Journal on Internet of Things
DOI: 10.32604/jiot.2021.015900
Article

Security Attacks on the IoT Network with 5G Wireless Communication

Ghada Sultan Aljumaie, Ghada Hisham Alzeer and Sultan S. Alshamrani*

Department of Cyber Security, College of Computers and Information Technology, Taif, 21944, Saudi Arabia
*Corresponding Author: Sultan S. Alshamrani. Email: susamash@tu.edu.sa
Received: 19 May 2021; Accepted: 18 July 2021

Abstract: The term Internet of Things has increased in popularity in recent years and has spread to be used in many applications around us, such as healthcare applications, smart homes and smart cities, IoT is a group of smart devices equipped with sensors that have the ability to calculate data, and carry out actions in the environment in which they are located, they are connected to each other through the Internet and recently it has become supported by 5G technology due to many advantages such as its ability to provide a fast connection, despite the efficiency of the IoT supported by the five G technology, it is subject to many security challenges. In this paper, we conducted a comprehensive review of previous research related to the security requirements of the IoT and security attacks.

Keywords: Internet of Things; IoT; 5G; security

1 Introduction

We see remarkable advances in information and communication technology (ICT), which involves wireless communications used in mobile phones (MP). Mobile phones of the first generation were briefly used in a few countries in the late 1980s. After that we had the second generation (2G), the third generation (3G) and the fourth generation (4G, LTE) and they spread enormously through society. Today, the number of computers is more than the population of the planet [1]. Now we have the fifth generation of wireless systems, 5G is not a new technology, but rather an extension of the old 1G to the current 4G technologies [1]. Wireless communication devices have several security vulnerabilities. Cell phones have been targeted for unauthorized copying or spoofing in the first generation (1G) wireless network. In the second generation (2G) of wireless networks, one of the common attacks at the time was the sending of unauthorized messages containing false information or the transmission of unwanted marketing information [2]. In 4G networks, with the spread of smart devices, multimedia and other services, security is becoming more complicated and more threatening [2]. While 5G networks offer fast-paced mobile data speeds and some tremendous potential, there are security concerns that will lead to major security challenges in the future [2]. Fig. 1 shows the evolution of wireless networks and the comparison between 3G, 4G and 5G is shown in Table 1.

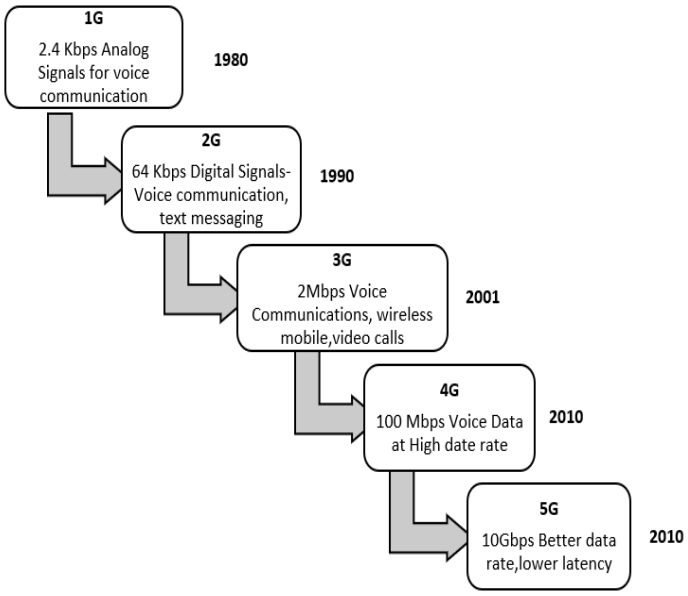

Figure 1: The evolution of wireless networks

Table 1: Comparison of 3G, 4G and 5G features

Features	3G	4G	5G
Start From	2002	2010	2015
Standards	WCDMA, CD, MA200	OFDMA, MC-CDMA	CDMA, BDMA
Network architecture	IP technology and bandwidth CDMA	Combined IP and combination of board band standards like LAN, WAN, WLAN, PAN	Combined IP and combination of board band standards like LAN, WAN, PANW, LAN and WWWW
Date rate	2 Mbps	2 Mbps to 1 Gbps	1 Gbps & higher
Frequency	1.8 to 2.5 GHZ	2-8 GHZ	3–300 GHZ
Core type network	Packet network	All IP network	Flatter IP network & 5G network Interfacing (5G-NI)
Hand over off	Horizontal	Vertical, Horizontal	Vertical, Horizontal

