How Public Key Cryptography Influences Wireless Sensor Node Lifetime

Krzysztof Piotrowski
piotrowski@ihp-microelectronics.com

Peter Langendoerfer
langendoerfer@ihp-microelectronics.com

Steffen Peter
peter@ihp-microelectronics.com

IHP
Im Technologiepark 25
15236 Frankfurt (Oder), Germany

ABSTRACT

In this paper we try to estimate the real influence of public key cryptography (PKC) to the lifetime of a sensor node in wireless sensor networks. We investigate four types of nodes; MICA2DOT, MICA2, MICAz and TelosB. For all these nodes we estimate the power consumption for most common RSA and ECC operations, i.e., signature generation and verification as well as key exchange mechanisms. We also estimate the power consumed by the transmission of their results. Our results show that the application of strong cryptography is feasible. Even for the most constrained node performing the ECC-160 signature once every 10 minutes increases the duty cycle only by about 0.5 per cent, i.e., the influence to the lifetime is not significant. Nevertheless, the public key cryptography shall be used with care.

Categories and Subject Descriptors

D.2.8 [**Software Engineering**]: Metrics—*complexity measures, performance measures*

General Terms

Security, Performance

Keywords

Wireless Sensor Networks, Cryptography, Complexity, Performance, Elliptic Curve Cryptography, RSA

1. INTRODUCTION

Many applications in the area of Wireless Sensor Networks (WSN) would gain a lot from the availability of strong public key cryptography (PKC). The most important advantage is the availability of authentication and key exchange mechanisms that are more secure and reliable compared to secret key cryptography. However, besides the advantages, the public key cryptography has also one main disadvantage. It is computationally expensive. It is nowadays clear that it is possible to apply it but the question that remains is how the application of strong public key cryptography affects the lifetime of the energy source and thus the lifetime of the sensor. That is why here we try to investigate the costs of public key cryptography in WSN and their influence to the node lifetime. We distinguish between the energy consumption for the calculations and the energy used to transfer their results.

It is not easy to judge whether the PKC is generally too expensive for WSN or not. The verdict depends on many application specific factors, e.g., how often shall the crypto operations be performed and if the calculation shall always be followed by the transmission of the resulting signature or encrypted data.

The paper is structured as follows. In the following section we present the sensor nodes for which we provide our evaluation. Then we provide information about the power consumption, i.e., the costs for cryptographic operations in software and costs for data transmission. Based on the data provided we estimate the lifetime of a sensor node. Finally, we draw conclusions and present our plans for further work.

2. THE SENSORS

The sensor nodes we are focusing on in this paper can be divided into two groups depending on the processing unit. The first group is the MICA family[6] (MICA2DOT, MICA2 and MICAz), based on the ATmega128L[1] microcontroller from ATMEL. The second group includes sensor nodes based on the MSP430F1611[10] from Texas Instruments, like TelosB[5] and Tmote Sky[2]. Since the design of the Tmote Sky is based on TelosB in this paper we will refer to TelosB only.

In this section we will try to estimate the performance ratio between these nodes focusing on pure cryptographic calculations. We will normalize the computational performance of these nodes using the results of the weakest one. Combining the ratio with the power consumption of each node we will further estimate the energy consumed by public key cryptography for all sensor nodes given more detailed energy consumption measurements for one type of node.

First we use the information from the microcontrollers' documentations to calculate the overall energy consumption

SASN'06, October 30, 2006, Alexandria, Virginia, USA.

Table 1: Time needed by the sensor nodes to perform SSL/TLS handshake

Sensor node	RSA-1024 handshake	Performance ratio (RSA)
MICA2DOT	22.00 s	1.00
MICA2/MICAz	12.00 s	1.83
TelosB	5.70 s	3.86
Sensor node	ECC-160 handshake	Performance ratio (ECC)
MICA2DOT	1.60 s	1.00
MICA2/MICAz	0.87 s	1.85
TelosB	0.50 s	3.20

Table 2: Power consumed by the sensor nodes to perform SSL/TLS handshake

Sensor node	RSA-1024 handshake	Power consumption ratio (RSA)
MICA2DOT	363.00 mWs	1.00
MICA2/MICAz	360.00 mWs	0.99
TelosB	68.40 mWs	0.19
Sensor node	ECC-160 handshake	Power consumption ratio (ECC)
MICA2DOT	26.40 mWs	1.00
MICA2/MICAz	26.10 mWs	0.99
TelosB	6.00 mWs	0.23

and also the amount of energy consumed per clock cycle. In each case the estimated power consumption is calculated at 3V power supply voltage and at clock frequency as specified for the node.

