Nodal Level Adaptive Security for IOT-Enabled Sensors through Dynamic Reconfigurable Encryption

R. Nithya Paranthaman, D. Dhanasekaran

Abstract: IOT-enabled sensors have been deployed in the wide area to perform various applications. Information security is an important aspect in wireless sensor networks. Since the attackers can be able to hack the information even at the node level, improved security mechanism have to be implemented. In this paper, nodal level security is done through dynamic encryption technique. The advantage of dynamic encryption is achieved by adaptive security. The proposed method involves a system-on-chip (SoC) design to provide a dynamically reconfigurable encryption methodology which leads to improved security level and also the energy efficiency. Dynamic encryption creates the confusion among the hackers about the tracking of security keys. The results shows that by dynamically selecting the encryption module through soft-core processor based on the available power budget, an energy efficient security solution is obtained for sensor nodes with reduced resources utilization.

Keywords:AES, DES, Dynamic Encryption, IoT, Sensors, SoC, Soft-core Processor.

I. INTRODUCTION

A sensor node consists of different computational components to perform the task of sensing, processing and transmitting data. The sensor nodes are constrained to energy, processing capability and memory and also there may be a possibility of malicious attacks in the environment. Security is a major concern in IOT. Security may be provided either at the network level or at the sensor node level. Nodal level security is possible through cryptography. Various encryption algorithms will provide different strengths of security. But always there occurs a tradeoff between the lifetime and security of a sensor node. In order to provide high level security, more energy consumption will be needed which in turn reduces the lifetime of the sensor node.

So, the sensor node is made to be dynamically reconfigurable to provide different levels of security based on the available power budget.

Aditi Rani, 2017 et al given a survey on security in wireless sensor networks which clearly illustrate the hierarchy of security. Security aspects at the network level are resolved by key management and secure routing protocols whereas the security at the node level is resolved only through cryptography and authentication mechanism [1]. Antonio Vincenzo Taddeo, 2010 et al deals with the method for security self-adaptation which allows the devices to adapt the desired security technique gradually which satisfies the available power constraints and also achieves the maximum level of security. [2]

Jahnavi Kulkarni, 2017 et al uses the cryptographic units for providing security on-chip in wireless sensor networks. Flexibility is obtained by controlling the security factors in a system on-chip design[3]. Another advantage of on-chip design is the reduced deployment time. Sensor nodes of the upcoming generation have the capability of reconfigure themselves dynamically which is proposed in Ref. [4] by S.Charoenpanyasak, 2011 et al.

D.Oliveira, 2018 et al proposed a architecture for IOT device security which comprises of scavenging techniques for powering the cryptographic units [5]. Khalad khatib, 2018 et al provides a different encryption algorithms in which any one of them can be chosen based on the maximum available power [6]. Partial reconfiguration technique achieves minimal power and area for swapping between different algorithms.

II. CONCEPT OF ADAPTIVE SECURITY

This is needed for a more optimized sensor node to dynamically select the encryption algorithm. For adaptive security, various approaches have been employed earlier. All adaptive mechanisms employed are subjected to the constraints which may limit the performance of the system. A sensor node consists of a processing unit, memory and radiofrequency module for transmission and reception. Along with the existing structure, externally the reconfigurable module can be connected for achieving adaptive security.DPR allows the switching of modules during runtime without disturbing the other modules in the sensor node. The dynamic part contains a set of reconfigurable partitions. Power adaptive encryption solution is to be provided.

Revised Manuscript Received on August 30, 2019.

* Correspondence Author

R. Nithya Paranthaman*, Department of ECE,Saveetha School of Engineering, Saveetha university, Saveetha Nagar, Thandalam,Chennai, TamilNadu, India.Email:nithyar.sse@saveetha.com

Dr. D.Dhanasekaran, Principal, Department of ECE, Saveetha School of Engineering, Saveetha university, Saveetha Nagar, Thandalam,Chennai, TamilNadu, India. Email:principal.sse@saveetha.com

Retrieval Number F8738088619/2019©BEIESP
DOI: 10.35940/ijeat.F8738.088619

The choice is based on the amount of energy spent for each operation. Various choices may be the blocks created using FPGA for different encryption algorithms are AES-256, AES-192,AES-128,DES and ECC.

