University Of Helsinki

Research proposal for Doctoral Studies

on

Cryptographic Techniques in 5G Networks

Author:
Md. Mohsin Ali Khan

Supervisor:
Professor Valtteri Niemi

January 18, 2016

Evolution of Mobile Network

The journey of mobile networks was commercially started in mid-1980 across Europe. At the beginning, the systems were called public-access mobile communications systems. Because these systems were based on analogue technology, they were very much vulnerable to all kind of security and privacy attacks. The problems caused by these weaknesses were significant factors in triggering a standardization effort and the world experienced the emergence of a second generation system in early 1990s. It is known as GSM. Being an international standard, GSM brings economy of scale and competition. It also enabled users to roam across borders from one network to another. Being digital, GSM system enabled more flexibility and efficiency in transmission. The digital nature of GSM also enabled the introduction of cryptographic primitives in authenticating a user and encrypting the air interface of the user traffic. Thus GSM became the most successful mobile communication system at that time. However, GSM still had weaknesses in its security. For example, the fake base station attack was possible.

Like is the case for any important system, the scientific community continued to improve GSM. Many improvement directions were identified from the privacy, security and efficiency point of view. As a result of the standardization work, we got a third generation system known as UMTS in the beginning of this century. Among many other improvements, e.g. higher data communication rate, UMTS introduced improvements in security, e.g. integrity protection of its signalling and countered the problem of replaying authentication messages. The start and end point of encryption was pushed from the base station to further into the network. The introduction of mutual authentication between the network and the user solved the fake base station attack in its general form but the so called IMSI catching attack breaching the identity privacy of a user was still possible. UMTS also adopted more publicly scrutinized cryptographic algorithms which increased the trust. Thus UMTS was another success in this long journey. The success story did not stop with UMTS. In the beginning of 2010s, the fourth generation mobile network known as LTE has started to be commercially deployed. LTE has superior capability over all the previous generation mobile networks in many aspects. In LTE, every sort of communication including voice is IP based. LTE also has improved its transmission rate dramatically. The security features of UMTS have been significantly adapted, enhanced and expanded to cater the changes in LTE. Nevertheless, the continuous effort to achieve excellence in communication to the real ubiquitous level doesn't stop with LTE. Now the global alliances of mobile network vendors and service providers prepare for 5th generation mobile networks.

5G Network

5G is the next generation commercial mobile network in the line of evolution of mobile networks since 1980s. While GSM and UMTS are still being widely deployed all over the world and LTE has just started its commercial journey, the idea of a 5G network is getting significant momentum. However, there is still a long way to go to freeze the functionality expected from a 5G network. And consequently a huge standardization effort is waiting down the road. Nevertheless, few important associations like 5G PPP and NGMN have presented their visions for a 5G network. Though these visions are not yet finalized, some problems and questions around the use of cryptographic techniques need to be solved and answered in order to develop a successful 5G network.

Next, we will present the visions of 5G PPP and NGMN and then we will also present the problems and questions that we think needs a solution or answer during the standardization.

NGMN defines the following requirements for 5G networks:

1. Data rates of several tens of megabits per second should be supported for tens of thousands of users
2. 1 gigabit per second to be offered simultaneously to tens of workers on the same office floor
3. Several hundreds of thousands of simultaneous connections to be supported for massive sensor deployments
4. Spectral efficiency should be significantly enhanced compared to 4G
5. Coverage should be improved
6. Signalling efficiency should be enhanced
7. Latency should be reduced significantly compared to LTE

By 5G PPP, the following high level Key Performance Indicators (KPIs) are proposed to frame the research activities:

1. Providing 1000 times higher wireless area capacity and more varied service capabilities compared to 2010.
2. Saving up to 90 percent of energy per service provided. The main focus will be in mobile communication networks where the dominating energy consumption comes from the radio access network.
3. Reducing the average service creation time cycle from 90 hours to 90 minutes. Creating a secure, reliable and dependable Internet with a zero perceived downtime for services provision.

4. Facilitating very dense deployments of wireless communication links to connect over 7 trillion wireless devices serving over 7 billion people.

