Balance of Security Strength and Energy for a PMU Monitoring System in Smart Grid

Meikang Qiu, Huazhong University of Science and Technology and University of Kentucky

Hai Su, University of Kentucky

Min Chen, Huazhong University of Science and Technology and St. Francis Xavier University

Zhong Ming, Shenzhen University

Laurence T. Yang, Huazhong University of Science and Technology and St. Francis Xavier University

ABSTRACT

An efficient dependable smart power grid relies on the secure real-time data collection and transmission service provided by a monitoring system. In such a system, the measuring units, such as phasor measurement units (PMUs) and smart meters (SMs), are critical. These measuring equipments function as sensors in the smart grid. Data exchanges between these sensors and the central controller are protected by various security protocols. These protocols usually contain computationally intensive cryptographic algorithms that cause heavy energy overhead to the sensor nodes. Since PMUs and SMs are mostly energy-constrained, the problem of how to ensure the secure communication with minimum energy cost becomes a critical issue for the functionality of the whole smart grid. In this article, we focus on the low power secure communication of the PMUs and SMs. We take two wireless sensor platforms as examples to experimentally investigate the approaches and principles of reconciling the two conflicting system requirements–communication security and low energy consumptions. The proposed methods are general ones and applicable to other energy-constrained yet security sensitive systems.

INTRODUCTION

The ever increasing global population imposes demanding requirement on the electric power supply. Nevertheless, the global warming and the sustainability of the cities render constraints on the power generation by the traditional environment-hostile power plants. Viable measures for supporting the continuously increasing global economy is to upgrade the current power grid to a smarter grid. The smart grid can deal with the problem by two strategies. One is to improve the efficiency of the current power grid through smartly managing the production, distribution and consumption of electricity. The other is to incorporate the renewable energy resources, like solar, tide and wind sources, into the whole power grid. The green energy lowers the energy price and reduce the greenhouse gas emission.

To achieve above goals, the technologies, including communication technologies, networked control and optimization technologies have to be incorporated into the energy management system (EMS). A fundamental part of such a system is a wide area monitoring system (WAMS) based on a comprehensive communication network [1], including sensor network, WiFi, satellite communication, cellular network, and Internet, etc. The communication network is responsible for information collection and control message transmission, especially when the volatile renewable energy sources are connected to the smart grid. The knowledge of the state information enables the grid operators to adapt their power production and distribution dynamically in real-time. Unlike the communications in the traditional power grid, in the smart grid the ubiquitous communication network extends the system monitoring and control to the end-user level. The end users will be liberated to choose different power suppliers or manipulate their energy usage dynamically. For example, the General Electric's (GE's) smart-grid refrigerator can reduce the consumption significantly by adjusting its working cycle as response to the price signal from the smart grid.

Two types of important nodes in the smart grid are the phasor measurement unit (PMU) and the smart meter (SM). The PMU was first invented at Virginia Tech. Nowadays there are less than 200 PMUs deployed distributedly in

0163-6804/12/$25.00 © 2012 IEEE

U.S. There will be thousands of them in future. PMUs receive a common time reference from the GPS satellites. With the common time reference they can generate the absolute time-stamped voltage and current phasors. The system controller can generate assessment of the system state and power quality by comparing the phasors reported from different PMUs [2]. As an important part of the smart grid, the PMUs are usually equipped with wireless communication components that enable remote data report and control. The SMs are electrical meters armed with two-way real-time communication technologies. Such design allows the price-setting agencies to set the price according to the real-time energy consumption information.

The network based monitoring system provides efficient remote monitoring and control yet exposes the smart grid to potential cyber attacks. Some misleading information or stale information can cause catastrophic consequences to the system, and thus to the customers [3]. For example, malicious modification of phasor information can cause wrong management operations. Malicious analysis against the smart meter data can reveal the living schedule of the householders or production activities of a plant [4]. Even worse, due to the interconnection of the system, terrorists could collect 80 percent of the sensitive information that can be used to plot attacks on the whole smart grid. Thus, communication security (i.e., integrity, authenticity, availability and confidentiality) over the whole system has to be enforced by some cryptographic algorithms [5].

Because the transmission platforms are usually energy-constraint systems, the computation overhead introduced by the cryptographic algorithms can harm the lifetime of the system. Thus, exploring how to implement these algorithms with lower energy consumption while maintaining their security strength arises as a desirable practice. Different implementations of the cryptographic algorithms incur distinct energy costs. These algorithms can be implemented either by dedicated hardware chips or by softwares. The energy cost components of these two types of implementations mainly consist of dynamic power consumption and static power consumption. The dynamic power consumption stems from the instruction execution, memory accesses and operations of the analog chips. The static power consumption are proportional to the active time of the device. Usually the dynamic power consumption accounts for the major part of the total power consumption [6]. When the cryptographic algorithms are implemented by dedicated chips, the dynamic power consumption on CPU is not increased significantly, but the dedicated chips consume more energy. Compared to the hardware implementation, the software implementation executes the algorithms on CPU. The total increased energy cost is less than that of the hardware implementation. According to the works in [7], the more complex the software is, the larger optimization space for power saving is expected. In this article we focus on minimizing the energy consumption reduction through code optimization for the typical cryptographic algorithms.