The Internet of Things is an important term which plays an important role in our lives. It is a group of smart devices equipped with sensors that have the ability to calculate data and perform actions in the environment in which they are located, which are connected to each other via the Internet [3]. There are many differences between consumer IoT (cIoT) and industrial IoT (iIoT). The goal of the cIoT is to save time and money by linking the user's environment-related data (such as towns, offices and homes) to consumer electronic devices, i.e., the interaction of a computer with a user. As far as iIoT is concerned, it requires integration between operating technology (OT) and information technology (IT) as it analyses the data obtained by the sensors. iIoT is an interaction between a computer and a machine(M2M) [4]. Many wireless technologies are used in IoT applications, such as 3G/4G with Wi-Fi Bluetooth and ZigBee. Currently, 2G networks that are designed to transmit voice cover about 90% of the world, while the 3G networks designed to transmit voice and data covered about 65% of the world's population, and the 4G networks designed for the broadband internet. In 2012, the fastest type of this network, called

'long term evolution' (LTE), finally, the 5G networks have been developed to solve the 4G networks problems such as speed (the 5G network is 10 times faster than the 4G), intelligence, computing capabilities, etc., as the 5G network provides a wider and faster Internet connection and interacts with the environment by analyzing the data collected by smart sensors.

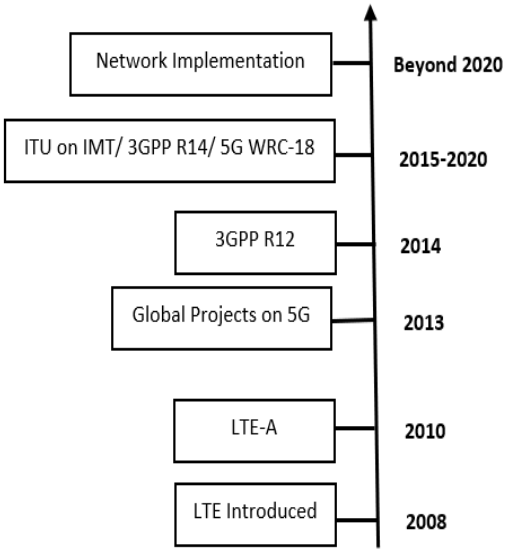

Figure 2: The evolution of cellular networks [3]

The 5G-IoT applications are expected to be available in real time and when needed over the Internet, end-to-end coordinated, fixable, intelligent and automated actions in each phase. The 5G-IoT provides: An independent network which are logically and based on applications' requirements and use Cloud Radio Access Network (C-RAN) which is a mobile network architecture, by using this network the operators can solve the challenges they faced [5] such as the huge connections for a multiple of standards and can perform deployment of the RAN functions that needed by 5G networks. Also facilitate the basic of network architecture to perform on-demand configuration for network functions [6].

The paper was divided into several sections. In the first section we discussed the types of wireless communications and the extent of their development until the emergence of the 5G, we also discussed the term IoT supported by 5G technology. Then, In the second section, we have highlighted the security requirements of the Internet of things in terms of data security, communication security and device security, In the next section, we discuss the safety requirements for IoT with 5G seen by the other researcher. In the fourth section, we mentioned the common types of threats and attacks in the IoT with 5G technology. In the five sections, we mentioned the security solutions in IoT with 5G technology. In the final section of the paper, we mentioned our future work.

2 Background

2.1 IoT Security Requirements

2.1.1 Data Security

IoT data are transmitted through multiple network hops, a strong encryption mechanism is necessary to maintain the confidentiality of the data and also to preserve the data stored on the device, as it is vulnerable to privacy breach by breaching the nodes on the Internet of Things. Hacked IoT devices can harm data integrity, such as data stored and used for malicious purposes [7]. **Privacy** includes hiding important personal information and being able to control it [8]. Data privacy must be analyzed while collecting, transmitting and storing data. There are many practical solutions so that we can deal with data privacy. Such as anonymization, pseudo-random number generators, block ciphers, and flow ciphers [9]. Most mobile applications require permission to access a user's personal information before installing

them, but do not mention where this data is stored and for what purpose it is used. Some threats target the user's privacy such as semantic information attacks, timing attacks [10]. Effect on 5G networks of different parties such as Virtual MNOs (VMNOs), Communication Service, Providers (CSPs) and network infrastructure providers, each one of them has its security and privacy, policies. These differences affect privacy, security and access control [11]. **Data Confidentiality** is the process of hiding private information from the unauthorized IoT objects [12], Data confidentiality is an important issue that requires a lot of attention. In order to provide data protection and confidentiality, it is best to use lightweight graphic encryption algorithms [13]. Data Confidentiality is classified into two types of data confidentiality and also the confidentiality of privacy, the first type depends on preventing unauthorized users from accessing and disclosing the data. The second type includes preventing access and controlling and influencing user data. **Integrity** is to ensure that the content of the message is free from any influence or modification. Authentication in 5G performed in three different ways: authentication by the network only, authentication by the service provider only, and authentication by both network and service provider [14].

