Noname manuscript No.
(will be inserted by the editor)

AES and SNOW 3G are feasible choices for a 5G phone from energy perspective

Mohsin Khan · Valtteri Niemi

Received: date / Accepted: date

Abstract The aspirations for a 5th generation (5G) mobile network are high. It has a vision of unprecedented data-rate and extremely pervasive connectivity. To cater such aspirations in a mobile phone, many existing efficiency aspects of a mobile phone need to be reviewed. We look into the matter of required energy to encrypt and decrypt the huge amount of traffic that will leave from and enter into a 5G enabled mobile phone. In this paper, we present an account of the power consumption details of the efficient hardware implementations of AES and SNOW 3G. We also present an account of the power consumption details of LTE protocol stack on some cutting edge hardware platforms. Based on the aforementioned two accounts, we argue that the energy requirement for the current encryption systems AES and SNOW 3G will not impact the battery-life of a 5G enabled mobile phone by any significant proportion.

Keywords 5G · Cryptosystem · ASIC

1 Introduction

To facilitate our discussion, we need to know what are the data that will be encrypted and decrypted in a 5G phone. We also need to know where and how many times the encryption and decryption will take place across the protocol stack on the phone. But 5G is not yet a reality and we do not have exact answers to these questions. So, we assume things, that will be true for a 5G network and argue on the basis of those assumptions. We turn to the LTE network to make the assumptions. In an LTE phone, the data that leave and enter the phone can be broadly classified into three categories. The first one are the control signals in between the phone and the core network. The second one are the control signals in between the phone and the radio network. And the third one are the user data which the user sends and receives at the phone's application layer. Both of the first two categories are privacy and integrity protected. For the third category, only the privacy is protected. Also note that, from the volume point of view, the major share of data belong to the third category. Comparing to the the third category, the cryptographic computational need required for the data of first and second categories is negligible. The user data in an LTE phone is only once encrypted and decrypted across the protocol stack in PDCP layer. In an LTE phone this encryption is done by an application specific integrated circuit (ASIC).

For a 5G phone, we assume that the user data will remain as the major share of the total data leaving and entering the phone. The cryptographic computational need for the total volume of control signals will be negligible in comparison with that of the user data. The user data will only once be encrypted and decrypted somewhere across the protocol stack. From hardware point of view it will still be in an ASIC. In order to have a pessimistic estimation, we assume that integrity protection of user data will be introduced in 5G. Based on these assumptions, we will look into the cryptographic energy requirements and also the total energy requirements across the whole protocol stack of an LTE phone. Then we will scale up the data-rate from 100 Mbps to 1 Gbps and see how much extra pressure it puts on the battery of the phone in comparison with other en-

Mohsin Khan
University of Helsinki
E-mail: mohsin.khan@helsinki.fi

Valtteri Niemi
University of Helsinki
E-mail: valtteri.niemi@helsinki.fi

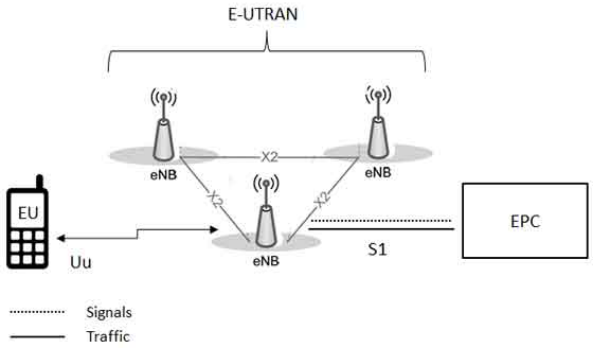

Fig. 1 LTE Architecture, it is a dummy figure, I will draw my own figure

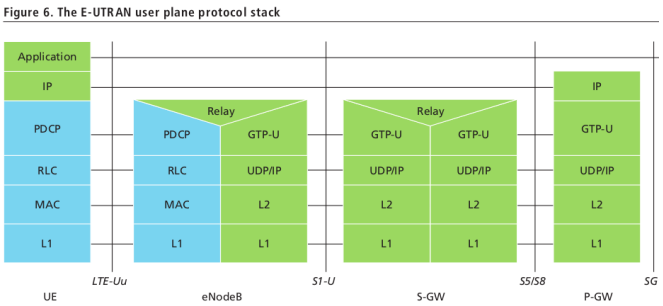

Fig. 2 Protocol stack, it is a dummy figure, I will draw my own figure

ergy hungry aspects of the phone like display and radio signalling.

