Emerging 5G networks and internet of things forensics

Nurullayev Doston Zafar o'g'li

Tashkent State University of Law

dostonbeknurullayev@gmail.com.

Abstract

Nowadays 5G technologies are becoming more mainstream thanks to great efforts from telecommunication companies, research facilities, and governments. This technology is often associated with the Internet of Things to improve the quality of life for citizens by automating and gathering data recollection processes. My article presents the 5G and internet of things forensics, explaining common architectures, typical forensics implementations, and recurring problems. This development will have a significant impact and add improvements to digital extended reality, autonomous systems, vehicular ad hoc networks (VANETs), artificial intelligence (AI), underwater communications, blockchain technology, pervasive biomedical informatics and smart cities built on the digital infrastructure backbone of the Internet of Things (IoT). To tell the truth 5G also presents a detailed and explained overview of interference in general wireless applications, interference unique to 5G and IoT, and possible optimization techniques to overcome these challenges. This manuscript highlights the importance of addressing interference and optimizing network performance in 5G networks to ensure reliable and efficient connectivity for IoT devices, which is essential for adequately functioning business processes. This insight can be helpful for businesses that rely on these technologies to improve their productivity, reduce downtime, and enhance customer satisfaction. The ubiquitous nature of this large-scale 5G-enabled IoT that offers faster connectivity capabilities and integrates both terrestrial and non-terrestrial networks will not only create new data security and privacy issues but also provide a treasure trove of digital evidence useful for digital forensic examiners investigating security incidents and cybercrime. We also

highlight the potential of the convergence of networks and services in increasing the availability and speed of access to the internet, enabling a range of new and innovative applications and services. However, for digital forensic examiners, evidence collection, preservation and analysis will become a priority in the successful deployment of 5G IoT networks. In this study, we define key applications of 5G network technology to the Internet of Things and its existing architectures. The survey introduces potential digital forensic challenges and related issues affecting digital forensic investigations specific to 5G IoT networks. Finally, we highlight and discuss forensic readiness and future research directions for identified challenges within the 5G IoT network environments.

Keywords: 5G technologies; interference; wireless network optimization; internet of things

Introduction:

The COVID-19 pandemic shifted the general public's attention to digital solutions and brought immense demand to the telecommunications market. The convergence of 5G technology and internet of things forensics is the next natural step for two advanced technologies developed to make the lives of their users more accessible, more comfortable, and more productive[1]. One of the most standard technologies to be brought into the mainstream area is 5G, which will allow for new business opportunities by being complemented with Industry 4G, IoT devices, and Smart Cities and improve overall connectivity around the globe. The Internet of Things is an ecosystem of increasing complexity: a universe of connected things capable of capturing critical data and carrying out advanced analysis using cloud-based functionalities to extract valuable information. This technology poses a great opportunity for a multitude of actors in all sectors of activity. Many companies are organizing to focus on IoT and connectivity when developing their products and services of the future.

[1] Antonio Acien and Ana Nieto and Javier Lopez (2018): Modelo para la clasificación y análisis de ataques Cross-Platform. In: IV Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2018), Servicio Editorial de Mondragon Unibertsitatea Servicio Editorial de Mondragon Unibertsitatea, Donostia-San Sebastián (España), 2018, ISBN: 978-84-09-02697-5

Fifth-generation (5G) wireless communication technology has been a key enabler in the proliferation and growth of Internet of Things (IoT) applications (S. Li et al., 2018) which has seen billion of devices connected by wireless communication technologies. Compared to wireless technologies, such as 2G/3G/4G, Wi-Fi, Bluetooth, and so forth, 5G offers improved latency, spectrum efficiency, reliability, and a transmission rate of between 10 and 20 Gps which is 100 times higher than 4G (Gai et al., 2021; Lu & Zheng, 2020). It has also taken communication previously limited to only humans to communication between humans and objects. There is great interest in the new applications of mobile technology merging 5G and the Internet of Things technologies. In the design of new applications or technological accessories using 5G and the Internet of Things, compliance with the permitted exposure limits are contemplated. International exposure guidelines have been developed due to extensive research carried out over many decades. All the analyses carried out by independent public health authorities, expert groups, and the World Health Organization (WHO) agree that these guidelines guarantee protection for all people against any health danger. As with all technological generations, 5G dramatically improves energy efficiency department and speed rates. However, this technology has recently been in the public eye for its implementation challenges. However, the full potential of promising new IoT services from extended reality (XR), artificial intelligence (AI), autonomous systems, and telemedicine to underwater sea-based communication and intelligent vehicular ad hoc networks (VANETs) cannot be realized with 5G (Saad et al., 2020). These services are mostly based on ultra-high reliability, high data rates, unmanned mobility management, and long-distance communication (L. U. Khan et al., 2020), which exposes the limitations in the inherent properties of 5G.Moreover, newer forensic analysis challenges will also emerge in the state-of-the-art technologies enabled by 6G that include faster ubiquitous IoT services and applications, where various sensors and networks based on big data and deep learning are interconnected in real and virtual environments (Lu & Zheng, 2020). Hence this increase in IoT connectivity will not only expose the network