2.1.2 Communication Security

Security is one of the most important requirements of cellular systems. AAC (Authentication and Access Control) plays an important role in ensuring the required level of security [15]. Authentication the parties to the communication who want to communicate with each other must authenticate to achieve a secure connection on the Internet of Things [16]. In the 5G networks, authentication is important and is classified into entity authentication and message authentication, in 5G the authentication is between user equipment (UE) and mobility management entity (MME) and the service provider as well [17]. Access control. It is used to prevent illegal users from accessing resources, it also prevents legitimate users from accessing resources in an unauthorized way, and it enables legitimate users to access resources in a licensed manner [18], non-repudiation it is used to ensure that the IoT node cannot be denied when sending and that the recipient cannot deny that the message has been received [19], non-repudiation can be achieved in several ways, including the use of Public Key Cryptography (PKC) [20].

2.1.3 Device Security

Availability is defined as the user’s ability to access the service at any time, and it is a basic requirement in IoT, there are many attacks on IoT devices that deny users services through traditional denial of service attacks or through other types of attacks such as jamming adversaries, sinkhole attacks, or replay attacks [16].

3 Security in IoT with 5G Technology

3.1 Authenticity and Access Control to Secure Communication

The authors in the paper [21] introduce a lightweight mutual authentication protocol with Pseudonyms in the Tag for IoT in 5G, that depend only on Bit and XOR operations for mutual authentication and prevents denial of service (DoS) attacks Also, it can resist the de-sync attack. Where the new and old private key for the session and the IDS are stored in the database, in case the private key of the new session fails to update the tag, the corresponding old private key and IDS are used. they prove that their protocol has a high level of performance and security. In the paper [22], the authors propose a secure and efficient authentication framework that supports network segmentation and fog computing to enable users to efficiently establish connections with the 5G network and access IoT services, Authentication is achieved to ensure the confidentiality of the service data and the reliability of the users. Users can anonymously authenticate with IoT servers by authorizing both the 5G core network and IoT servers the authors demonstrated their protocol adequacy under the 5G infrastructure. The authors in [23] introduce a lightweight authentication protocol for e-health clouds in applications that rely on the Internet of things based on 5G technology, the protocol prevents some common attacks, such as user anonymity, impersonation, stolen smart card attacks, and password guessing, after analysis they demonstrated that their proposed protocol is very effective and secure. The authors in [24] present the SSAAC (Chip Specific

Authentication and Access Control) mechanism, which allows third parties who provide the Internet of Things devices to authenticate and control access to these devices, in addition to providing connectivity to their customers within their production devices, thus reducing the connection provider's CN load, while ,They assessed feasibility by implementing it across OAI-RAN and testing its effect on actual RAN, Then they analyzed the security aspects of their proposed approach. And its effect on reducing the communication provider's CN signals load by comparing it with the signal load of current AAC mechanisms. In this paper [25], the authors introduced a new security feature that involves different technologies applied to 5G such as the Internet of Things. Then, they have proposed a new wireless security architecture for 5G networks It is based on providing flexible authentication and analysis of identity management, finally they mention some the challenges and future directions of 5G wireless security.

3.2 Data Confidentiality/Privacy

The authors of the paper [26] designed a secure D2D connection based on Elliptic Curve Encryption (ECC) and Certified Lightweight Encryption (AEAD) to cover devices with limited IoT resources, to create secure D2D connections and they achieved authentication/data integrity and anonymity, Their design delivers higher performance and better energy efficiency than the AEAD encryption based communication system, and their design also provides security against security threats such as eavesdropping, impersonation, privacy sniffing, and location spoofing. In the paper [27], the authors presented a protocol that supports 5G vehicle network technology that facilitates reliable, safe and privacy-sensitive video reporting, this in-vehicle service is designed for immediate reporting of traffic accident videos so that ambulances can respond in a timely manner to accidents. It has taken an interest in implementing the reporting service in vehicle networks with 5G technology due to the high level of security and privacy. Table 2 summarizes the references and Security requirement.

