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

Meikang Qiu*, Hai Su, Min Chen, Zhong Ming, Laurence T. Yang

ABSTRACT

An efficient and dependable smart power grid relies on the secure and reliable real-time data collection and transmission service provided by a monitoring system. The key components of the system are some measuring units, such as Phasor Measurement Units (PMU) and smart meters (SM). These measuring equipments function as sensors of the smart grid. And the 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 burden to the sensor nodes. Since the PMUs and SMs are mostly energy-constrained, the problem of how to ensure the communication security with minimum energy cost becomes a critical issue for the functionality of the whole smart grid. In this paper, 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 for reconciling the two conflicting system requirements—communication security and low energy consumptions. The introduced methods are general ones and applicable to other energy-constrained yet security sensitive systems.

Index Terms

Smart Grid, Security, Cryptographic algorithm, PMU, Low energy consumption.

1 ABSTRACT

An efficient and dependable smart power grid relies on the secure and reliable real-time data collection and transmission service provided by a monitoring system. The key components of the system are some measuring units, such as Phasor Measurement Units (PMU) and smart meters (SM). These measuring equipments function as sensors of the smart grid. And the 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 burden to the sensor nodes. Since the PMUs and SMs are mostly energy-constrained, the problem of how to ensure the communication security with minimum energy cost becomes a critical issue for the functionality of the whole smart grid. In this paper, 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 for reconciling the two conflicting system requirements—communication security and low energy consumptions. The introduced methods are general ones and applicable to other energy-constrained yet security sensitive systems.

Index Terms

Smart Grid, Security, Cryptographic algorithm, PMU, Low energy consumption.
2 INTRODUCTION

The ever increasing global population imposes demanding requirement on the power supply. While the fragile environment condition and the sustainability of cities put contradicting constraints on the increase of power generation from traditional environment-hostile power plants [1]. Viable measurements for supporting the continuously increasing global economy is to extend the current power grids to smart grids. The smart grid can reconcile the contradiction by two strategies. One is to improve the efficiency of the current power grid through smartly managing the use and supply of electricity. The other is to incorporate the renewable energy resources, like solar, tide or wind sources, into the whole power grid. The green energy can lower the energy price and reduce greenhouse gas emission.

The first strategy calls for intelligent management of the use and the supply of the power, which requires the state information from the customers, power distribution and transmission infrastructures. These information can facilitate the grid operator to adjust their power production and distribution dynamically in real time to avoid energy wasting and system outage. It is believed that the Chile blackout in March 2010, that 90% of the population of the country, would have been less impactive if such an intelligent system was in place.

From the customer’s point of view, the system can also facilitate money saving for the customers by intelligently scheduling power use and choosing the power supplier. The billing rate of the electricity has been dynamically changing hourly for each day. The smart grid technology enables the customer to optimally schedule the usage of electricity to reduce cost. With a power grid that includes low cost renewable energy sources as parts of it, the customers can enjoy even cheaper energy when enough energy can be obtained from the renewable energy sources. And even some households can harvest energy and sell it into the power grid. When the flexibility in the power supplier selection is achieved, the consumers are liberated to choose the sellers based on the real-time price information with finer temporal granularity. Some consumers may shift their power use from the peak hours which can reduce the power demand and power price at the peak hours. From the perspective of the power suppliers, they can dynamically tune the power price and power generation to gain more interest. In this way, the interaction between the consumers and the supplier can achieve a more efficient energy generation and consumption.

Connecting the renewable power plant to the power grid can contribute to the power supply at peak hours. The green energies are generated from sunlight, wind farm or tides or geothermal heat. The amount of the available energy usually change fast from hour to hour and day to day. And the location of the renewable power plants are usually highly distributed. Since the electricity storage capacity of the current technologies is very limited compared to the amount of the energy generated from the renewable sources in natural force surges. The challenge is how to smoothly exploit the fluctuating nature of these renewable energy sources. The smart grid provides real-time response to absorb and make use of the energy surge to reduce the cost of the traditional energy generation.

The smart grid is featured by high efficiency, stability and robustness. All these appreciable properties are achieved by integrating the communication technologies, automated control and optimization into the system management. An essential fundamental part of such informatized system is a Wide Area Monitoring system (WAMS) based on a comprehensive communication network [2] that includes sensor network, WiFi, satellite communication, cellular network and Internet, etc. The communication network
is responsible for information collection, transmission and system control. Unlike the traditional power grid, the ubiquitous communication network extends the system monitoring and control to the end-user level. For example, the General Electric’s (GE) 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 PMU and SM. The PMU was first invented at Virginia Tech. And nowadays they are deployed distributedly over the power grid. They receive the common time reference from the GPS satellite. 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 [3]. Nowadays, as an important part of smart grids, the PMUs are usually equipped with wireless communication components that enable remote data report and control. The smart meters 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 the potential cyber attacks from Internet. Any misleading information or stale information can cause catastrophic consequences to the system, and thus to the customers [4]. For example, if the phasor information is modified in its transmission, the wrong assessment can cause wrong management operations. Malicious analysis against the smart meter data could reveal the living schedule of the householders or production activities of a plant [5]. Even worse, due to the interconnection of the system, terrorists could collect 80% of the sensitive information that can be used to plot attacks on the whole smart grid [6]. Thus, communication security (i.e., integrity, authenticity, availability and confidentiality) over the whole system has to be enforced by some information security protocols.