communication surface area to exacerbate threats currently seen in 5G networks but also create a spike in prevalent and persistent security-related attacks and incidents that require different digital forensic investigation approaches in 6G networks. Moreover, sifting through the sheer amount of data for valuable forensic artifacts to provide an end-to-end analysis of evidential data is not just difficult but will become increasingly challenging and close to impossible in fully distributed autonomous systems, underwater locations, and virtual and XR environments. Therefore, forensic examiners and incident responders will require specialized methods, procedures, and tools for identifying, collecting, preserving, and analyzing evidential data in large-scale heterogeneous 5G IoT network environments.

Methodology

In my article, a broad overview of the digital forensic challenges related to 5G IoT networks is first introduced. We discuss the key enabling technologies for 5G networks including an overview of 5G-enabled environments to help understand why conducting digital forensic investigations in these environments will require a different approach. Hence, the key contributions of this survey can be summarized as follows:

- The promising smart IoT network environments that 5G wireless communication technology will support are outlined.
- The digital forensics issues and challenges in the key areas of the 5G IoT networks are identified and presented with a detailed discussion on specific digital forensic investigation challenges.[2]

We highlight forensic readiness and future research directions toward conducting digital forensic investigations in these large-scale heterogeneous 5G-enabled IoT networks.The rest of this article is organized as follows. Based on the requirements above, the following are the 5G network deployment requirements:

[2] Huang, H.; Savkin, A.V. A method for optimized deployment of unmanned aerial vehicles for maximum coverage and minimum interference in cellular networks. IEEE Trans. Ind. Inform. 2018.

Millimeter wave (mmWave) frequencies for higher bandwidth and faster data rates.Massive MIMO (multiple input, multiple output) technology for increasing spatial streams and improving the wireless channel's efficiency. The combination of these technologies in 5G networks can enable a wide range of applications, from IoT services to high-bandwidth applications, such as virtual reality and augmented reality. 5G networks aim to provide the necessary performance metrics to support these applications, enabling the growth of the IoT ecosystem and a new era of connectivity.

Results

Proactive digital forensics is a relatively new term that has not yet been applied to 5G environments. Unlike traditional digital forensics, proactive approaches are more dynamic, enabling the system to collect digital evidence periodically, without stopping the functioning of the IT infrastructure (in optimal cases). Although not all systems support this type of action, proactive digital forensic solutions for 5G would allow them to slow down attacks if these are combined with known network security elements. In addition to showing the requirements per layer, it is sought to break down the inter-layer requirements to facilitate the identification of common requirements. In general, the analysis carried out is aimed at finding ways to facilitate orchestration and cooperation between services at different levels. In this case, different forms of crowdsourcing applicable to the 5G-ToT ecosystem are analysed, and a proof of concept considering the Digital Witness solution is shown. Precisely, one of the priority actions in this line is the implementation of a prototype that demonstrates the possible acquisition and management of electronic evidence satisfying digital forensic requirements in 5G-IoT ecosystems, following the IoT-Forensic approach impulsed by the IoTest project[3].

Discussion

In recent years, the deployment of 5G networks has gained significant attention due to its potential to revolutionize the communication industry. One of the areas

[3] Hunukumbure, M.; Tsoukaneri, G. Cost analysis for drone based 5G eMBB provision to emergency services. In Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 9–13 December 2019; IEEE: Piscataway, NJ, USA, 2019;

where 5G networks are expected to have a substantial impact is the IoT services. This literature review article aims to provide an in-depth analysis of the impact of 5G networks on IoT services, specifically examining the issue of interference in this type of network and its related technologies. As a result of new technologies in mobile communications, 5G can provide a solution in a smart city context. Each IoT device can consume a reduced bandwidth, but the problem arises when the number of IoT devices increases. For this reason, it is essential to provide high beam width for better communication between IoT devices. One of the main benefits of the convergence of 5G networks and IoT services is the ability to support massive machine-to-machine communication. The emergence of 5G networks and Internet of Things services has brought about a new era of connectivity and transformation to various industries. With the increasing number of connected devices, there is a need for a network that can handle the massive data transfer, low latency, and high-speed communication required by IoT devices. The convergence of 5G networks and IoT services is expected to revolutionize the way devices communicate with each other and the internet. In this section, we will critically discuss the related impact of network and service convergence between 5G networks and IoT services. The integration of 5G networks with IoT devices creates a seamless connection, allowing devices to communicate with each other and the internet at high speeds and low latency. This has significant implications for industries such as healthcare, transportation, and manufacturing, where large volumes of data need to be transmitted in real time to enable efficient operations. For instance, connected cars, trains, and airplanes can communicate with each other and other connected devices in real time, leading to improved safety and efficiency. Another impact of the convergence of 5G networks and IoT services is the creation of new business models and revenue streams. With the increased speed and capacity of 5G networks, service providers can offer new IoT services such as smart homes, smart cities, and smart factories. This creates an opportunity for service providers to develop new business models and revenue streams, such as selling data insights, providing managed services, and offering customized

