Investigations of Security Threats and Solutions for 5G and next Generation IoT Systems – PhD Research Proposal

# Introduction

The advent of digital technologies in the past 40 years culminated in the use of various mobile and telecommunication technologies. The 3rd and 4th Generation networks were used over the past three decades and today, most people are transitioning to the 5th Generation systems (Fouque, Onete, & Richard, 2016). The evolution to 5th Generation technology involves the creation of highly-decentralized architectures and the reliance on Internet of Things (IoT) which improves telecommunications significantly. On the downside though, 5th Generation and future networks come with inherent risks including malware, denial-of-service as well as mass surveillance attacks (Bellare, Paterson, & Rogaway, 2014).

The emergence of 5G technology and 6G wireless technologies alongside Internet of things is moving at an extremely fast pace. This creates novel risk sand issues to network security and users of such systems. The proposed research will involve an extensive study of the key components of risks in these emerging digital technologies in order to formulate network security and strategic measures to detect and control these risks.

The proposed study will involve an overview of open technological problems and challenges inherent in 5G and future technologies that affect secure communications in order to standardize these new systems with the trust model through the 3GPP framework. This will involve a review of the unique risks inherent in 5G/6G telecommunication networks and Internet of Things (IoT) systems. This will culminate in the identification of security risk management, the promotion of secure communication and maintaining privacy and trust in 5G/6G technologies and IoT networks.

# Research Background

5G technology provides the possibility of connecting people to the internet everywhere in order to ensure a massive number of devices connected to high-speed internet in an ultrareliable and highly affordable manner (Ahmad, et al., 2017). 5G technology gives room for the scaling of technology and the utilization of new methods and mechanisms in order to provide Wi-Fi connections across many devices (Carmo, Dantas Silva, Neto, & Aguiar, 2019). This has caused the use of the Internet to move from merely connecting people to one where more devices are increasingly being granted Internet functionalities as well as algorithms that boost their functionalities.

The other side of the benefits of 5G technology and advanced networks that support IoT include the fact that it increases the possibilities for malicious attacks on each system. This is due to the fact that the new technologies enabled by 5G technology like cloud computing, Software Defined Networking (SDN) as well as Network Function Virtualization (NFV) is increasing and it comes with many inherent issues and risks (Ahmad, et al., 2017). These risks can be exploited by malicious persons who want to break into a system and this increases the possibility of attacks and misuse of systems.

Privacy and security remain on top of the list of possible actions and activities that could lead to the abuse of a 5G and IoT system (Ahmad, et al., 2017). There are numerous systems that are put in place to limit and restrict these systems. However, the advancement of 5G technologies and high levels of functionality of IoT systems would create new challenges that need to be carefully understood and handled in order to prevent them from getting out of hand and being replicated at a fast rate.

There are many methods of dealing with these risks and situations. This include the use of middleware which is popular in IoT software technology (Amaral, et al., 2016). Middleware is utilized in the development, management and integration of several different devices and applications to manage the risks and deal with them in today’s ultramodern technologies for digital communication. As such, it is possible to manage and deal with the risks to a certain level. In spite of these possibilities, the risks remain high and there are many inherent issues in 5G network systems. This would require a close evaluation in order to understand, appreciate and deal with them in the progressively improving systems.

# Motivation for Research

As the world is moving towards large-scale adoption of 5G and 6G wireless technologies and the number of devices categorized as IoT devices is set to increase, there is the need for careful evaluation and analysis of circumstances and factors relating to its security. It is apparent that many of the things and pointers related to security in these devices are set to increase. This means there are privacy and trust risks that are inherent in this revolution that would get people using record numbers of devices connected to a faster and more functional internet system.

There are some groups like the 3GPP group that has set up standalone systems that can be used to create a holistic system of dealing with security risks and threats in 5G and advanced internet systems (Prasad, Zugenmaier, Escott, & Soveri, 2018). The proposed research for a doctorate in philosophy study would involve a critical review and analysis of key trends and pointers in the emerging 5G/6G wireless technologies. This will be done within the 3GPP framework and will involve trying to understand the risks and study them proactively in order to understand how it works and provide a framework for the protection of these systems through higher and better technologies.

I hold a Masters in Information Technology Security and I am currently a lecturer in X university. From the years of practice and my observation of information systems, it is apparent that 5G and IoT will create new problems and challenges that would demand a strategic solution from technology professionals. If it is managed properly, the problems can be summarily resolved at the core and this can guarantee better results and outcomes. On the other hand, leaving these problems unchecked would most likely cause serious problems and issues that would be more difficult to handle in future. The 3GPP framework creates a standardized and systematic system for the resolution of the most vital issues in 5G systems in order to deal with these risks and issues.