The typical cryptographic algorithms, such as HASH function, RC5, Data Encryption Standard (DES), Advanced Encryption Standard (AES), RSA, ELGamal encryption, and Shamir's key sharing, are the building blocks of the cyber security systems. The computational complexity of these algorithms is the major contributor of the energy overhead of the sensors. Usually, the computational complexity is determined by the implementation method and the parameter configurations of the algorithms, such as the key length, number of iterations and operation modes. The energy consumption of the algorithm execution is positively correlated to the computation complexity. Therefore, we can manipulate the parameters of the cryptographic algorithms to strike a balance between the required security strengths and their corresponding energy consumptions. We also leverage the code optimization to further reduce the energy cost of the system. The energy optimization presented in this article serves for two objectives:

- Lower the total energy cost at the system level
- Prolonging the lifetime of the system

We choose to study and verify our approach on the real wireless sensor nodes. We first introduce our measurement results of the energy consumption of the cryptographic algorithms implemented on CrossBow and Ember sensors that are most common sensor platforms; then we present an array of code optimization methods for increasing the energy efficiency of the instances of the cryptographic algorithms; finally, we suggest a set of principles for cryptographic algorithm implementation with energy concern.

The rest of this article is organized as follows: a brief survey of the related works are summarized. Some preliminaries of the monitoring system security and energy issues are introduced. We present our measurement results of the energy consumption of several widely used cryptographic algorithms. Following above observation, we present our code optimization approach for energy cost reduction. Finally, we summarize the principles for energy-efficient implementation of the cryptographic algorithms.

The Smart Grid System

Generally, the smart grid is an autonomous system consisting of information collection network, data management center and power grid control center and power transmission infrastructures, as shown in Fig. 1. The information collection network is essentially a compound network consisting of a multi-hop *ad hoc* network, WiFi, satellite communication, cellular network, and Internet. The sensor nodes, such as PMUs and SMs, are deployed over the power grid to monitor the states of the system. The data management center communicates with the sensors and the control centers through the network. It analyzes the information of the power grid and makes corresponding decisions. The power grid control centers receive instructions from the data manage center and actuate the power system according to the received instructions. The whole system works in a real-time manner, which means real-time situation awareness, real-time response, and real-time control.

Basically, most of the PMUs and SMs in the WAMS are deployed in the wild. The collected data is usually transmitted through wireless links that rely on the open media. The adversaries can easily physically destroy or replicate these devices by capturing them.

Security consequences	Attack method
Loss of confidentiality	(i) Eavesdropping and analyzing the wireless transmission; (ii) node capturing and replication
Loss of authenticity	(i) message modification and insertion; message replay; (ii) node capturing and replication; (iii) Sybil attack in which a small number of malicious nodes forge a large number of fake identifications to cheat the disrupt the message routing.
Loss of integrity	message modification
Loss of availability	(i) message blocking by collaboration of the malicious nodes, wireless channel jamming; (ii) fake data request to the sensors that cause unnecessary energy consumption.

Table 1. *Potential attacks against WAMS.*

In the smart grid, data collection is performed by the measuring devices, such as PMUs and SMs. Those measuring nodes are usually implemented as embedded systems to perform data processing and two-way communications. Due to the vast amount of deployment, each node is relatively cheap and simple. Thus, they have very limited on-board resources. For example, they usually have one simple low speed Micro Control Unit (MCU) as the processor, very limited memory space and very tight power budget due to their deploying areas, cost and physical sizes. The MCU is a small computer integrated on a single chip. It runs programs to support computation and control tasks in an embedded system. The MCUs are usually much simpler than the CPUs for the general purpose computers. Therefore, only some basic tasks, like simple computation and communication, can be implemented on these nodes.

SECURITY RISKS

VULNERABILITIES OF THE SMART GRID

Basically, most of the PMUs and SMs in the WAMS are deployed in the wild. The collected data is usually transmitted through wireless links that rely on the open media (i.e., wireless channel). The adversaries can easily physically destroy or replicate these devices by capturing them. The attackers can also launch attacks by setting up some hacker equipment. We summarize some potential attacks against the WAMS in Table 1.

ENERGY CONSUMPTION OF THE CRYPTOGRAPHIC ALGORITHMS

In the information security literature, there has been plenty of works addressing the defending schemes against the attacks in either wired network or wireless network. Generally, the confidentiality can be enforced by encryption algorithms, the authenticity can be achieved by digital signature schemes, the integrity can be ensured by the Message Authentication Codes (MACs), and the availability can be preserved by introducing redundancy into the data transmission. The additional energy cost incurred by publickey encryption algorithms have been investigated in [8–10]. However, these works only provide energy consumption measurement of the public-key algorithms. Other commonly used algorithms are not considered. In this article, we consider symmetric encryption algorithms and integrity protection algorithms. As a matter of fact:

- Providing protections over all the aspects of the security risks is prohibitively energy consuming for the sensor nodes
- Not all the algorithms are necessary for all the sensor nodes in the WAMS

For example, for the relay nodes, they need the authentication but the encryption operation. They just need authenticate themselves to their next hops and forward their received cipher text to their next hops. Therefore, we classify the security of the nodes into four levels: Level 0, non-security service; Level 1, single security service (one encryption or authentication); Level 2, double security services (one encryption and authentication), and Level 3, triple security services (two encryptions and authentication).

