RC5 ALGORITHM: POTENTIAL CIPHER SOLUTION FOR SECURITY IN WIRELESS BODY SENSOR NETWORKS (WBSN)

Dhanashri H. Gawali[1] and Vijay M. Wadhai[2]

[1]Department of E&TC, Maharashtra Academy of Engineering, Alandi(D), Pune, India
Dhanashree.gawali@gmail.com
[2]MAEER's MIT College of Engineering, Pune, India
wadhai.vijay@gmail.com

ABSTRACT

The patient-related data stored in the WBSN plays an important role in medical diagnosis and treatment; hence it is essential to ensure the security of these data. Access to patient-related data must be strictly limited only to authorized users; otherwise, the patient's privacy could be abused. There has been very little study done in encryption algorithms suitable for WBSN. In this paper we focus on RC5 encryption algorithm as a potential cipher solution for providing data protection in WBSN. RC5 can be considered as one of the best ciphers in terms of overall performance, when used in nodes with limited memory and processing capabilities. In WBSN the size of data varies for different medical (health parameters such as ECG, EEG, Blood pressure, Blood Sugar etc) or nonmedical (video, audio etc) applications. RC5 is a highly efficient and flexible cryptographic algorithm, for which many parameters (key size, block size, number of rounds) can be adjusted to tradeoff security strength with power consumption and computational overhead. Thus RC5 with suitable parameters may perform well for WBSN applications with different data size. Implementations for WBSN nodes are in evolving stage now. This paper further presents a brief survey of various implementations of RC5 algorithm to convince its suitability for WBSN.

KEYWORDS

RC5 Algorithm, WBSN, WBAN, Network security, encryption,

1. INTRODUCTION

Wireless Body Sensor Networks (WBSNs) comprised of physically small-sized sensor nodes exchanging mainly human body vital information with each other. WBSN enables collection of a patient's vital body parameters and movements by small wearable or implantable sensors and communicate this data using short-range wireless communication techniques. The wearable medical devices includes Temperature measurement, Respiration monitor, Heart rate monitor, Pulse oximeter SpO2, Blood pressure monitor, pH monitor, Glucose sensor etc. The implantable medical devices are those that are inserted inside human body. These devices include Cardiac arrhythmia monitor/recorder, Brain liquid pressure sensor, Glucose sensor, Endoscope capsule etc [proposed MAC]. The patient-related data stored in the WBSN plays an important role in medical diagnosis and treatment; hence it is essential to ensure the security of these data. Failure to obtain authentic and correct medical data will possibly prevent a patient from being treated effectively, or even lead to wrong treatments. Access to patient-related data must be strictly limited only to authorized users; otherwise, the patients' privacy could be abused. However, in

DOI: 10.5121/ijassn.2012.2301

WBANs, distributively stored private data may easily be leaked due to physical compromise of a node. Therefore, data encryption and cryptographically enforced access control is needed to protect the privacy of patients [1]. As explained in [1], data access security requirements include access control (privacy) to prevent unauthorized access to patient-related data generated by the WBSN. Security schemes generally include encryption and authentication. There has been very little study done in encryption algorithms suitable for WBSN. In this paper we focus on RC5 encryption algorithm as a potential cipher solution for providing data protection in WBSN. RC5 is a parameterized algorithm, with a variable block size, a variable number of rounds, and a variable-length secret key. This provides good flexibility in both the performance characteristics and the level of security [2].