- TelosB with TI MSP430F1611 at 8 MHz, 4mA → 12 mW,
  - 12 mW / 8MHz = 1.5 nWs,
- MICA2DOT with ATMEL ATmega128L at 4 MHz, 5.5mA → 16.5 mW,
  - 16.5 mW / 4 MHz = 4.125 nWs,
- MICA2 and MICAz with ATmega128L at 7.37 MHz, 10 mA → 30 mW,
  - 30 mW / 7.37 MHz = 4.07 nWs.

This shows that the MSP430 requires only about 40% energy consumed by ATmega running at about the same clock frequency.

The performance ratio between MICA2DOT and MICA2 or MICAz can be estimated easily since both use the same processing unit. The amount of clock cycles will not change and the only difference will be in time needed to perform the same calculation, thus, the performance ratio between nodes belonging to the MICA family is equal to the clock frequency ratio. And thus, if we take the performance of MICA2DOT as one unit, the performance of MICA2 or MICAz will be about 1,85.

In order to estimate the performance ratio between different types of microcontrollers we will use measurements from [4]. In this paper the authors measured the time needed by TelosB and MICA nodes to perform the handshake server side step of the secure SSL/TLS communication. In other words this handshake step is the server side part of the key exchange mechanism. Each type of sensor node performed two kinds of handshake, i.e., the RSA and the ECC based handshake. Table 1 presents the time needed for the calculations only to make the results independent from the type of radio device available at the sensor node [4].

The modulo exponentiation with the big private exponent is the main and most expensive part of the full RSA-1024 handshake. The complete handshake needed about 22 seconds on MICA2DOT, 12 seconds on MICA2/MICAz and about 5.7 seconds on TelosB sensor node.

In the case of full ECC-160 handshake, where the main and most expensive operation is the scalar point multiplication, the time needed was 1.6 seconds on MICA2DOT, 0.87 second on MICA2/MICAz and 0.5 second on TelosB.

Since both types of handshake provide the same functionality we think that the RSA cryptography is not really reasonable for WSN. The same conclusion was drawn in [11]. The reason for this is the enormous time and thus power consumption for RSA calculations and the much larger amount of data to be transmitted.

Based on the measurements for the ECC handshake the computing performance of the TelosB is about 3.2 compared to the performance of the MICA2DOT. The TelosB is also about 1.75 times faster than the MICA2/MICAz nodes. This is the advantage of the 16-bit processing unit of the TelosB.

Knowing the time needed by each type of node we estimate the power consumed by the nodes while calculating the above mentioned operations (see Table 2). Based on these results we create another factor, the power consumption ratio—the power consumed by the cryptographic operations normalized using the power consumed by the least effective node.

Since the clock cost is almost the same for all nodes of the MICA family the power consumption will also be the same. What is interesting, in case of ECC the power consumed by the TelosB node is only 23% of the power consumed by the MICA nodes performing the same operation.

Knowing the performance and power consumption ratios for these sensor nodes we can proceed to a more detailed study on the power consumption of public key cryptography in WSN.

3. POWER CONSUMPTION CAUSED BY APPLYING PUBLIC KEY CRYPTOGRAPHY

3.1 Cryptographic operations

The application of cryptography involves many mechanisms that create the environment for the main operations like encryption, decryption, signature generation and verification. The cost of modular exponentiation (RSA) or point multiplication (ECC) is of course the main indicator of the implementation's efficiency. But besides these two operations cryptography requires also additional operations, e.g., hash value calculations, random number generation and testing if a number is a prime.

Table 3: Power consumption for signature generation/verification and key exchange for the client and server side on a MICA2DOT

Cryptosystem	Signature	
	Generation	Verification
RSA-1024	304.00 mWs	11.90 mWs
ECC-160	22.82 mWs	45.09 mWs
RSA-2048	2302.70 mWs	53.70 mWs
ECC-224	61.54 mWs	121.98 mWs

Cryptosystem	Key exchange	
	Client	Server
RSA-1024	15.40 mWs	304.00 mWs
ECC-160	22.30 mWs	22.30 mWs
RSA-2048	57.20 mWs	2302.70 mWs
ECC-224	60.40 mWs	60.40 mWs

Table 4: Time consumed for signature generation/verification and key exchange for the client and server side on a MICA2DOT (using the active power consumption equal to 13.8 mW)