Those different levels of security have various corresponding energy consumptions for the nodes. We use CrossBow MICA2 sensor node as our experiment platform. The energy consumption of the node can be partitioned into two parts:

- The background energy consumption due to the ordinary functions of the applications
- The superposition energy consumption due to the execution of the security services

From the system perspective, the background energy consumption is dominated by the sensing circuit, the peripherals, the MCU and the RF circuit. Since the computation overhead incurred by the security applications is executed exclusively on the MCU of the node, the additional energy consumption is dominated by the computational complexity of the cryptographic algorithms. We use Tektronix TDS5032B oscilloscope to measure the voltage variation and operating time of the sensor node. We derive the current measurement from a sensitive resistor. The power and energy consumption can then be calculated from the measured voltage and current. Figure 2 shows the statistics of the power consumption of the sensor node with different security configurations. The vertical coordinate denotes the energy consumption normalized to the energy consumption of the sensory circuit. It can be seen that compared to the power consumption when there is no security applications (Level 0), the total power consumption increases significantly when security measurements are implemented. The increment of power consumption mainly comes from the increased power cost of the MCU and the RF module. This is because the MCU performs the arithmetic calculations of the cryptographic algorithms and the secured data usually contains extra security bits that consume more radio transmission power.

For the nodes with low computational power, the power consumption for the different levels of security can vary largely. However, for the nodes that have relatively higher computation capability, the power costs for different levels are more constant. In addition, increasing the data transmission speed can help to reduce the energy consumption.

Energy Consumption Measurements

In this section, we present the measurement results of the energy consumption of the cryptographic algorithms implemented on CrossBow MICA2 and Ember platforms. Based on the observation obtained from Fig. 2, the energy reduction space lies in the energy consumptions of the MCU, we only present the energy consumption profile of the MCU and the whole platform. Since the energy consumption varies for the lengths of the messages as well as the different cryptographic algorithms, we first measured the energy consumption of the MCU and the platform with respect to the different message lengths. We plot the results in Fig. 3 as the baseline for later comparisons. Because the two platforms use the same MCU for the same application configuration, the energy consumptions of the MCUs are the same. The difference lies in the total energy consumptions. This inconformity is due to their different configurations in their RF modules. The transceiver chip of CrossBow sensor works at 868/915 MHz radio frequency with data rate of 19.2-38.4 kb/s. While that of Ember sensor works at 2.4 GHz with data rate of 250 kb/s. For the same transmission distance, the energy consumption for transmission of Ember platform is far less than that of CrossBow platform. This is because higher data rate shorten the transmission interval.

Energy Consumption of Cryptographic Algorithm on CrossBow Sensor

We present the measurement results of the energy consumptions of the MCU and the whole platform on CrossBow node when cryptographic algorithms are implemented in Fig. 3a. For the MCU, the energy consumption is significantly increased. We show the energy consumption of level 0 as baseline in the figure. It can be seen that the energy consumed by the MCU for level 1 security enforcement (i.e. single encryption or authentication) is 1 to 15 times higher than that of the level 0. The energy for MCU of level 2 (i.e., encryption combined with authentication) ranges from 9 to 23 times of that of the level 0. The total energy consumption profiles are shown in Fig. 3b. Compared to the total energy consumption for level 0, the encryption services increases the total energy consumption for CrossBow platform by 4 percent to 20 percent for using RC5, DES and AES. When the authentication service is employed, the energy consumption get increased by 94.3 percent on average. This is because the authentication algorithm SHA-1 generates and adds 20 bytes authentication message to the original data, which increases the energy for transmission. An increment of 94.3 percent in energy consumption implies that the lifetime of CrossBow sensor is cut off to the half.

