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

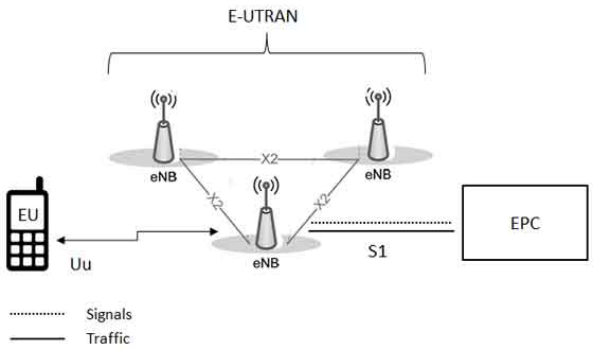

Fig. 1 LTE Architecture, it is a dummy figure, I will draw my own figure

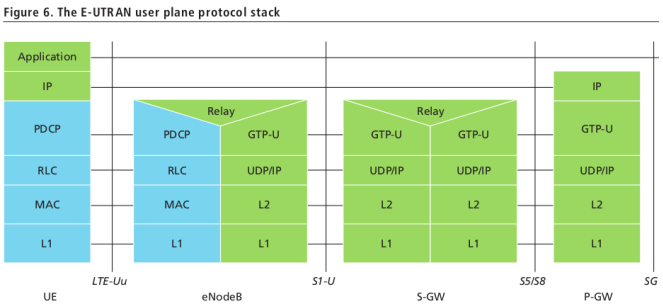

Fig. 2 Protocol stack, it is a dummy figure, I will draw my own figure

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. (cite)

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 [9], 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. So, more advanced hardware acceleration methods were required while keeping the energy and area requirement at a reasonable level for a mobile phone.

In [4], a study conducted on the L2 DL (MAC, PDCP, RLC) layer, the authors have shown that by a smart DMA (direct memory access) controller, the required throughput for LTE which is at most 100 Mbps can be achieved. However, to achive this required through-

put, 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 decryption consumes around 5 percent of the power budget of L2 DL. From energy point of view, it consumes 5.7 millijoule energy to decrypt one giga bit of information. The area effort is also only 15 percent of the total requirement of L2 DL. The figure 6 and 8 in [4] presents the detailed comparison.

In more recent studies, we have found that there have been even further improvement on the energy and area efficiency in the implementations of AES and SNOW 3G. Since the adoption of Rijndael as AES by NIST, there have been a number of hardware implementations of AES to achieve efficiency and high throughput. The below table gives a picture

AES Implementations						
Year	Ref	TP (Gbps)	Gates(K)	Power (mW)	TP/KG in Gpbs	μJoule/Gb
2001	[7]	2.6	21.3	-	0.122	-
2001	[7]	.311	5.4	-	0.0576	-
2001	[6]	.24	4	-	0.06	-
2006	[5]	.570	-	20.34	-	35684
2006	[5]	.569	-	192.5	-	338312
2007	[1]	.384	21	-	0.018	-
2009	[2]	1.16	19.47	-	0.056	-
2009	[3]	1.86	15.25	.78	0.015	419
2011	[10]	.114	–	.02	-	186.18
2012	[8]	1.6	58.445	22.85	-	14281

According to figure 9 in [10], the SAME implementation achieves $5.5Mbps/\mu J$. Which means it spends $114/5.5 = 20.72\mu J = .02mW$ to encrypt/decrypt 114 Mbit. Now, by scaling up by 10 times, it will spend $.02 * 10 = .2mW = .2mJ$ to achieve 1.14Gbps throughput. Which is sufficient for 5G and almost 20 times more energy efficient than that of [4]. In [3], the implementation takes .5 millijoule per gigabit of data. This is 10 times more energy efficient than that of in [4] and it provides enough throughput. Also another implementation that provides with the required throughput requires 14.21 millijoule of energy to encrypt/decrypt one gigabit of data. This implementation is 3 times more energy hungry than that of [3].

Let us assume that the energy share required for encryption is e unit, and the rest of the task of L2 layer requires r unit. The energy share of encryption is then $\frac{e}{e+r} * 100$ percent. So, if in the hardware acceleration of [4], the AES engine is replaced by that of [10], the energy share for encryption becomes .26 percent. Now if there is no further improvement in the energy efficiency of the AES engines but the rest of the L2 layer improves by a factor of α, then the energy share of the AES engine would be $\frac{e}{e+\frac{r}{\alpha}} * 100 \leq .26\alpha$ percent. In the next section, we make an overall comparison to see how much these numbers matters in the context of the energy requirement for the whole mobile phone.

4 Overall comparison

References

1. Cao Q, Li S (2007) An area optimized reconfigurable encryptor for aes-rijndael. In: 2007 Design, Automation and Test in Europe Conference and Exhibition, DOI 10.1109/DATE.2007.364444
2. Cao Q, Li S (2009) A high-throughput cost-effective asic implementation of the aes algorithm. In: 2009 IEEE 8th International Conference on ASIC, DOI 10.1109/ASICON.2009.5351572
3. Hessel S, Szczesny D, Lohmann N, Bilgic A, Hausner J (2009) Implementation and benchmarking of hardware accelerators for ciphering in lte terminals. In: Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, DOI 10.1109/GLOCOM.2009.5426313
4. Hessel S, Szczesny D, Bruns F, Bilgic A, Hausner J (2010) Architectural Analysis of a smart DMA Controller for Protocol Stack Acceleration in LTE Terminals. In: Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd, DOI 10.1109/VETECF.2010.5594536
5. Huang YJ, Lin YS, Hung KY, Lin KC (2006) Efficient implementation of aes ip. In: APCCAS 2006 - 2006 IEEE Asia Pacific Conference on Circuits and Systems, DOI 10.1109/APCCAS.2006.342467
6. Rudra A, Dubey PK, Jutla CS, Kumar V, Rao JR, Rohatgi P (2001) Efficient rijndael encryption implementation with composite field arithmetic. In: Cryptographic Hardware and Embedded Systems CHES 2001, Lecture Notes in Computer Science, vol 2162, pp 171–184
7. Satoh A, Morioka S, Takano K, Munetoh S (2001) A compact rijndael hardware architecture with s-box optimization. In: Advances in Cryptology ASIACRYPT 2001, vol 2248, pp 239–254
8. Shastry PVS, Kulkarni A, Sutaone MS (2012) Asic implementation of aesn. In: 2012 Annual IEEE India Conference (INDICON), DOI 10.1109/INDCON.2012.6420811
9. 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
10. Traboulsi S, Sbeiti M, Szczesny D, Showk A, Bilgic A (2011) High-performance and energy-efficient sliced aes multi-block encryption for lte mobile devices. In: Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference

on, DOI 10.1109/ICCSN.2011.6014927