5. Enabling advanced User controlled privacy.

Research Problems

1. Energy Efficiency of radio interface encryption:
   Like in all other evolutionary steps previously, we see that in 5G, the data rate is going to be very high in comparison with what we have in 4G. This brings up the classical problem of energy consumption of a handset once again with a more difficult challenge. It is known that significant amount of energy is consumed by the radio interface resources. And scientists are working on making the radio interface resources more energy efficient. However, it is not clear yet how much energy is going to be consumed for radio interface encryption alone. Do we need lightweight cryptography in 5G networks for the radio interface encryption to contribute in the effort of making the user devices more energy efficient? If yes, then can the currently available lightweight cryptosystems provide the necessary security?

2. Privacy:
   User identity privacy is a problem that retained in all previous generations. It is possible to make an active attack on a user to make him revealing his permanent identity, called IMSI, by setting up a false base station. While standardization of both 3G and 4G was ongoing, this problem was discussed in detail and the most feasible solutions were identified. These were based on either the use of public key methods or symmetric key methods with pseudonyms. All these methods have serious issues and none of them were accepted as an economically viable solution and were not adopted. Now the same question arises once again while standardizing 5G. The question is whether an economically viable solution can finally be developed for 5G networks.

3. Lightweight Authentication and Key Agreement:
   In the future, it is expected that almost everything of our daily online life will be connected by 5G. Many of Internet-connected entities will have limited computing resources from both clock speed and peak power point of view. Furthermore, many of the services offered by service providers are very much latency sensitive. Both of these aspects emphasize the need for a lightweight authentication and key agreement protocol. The research problem is to study and improve the existing lightweight AKA protocol or develop a new one using the existing lightweight cryptosystems. Lightweight in the sense of power consumption and and required clock cycles.

Methodology and Outcomes

The research will be carried on both practically and theoretically depending on the problems that need to be solved. The problem of energy efficiency of radio interface encryption has to be addressed by a practical experiment. There will be many tiny details in the design of the experiment but in a nutshell, the experiment will focus on the difference of doing the same thing in two alternative ways. The two ways are with or without encryption. The experiment will justify if we need lightweight cryptography for radio interface encryption. If the answer is yes, a theoretical study and argument has to be presented about the feasibility of using lightweight cryptography from security point of view.

The problem of identity privacy has to be addressed theoretically. Different existing techniques and proposals of using public key cryptosystem and symmetric key with pseudonyms have to be studied, evaluated and improved if required, to make them applicable to solve the identity privacy problem. The problem of lightweight AKA has to be addressed both theoretically and practically. A lightweight AKA protocol has to be chosen, improved or newly developed theoretically. Then experiment has to be carried out confirming its lightweight nature which is comparable with that of the existing AKA protocols.

Schedule

We target for completing the thesis by the end of 2019. In the first year of the study, 30 credit unit of studies will be completed and the research will primarily focus on the problem of energy efficiency of radio interface encryption. A scientific research paper on this problem is expected to be published in a prestigious conference by mid 2017. In the second year of study, another 24 credit units of studies will be completed and the research will primarily focus on the problem of user identity privacy. A scientific research paper is expected to be published in a journal/conference by mid 2018. In the third year of the studies, the research will focus on lightweight AKA. Two more research papers are planned to be published before mid 2019, potentially one on lightweight AKA and another one on research problems that have been identified during doctoral studies. Preparation will be started for writing the thesis from the beginning of 2019. From mid 2019, writing PhD thesis will be started and be completed by end of 2019.

Funding Plan

First 6 months of research work has already been carried out according to the objectives of the research plan, and funded by the starting package of Professor Niemi. The following 24 months (years 2016 and 2017) are funded by the collaborative project with Huawei Technologies "Security of 5G mobile networks".

The intention is to fund the remainder of the research by a continuation project with Huawei.

1 References

[1] https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf

[2] https://5g-ppp.eu/wp-content/uploads/2014/02/Advanced-5G-Network-Infrastructure-PPP-in-H2020_Final_November-2013.pdf

[2] https://5g-ppp.eu/wp-content/uploads/2014/02/Advanced-5G-Network-Infrastructure-PPP-in-H2020_Final_November-2013.pdf