The paper is organized by first giving a very short introduction to the architecture, the protocol stack and the cryptographic specifications of the LTE network in section 2. In section 3, we present the experimental results about the energy requirements of the two cryptosystems of interest, which are AES and SNOW 3G. In this section we also present the experimental result about the energy consumption across the whole protocol stack of the link layer. In section 4 we present the energy consumption distribution of the whole phone among it's different functional modules and show that the energy needed for cryptographic computation is not a threat for the battery life of the phone.

2 LTE specifications

An LTE network is comprised of broadly three components. The user equipment (UE), evolved radio network (E-UTRAN) known as radio network and evolved packet core (EPC) known as core network. The user equipment consists of a mobile equipment (ME) or a mobile phone for the context of this paper, and an universal integrated circuit card (UICC). The UICC hosts an application called subscriber identification module (SIM). In this paper when we refer to the user equipment, we mean it to be the mobile phone since the UICC does not have much functionality to consume a lot of energy.

The UE is connected to the network via a radio link only with the radio network. The entity of the E-UTRAN that has the radio link with the UE is called eNodeB which is tradionally known as a base station. However, the UE also establishes a direct logical connection with an entity of the core network known as mobility management entity (MME). This logical connection is used only for the control signals for the core network and hence we do not focus on it in this paper. The user data as mentioned in the introduction travels from the UE to the eNodeB. Figure 2 shows the protocol stack that the data travel across at the UE and at eNodeB. The L1 layer is the physical layer. We logically bundle the PDCP,RLC and MAC layers as layer 2 (L2) layer. All the encryption and decryption takes place at the PDCP layer (cite)

According to there are two encryption schemes in the 4th generation cellular network (LTE) developed by 3GPP. One is EEA1 in which the stream cipher SNOW 3G is used. The other is EEA2 in which the block cipher AES is used. The aspiration about 5G networks is to obtain at least 1Gbps data-rate. The question arises, if there are implementations of these two encryption systems that can achieve the required throughput and still be enough energy efficient to use in a mobile phone.

3 Throughput and energy requirements of AES and SNOW 3G

In [1], the authors in their experiment showed that the computing power of a single embedded processor at reasonable clock frequencies is not enough to cope with the L2 requirements of LTE and next generation mobile devices. They illustrated that a conventional hardware acceleration approach for the encryption algorithms fail to offer the performance required by LTE and future mobile devices. The AES decryption was identified as the major time critical software algorithm, demanding half of the entire L2 DL execution time.

In a study in conducted in 2010 on the L2 DL layer (MAC,PDCP,RLC) layer, it has has been shown that by an sDMA, the authors did not mention anything about the achieved throughput but said that, it is enough for an LTE terminal. However, to achive this required throughput, the implementation consumed 9.5 mW of power whereas AES and SNOW 3G each required .5 and .57 mW of power respectively. Which means the

encryption/decryption consumes around 5 percent of the power budget of L2 DL. (see in figure 6)AES

Whereas, a very recent study done in 2014, presented in conducted on the UDP/IP layer, shows that (in Table II) an ASIC implementation consumes 14.62 nano Joule of energy for a Kilobyte data in this layer. Which means it takes $(14.62/8) * 1000 = 1827$ micro Joule of energy for 1 Giga bit data while providing throughtput of 2.24 Gbps..

Researchers have focused on implementing these cryptosystems both in hardware and software to achieve the required throughput. Looking up in the existing literature, it has been found that there exists implementations of these two cryptosystems that can achieve the required throughput even for a 5G network, that is at least 1 Gbps. However, there is no concrete account available of the power consumption of these implementations that enables the readers to estimate the energy share of the task of encryption across the entire protocol stack.

We have studied, collected and rendered the relevant information available in the literature into this single article in an easily comprehensible and comparable manner and make a case that the energy share of data encryption is too low to think of any alternative lightweight encryption for 5G enabled mobile phone.

4 Overall comparison

5 Encryption is time consuming

6 AES

Since the adoption of Rijndael as AES by NIST, there have been number of hardware implementations of AES to achieve efficiency and high throughput. The below table gives a picture

So far the best power figure is found in
According to figure 9 in
Comparing the best figure from the above table with
In the study in

So, with the current best implementation of the encryptor/decryptor hardware engine, in near future the power budget will only increase. However, now we need to check if 10 percent of the power budget for encryption will be good enough for a 5G phone or not.

References

1. Szczesny D, Showk A, Hessel S, Bilgic A, Uwe Hildebrand VF (2009) Performance analysis of lte protocol processing on an arm based mobile platform. In: System-on-Chip, 2009. SOC 2009. International Symposium on, DOI 10.1109/SOCC.2009.5335678