Table 2: References and security requirement

Paper	Year	Authentication	Access control	Integrity	Confidentiality	Availability	IoT	5G
[21]	2017	YES			YES		YES	YES
[22]	2018	YES		YES	YES	YES	YES	YES
[23]	2020	YES		YES	YES	YES	YES	YES
[24]	2020	YES	YES		YES		YES	YES
[25]	2017	YES	YES	YES	YES	YES	YES	YES
[26]	2020	YES		YES	YES	YES	YES	YES
[27]	2016	YES		YES	YES			YES

4 Threats and Attack in IoT with 5G Technology

The paper [28] showed the fundamental challenges of Next Generation Mobile Networks (NGMN): Flash network traffic: a huge number of end-users, Internet of Things (IoT) devices. Security of radio interfaces: Sending Radio interface encryption keys across insecure channels. User plane integrity: Level of user's data does not have cryptographic integrity protection. Mandated security in the network: Constraints of Service-driven on the architecture of the security system bring into being the optional use of security measures. Roaming security: Peregrination from one operator network to another make an issue in security since no continuously updating for User-security parameters. Denial of Service (DoS) attacks on the infrastructure: Visible nature of network control elements, and unencrypted control channels. Signaling storms: Distributed control systems requiring coordination, e.g., Non-Access Stratum (NAS) layer of Third Generation Partnership Project (3GPP) protocols

DoS attacks on end-user devices: No security measures for operating systems, applications, and configuration data on user devices depending on The Open Networking Foundation (ONF), which is a concern to increase the adoption of both SDN and NFV and issue technical and security specifications [29] focused on the security of technologies that outlined by NGMN, including Mobile Clouds, SDN and NFV, Communication Channels and Privacy in 5G. This section explores Mobile Clouds, SDN and NFV.

Mobile Clouds The possible threat on the front-end of the MCC architecture by using malignant software such as spyware, malware. The threats on the back-end platform have a range from data-replication to (HX-DoS) attacks. For Network-based mobile security threats, the Radio Access Technologies (RATs) such as Wi-Fi, 4G Long Term Evolution (LTE) can attack using Wi-Fi sniffing, DoS attacks and many others [30].

Security Challenges in SDN and NFV SDN focuses on programming in communication networks and centralizes network control platforms. These two points give the adversary distinct chances to break the network security. For instance, centralized network control platforms provide a great opportunity for DoS attacks and unintended software in Application Programming Interfaces (APIs) may lead to network disruption. The NFV plays a significant role in future networks, but also has security challenges concentrated in confidentiality, integrity, authenticity and nonrepudiation [31]. The dynamic nature of Virtual Network Functions (VNFs) can be one of the challenges faced NFG. It may cause error configuration then creates multiple security vulnerabilities. Table 3 from paper [29] summarized security challenges in 5G technology.

Table 3: Summarized security challenges in 5G technology

Security threat	**Target point/Network element**	**Effected technology**				**Privacy**
		DNS	**NFV**	**Channels**	**Cloud**	
DoS attack	Centralized control elements	YES	YES		YES	
Hijacking attacks	SDN controller, hypervisor	YES	YES			
Signaling storms	5G core network elements			YES	YES	
Resource (slice) theft	Hypervisor, shared cloud resources		YES		YES	
Configuration attacks	SDN (virtual) switches, routers	YES	YES			
Saturation attacks	SDN controller and switches	YES				
Penetration attacks	Virtual resources, clouds		YES		YES	
User identity theft	User information data bases				YES	YES
TCP level attacks	SDN controller-switch communication	YES		YES		
Man-in-the-middle attack	SDN controller-communication	YES		YES		YES
Reset and IP spoofing	Control channels			YES		
Scanning attacks	Open air interfaces			YES		YES
Security keys exposure	Unencrypted channels			YES		
Semantic information attacks	Subscriber location			YES		YES

Timing attacks	Subscriber location		YES	YES
Boundary attacks	Subscriber location			YES
IMSI catching attacks	Subscriber identity	YES		YES

4.1 Eavesdropping Attack

The paper [25] mentioned one of a popular type of attack, the adversary can eavesdrop on a message and know its content without anyone feeling this way. To avoid their occurrence, messages are encrypted, but even with their encryption, the attackers can analyze the pattern of communication between the parties and the message traffic, then extract the meaning. One of the challenges in the 5G network is HetNet technology, which leads more difficult to resist eavesdropping attacks. Due to the need to increase the security of the physical layer in the 5G networks, the paper [32] proposed a hybrid security anti-eavesdropping system model and is characterized by being unicast or multiplexing in the case of eavesdropping devices in Three-Dimensional Multi-Input Multi-Output (3D MIMO). The users were divided into three groups: a multicast group (in which multicast transmission beam forming were created), an unicast group (in which linear transmission was pre- coded), and an eavesdropping group (in which secret signals could not be obtained due to anti-eavesdropping). Using the zero-space method, interference between groups of users is prevented. The system has proven its effectiveness by discouraging eavesdropping and increasing confidentiality, but at the same time the system's performance has also decreased, and with this, the proposed system works in a much better way than the traditional system.