Because the transmission platforms are usually energy-constraint systems, the computation overhead introduced by the security protocols can harm the lifetime of the system. Thus, exploring how to implement those security algorithms with lower energy consumption while maintaining their security strength arises as a desirable practice.

Different implementation of the security algorithms can incur distinct energy consumption levels. The security algorithms can be implemented either by dedicated hardware chips or by softwares. The 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 operation of the analog chips. The static power consumption are proportional to the active time of the device. Usually the dynamic power consumption account for the major part of the total power consumption [7]. When the security algorithms are implemented by dedicated chips, the dynamic power consumption on CPU is not increased significantly, but the dedicated chip consumes more energy. Compared to the hardware implementation, the software implementation executes the algorithms on CPU, the total increased power is less than that of the hardware implementation. And according to the works in [8], the more complex the software is the larger optimization space for power saving can be expected. In this paper 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 security systems. The computational complexity of these algorithms is the major factor that
increases the energy overhead of the sensors. And the computational complexity is determined by the implementation method and selection of parameters of the algorithms, such as the key length, number of iterations and operation mode. The energy consumption of the algorithm execution is positively correlated to the computation complexity. Thus, we can manipulate the parameters of the security algorithms to strike a balance between required security level and energy consumption. 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: 1) lower the total energy cost at the system level and 2) prolong 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 security algorithms implemented on CrossBow and Ember sensor platforms that are most common sensor platforms; then we present a bunch of code optimization methods for increasing the energy efficiency of the instances of the security algorithms; lastly, we suggest a set of principles for security algorithm implementation with energy concern.

The rest of this paper is organized as follows: a brief survey of the related works are summarized in section 2. In section 3 some preliminaries of the monitoring system security and energy issues are introduced. In section 4 we present our measurement results of the energy consumption of several widely used security 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 security algorithms.

3 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 multi-hop Ad Hoc network, WiFi, satellite communication, cellular network and Internet. The sensor nodes are deployed over the power grid and can monitor the function of the power grid. The data management center communicates with the sensors and the control centers through the network. It serves to analyze the information of the power grid and make 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 data analysis and response, and real-time control and protection can be achieved.

In an smart grid, the data collection are performed by the measuring nodes. And those measuring nodes are usually combined with embedded systems to perform data processing and two-communications. Due to the vast amount of deployment, each node is relatively cheap. Thus, they have very limited on-board resources. For example, they usually have one simple low speed Micro Control Unit (MCU) as its CPU, and very limited memory space, and very tight power budget due to their deploying area, cost and physical size. Therefore, only some basic tasks, like simple computation and communication, can be implemented on the nodes.
Fig. 1: The smart grid with wide area monitoring system (WAMS).

4 SECURITY RISKS

4.1 Vulnerabilities of the Smart Grid

Basically, most of the smart grid sensors are deployed in the wild. And a large portion of data transmissions are fulfilled through wireless communication which relies on the open media (i.e., wireless channels). The adversaries can easily physically destroy or replicate the nodes by capturing them. The attackers can also launch attacks by setting up some hacker equipments. We summarize the potential attacks against the smart grid in table 1.

<table>
<thead>
<tr>
<th>security consequences</th>
<th>Attack method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of confidentiality</td>
<td>(i) eavesdropping and analyzing the wireless transmission; (ii) node capturing and replication.</td>
</tr>
<tr>
<td>Loss of authenticity</td>
<td>(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.</td>
</tr>
<tr>
<td>Loss of integrity</td>
<td>message modification</td>
</tr>
<tr>
<td>Loss of availability</td>
<td>(i) message blocking by collaboration of the malicious nodes, wireless channel jamming; (ii) fake data request to the sensors that cause unnecessary energy consumption.</td>
</tr>
</tbody>
</table>

TABLE 1: Potential attacks against smart grid.

4.2 Energy Consumption of the Security Algorithms

In the information security literature, there has been a bunch 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, and the integrity can be ensured by the Message Authentication Codes (MAC), and the availability can be
preserved by introducing redundancy and randomness into the data transmission, like Secure Message Transmission (SMT) [9] and uncoordinated frequency hopping [10]. However, to provide protections over all the aspects of the security risks is prohibitively energy consuming for the cheap sensor nodes. Thus, we classify the security of the nodes into four levels: Level 0, non-security service; Level 1, single security service; Level 2, double security services, and Level 3, triple security services.