III. PROPOSED METHOD OF SOC DESIGN FOR SENSOR NODE SECURITY

Based on the security level needed and also on the available power budget, the encryption algorithm can be selected at runtime. Each of the encryption algorithms is structured as a separate module in the system-on-chip design. The control of which module to be selected is provided by the soft-core processor. Power required by each module can be estimated individually through execution. For implementation purpose, two modules are created to show the dynamic selection of encryption. One module provides AES-128 encryption algorithm whereas the other module provides DES algorithm since it is a dynamic approach, it is very difficult for the hackers to crack the keys of the algorithm. Because, it will be very hard to guess which algorithm is currently executing to provide data security.

A. DES Encryption Module

Data Encryption Standard (DES) is one of the methods of performing symmetric key encryption. It will handle the input data in blocks. So, the 64-bit block of plaintext is provided as the input to the encryption algorithm. The length of the key is 56-bits. The first step in DES involves permutation of the 64-bit plain text. This can be done through swapping function. After initial permutation, the block is splitted into two 32-bit sub blocks. The 32-bit right side sub block involved in 16 rounds of similar function with different sub keys. After 16th round, the inverse operation of permutation is done which completes the encryption process. The output of the process is the 64-bit cipher text.The RTL view of the DES module is shown in Fig. 1.

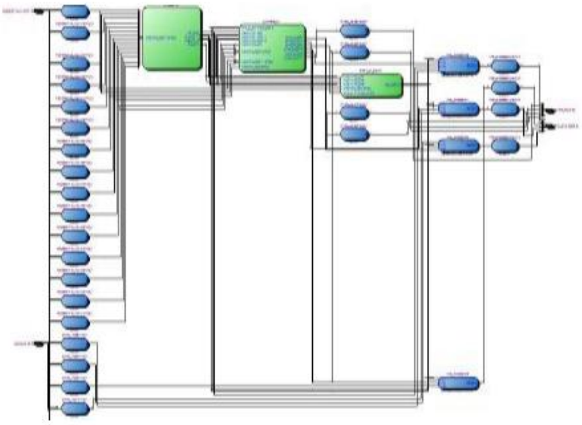


Fig.1. RTL view of DES encryption Module

B. AES Encryption Module

Advanced encryption standard (AES) is the symmetric block cipher with a block length of 128- bits. AES allows for three different key lengths: 128,192 (or) 256 bits. Here, AES with a key length of 128 bits is implemented. The number of rounds involved depends on the length of the key. Initially the input plain text is converted into an array format. Next, the substitution process is done through different substitution tables. Then the shifting of rows and mixing columns need to be done. The shifting of rows can be performed using shift operator whereas the mixing of columns is a complex process which is achieved through Galois Field multiplication. This step requires two different tables called L table and E table. Finally each of the columns is XORed with different sub keys. The RTL view of created AES-128 module is shown in Fig.2.