4.2 Jamming Attack

Jamming is an attack that may cause a loss of communication between the two ends or disrupt the legitimate users' access to resources, and it is considered an active attack, in the physical layer anti-jamming techniques are used, such as direct sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS), but in the 5G networks, these technologies are incompatible with some applications of this network [25]. The paper [33], a comprehensive survey of the jamming attacks on the 5G New Radio (NR) was conducted, and the researchers concluded that the 5G NR architecture enhances the network's ability to combat jamming attacks, but despite this, the researchers considered that the 5G NRis not considered safe against jamming attacks. In the paper [34], the researchers studied and analyzed the 5G NR against jamming, spoofing, and sniffing attacks by studying individual physical signals and channels, and concluded that it would be a good idea to relax restrictions while implementing 5G NR chips.

4.3 DoS and DDoS Attacks

It is an active attack that can drain all network resources and may use jamming to achieve this goal by randomly forging some packet data packets, a huge number of packets are sent to OpenFlow switch. It attacks many types of layers and is considered a serious threat to 5G users [25]. In the paper [35], the authors found that Software Defined Networking (SDN) (one of the pillars of 5G networks) are an effective way to combat and detect Denial of Service (DoS) and Distributed DoS (DDoS) attacks. the writers used empirical evaluation based on entropy and use SDN in three scenarios two of them are IoT scenarios. And they found this method efficient based on the results. The paper [36] included a focus on DOS/DDoS and Authentication attacks within the range of Software Defined Networking (SDN), Network Function Virtualization (NFV) and cloud computing all in the 5G networks. The authors mentioned potentially effective mechanisms such as IPSec protocol and they proposed use dual homed switching network (DSN).

4.4 MITM Attack

One of the common active attacks in which the enemy intercepts communication between two parties to take the content of the message and modify it or replace it, in this case, authentication is

considered an important matter between the mobile device and the base station [25]. The paper [37] mentioned that there are cases in which the man-in-the-middle (MITM) attack can be distinguished when there is an unjustified delay in the arrival of the packet or taking a long time to travel compared to its counterparts. Researchers have proposed a model in order to discover the MITM attack. The paper suggested the use of a model that establishes a set of nodes to route packets between IoT devices and users and performs several functions such as choosing the best and safest route, avoiding potentially unsafe paths, determining the travel time for packets so that it is less prone to fluctuations, and using a trusted time server (TTS) to make time estimated travel is more accurate and finally provides a feature to check the security of packets. All this should increase the security during the transmission of the packets and facilitate the detection of the presence of the MITM attack. The paper [38] also mentioned that a MITM Attacks targeting OpenFlow channel security can be resolved by the Bloom filter model proposed by the researchers. This model is lightweight, stretch the OpenFlow protocol, and can detect hidden modifications to the data packets that the attacker might make.

4.5 Side Channel Attack

The attack on the network slicing increased due to logical rather than physical isolation, especially if the chips shared the same resources within the same device which called Side-Channel Attack (SCA) as mentioned in paper [39]. The researchers first allocated heterogeneous resources for both the enhanced Mobile Broadband (eMBB) and Ultra- Reliable Low Latency Communications (URLLC) found in the 5G-RAN. Then they proposed to use a routing algorithm for the SCA-RA in order to avoid the SCA attack problem and increase the number of layers that the 5G RAN can accommodate, and the results showed that this algorithm can reduce the blocking of slide requests also can reduce using resources in 5GRAN.

The authors [40], took an interest in introducing a secure cryptographic model called Tiny Encryption Design (TED), that was ultra-light and turned out to be resistant to SCA attacks. Table 4 summarizes the references and Security attack.

Table 4: References and security attack

Paper	Year	Attacks				
		Eaves dropping	JAMMUNG	DoS, DDoS	MITM	Side channel
[25]	2018	YES	YES	YES	YES	
[32]	2019	YES				
[33]	2020		YES			
[34]	2018		YES			
[35]	2020			YES		
[36]	2019		YES	YES		
[37]	2019				YES	
[38]	2017				YES	
[39]	2019			YES		YES
[40]	2020					YES

5 IoT and 5G Security Solution

5.1 Security Solutions for Mobile Clouds

One of the most effective solutions is the use of virtualization VM, as this type isolates the network user from others. Also, the encryption methods of operating and the dynamic allocation of data processing centers must be improved. As for the security measures for storage, it should be energy-saving, achieve

data integrity, and also allows outsourcing to make storage more flexible. In applications, they should be protected and verified properly, in addition to using a Mobil Cloud which is a security framework for mobiles and communications.