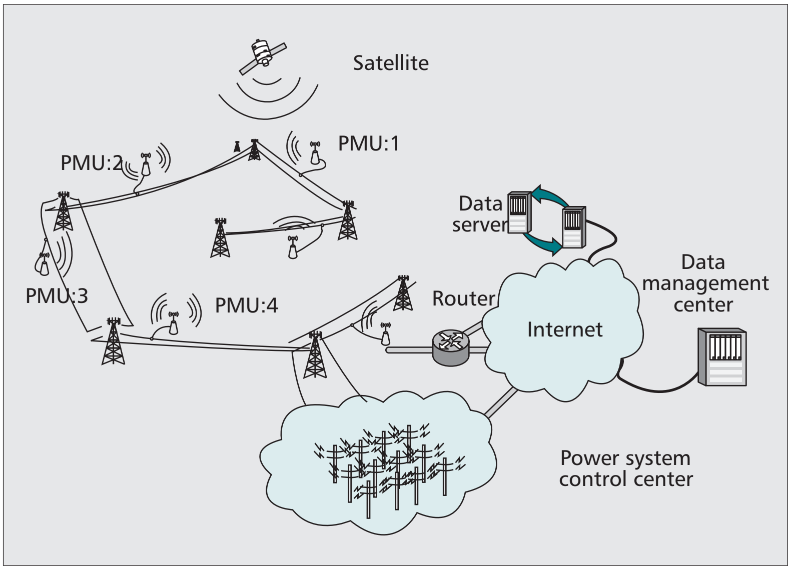

Figure 1. *The smart grid with wide area monitoring system (WAMS).*

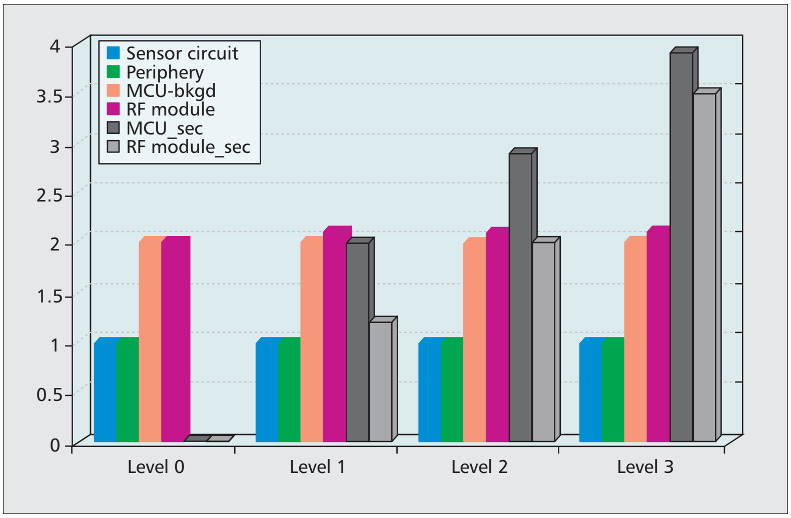

Figure 2. *Security level vs. energy consumption.*

Energy Consumption of Cryptographic Algorithms on Ember Sensor

Similar to the measurement of the energy consumption with security service enforced on CrossBow, we present the measurement results of Ember sensor in Figs. 3c and 3d. Compared to the level 0 baseline, the energy for security consumed by MCU is increased by from 2 to 9 times.

The total energy consumption profile is shown in the Fig. 3d. It can be seen that the energy consumed by the stand-alone implementations of the SHA-1, RC5, DES and AES doubled the energy consumption compared to the level 0 implementation. This implies that authentication and encryption algorithms does not make much difference in terms of total energy consumption. Level 2 implementations can cause 2.9 times more energy cost, which means that the lifetime of the sensor is reduced to around 30 percent of that when no security service is enforced.