Cryptosystem	Signature	
	Generation	Verification
RSA-1024	22.03 s	0.86 s
ECC-160	1.65 s	3.27 s
RSA-2048	166.86 s	3.89 s
ECC-224	4.46 s	8.84 s

Cryptosystem	Key exchange	
	Client	Server
RSA-1024	1.12 s	22.03 s
ECC-160	1.62 s	1.62 s
RSA-2048	4.14 s	166.86 s
ECC-224	4.38 s	4.38 s

Another paper [12] provides detailed measurements for the MICA2DOT. The authors measured power consumption for the MICA2DOT for the following cryptographic operations:

- Signature generation/verification and client/server key exchange operations (see Table 3 [12]),
- Calculation of SHA-1 hash value (5.9 μWs/byte),
- AES-128 encryption / decryption (1.62 μWs/byte and 2.49 μWs/byte).

However, in that paper the power consumption of active MICA2DOT is said to be 13.8 mW. That is less than our estimated 16.5 mW, but the difference may be caused by supply voltage lower than 3V. We used the power consumption presented in [12] to estimate the time needed by the MICA2DOT. See Table 4. These data were used to calculate the time and power consumption for all other nodes.

Tables 6 and 7 present the estimated power consumption and time needed by MICA2/MICAz and TelosB nodes to perform key exchange as client and server, respectively, as well as signature generation and verification. Even for the most powerfull TelosB the RSA private key operations are very time and energy consuming.

Once again the results show that RSA is not well suited for WSN. Comparing ECC-160 and RSA-1024 yields in the

Table 5: Estimated power consumption for signature generation/verification and key exchange for the client and server side on a MICA2DOT (based on the time results in Table 4 and assuming the active power consumption is equal to 16.5 mW)

Cryptosystem	Signature	
	Generation	Verification
RSA-1024	363.50 mWs	14.19 mWs
ECC-160	27.23 mWs	53.96 mWs
RSA-2048	2753.19 mWs	64.19 mWs
ECC-224	73.59 mWs	145.86 mWs

Cryptosystem	Key exchange	
	Client	Server
RSA-1024	18.48 mWs	363.50 mWs
ECC-160	26.73 mWs	26.73 mWs
RSA-2048	68.31 mWs	2753.19 mWs
ECC-224	72.27 mWs	72.27 mWs

Table 6: Estimated time and power consumption for signature generation/verification and key exchange for the client and server side on a MICA2/MICAz

Cryptosystem	Signature	
	Generation	Verification
RSA-1024	359.87 mWs 12.04 s	14.05 mWs 0.47 s
ECC-160	26.96 mWs 0.89 s	53.42 mWs 1.77 s
RSA-2048	2725.66 mWs 91.18 s	63.55 mWs 2.13 s
ECC-224	72.85 mWs 2.41 s	144.40 mWs 4.78 s

Cryptosystem	Key exchange	
	Client	Server
RSA-1024	18.30 mWs 0.61 s	359.87 mWs 12.04 s
ECC-160	26.46 mWs 0.88 s	26.46 mWs 0.88 s
RSA-2048	67.63 mWs 2.26 s	2725.66 mWs 91.18 s
ECC-224	71.55 mWs 2.38 s	71.55 mWs 2.38 s

Table 7: Estimated time and power consumption for signature generation/verification and key exchange for the client and server side on a TelosB

Cryptosystem	Signature	
	Generation	Verification
RSA-1024	68.97 mWs 5.66 s	2.70 mWs 0.22 s
ECC-160	6.26 mWs 0.52 s	12.41 mWs 1.02 s
RSA-2048	523.10 mWs 42.89 s	12.20 mWs 1.00 s
ECC-224	16.93 mWs 1.39 s	33.55 mWs 2.76 s

Cryptosystem	Key exchange	
	Client	Server
RSA-1024	3.51 mWs 0.29 s	68.97 mWs 5.66 s
ECC-160	6.15 mWs 0.51 s	6.15 mWs 0.51 s
RSA-2048	12.98 mWs 1.06 s	523.10 mWs 42.89 s
ECC-224	16.62 mWs 1.37 s	16.62 mWs 1.37 s

conclusion that the effort for RSA cryptography is too big. While the application of the even stronger ECC-224 still seems to be feasible, the time and power consumption for the equivalent RSA-2048 is far beyond the acceptable level.