Those different levels of security have various corresponding energy consumptions for the nodes. The energy consumption of the node can be partitioned into two parts: 1) the background energy consumption due to the ordinary functions of the applications; 2) 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 periphery circuit, 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 security algorithms. Fig. 2 shows the statistics of the power consumption of the sensor node with different security configurations. 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 taken. And the increment of power consumption mainly comes from the increased power cost of CPU and RF module. This is because the CPU performs the arithmetic calculations of the security 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. And increasing the data transmission speed can help to reduce the energy consumption.

5 ENERGY CONSUMPTION MEASUREMENTS

In this section, we present the measurement results of the energy consumption of the security 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 CPU, we only present the energy consumption profile of the CPU and the whole platform. Since the energy consumption varies for the lengths of the messages as well as the different security algorithms, we first measured the energy...
consumption of the CPU and the platform with respect to the different message lengths. We plot the results in Fig. 3 as baseline for later comparisons. Because the two platforms use the same processor for the same application configuration the energy consumptions of the CPUs 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 the 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 the Ember platform is far less than that of the CrossBow platform because of its higher data rate, thus shorter transmission interval.

5.1 Energy Consumption of Security Algorithm on CrossBow Sensor

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

5.2 Energy Consumption of Security Algorithms on Ember Sensor

Similar to the measurement of the energy consumption with security enforced on CrossBow, we present the measurement results of the Ember sensor in Fig. 3 (c) and (d). Compared to the level 0 base line, the energy for security consumed by CPU is increased by from 2 to 9 times.

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

6 ENERGY OPTIMIZATION FOR ENCRYPTION ALGORITHMS

6.1 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 operations which are SubByte, ShiftRow, MixColumns and AddRoundKey as shown in the dash line in Fig. 4 (a). The main body consumes major portion of the security energy. The functions of these subroutines are just mapping the input to an output, which can be implemented by pre-defined look-up tables. This technique 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 the operations in one iteration. Doing so can reduce the time for jumps and branches. For instance, a one-time loop unrolling is shown in Fig. 4 (b). 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. 5 (a). 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 i) without look-up table, the loop unfolding alone makes no significant difference in energy consumption; ii) With the subroutine SubByte being implemented by look-up table, the energy cost for 0 and 1 loop unrolling are reduced by 41.5%. This is because the look-up table saves CPU 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 look-
up tables and loop-unrollings do not ensure energy reduction. Therefore, there exists a tradeoff between the CPU computation saving and the increase of memory access. The lowest energy consumption comes with the combination of the one look-up table and one-time loop unrolling.

Fig. 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.
6.2 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 ECB, CBC, CFB and OFB. Among those operation modes, the ECB is the simplest one and consumes the least energy, and the OFB consumes the most. Due to the limited space, we omit the measurement results here.

We experimented the RC5 on CrossBow sensor with different key lengths and number of iterations. The results are shown in Fig. 5 (b). It can be seen that the number of iteration affects the energy consumption a lot. And the energy consumption variation due to the change in key size becomes ignorable as the increase of the number of iteration. 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. The must be a balance between the security and energy saving.

7 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.

Concern 1: the tradeoff between security and energy. A tradeoff between the security strength and energy and time for processing 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. 3 (a) and (c)) 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 section 6, the computations in the loop can be substituted by look-up tables to reduce the computation energy. And the loops can be unrolled to reduce the program jumps and branches. However, 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 model, key length and the number of iterations. Based on the measurement result presented in last section, we summarize the following principles for parameter selection: i) 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; ii) 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.
8 DISCUSSION

As a matter of fact the security risks in the smart grid are not completely defeated by the security 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 security 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 huge exploring space in energy efficient implementation of those security mechanisms for the smart grid devices.

9 CONCLUSION

Smart grid is considered as the most promising technology for solving the energy crisis in the near future. However, the cyber security issue is the enabler of such appreciable system. And the remotely deployed sensors are mostly energy-constrained. Security algorithms increase the energy consumption largely. 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 the data transmission while keeping energy consumption low. In this article, we introduced measurement results of the energy consumption of the security algorithms when implemented on CrossBow and Ember sensors. Based on the measurements, we proposed an array of novel energy reduction techniques to strike a balance between the security strength and energy consumption. And finally, we summarized the principles for energy-efficient implementation of the security algorithms on energy-constrained platforms.

ACKNOWLEDGEMENTS

This work was supported in part by the NSFC 61071061, the University of Kentucky Start Up Fund; SZ-HK Innovation Circle proj. ZYB200907060012A, NSF GD:10351806001000000, S&T proj. of SZ JC200903120046A;

REFERENCES