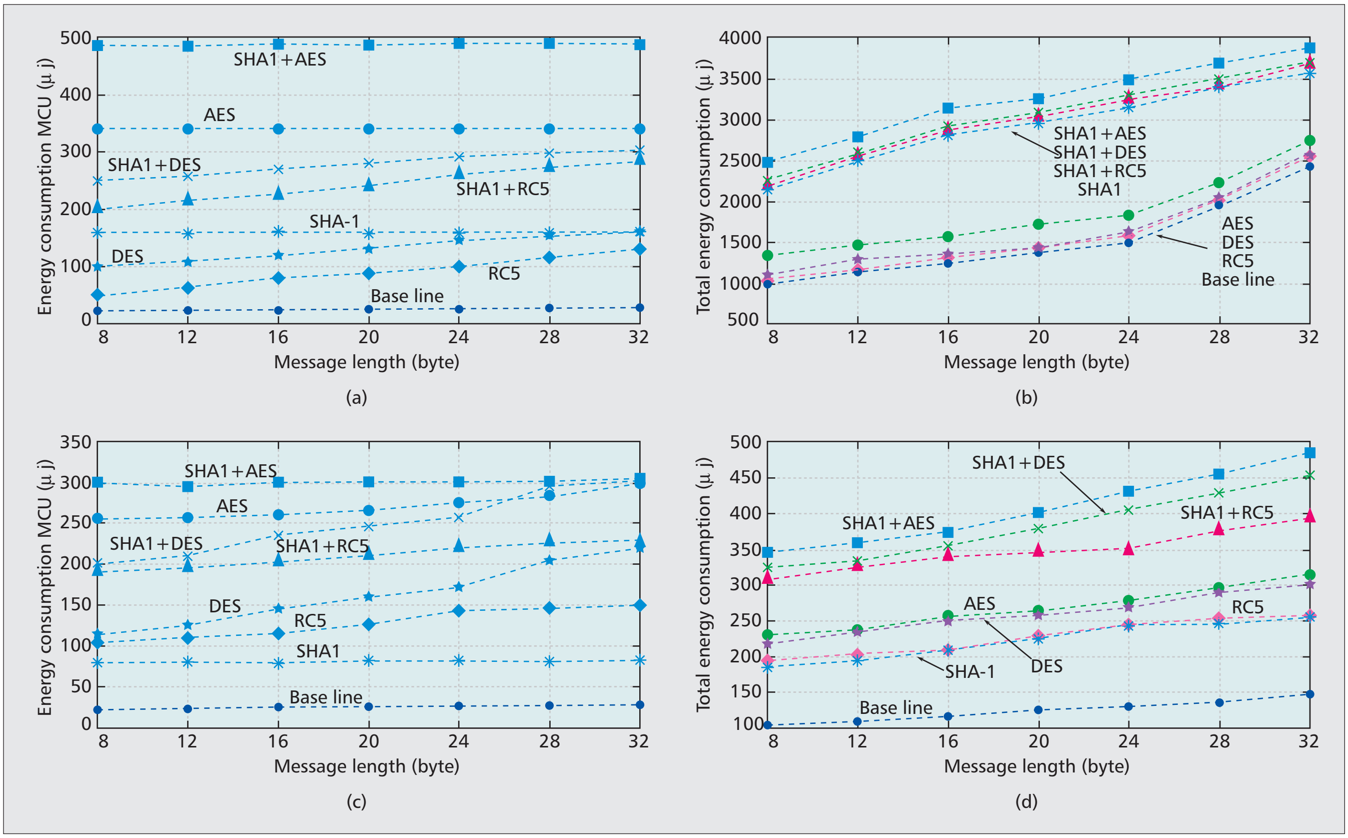

Figure 3. *a) MCU energy consumption profile of the algorithms on CrossBow platform; b) total energy consumption of the various algorithms on CrossBow platform; c) MCU energy consumption profile of the algorithms on Ember platform; d) total energy consumption of the various algorithms on Ember platform.*

Energy Optimization for Encryption Algorithms

The Structure of Energy Consumption of AES

RC5, DES and AES are all symmetric-key encryption algorithms in which the plain text or cipher text are processed with substitution iteratively. Based on such iterative structure, look-up table and loop unrolling can be used to reduce the computational complexity. In this section, we demonstrate the proposed energy saving code optimization through optimizing energy consumption for AES algorithm.

The procedure of AES algorithm proceeds in multiple rounds. The main body of the algorithm consists of four steps, including **SbuByte, ShiftRow**, **MixColumns** and **AddRoundKey** as shown in the dashed line in Fig. 4a. The main body consumes the major portion of the security energy. The functions of these subroutines are just to map the inputs to their corresponding outputs. Besides the step SbuByte that is originally a look-up table, other three steps can also be implemented by pre-defined look-up tables. Look-up tables are usually used to improve the computation efficiency of some complicated functions. In a look-up table implementation, all the possible outputs of the function are pre-calculated and stored in the memory. Each time the output of an input is looked up in the memory instead of being calculated in the MCU. The look-up table can save the computation operations at cost of storage space.

The loop unrolling technique can reduce the number of loops by increasing the parallelism of operations in one iteration. Doing so can reduce the time for jumps, branches, and cache miss, which reduces the execution time of the program. For instance, a one-time loop unrolling is shown in Fig. 4b. The loop body in Fig. 4a is instanced twice in one round of the loop. The total number of the loop jumps is halved. Obviously loop unrolling increases the size of the program. When implementing the algorithms by loop unrolling, we have to take into account the total available memory space. In the following, we show the effect of the loop-up table and loop unrolling on the security energy consumption.

We implemented the AES encryption on CrossBow sensor with different parameters in code optimization. The configuration and results are shown in the Fig. 5a. The energy consumption shown in the figure is normalized with respect to the energy consumption when there is no code optimization used. It can be seen that

- Without look-up table implementation of the subroutines **ShiftRow**, **MixColumns** and **AddRoundKey**, the loop unfolding alone makes no significant difference in energy consumption
- With the subroutine **ShiftRow** being imple-

mented by look-up table, the energy cost for 0 and 1 loop unrolling are reduced by 41.5 percent

This is because the lookup table saves MCU computations but increases the energy consumed by accessing memory as well. Similarly, the loop unrolling increases the program efficiency as well as the energy for accessing the memory. It can be seen that too many lookup tables and loop-unrollings do not ensure energy reduction. Therefore, there is a trade-off between the MCU computation saving and the increase of memory access. The lowest energy consumption comes with the combination of the one lookup table and one-time loop unrolling.

Configuration of Encryption Algorithms

In this subsection, we reveal the effects of key length, encryption mode, and number of iterations on the energy consumption. For the encryption algorithms, there are four optional operation modes which are electric codebook (ECB), cipher-block chaining (CBC), cipher feedback (CFB) and output feedback (OFB). In the ECB mode, the plaintext is divided into blocks. Each block is encrypted independently. The same plaintext will be encrypted into the same ciphertext. The ECB mode has the least security strength. In the CBC mode, each block of plaintext is XORed with its predecessor ciphertext block before being encrypted. This mode gives out more secure ciphertext compared to the ECB mode. The CFB mode is similar to the CBC mode. The OFB mode makes a block cipher into a synchronous stream cipher. Those key stream blocks are XORed with the plaintext blocks to get the ciphertext. Among those operation modes, the ECB is the simplest one and consumes the least energy, while the OFB consumes the most. We implemented the AES on CrossBow under the four modes. In our experiment we encrypted a 32-byte data with key size of 128 bits, 256 bits, and 512 bits. According to our measurements, the ECB mode consumed the least energy regardless of the key size.