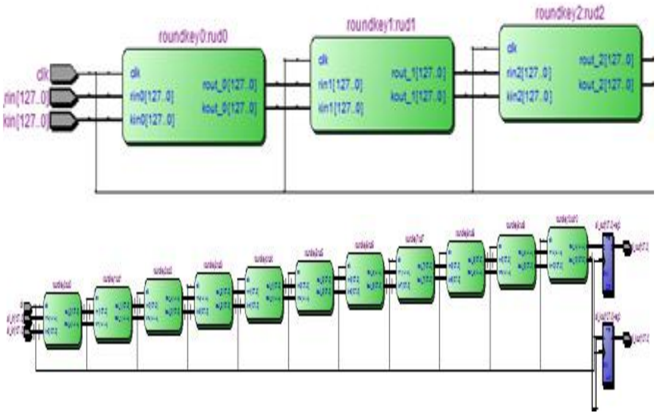
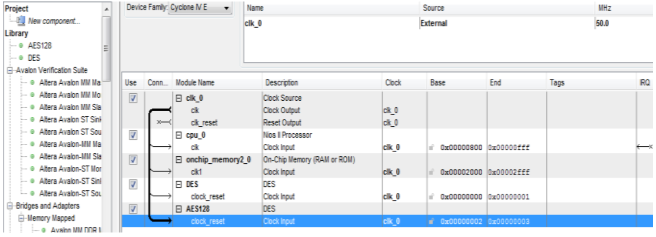


Fig.2 RTL view of AES-128 Module

C. System-on-Chip design

The encryption modules after synthesis are included as a custom component in the library. Once the module is created, it can be instantiated number of times in the system design. Each encryption module has its own address space to perform the computation. The external clock interface and on-chip memory are also included in the design. The controller is also included as a component for dynamic switching of encryption technique. The controller, here is the NIOS-II processor which is the soft-core processor from Altera. The instruction to the encryption unit is provided by NIOS-II processor using the address which is created in the design. The entire Soc design with all included components is illustrated in Fig. 3.



Device Family: Cyclone IV E

Name	Source	MHz
clk_0	External	50.0

Use	Conn...	Module Name	Description	Clock	Base	End	Tags	IRQ
☑		⊟ clk_0	Clock Source					
		clk	Clock Output	clk_0				
		clk_reset	Reset Output	clk_0				
☑		⊟ cpu_0	Nios II Processor					
		clk	Clock Input	clk_0	0x00000800	0x00000fff		
☑		⊟ onchip_memory2_0	On-Chip Memory (RAM or ROM)					
		clk1	Clock Input	clk_0	0x00002000	0x00002fff		
☑		⊟ DES	DES					
		clock_reset	Clock Input	clk_0	0x00000000	0x00000001		
☑		⊟ AES128	DES					
		clock_reset	Clock Input	clk_0	0x00000002	0x00000003		

Fig.3. System on Chip design for dynamic encryption

D. Implementation of Dynamic encryption

The sensor node available power budget is estimated at every data transmission. Information security is provided based on the available power budget. The power consumption of the different encryption modules is estimated already through power play power analyzer tool. The threshold level is fixed for the selection of encryption modules. Here two different encryption modules like DES and AES-128 with their value of power consumption is obtained. Now the selection of any one of the module is done through the Nios-II processor based on the threshold.

The DES encryption module consumes the power of 57.70 mw whereas the AES-128 encryption module consumes 141.75 mw of power. So, the threshold is fixed as 100 mw. If the power estimated before data transmission shows the available power lesser than the threshold, then DES module is selected for encryption by the NIOS-II processor. If the available power is greater than the threshold, then AES-128 module is selected. The flowchart for the dynamic selection of encryption algorithm is specified below in Fig.4.

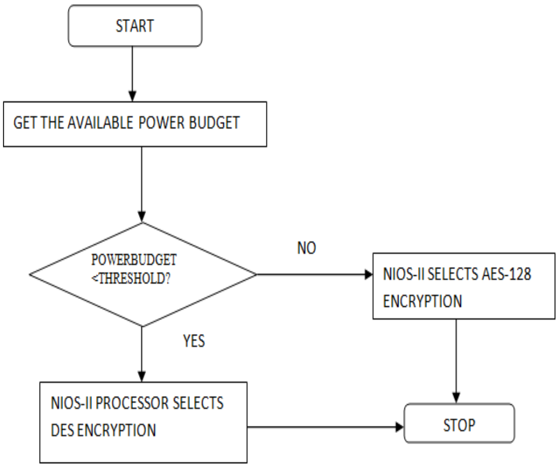

START
GET THE AVAILABLE POWER BUDGET
POWERBUDGET <THRESHOLD?
NO
NIOS-II SELECTS AES-128 ENCRYPTION
YES
NIOS-II PROCESSOR SELECTS DES ENCRYPTION
STOP

Fig.4. Flowchart for Dynamic Encryption technique

IV. ANALYSIS OF DYNAMICENCRYPTION

Dynamic encryption was analyzed with the following parameters: Estimated Logic Elements, Average Fan-out and Power dissipation. Comparative analysis is done with DES and AES-128 modules which are listed out in Table. I.