The one big potential advantage of RSA is its computational asymmetry, i.e., the private key operations are very expensive while the public key operations are very cheap. This might be useful for the case where the sensor node communicates with a device that is not constrained with respect to computation power and energy, e.g., a laptop or PDA that reads the measurements out of the node. [13] proposes an architecture that exactly exploits this phenomenon. But if two sensor nodes communicate with each other the RSA is not reasonable anymore.

The time needed for a cryptographic operation limits also the maximum frequency of its occurence. In most cases it should not be a problem, but imagine a situation where a sensor node has to sign or encrypt every reading it makes. In this extreme case if it needs 5 seconds for the signature or encryption then the maximum sensing rate is once every 5 seconds with a 100% duty cycle. But if we can reduce the time for signature or encryption to 1 second, the same number of sensor readings can be executed with a duty cycle reduced to 20%. This underpins again the advantage provided by applying ECC.

In addition to the calculation power transmission power has to be considered. We provide some estimations for this in the next subsection.

3.2 Power Consumption of Transmission

Another issue is the size of the key that directly influences the size of the signature and of the encrypted message. Mentioning the public key encryption we mean an encryption of a single data block that is smaller than the used key. Encryption of a block much bigger than the key causes waste of energy and the symmetric cryptography shall be used in this case. Transmission of data touches another important factor for the estimation of power consumption, which is the energy consumed by the RF part of the sensor.

Table 8: Current and power consumption of the ZigBee transceiver CC2420. Power consumption calculated at 3V supply voltage. Power consumption per bit at transmission speed of 250 kbit/s

Type of transmission	Current [mA]	Power [mW]	Power per bit [μWs/bit]
RX	18.8	56.4	0.226
TX -25 dBm	8.5	25.5	0.102
TX -15 dBm	9.9	29.7	0.119
TX -10 dBm	11.0	33.0	0.132
TX -5 dBm	14.0	42.0	0.168
TX 0 dBm	17.4	52.2	0.209

Table 9: Power consumption of the 433 MHz and 868 MHz transceiver CC1000. Power consumption calculated at 3V supply voltage. Power consumption per bit at transmission speed of 38.4 kbit/s

Type of transmission	Current [mA]	Power [mW]	Power per bit [μWs/bit]
433 MHz			
RX	7.4	22.2	0.578
TX -20 dBm	5.3	15.9	0.414
TX -5 dBm	8.9	26.7	0.696
TX 0 dBm	10.4	31.2	0.812
TX 5 dBm	14.8	44.6	1.160
TX 10 dBm	26.7	80.1	2.086
868 MHz			
RX	9.6	28.8	0.750
TX -20 dBm	8.6	25.8	0.672
TX -5 dBm	13.8	41.4	1.078
TX 0 dBm	16.5	49.5	1.290
TX 5 dBm	25.4	76.2	1.984
TX 10 dBm	—	—	—

All four types of sensor nodes use single chip transceivers. MICA2 and MICA2DOT use 433 MHz or 868 MHz radio chip CC1000 [8] and MICAz and TelosB use ZigBee 2.4 GHz radio chip CC2420 [7], both from Chipcon (now part of Texas Instruments). The two radio types differ in performance. ZigBee devices transmit data with 250 kbit/s data rate with maximum power of 0 dBm and CC1000 chip allows data rates up to 76.8 kbit/s with maximum power of 10 dBm (433 MHz) or 5 dBm (868 MHz). The MICA nodes that use the cc1000 chip use Manchester encoding reducing the maximum transmission rate to 38.4 kbit/s.

The power consumption data for both chips are shown in Table 8 and Table 9. This data shows that the higher power consumption of cc2420 is compensated by the lower cost of per bit transmission. Now we can calculate energy consumed by the transmission of the cryptographic results. The best example of these is the digital signature. The RSA signature is represented by an integer smaller than the used modulus, and in case of ECDSA the signature are two integers smaller than the order of the base point of the used curve. Thus, in case of RSA signature the size of it is about the key size, and for ECDSA the size of a signature is about double the key size.