Thus, the proposed research will provide a basis for a critical review of asking the question of how to provide a secure and versatile system of establishing secure channels between devises. This will help to provide secure privacy-preserving protocols that would allow large 5G devices to authenticate and secure the connections they undertake in the emerging advanced technologies

# Research Methods

The research would be divided into four key phases in order to gain an understanding of the issues and gather information. These stages are:

1. Theoretical review;
2. Analysis of key variables;
3. Experimentation and
4. Documentation

The theoretical review will involve a strategic technical analysis of the security systems of 5G mobile networks and IoT systems. This will involve the review of the inherent risk systems and processes that define 5G technologies and IoT system. As part of this stage, there will be the review of best practices in protecting the security, privacy and integrity of information systems in the 5G era. This documentation of the dominant practices and systems will be analyzed in the face of risks and possible issues that could come up. This will be done through a literature review that will include the gathering of information from scholarly sources as well as interviews with experts and practitioners in the field. This will include a review or survey of paper on 5G/IoT.

The analysis phase will cover the identification of key risks and possible risk management systems. This will involve an in-depth review of specific issues that will be identified in the first phase. They will be examined from a strategic context that would explain how a broad overview of plans can be put in place to maintain integrity of systems that use 5G technology and IoT. This phase will cover the review of the best practices that have evolved over the years and how they can be applied to the fast-growing systems and methods. Data from this section will also be from scholarly sources and interviews with experts and practitioners to understand the best ways of dealing with the emerging risks that come with massive issues and problems. This will involve case study and evaluations that would cover the key pointers: privacy, hacking, surveillance, malware and denial of access. These pointers will help to identify the realities in dealing with 5G technology and IoT and the possible solutions to these matters and issues. This will be evidenced by a conference paper that will be submitted at the end of the year.

The third phase of the study will be launched after the general information about the strategic systems and security/technical matters are understood and appreciated. The third phase will include experimentation and a critical analysis and evaluation of a specific project that would be studied by applying different situations and scenarios in order to understand the possible approaches and methods that can be applied. This experimentation process will seek to first apply the best practices to a system and test it on various different scenarios and trends that could happen in real life situations and circumstances. This would be studied and evaluated in order to identify the best and most appropriate mechanisms that can be used to prevent hacking, promote privacy and prevent surveillance, malware amongst others. The experiment will involve the use of a strategic threat prevention method that would be mainly powered by a system deduced from the first to phases. This will be applied and studied in many scenarios that would provide a reasonable understanding of the risks and possible solutions to core elements of security in the evolution of 5G technology and IoT. This phase will culminate in an external presentation that would be used to present information and ideas from the study.

The final phase of the fieldwork will be earmarked by the documentation of the key findings of the research. This will be something that would focus on the compilation of the key observation and major findings in order to present a mechanism of forecasting the risks and the provision of a central mechanism in order to resolve risks and provide solutions. The entire process would include the identification of the main matters that are topical and can be used as a basis for improvements and enhancement with time. This will revolve around the key pointers that would be applicable in an international and universal context for the attainment of best results.

# Timetable

The research will be conducted over a 3-year period. This timeframe will be further divided up into Quarters in each year. There would be targets that would be met in each quarter that corresponds to the four key stages of the research. This is shown in the table below:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Stage | Deliverable | Year 1 | Year 2 | Year 3 |
| Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 |
| 1 | Theory Stage | Review/Survey Paper |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | Analysis Stage | Conference Papers |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | Experiment | External Presentation |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Documentation | Final Project |  |  |  |  |  |  |  |  |  |  |  |  |

At the theory stage, there will be a review of general information from interviews and literature reviews to identify the typical security risks in 5G and IoT systems. This will be the main focus of the first six months of work.

A detailed insight to the components of these risks will be conducted over a period of 1 year. This will involve the identification of the key components of each of the risks and it will commence concurrently with the theory stage after the third month of research.

The experiment system will be modeled end applied at the beginning of the second year of studies. This will include the identification of a system to be studied over the period and evaluated on the basis of some scenarios and extrapolations. This will be studied and recorded throughout Year 2 into the third year.

Findings will be documented after the end of the first quarter of the final year. This will bring together all the components of the study and the key findings.

# References

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2017). 5G security: Analysis of threats and solutions. *IEE*.

Amaral, L. A., de Matos, E., Tiburski, R. T., Hessel, F., Lunardi, W. T., & Marczak, S. (2016). Middleware Technology for IoT Systems: Challenges and Perspectives Toward 5G. *Internet of Things (IoT) in 5G Mobile Technologies*, 333-367.

Bellare, M., Paterson, K. G., & Rogaway, P. (2014). Security of symmetric encryption against mass surveillance. *CRYPTO*, 1-19.

Carmo, M., Dantas Silva, F., Neto, A. V., & Aguiar, R. (2019). Network-Cloud Slicing Definitions for Wi-Fi Sharing Systems to Enhance 5G Ultra Dense Network Capabilities. *Wireless Communications and Mobile Computing*, 1-15.

Fouque, P. A., Onete, C., & Richard, B. (2016). Achieving better privacy for the 3GPP AKA protocol. *PoPETS. vol. 4*, 255-275.

Prasad, A., Zugenmaier, A., Escott, A., & Soveri, M. C. (2018, August 6). *3GPP 5G Security*. Retrieved from 3GPP Systems: https://www.3gpp.org/news-events/1975-sec\_5g