We also experimented the RC5 on CrossBow sensor with different key lengths and number of iterations. The results are shown in Fig. 5b. The vertical coordinate measures the energy consumption per plain text byte in micro Joules. We show the energy consumptions of the algorithm with key lengths of 56, 128, and 256 bits in combinations with various numbers of iterations. It can be seen that the number of iteration affects the energy consumption a lot. The implementation with 16 iterations consumes 3.3 times more energy than that with 8 iterations. With the same number of iterations, the energy consumption variation due to the variation of key size is not significant. For the 16-iteration implementation, this variation becomes ignorable. Obviously, the longer key and more iterations there are, the more secure the system is. However, the energy consumption is higher for the more secure system. There must be a balance between the security and energy saving.

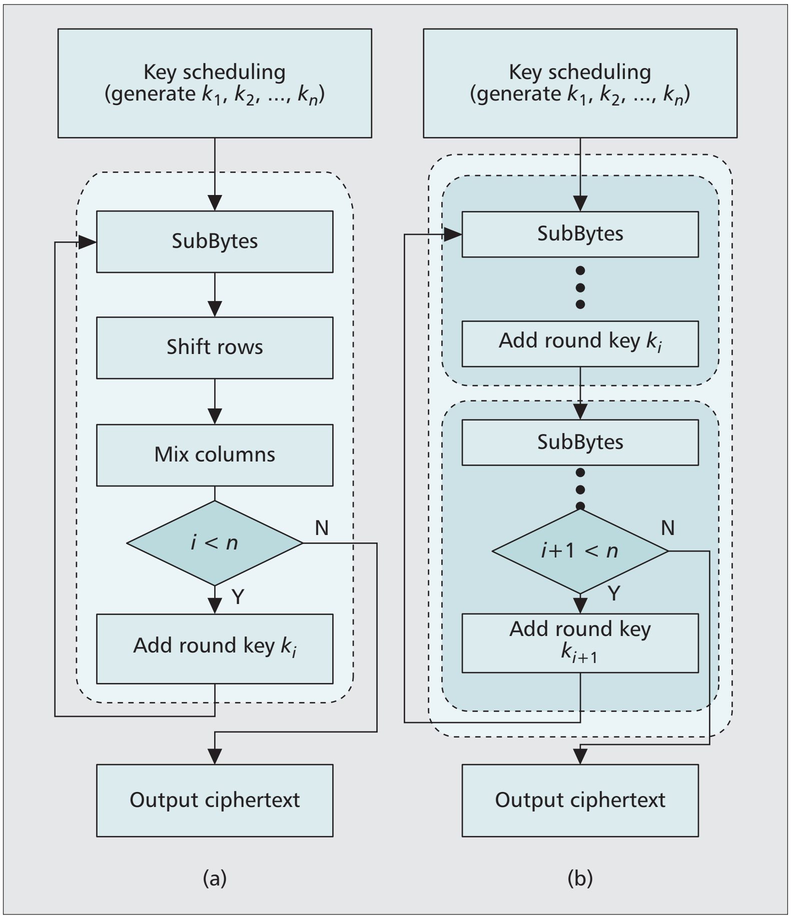

Figure 4. *a) one iteration of the AES encryption; b) an unrolling example for the iteration of AES.*

The Concerns for Energy-Efficient Implementation of the Security Algorithms

Based on the observations described in previous sections, in this section we propose the concerns for striking the balance between the security strength and the energy consumption for the energy constrained embedded systems, such as PMUs and SMs.

Concern 1: the tradeoff between security and energy. A tradeoff between the security strength and energy can be considered in implementation. Given the same security strength and time constraint, the concern on energy consumption is the key factor for encryption algorithm selection. Compared to other encryption algorithms, RC5 has significantly lower energy cost (see Fig. 3a and Fig. 3c) than DES and AES. Although RC5 has a lower security strength than AES, its low energy consumption makes it a desirable choice for the nodes that have very stringent energy budget.

Concern 2: potential energy saving lies in intra-iteration. For implementing a given algorithm, as suggested in the previous section, the computations in the loop can be substituted by look-up tables to reduce the computation energy. Furthermore, the loops can be unrolled to reduce the program jumps and branches. How-