Table 10: Power consumed while reception of a signature on cc2420 and cc1000 single chip transceiver

Signature	Size	cc2420	cc1000	
			433 MHz	868 MHz
	[bit]	[μJ]	[μWs]	[μWs]
ECDSA-160	320	72.32	184.96	240.00
RSA-1024	1024	231.42	591.87	768.00
ECDSA-224	448	101.25	258.94	336.00
RSA-2048	2048	462.85	1183.74	1536.00

Table 11: Power consumed while sending a signature on cc2420 and cc1000 single chip transceiver with -5 dBm and 0 dBm output power

Signature	Size	cc2420	cc1000	
			433 MHz	868 MHz
	[bit]	[μWs]	[μWs]	[μWs]
Output power -5 dBm				
ECDSA-160	320	53.76	222.72	344.96
RSA-1024	1024	172.03	712.70	1103.87
ECDSA-224	448	75.26	311.80	482.94
RSA-2048	2048	344.06	1425.41	2207.74
Output power 0 dBm				
ECDSA-160	320	66.88	259.84	412.80
RSA-1024	1024	214.01	831.49	1320.96
ECDSA-224	448	93.63	363.78	577.92
RSA-2048	2048	428.03	1662.98	2641.92
Output power 5 dBm				
ECDSA-160	320	—	371.20	634.88
RSA-1024	1024	—	1187.84	2031.62
ECDSA-224	448	—	519.68	888.83
RSA-2048	2048	—	2375.68	4063.23

So for the measured approaches the size of a signature is as follows:

- 320 bits for ECDSA-160,
- 1024 bits for RSA-1024,
- 448 bits for ECDSA-224,
- 2048 bits for RSA-2048.

The key exchange mechanism requires at least the transmission of the calculation results. For ECC it is the resulting point and for RSA the integer, in both cases the size of data is comparable with the size of the signature for the corresponding signature scheme.

The costs of signature reception for both transceivers are presented in Table 10. Table 11 presents the power consumption for sending a signature. Since the sending power for those two transceivers differs, we compare the costs of sending a signature for -5 dBm, 0 dBm and for the cc1000 also for 5 dBm output power. Note that in a real application the sending power is adjustable and depends on the environmental conditions and distance between the communication partners. Thus, the values presented here are somehowe idealized.

In case of digital signature there are four steps to be done; generation, transmission, reception and verification. The two communication partners share the effort, the first one generates and transmits the signature and the second one receives it and verifies.

Let us take the less expensive signature ECDSA-160 as an example. In order to point out very clear that the applicability of PKC does not depend on power consumed by transmitting keys, signatures etc. we will discuss some sample sensor node configurations. The transmission power has the highest impact in case that we combine a MSP430 microcontroller, the one with the lowest power consumption, with a cc1000 transceiver working in the 868MHz frequency band with 5 dBm output power, thus consuming the highest energy for transmission. Even with this worst case combination sending a signature requires only ten per cent of its generation. The reception needs only four per cent of the energy needed for verifying the signature.

For the TelosB node the cost of communication is about 1 per cent for ECDSA-160, about 2 per cent for MICA2DOT and MICA2. For MICAz the significance of communication costs goes below 0.3 per cent.

4. SENSOR LIFETIME ESTIMATION

Batteries are the standard power source for all the above mentioned nodes. The MICA2, MICAz and TelosB nodes are powered by 2 AA cells and MICA2DOT is powered by CR2354 lithium coin cell battery. To estimate the available amount of energy we need to know the capacity of the batteries.

The rated capacity of an AA alkaline battery is about 2500 mAh. However, the manufacturers define the capacity as the amount of energy that can be delivered until the voltage of a single AA cell reaches 0.8 V. And since the sensor nodes are powered by two AA batteries the voltage of such a battery pack is 1.6 V that is below the acceptable voltage for the node.

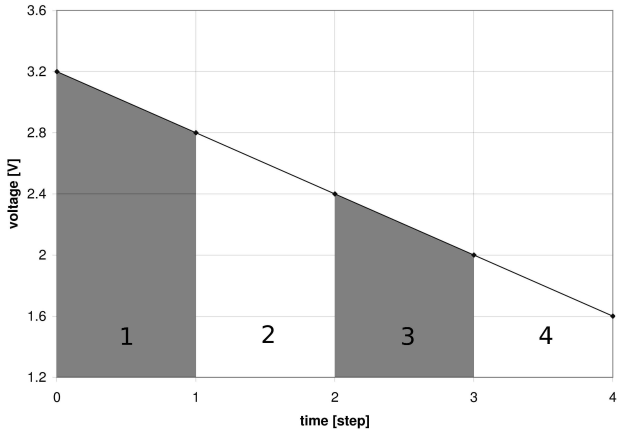

Figure 1: The voltage drop for a battery pack consisting of two AA cells while discharging with a constant current. The areas 1, 2, 3 and 4 represent the percentage of the energy available in each voltage range