5.2 Security Solutions for SDN and NFV

It is easy to detect threats in SDN because it constantly gathers information from a number of network tools and is distinguished by its framework that involves interactive security monitoring systems that track traffic and can adjust security policies and measures based on their analysis. VNFs can achieve the protection concept by coordinating security with the ETSI NFV architecture [41].

5.3 Security Solutions for Communication Channels

To address the security challenges, modern security methods can be used, such as securing the physical layer by via Radio-Frequency (RF) [42], or using one of the encryption protocols as HIP [43] also use asymmetric security method [44].

5.4 Security Solutions for Privacy in 5G

Encryption is useful as a data encryption first and then sends it to the Location-Based Services (LBS) provider [45]. Also using obfuscates quality of the transmitted data for privacy and avoids location attack [25]. Table 5 summarized security technologies and solutions.

Tables 5: Security technologies and solutions

Security technology	Primary focus	Solutions				Privacy
		SDN	NFV	Channels	Cloud	
DoS, DDoS detection	Security of centralized control points	YES	YES			
Configuration verification	Flow rules verification in SDN switches	YES				YES
Access control	Control access to SDN and core network elements	YES	YES		YES	
Traffic isolation	Ensures isolation for VNFs and virtual slices		YES			
Link security	Provide security to control channels	YES		YES		

6 Discussions

After our study of security requirements, our main concern became to meet these requirements, we found many researches related to that, but some research was selected based on what meets these requirements in the 5G Internet of Things. In order to achieve reliability and access control, we discussed several papers, in two of these papers [21,23] the authors presented a lightweight protocol for achieving authentication, in our opinion, their use of a lightweight protocol was an excellent option as they consume fewer resources during the calculation and it is more efficient compared to the traditional protocol, the difference between them is the first protocol depend on XOR and shit operations only, not hash function or other cryptographic operations [21], while the other protocol depends on hash function, and elliptic curve cryptosystem [23]. In another paper [22], the authors present a framework relies on a diffie-hellman key exchange, for a service-oriented three-party key agreement to agree to session keys between IoT servers, users, and local fog. In another research [24] the authors presented the Chip Specific Authentication and Access Control mechanism by authorize AAC devices to third parties that provide these devices in 5G RAN. In our opinion, their approach is good because it provides an embedded connection to its customers within their production devices, and this will increase the level of security. In [25], the authors provided a flexible authentication mechanism for 5G wireless networks in order to

ensure security while meeting quality of service requirements. The inputs were user equipment, access to technology, service requirements and security requirements. The output is a trust model and a cryptographic function. The D2D communication system proposed by the authors [26] used SUCI to establish a D2D connection, coding using lightweight AEAD. AEAD encryption provides integrity and data confidentiality in addition to authentication. The authors in [27] used the Advanced Encryption Standard (AES) Cipher Algorithm in Cipher Block Chaining (CBC).

After mentioning several studies on common attacks on 5G networks and how to detect and prevent them, we will present an analytical review of the studies mentioned in this paper. Firstly, the unicast/ multicast MIMO security system model mentioned in one of the studies is effective in combating eavesdropping but may impair the efficiency of the system especially if it is the unicast security model. HetNet is one of the most important 5G technologies in terms of its efficiency and high coverage, but it is highly vulnerable to eavesdropping attacks, so there is a need for more research and development of technologies that will increase its security. As for the scientific papers focusing on jamming attacks, it has been mentioned that NR technology has proven to be effective against jamming attacks, although, despite its ability to resist jamming attacks, it is not considered completely safe and does not conform to the Osmotic/Catalytic framework in which the safety features are combined based on catalytic and osmotic computing in the 5G networks. The use of Software Defined Networks (SDN) has been suggested and proved to be effective in combating jamming attacks, although it is considered more expensive. Also, there are authors who have suggested intensifying studies in the use of DSN technology, which solves many problems facing the SDN. In the matter of fighting MITM attacks, one paper suggested creating a model that detects anomalies when converting text data. It has given good results, but it needs to develop and communicate with the relevant authorities of international standards to amend the existing protocols in mobile health networks or LPWANs. The Bloom filter, as mentioned by the authors, is an effective way to combat MITM attacks and is lightweight. one of paper proposed to use a routing algorithm for the SCARS, it is true that it was an effective experiment but to reduce the cost of using the wavelength must be considered. The use of Tiny Encryption Design (TED), which is characterized by its ultra-lightness, can be improved by searching for masked S-boxes and inverse masked Sboxes to increase preventing against SCA attacks. Also, in general, consideration should be given to the cost, efficiency, time-saving of each method when it designed.