Table - I: Comparative analysis of encryption modules

Parameters	**DES**	**AES-128**
Estimated Logic Elements	10000	91,816
Average Fan-out	1.52	3.09
Power Dissipation	57.70 mw	141.75 mw

Fig.5 shows the usage of logic elements of the encryption modules. Fig.6 shows the reduction in average fan-out for DES module compared to AES. Fig.7 illustrates the power dissipation in the encryption modules. The results show that by switching from AES-128 to DES module, the overall resources utilization gets reduced. Power consumption of the sensor node for providing information security also gets reduced which in turn increases the lifetime of the sensor node. Another advantage of performing dynamic encryption is the resistance against hacking. Since the encryption technique is varied for each data transmission, it is very hard to hack the secret keys of encryption in the sensor node

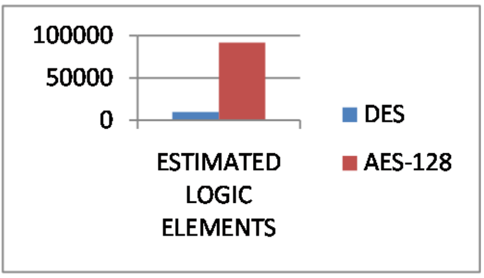


Fig.5. Estimated Logic Elements

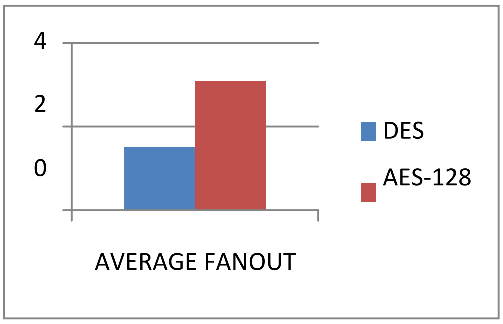


Fig.6. Average Fan-out

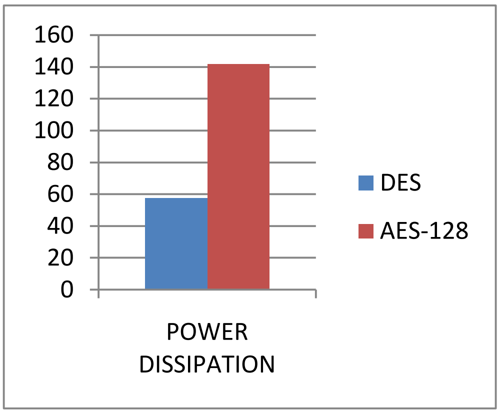


Fig.7. Power dissipation of encryption module

IV. RESULTS AND DISCUSSION

From the analysis of reconfiguration, it is clear that reconfigurable encryption leads to reduced power consumption. Thus, this technique provides a power efficient solution for a sensor node. This method also achieves different security levels which causes confusion among the hackers for generating the public key. Cost analysis is also an important parameter to be considered. The design of IoT-enabled sensor node with reconfigurable encryption needs a single programmable SoC board which cost around $249. It seems to be less expensive but providing a very high level of data confidentiality. So, by considering all parameters such as power, cost and resource utilization ,it is concluded that the dynamic reconfigurable encryption is the optimal method for providing node level adaptive security.