The standard approach is to simply use the battery until the voltage goes below the threshold. In this paper we will focus on this method. In this case the calculation of available battery capacity has to take into account that some energy will not be available. The voltage of a new alkaline

AA cell is usually about 1.6 V and as the current is drawn the voltage drops almost linear. We will use this effect to estimate the amount of energy that can be delivered by the double AA cell battery pack that delivers nominal 3.2 V. Assuming linear or almost linear voltage drop to 1.6 V the average voltage for the pack is 2.4 V. The product of time and current is said to be 2500 mAh, which means that the energy that could be delivered is equal to 6000 mWh or simply 21600 Ws. Figure 1 shows the voltage drop while discharging with constant current. The time within which the batteries reach the cut-off (1.6 V) voltage depends on the value of the current. The time axis is divided into four equal periods or steps. And since the current is constant the areas 1 to 4 under the line of voltage drop are proportional to the amount of energy delivered in each time period.

Thus, the energy capacity available by the battery pack can be divided into four partitions depending on the voltage range as follows:

- 3.2 V – 2.8 V — 31.25 % of 21600 Ws → 6750 Ws,
- 2.8 V – 2.4 V — 27.10 % of 21600 Ws → 5850 Ws,
- 2.4 V – 2.0 V — 22.90 % of 21600 Ws → 4950 Ws,
- 2.0 V – 1.6 V — 18.75 % of 21600 Ws → 4050 Ws.

For instance, if a device accepts voltage range between 2.0 V and 3.2 V then the amount of energy available will reach 81.75 % of the whole battery pack capacity, i.e., the device can consume up to 17550 Ws and 4050 Ws will be useless.

Now we estimate the energy that is available for the sensor nodes while powered by such a battery pack. Actually, for the nodes we study, only the single chip transceivers cc2420 and cc1000 can work with supply voltage as low as 2.1 V. Both microcontroller types require voltage higher than 2.7 V. For the ATmega128L microcontroller used by the MICA family this value is the minimum for operation. And the MSP430F1611 from TelosB requires at least 2.7 V to be able to write to flash, though for code execution only it works even at 1.8 V, but only with reduced clock frequency. Also the external flash memory chips require at least 2.7 V supply voltage. This leads us to the conclusion that the estimation of available energy will be adequate if we choose the voltage between 2.8 V and 3.2 V as the useful range. Thus, the node powered by two AA alkaline batteries uses only 31.25 % of the total capacity, i.e., the node can consume about 6750 Ws until the batteries are useless.

For the cr2354 coin cell battery used by MICA2DOT, the rated capacity is 560 mAh, and according to [3] the discharge characteristics is quite flat while discharging with a small constant current of about 0.5 mA. The starting voltage is about 2.9 V at room temperature and about 80 % of the energy capacity can be delivered until the voltage drops below 2.8 V. Thus, the rated energy capacity is about 5500 Ws and the available 4400 Ws.

We estimated the energy consumed by the cryptographic operations for the supply voltage of 3.0 V and, since this is exactly the mean value of the chosen voltage range for the double AA battery pack, the errors in the further estimation for nodes powered by these batteries are minimized. In case of MICA2DOT the nominal voltage of the cr2354 battery is about 0.1 V lower than the ideal value, but we think the estimation error may be neglected.

Table 12: Estimated amount of signature generation / verification operations and key exchange operations for the client and server side on a MICA2/MICAz and TelosB with the 6750 Ws of energy available by the double AA battery pack as well as on the MICA2DOT with the 4400 Ws available by the cr2354 cell battery. If the calculation if followed by transmission the amount of operations is reduced by about 1 per cent

Node	Crypto-system	Signature	
		Generation	Verification
MICA2DOT	RSA-1024	12105	310078
MICA2/MICAz	RSA-1024	18757	480427
TelosB	RSA-1024	97867	2500000
MICA2DOT	ECC-160	161586	81542
MICA2/MICAz	ECC-160	250371	126357
TelosB	ECC-160	1078275	543916
MICA2DOT	RSA-2048	1598	68547
MICA2/MICAz	RSA-2048	2476	106216
TelosB	RSA-2048	12904	553279
MICA2DOT	ECC-224	59791	30166
MICA2/MICAz	ECC-224	92656	46745
TelosB	ECC-224	398701	201192
Node	Crypto-system	Key exchange	
		Client	Server
MICA2DOT	RSA-1024	238095	12105
MICA2/MICAz	RSA-1024	368852	18757
TelosB	RSA-1024	1923077	97867
MICA2DOT	ECC-160	164609	164609
MICA2/MICAz	ECC-160	255102	255102
TelosB	ECC-160	1097561	1097561
MICA2DOT	RSA-2048	64412	1598
MICA2/MICAz	RSA-2048	99808	2476
TelosB	RSA-2048	520031	12904
MICA2DOT	ECC-224	60883	60883
MICA2/MICAz	ECC-224	94340	94340
TelosB	ECC-224	406137	406137