solutions. For example, telecom operators can offer IoT connectivity as a service, which provides businesses with a cost-effective and scalable method to connect and manage their IoT devices. However, the convergence of 5G networks and IoT services also presents some challenges that need to be addressed. One of the challenges is the issue of security and privacy. As the number of connected devices grows, the potential for cyberattacks and data breaches also increases. Therefore, service providers and device manufacturers need to work together to ensure that IoT devices are secure and comply with data protection regulations. Additionally, the convergence of 5G networks and IoT services requires significant investments in infrastructure and technology. Service providers need to deploy a massive number of 5G base stations to enable reliable and consistent connectivity for IoT devices. The convergence of 5G networks and IoT services has the potential to revolutionize the way devices communicate with each other and the internet. It has significant implications for industries such as healthcare, transportation, and manufacturing, creating new business models and revenue streams. However, it also presents challenges such as security and privacy concerns and the need for significant investments in infrastructure and technology. Therefore, service providers and device manufacturers need to work together to address these challenges and ensure that the convergence of 5G networks and IoT services leads to a safer, more efficient, and connected world.

Conclusion

The convergence of 5G technology and the Internet of Things is an essential step towards achieving new business opportunities and improving connectivity worldwide. The ecosystem of IoT devices is complex, and choosing the right primary or complementary connectivity option depends on factors such as deployment costs, range, interference, and capabilities. Technical studies have shown that 5G and other services can coexist in specific frequency bands, provided that the technical conditions are adequately adapted. Compliance with the permitted exposure limits is also essential when designing new applications or technological accessories using 5G and IoT.

The convergence of networks and services, driven by 5G technology, is transforming the internet into a complex and multifaceted ecosystem integrated into nearly every aspect of our daily lives. The availability and speed of access to the internet are increasing, allowing users to access high-quality media content in real-time and internet service providers to offer a range of new services and applications. Cellular connectivity will enable the achievement of key IoT goals, such as reducing device complexity and cost, increasing coverage to support remote applications, and providing deployment flexibility, high capacity, and long battery life.Businesses can benefit greatly from the optimization of network performance in 5G networks, which is essential for adequately functioning business processes, improving productivity, reducing downtime, and enhancing customer satisfaction. The potential of the convergence of networks and services in increasing the availability and speed of access to the internet enables a range of new and innovative applications and services, transforming the way we live and work. Managing interference in 5G networks is a significant challenge in ensuring the reliability and performance of IoT services. Effective interference management techniques, diverse connectivity and latency requirements of IoT devices and applications, and external interference are significant issues that must be addressed to ensure that 5G networks can support the massive number of devices and applications that rely on them[4].

5G wireless communication technology is expected to outperform current wireless network technologies by providing revolutionary support and application via the IoT. Its envisioned development and application create a variety of digital forensics challenges. In this article, we presented and discussed the major forensic challenges of 5G IoT networks along with potential forensic readiness approaches, opportunities, and future research directions. At the time of writing, there are no studies that have presented forensic challenges specific to future 5G IoT networks. This study highlights the need for more in-depth studies, and the development of

[4] Zambianco, M.; Verticale, G. Interference minimization in 5G physical-layer network slicing. IEEE Trans. Commun. 2020.

scientifically validated forensic methodologies and tools to ensure successful digital investigations in future 6G IoT environments.

References

1. Antonio Acien and Ana Nieto and Javier Lopez (2018): Modelo para la clasificación y análisis de ataques Cross-Platform. In: IV Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2018), Servicio Editorial de Mondragon Unibertsitatea Servicio Editorial de Mondragon Unibertsitatea, Donostia-San Sebastián (España), 2018, ISBN: 978-84-09-02697-5.
2. Huang, H.; Savkin, A.V. A method for optimized deployment of unmanned aerial vehicles for maximum coverage and minimum interference in cellular networks. IEEE Trans. Ind. Inform. 2018.
3. Hunukumbure, M.; Tsoukaneri, G. Cost analysis for drone based 5G eMBB provision to emergency services. In Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 9–13 December 2019; IEEE: Piscataway, NJ, USA, 2019;
4. Zambianco, M.; Verticale, G. Interference minimization in 5G physical-layer network slicing. IEEE Trans. Commun. 2020.
5. Vermesan, O.; Friess, P. Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems; River Publishers: Ljubljana, Slovenia, 2013.
6. Minoli, D.; Occhiogrosso, B. Practical aspects for the integration of 5G networks and IoT applications in smart cities environments. Wirel. Commun. Mob. Comput. 2019.
7. Ivanova, D.; Markova, E.; Moltchanov, D.; Pirmagomedov, R.; Koucheryavy, Y.; Samouylov, K. Performance of priority-based traffic coexistence strategies in 5G mmWave industrial deployments. IEEE Access 2022.