V. FUTURESCOPE

The above method we discussed in the paper is suitable for providing node security. Suppose the sensor node transfer the data over the cloud, the node must share the public key to the cloud management system which further creates the possibility of hacking. So, whenever there occurs a data transfer over cloud, the processor has to select the encryption module which satisfies the data confidentiality even in the cloud. Such a encryptive module have to be developed which is considered as a future work of this paper.

REFERENCES

1. Aditi Rani and Sanjeet Kumar, "A Survey of security in wireless sensor networks", IEEE-CICT, 2017
2. Antonio Vincenzo Taddeo, Laura Micconi and Alberto Ferrante, " Gradual adaptation of security for sensor networks", IEEE-2010
3. Jahnavi Kulkarni, Karan Nair, Aditya Pappu, Sarthak Gadre, Ganesh Gore and Jonathan Joshi, "Using On-chip cryptographic units forsecurity in wireless sensor networks",Mumbai,India,IEEE-2017
4. S.Charoenpanyasak and W.Suntiamorntut, "The Next Generation of Sensor Node in Wireless Sensor Networks", Journal of telecommunications, volume 9, issue 2, july 2011
5. D.Oliveira, T.Gomes and S.Pinto, "Towards a Green and Secure Architecture for Reconfigurable IoT End-Devices", 9th ACM/IEEE International Conference on Cyber-Physical Systems, 2018
6. Khaled Khatib, Mostafa Ahmed, Ahmed Kamaleldin, Mohamed Abdelghany and Hassan Mostafa, "Dynamically Reconfigurable Power Efficient Security for Internet of Things Devices", 7th International Conference on Modern Circuits and Systems Technologies ,2018
7. NIOS-II Processor reference handbook, ALTERA Corporation, 2011.
8. NIOS-II Software developer's handbook, ALTERA Corporation, 2011.
9. B.Murali krishna, G.L.Madhumati and Habibulla Khan," dynamically evolvable hardware- software co-design based crypto system through partial reconfiguration", **Journal of Theoretical and Applied Information Technology,**31st May 2017
10. Miguel L. Silva and Joao Canas Ferreira, "Support for partial run-time reconfiguration of platform FPGAs", Journal of Systems Architecture, Volume 52,Issue 12,December 2006.
11. Katherine Compton and Scott Hauck ,"Reconfigurable computing: A survey of systems and software", *ACM computing surveys*,vol.34,No.2,pp.171-210,June 2002.
12. J.Burns, A,Doulin, J.Hogg, S.Singh and M.dewit, "A Dynamic reconfiguration run-time system", Field-programmable custom computing machines, *5th IEEE Annual Symposium*, April 1997.
13. Altera white paper,"FPGA Run-time Reconfiguration : Two approaches",2008.
14. Zain-ul-Abdin, Bertil Svensson, "Evolution in architectures and programming methodologies of course-grained reconfigurable computing", *International Journal of Microprocessors and Microsystems* 33,pp 161 – 178,2009.
15. J.G.Tong, I.D.L.Anderson and M.A.S.Khalid, "Soft-core processors for Embedded Systems", *International conference on microelectronics*, pp.170-173,dec 2006.

AUTHORS PROFILE

R.Nithya Paranthaman had completed her ME in the specialization of VLSI DESIGN with distinction in the year 2014. She got 14th Rank in Anna university during her postgraduate programme. Now she is currently doing her Phd in Saveetha University. She has 4 years of teaching experience.she is working as a Assistant Professor of ECE Department in Saveetha School of Engineering. Her areas of research includes Dynamic reconfiguration and IoT. She published an ieee conference paper related to dynamic reconfiguration in 2014.Recently she published an article related to dynamic encryption of sensor node in E-magazine of National Cyber safety and security standard.

Dr.D.Dhanasekaran received his PhD degree with the specialization of VLSI reconfigurable circuits. He had 29 years of teaching experience. He is working as a Principal in Saveetha school of Engineering. She published 50 Scopus indexed papers and two patents. His area of research includes VLSI circuits and IoT.