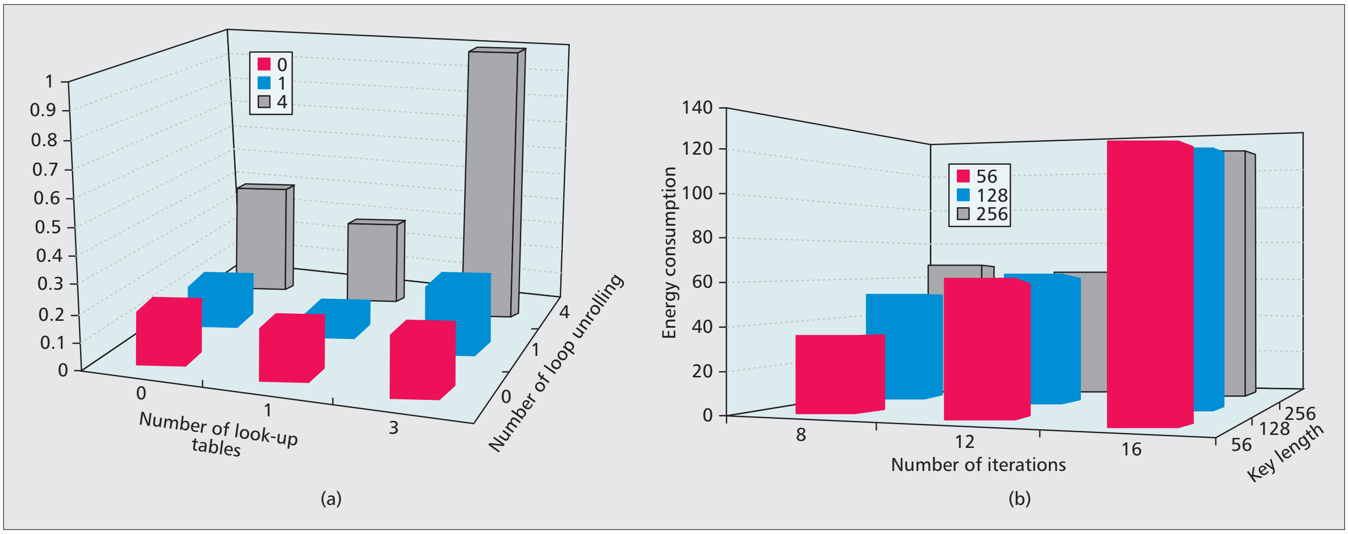

Figure 5. *a) The effect of the number of look-up tables and the number of loop-unrolling on the energy consumption of AES algorithm; b) the effect of the key length and the number of operation iterations on energy consumption for RC5 on CrossBow sensor.*

ever, the number of look-up tables and loop-unrolls should be carefully determined by experiments when designing.

Concern 3: the algorithm parameters. The energy consumption can be further reduced by carefully selecting the configuration of the encryption algorithms, such as operation modes, key lengths and the number of iterations. Based on the measurement results presented in the previous sections, we summarize the following principles for parameter selection:

- For the sensor with the tightest energy budget, ECB mode can be used to maximally save energy. For the sensors that have moderate tight energy budget, the other three operation modes can be used to enhance the security strength
- The number of iterations can cause large variation to the energy consumption, while the key length introduces less variation into the energy consumption. Therefore, the loss in security caused by less iterations can be compensated by increasing the key length.

Discussion

Note that we focus on implementing the cryptographic algorithms in an energy efficient way. We do not modify the nature of the cryptographic algorithms. The correctness and security strengths of the algorithms remain the same as they were implemented in the regular way with the same configurations. Our approach mainly serves two objectives:

- Exploring energy efficient implementation of the cryptographic algorithms for the wireless sensors in a WAMS
- Striking a tradeoff between the security strength and energy consumption for the wireless sensors in a WAMS

In an emergency situation, maintaining the functionality of the critical monitoring and control nodes is essential to the recovery of the smart grid. Our proposed method provides an optional design for such case.

As a matter of fact, the security risks in the smart grid are not completely defeated by the cryptographic algorithms introduced in this article. Because the smart grid relies on compound communication technologies, there could be potential cyber attacks ranging from wireless to wired network, from the remote to local adversaries and from the application layer to the physical layer of the network. Some known attacks include denial of service attack, sybil attack, node replication attack, and node capture attack, etc. The introduced cryptographic algorithms in this article are not panacea for the all these security problems for the smart grid. Although there have been various mechanisms for defeating these attacks, the energy consumption aspects of those mechanisms have not yet been examined. We believe that there is a huge exploring space in energy efficient implementation of those security mechanisms for the smart grid devices.

Conclusion

Smart grid is considered as one of the most promising technologies for solving the energy crisis in the near future. However, the cyber security issue is the enabler of such appreciable system. Because the remotely deployed sensors, such as PMUs and SMs, are mostly energy-constrained, cryptographic algorithms increase the energy consumption largely. The balance between the security and the energy consumption becomes critical for the functionality of the whole smart grid. It is challenging to ensure the security of the data transmission while keeping energy consumption low. In this article, we introduced measurement results of the energy consumption of the cryptographic algorithms, taking CrossBow and Ember sensors as examples. Based on the measurements, we proposed an array of novel energy reduction techniques to strike a tradeoff between the security strength and energy consumption. Finally, we summarized the principles for energy-efficient implementation of the cryptographic algorithms on energy-constrained platforms.

Acknowledgements

This work was supported in part by the University of Kentucky Start Up Fund; Korea-China S&T Joint Research Center NRF 2011-0019905 of MEST, Korean gov., and program NCET. NSFC 61170077, SZ-HK Innovation Circle proj. ZYB200907060012A, NSF GD:10351806001000000, S & T proj. of SZ JC200903120046A.

References

[1] B. Luitel and G. K. Venayagamoorthy, "Wide Area Monitoring in Power Systems Using Cellular Neural Networks," *Proc. IEEE Symp. Computational Intelligence Applications in Smart Grid (CIASG)*, Apr. 2011, pp. 1–8.

