational intelligence and security (CIS), pp 663–667
Zhou X, Maham B, Hjorungnes A (2012) Pilot contamination for active eavesdropping. IEEE Trans Wirel Commun 11(3):903–907
Zhu J, Schober R, Bhargava VK (2014) Secure transmission in multicell massive MIMO systems. IEEE Trans Wirel Commun 13(9):4766–4781

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.