With the values collected so far we calculate the amount of public key cryptography operations the nodes can perform with the available amount of energy. See Table 12. According to our estimations, at 100 % duty cycle, the processing unit of TelosB is able to run for 156.25 hours, MICA2/MICAz for 62.5 hours and MICA2DOT for 77.1 hours with the available energy. Thus, the use of public key cryptography shall not increase the duty cycle of the node in a significant manner. The results in Table 13 and Table 14 show that the numbers for ECC-160 are reasonable. They are even for RSA-1024, but in both cases, only if the operations are used with care. If the duty cycle is affected too much by the public key cryptography operations the lifetime of the sensor is reduced dramatically. But if the number of public key operations is small or is spread over time the theoretical lifetime of the node is several years, assuming the node does nothing else. Of course, such an assumption is silly, but the results indicate the influence of the public key cryptography to the lifetime of the node.

Table 13: Estimated duty cycle and lifetime for RSA-1024 signature generation on a MICA2, MICAz and TelosB with the 6750 Ws of energy available by the double AA battery pack as well as on the MICA2DOT with the 4400 Ws available by the cr2354 cell battery. If the calculation if followed by transmission the values are about 1 per cent worse

RSA-1024 signature generation		
Node	duty cycle [%]	lifetime [h]
	every 30s	
MICA2DOT	73.4333	100.91
MICA2/MICAz	40.1333	155.73
TelosB	18.8666	828.18
	every 60s	
MICA2DOT	36.7166	201.82
MICA2/MICAz	20.0666	311.46
TelosB	9.4333	1656.37
	every 600s	
MICA2DOT	3.6716	2018.19
MICA2/MICAz	2.0066	3114.62
TelosB	0.9433	16563.66
	every 3600s	
MICA2DOT	0.6119	12109.82
MICA2/MICAz	0.3344	18687.72
TelosB	0.1572	99381.98

Table 14: Estimated duty cycle and lifetime for ECC-160 signature generation on a MICA2/MICAz and TelosB with the 6750 Ws of energy available by the double AA battery pack as well as on the MICA2DOT with the 4400 Ws available by the cr2354 cell battery. If the calculation if followed by transmission the values are about 1 per cent worse

ECC-160 signature generation		
Node	duty cycle [%]	lifetime [h]
	every 5s	
MICA2DOT	33.0000	224.55
MICA2/MICAz	17.8000	351.12
TelosB	10.4000	1502.40
	every 30s	
MICA2DOT	5.5000	1347.27
MICA2/MICAz	2.9666	2106.74
TelosB	1.7333	9014.42
	every 300s	
MICA2DOT	0.5500	13472.73
MICA2/MICAz	0.2966	21067.41
TelosB	0.1733	90144.23
	every 600s	
MICA2DOT	0.2750	26945.45
MICA2/MICAz	0.1483	42134.48
TelosB	0.0866	180288.46

5. CONCLUSIONS

Based on the data presented in this article, we can conclude that transmission power is not an important factor when comparing cryptographic algorithms. Even sending a 2048 bit RSA signature by a transceiver that requires 1.0 μWs/bit, needs not more than 2 mWs for one signature. This is at least one order of magnitude less than the energy consumption required for the computation of the cryptographic operations. In large multi–hop networks it might become a factor. In that case a large signature increases the overall transmission power consumption in the network.

Indeed, transmission power becomes more important if the energy required for the cryptographic computations is reduced. It can be assumed that due to improved hardware designs and smaller design structures the power consumption for the actual computation can be reduced. Another possibility of reducing the required energy for cryptographic operations is the application of cryptographic co–processors. Such dedicated hardware solutions perform the required operations much faster—three orders of magnitude. Due to the shorter duty time, the total energy consumption is also much lower. For example, applying a 233 bit ECC accelerator, the signature generation requires merely 30 μWs. In this case, the several hundred μWs for the transmission of the 466 bit signature do have a significant impact.