7 Conclusion

One of the modern wireless technologies used in the Internet of Things is the 5G network technology, which is characterized by its ultra-fast speed and reduced consumption of network energy in addition to increasing battery life and many more. In this paper, we focused our efforts on presenting a comprehensive study on the security of the 5G networks associated with the Internet of Things. We mentioned the history of network development along with the development of the Internet of Things, and then we included the recent researches that talk about the security requirements in the 5G networks and the common attacks on them, In addition to the proposed solutions to these attacks. We have concluded with the analytical critique of the research mentioned in the paper.

Funding Statement: Taif University Researchers Supporting Project No. (TURSP-2020/215), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. X. Wang, F. Haider, X. Gao, X. H. You, Y. Yang *et al.,* "Cellular architecture and key technologies for 5G wireless communication networks," *IEEE Communications Magazine*, vol. 52, pp. 122–130, 2014.

[2] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila *et al.,* "5G security: Analysis of threats and solutions," in *IEEE Conf. on Standards for Communications and Networking* , vol. 10, pp. 193–199, 2017.

[3] G. Rajendran, R. R. Nivash, P. P. Parthy and S. Balamurugan, "Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures," in *Int. Carnahan Conf. on Security Technology*, vol. 10, pp. 1–6, 2019.

[4] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner *et al.,* "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications*, vol. 34, pp. 510–527, 2016.

[5] A. Checko, H. L. Christiansen, Y. Yan, L. Scolari, G. Kardaras *et al.,* "Cloud RAN for mobile networks–A technology overview," *IEEE Communications Surveys & Tutorials*, vol. 17, pp. 405–426, 2014.

[6] S. Li, L. D. Xu and S. Zhao, "5G Internet of Things: A survey," *Journal of Industrial Information Integration*, vol. 10, pp. 1–9, 2018.

[7] Khan, Minhaj, Ahmad, Salah and Khaled, "IoT security: Review, blockchain solutions, and open challenges," *Future Generations Computer Systems*, vol. 12, pp. 1–32, 2018.

[8] S. Misra, M. Maheswaran and S. Hashmi, *Security Challenges and Approaches in Internet of Things.* Springer Publishing Company, Incorporated, 2016, vol. 10, pp. 1–113.

[9] A. R. Sfar, E. Natalizio, Y. Challal and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digital Communications and Networks*, vol. 4, pp. 118–137, 2018.

[10] R. Yu, Z. Bai, L. Yang, P. Wang, O. A. Move *et al.,* "A location cloaking algorithm based on combinatorial optimization for location-based services in 5G networks," vol. 4, pp. 6515–6527, 2016.

[11] Z. Yan, P. Zhang and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking," *Security and Communication Networks*, vol. 9, pp. 3059–3069, 2016.

[12] D. M. Mendez, L. Papapanagiotou and B. Yang, "Internet of Things: Survey on security and privacy," *Information Security Journal: A Global Perspective*, vol. 2, pp. 1–16, 2017.

[13] S. Alam, M. M. Chowdhury and J. Noll, "Interoperability of security-enabled Internet of Things," *Wireless Personal Communications*, vol. 61, pp. 567–586, 2011.

[14] Huawei, *5G Security: Forward Thinking Huawei White Paper.* Shenzhen, China, 2019.

[15] S. Behrad, E. Bertin, S. Tuffin and N. Crespi, "A new scalable authentication and access control mechanism for 5G-based IoT," *Future Generation Computer Systems*, vol. 108, pp. 46–61, 2020.

[16] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101, pp. 55–82, 2018.

[17] L. Jing, X. Yang and C. L. P. Chen, "Authentication and access control in the internet of things," in *32nd Int. Conf. on Distributed Computing Systems Workshops*, vol. 23, pp. 588–592, 2012.

[18] M. M. Hossain, M. Fotouhi and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *IEEE World Cong. on Services*, vol. 12, pp. 21–28, 2015.

[19] Y. Aliouat, Z. Harous, S. Bentaleb, A. Bentaleb and A. Refoufi, "A review of security in Internet of Things," *Wireless Personal Communications*, vol. 108, pp. 325–344, 2019.

[20] K. Fan, P. Song and Y. Yang, "ULMAP: Ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G," *Mobile Information Systems*, vol. 3, pp. 1–7, 2017.

[21] J. Ni, X. Lin and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," *IEEE Journal on Selected Areas in Communications*, vol. 36, pp. 644–657, 2018.

[22] Minahil, M. F. Ayub, K. Mahmood, S. Kumari and A. K. Sangaiah, "Lightweight authentication protocol for e-health clouds in IoT based applications through 5G technology," *Digital Communications and Networks*, vol. 15, pp. 1–13, 2020.

[23] S. Behrad, E. Bertin, S. Tuffin and N. Crespi, "A new scalable authentication and access control mechanism for 5G-based IoT," *Future Generation Computer Systems*, vol. 108, pp. 46–61, 2020.