[2] J. Ma *et al.*, "Application of Phasor Measurement Unit on Locating Disturbance Source for Low-Frequency Oscillation," *IEEE Trans. Smart Grid*, vol. 1, no. 3, Dec. 2010, pp. 340–46.

[3] B. Luitel, G. Venayagamoorthy, and C. Johnson, "Enhanced Wide Area Monitoring System," *Innovative Smart Grid Technologies (ISGT)*, Jan. 2010, pp. 1–7.

[4] G. Bauer, K. Stockinger, and P. Lukowicz, "Recognizing the Use-Mode of Kitchen Appliances from Their Current Consumption," *Proc. EuroSSC*, 2009, pp. 163–76.

[5] M. Qiu *et al.*, "Energy-Efficient Security Algorithm for Power Gride Wide Area Monitoring System," *IEEE Trans. Smart Grid*, vol. 2, no. 4, Nov. 2011, pp. 715–23.

[6] M. Qiu *et al.*, "Dynamic and Leakage Energy Minimization with Soft Real-Time Loop Scheduling and Voltage Assignment," *IEEE Trans. Very Large Scale Integration Systems (TVLSI)*, vol. 18, no. 3, Mar. 2010, pp. 501–04.

[7] M. Qiu and E. H.-M. Sha, "Cost Minimization while Satisfying Hard/Soft Timing Constraints for Heterogeneous Embedded Systems," *ACM Trans. Design Automation of Electronic Systems (TODAES)*, vol. 14, no. 2, Article 25, Apr. 2009 (ACM TODAES 2011 Best Paper Award), pp. 1–30.

[8] A. Wander *et al.*, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," *PerCom*, 2005, pp. 324–28.

[9] F. Amin, A. H. Jahangir, and H. Rasifard, "Analysis of Public-Key Cryptography for Wireless Sensor Networks Security," *Proc. World Academy of Science, Engineering and Tech.*, 2008.

[10] G. de Meulenaer *et al.*, "On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks," *IEEE Int'l. Conf. Wireless and Mobile Computing, Networking and Commun.*, Oct. 2008, pp. 580–85.

Biographies

Meikang Qiu [SM'07] (mqiu@engr.uky.edu) received B.E. and M.E. degrees from Shanghai Jiao Tong University, China. He received M.S. and Ph.D. degrees in computer science from the University of Texas at Dallas in 2003 and 2007, respectively. He has worked at the Chinese Helicopter R&D Institute and IBM. Currently, he is an assistant professor of electrical and computer engineering and director of hardware/software codesign lab at the University of Kentucky. He is also a guest full professor at the School of Computer Science and Technology, Huazhong University of Science and Technology. He has published 140 papers, including 15 IEEE/ACM Transactions papers. He is the recipient of the *ACM Transactions on Design Automation of Electronic Systems* 2011 Best Paper Award. He also received three other best paper awards (IEEE EUC '09, IEEE/ACM GreenCom '10, and IEEE CSE '10) and one best paper nomination. He also holds two patents and has published three books. He has been an editor for several journals and chair for many international conferences. He served as Program Chair of IEEE EmbeddCom'09 and EM-Com '09. His research interests include embedded systems, computer security, and wireless sensor networks. His research has been supported by NSF, Air Force, and Navy of the USA.

Hai Su (hsu@engr.uky.edu) received B.E. and M.E. degrees from the University of Electronic Science and Technology of China in 2003 and 2006, respectively. He is now pursuing his Ph.D. degree in the Department of Electrical and Computer Engineering, University of Kentucky. His research interests include software/hardware co-design for embedded systems and wireless sensor networks.

Min Chen [SM] (minchen@ieee.org) is an assistant professor in the School of Computer Science and Engineering at Seoul National University (SNU). He received a Ph.D. in electrical engineering from South China University of Technology in 2004. He worked as a postdoctoral fellow in the Department of Electrical and Computer Engineering at UBC for three years since March 2009. Before joining UBC, he was a postdoctoral fellow at SNU for one and a half years. He has published more than 120 technical papers. He received the Best Paper Runner-Up Award from QShine 2008. He serves as Editor or Associate Editor for several journals. He was a TPC co-chair for several conferences.

Zhong Ming (mingz@szu.edu.cn) is a professor at the College of Computer and Software Engineering of Shenzhen University. He is a member of a council and senior member of the China Computer Federation. His major research interests are software engineering and embedded systems. He led two projects of theNational Natural Science Foundation, and two projects of the Natural Science Foundation of Guangdong Province, China.

Laurence T. Yang (ltyang@gmail.com) received his B.E in computer science from Tsinghua University, China, and Ph.D. in computer science from the University of Victoria, Canada. He is a professor in computer science and the director of the Parallel and Distributed Computing Laboratory, and Embedded and Ubiquitous Computing Laboratory at St Francis Xavier University, Canada. His research interests include parallel and distributed computing, and embedded and ubiquitous/pervasive computing. His research has been supported by NSERC and CFI of Canada.

The balance between security and energy consumption becomes critical for the functionality of the whole smart grid. It is challenging to ensure the security of data transmission while keeping energy consumption low.