Actually, these considerations lead to the conclusion that energy consumption of the computation of public key cryptography on WSNs is not a such an important issue as expected. Either the operations are performed so seldom that the required energy can be more or less ignored—for example in case a node is read once the year. Alternatively, performance requirements enforce dedicated hardware, which reduces the power consumption to a non relevant factor, regarding the power consumption needed for the transmission.

What still remains an issue is the energy source. One solution to avoid the loss of energy is to use boost voltage DC/DC converters that can work with input voltage as low as 0.9 V and deliver constant 3 V output voltage. In this case the energy from the batteries can be used in a more efficient way, i.e., even if the voltage goes below the acceptable value the remaining energy can still be used. However, this solution causes additional current consumption caused by the converter. According to the documentation of Texas Instruments' DC/DC converter family TPS61000 [9] the total losses in the converter are less than 50 mW, what is anyway too expensive for a wireless sensor node. Thus, this solution is acceptable if the converter is enabled only in case the voltage drops below acceptable level. Intelligent power management solutions can help extending the lifetime of the sensor node not only in case of public key cryptography applications, but can dramatically increase its applicability.

Our further work includes more empiric investigations. We are going to design a sensor node and study its energy consumption parameters regarding the application of public key cryptography. The node will be based on the MSP430 microcontroller since its power efficiency is much higher, compared to similar solutions. We are also going to investigate the influence of DC/DC converters to the battery usage efficiency compared to simple low voltage solutions.

6. REFERENCES

[1] ATMEL Corporation. *ATmega128(L) - 8-bit AVR Microcontroller with 128K Bytes In-System Programmable Flash*, 2006. Available at: http://www.atmel.com /dyn/resources/prod_documents/doc2467.pdf.

[2] Moteiv Corporation. *Tmote sky - ultra low power IEEE 802.15.4 compliant wireless sensor module*, 2006. Available at: http://www.moteiv.com/products/docs/tmote-sky-datasheet.pdf.

[3] Panasonic Industrial Europe GmbH. *CR2354 Lithium Battery datasheet*. Available at: http://www.panasonic-industrial.com/2464.pdf.

[4] Vipul Gupta, Matthew Millard, Stephen Fung, Yu Zhu, Nils Gura, Hans Eberle, and Sheueling Chang Shantz. Sizzle: A standards-based end-to-end security architecture for the embedded internet (best paper). In *PERCOM '05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*, pages 247–256, Washington, DC, USA, 2005. IEEE Computer Society.

[5] CrossBow Technology Inc. *TelosB Mote Platform Datasheet*. Available at: http://www.xbow.com/Products /Product_pdf_files/Wireless_pdf/TelosB_Datasheet.pdf.

[6] CrossBow Technology Inc. *MPR / MIB User's Manual*, 2005. Available at: http://www.xbow.com /Support/Support_pdf_files/MPR-MIB_Series_Users_Manual.pdf.

[7] Texas Instruments Inc. *Single-Chip 2.4 GHz IEEE 802.15.4 Compliant and ZigBee(TM) Ready RF Transceiver*. Available at: http://www-s.ti.com/sc/ds/cc2420.pdf.

[8] Texas Instruments Inc. *Single-Chip Very Low Power RF Transceiver*. Available at: http://www-s.ti.com/sc/ds/cc1000.pdf.

[9] Texas Instruments Inc. *TPS61000 SINGLE- AND DUAL-CELL BOOST CONVERTER WITH START-UP INTO FULL LOAD*, 2003. Available at: http://www-s.ti.com/sc/ds/tps61003.pdf.

[10] Texas Instruments Inc. *MSP430 Family of Ultra-lowpower 16-bit RISC Processors*, 2005. Available at: http://www-s.ti.com/sc/ds/msp430f1611.pdf.

[11] David J. Malan, Matt Welsh, and Michael D. Smith. A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In *Proceedings of the First IEEE International Conference on Sensor and Ad Hoc Communications and Networks*, Washington, DC, USA, 2004. IEEE Computer Society.

[12] Arvinderpal S. Wander, Nils Gura, Hans Eberle, Vipul Gupta, and Sheueling Chang Shantz. Energy analysis of public-key cryptography for wireless sensor networks. In *PERCOM '05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*, pages 324–328, Washington, DC, USA, 2005. IEEE Computer Society.

[13] Ronald Watro, Derrick Kong, Sue fen Cuti, Charles Gardiner, Charles Lynn, and Peter Kruus. Tinypk: securing sensor networks with public key technology. In *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 59–64, New York, NY, USA, 2004. ACM Press.