[24] D. Fang, Y. Qian and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2017.

[25] B. Seok, J. C. S. Sicato, T. Erzhena, C. Xuan and J. H. Park, "Secure D2D communication for 5G IoT network based on lightweight cryptography," *Applied Sciences*, vol. 10, pp. 1–14, 2020.

[26] M. H. Eiza, Q. Ni and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 65, pp. 7868–7881, 2016.

[27] N. Alliance, *Next Generation Mobile Networks (5G White Paper)*. 2015.

[28] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe and A. Gurtov, "5G security: Analysis of threats and solutions," in *IEEE Conf. on Standards for Communications and Networking*, vol. 17, pp. 193–199, 2017.

[29] S. S. Vikas, K. Pawan, A. K. Gurudatt and G. Shyam, "Mobile cloud computing: Security threats," in *Int. Conf. on Electronics and Communication Systems*, vol. 14, pp. 1–4, 2014.

[30] H. Lauer amd N. Kuntze, "Hypervisor-based attestation of virtual environments," in *Int. IEEE Conf. on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Comuting*, vol. 125, pp. 333–340, 2016.

[31] K. Xiao, J. Zhao, M. Jiang and F. Wang, "An anti-eavesdropping scheme for hybrid multicast services with massive MIMO in 5G," *Journal of Computational Methods in Sciences and Engineering*, vol. 19, pp. 71–81 ,2019.

[32] Y. Arjoune and S. Faruque, "Smart jamming attacks in 5G new radio: A review," in *10th Annual Computing and Communication Workshop and Conf.*, vol. 75, pp. 1010–1015, 2020.

[33] M. Lichtman, R. Rao, V. Marojevic, J. Reed and R. P. Jover, "5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation," in *IEEE Int. Conf. on Communications Workshops*, vol. 8, pp. 1–6, 2018.

[34] J. G. Brajones, J. C. Murillo, J. F. V. Valdés and L. Valero, "Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: An experimental approach," *Sensors*, vol. 20, pp. 1–19, 2020.

[35] M. A. Javed and S. K. Niazi, "5G security artifacts (DoS/DDoS and Authentication)," in *Int. Conf. on Communication Technologies*, vol. 19, pp. 127–133, 2019.

[36] J. J. Kang, K. Fahd, S. Venkatraman, R. Trujillo-Rasua and P. H. Dowland, "Hybrid routing for Man-in-the-Middle (MITM) attack detection in IoT networks," in *29th Int. Telecommunication Networks and Applications Conf.*, vol. 25, pp. 1–8, 2019.

[37] Z. Qin, E. Novak and Q. Li, "Securing SDN infrastructure of IoT–fog networks from MitM attacks," *IEEE Internet of Things Journal*, vol. 4, pp. 1156–1164, 2017.

[38] Y. Li, Y. Zhao, J. Li, J. Zhang, X. Yu *et al.,* "Side channel attack-aware resource allocation for URLLC and eMBB slices in 5G RAN," *IEEE Access*, vol. 8, pp. 2090–2099, 2019.

[39] C. Thorat, V. Inamdar and B. Jadhav, "Ted: A lightweight block cipher for IoT devices with side-channel attack resistance," *International Journal on Information Technologies & Security*, vol. 12, pp. 83–96, 2020.

[40] B. Jaeger, "Security orchestrator: Introducing a security orchestrator in the context of the ETSI NFV reference architecture," in *IEEE Trustcom/BigDataSE/ISPA,* vol. 1, pp. 1255–1260, 2015.

[41] B. Gianmarco, G. Raimondo and C. P. Eduardo, "An analysis of the privacy threat in vehicular Ad Hoc networks due to radio frequency fingerprinting," *Mobile Information Systems,* vol. 17, pp. 1–13, 2017.

[42] I. Ahmad, M. Liyanage, A. Gurtov and M. Ylianttila, "Analysis of deployment challenges of host identity protocol," in *European Conf. on Networks and Communications*, vol. 17, pp. 1–6, 2017.

[43] C. Zhao, L. Huang, Y. Zhao and X. Du, "Secure machine-type communications toward LTE heterogeneous networks," *IEEE Wireless Communications*, vol. 24, pp. 82–87, 2017.

[44] X. Pan and Z. Xiao, "Survey of location privacy preserving," *Journal of Frontiers of Computer Science and Technology*, vol. 1, pp. 268–281, 2007.

[45] W. Ynag and C. Fung, "A survey on security in network functions virtualization," in *IEEE NetSoft Conf. and Workshops*, vol. 16, pp. 15–19, 2016.