2. SECURITY SCHEME FOR WBSN

Many security schemes have been suggested for Wireless Sensor Network (WSN), however very few of them can be used in WBSN. In IEEE 802.15.4 the application has a choice of security modes that control the different security levels. Each security mode has different security properties, protection levels, and frame formats. In WSN solutions, the encryption is usually accomplished by using a symmetric cryptosystem such as RC5 or Advanced Encryption Standard (AES). Symmetric encryption algorithms seem to be inherently well suited to low-end devices, because they have relatively low overhead. In practice, however, many low-end microprocessors are only 4-bit or 8-bit, and do not provide (efficient) multiplication or variable rotate/shift instructions. Hence many symmetric ciphers are too expensive to implement on some target platform [14]. Depending on the implementation, AES may be either too big or too slow for some application. [3] describes various security modes defined in the IEEE 802.15.4 standard, broadly classified into no security, encryption only (AES-CTR), authentication only (AES-CBCMAC), and encryption and authentication (AES-CCM) modes. The IEEE 802.15.4-based security modes can be improved for a WBSN according to the application requirements. Thus few proposed 802.15.6 WBAN MAC (Medium Access Control) protocols suggests AES based security solution for WBAN [4]. Although the National Institute of Standards and Technology's (NIST) AES cipher is more widespread than RC5 and has inbuilt hardware support among some microcontroller manufacturers, AES is found slower and has higher memory requirements than RC5, which makes RC5 a better cipher solution for devices with limited resources [16]. RC5 can be considered as one of the best ciphers in terms of overall performance, when used in nodes with limited memory and processing capabilities. As an industry standard, RC5 can also be utilized in other types of wireless networks such as WBSN.

3. RC5 PROTOCOL AS A CIPHER SOLUTION FOR WBSN

In a system with resource and energy constraints, such as a WBSN node, we need to consider the balance of the three factors: energy consumption, security strength, and time or computational overhead. This section throws some light on how RC5 algorithm affects sensor nodes and sensor network performance. The focus is on security and performance trade-offs, especially in energy consumption, memory requirement and computation time. Security concerns are motivated by the deployment of a large number of sensory devices in the field. Limitations in processing power, battery life, communication bandwidth and memory constrain the applicability of existing cryptography standards for small embedded devices[6]. RC5 is simple and easy to implement, and also more amenable to analysis than many other block ciphers. RC5 does not rely on multiplication and does not require large tables. Hence, RC5 block cipher offers a computationally inexpensive way of providing secure encryption. RC5 is suitable for resource-constrained sensor nodes for the following reasons. RC5 is a simple and fast cipher using only

common microcontrollers operations; it has a low memory requirement[17] making it suitable for sensor applications; the same lightweight algorithm can be used for both encryption and decryption; and heavy use of data-dependent rotations provides high security.

3.1 Security Strength

RC5 involves data dependent rotations which may help frustrate differential cryptanalysis and linear cryptanalysis since bits are rotated to random positions in each round. There is no obvious way in which an RC5 key can be weak other than by being too short[13]. The standard key length of RC5 is 128 bits has managed to withstand years of cryptanalysis. Also the RC5 block cipher has built-in parameter variability that provides flexibility at all levels of security and efficiency [5]. RC5 is better than DES in security strength and implementation efficiency[15].

3.2 Energy Consumption

Security protocols and the cryptographic algorithms contain security considerations from a functional perspective, however many embedded systems are constrained by the environments they operate in and the resources they possess. For such systems, there are several challenges that need to be addressed in order to enable secure computing and communications. For battery-powered embedded systems, perhaps one of the foremost challenges is the mismatch between the energy and performance requirements of security processing [study of energy consumption]. According to energy consumption, shown in [15] for different length encryption data, the energy consumption of RC5 is significantly lower than that of AES and DES. Thus RC5 may be considered as a potential candidate for energy efficient cipher solution for WBSN as well.
In [7], they presented a new method of applying cryptography techniques in WSNs and evaluated the energy consumption of various schemes such as Public Key cryptography, Symmetric Key cryptography and Hybrid cryptography. To provide a valid and fair comparison they assumed the three security schemes were executed on Atmega 128 16MHz 8-bit architecture AVR. The energy consumptions depicted in [7] show that source node using RC5 saves about 72% of the energy consumed by the hybrid scheme and 82% of the energy consumed ECC. It also shows that the intermediate node consumes additional 19% of the energy consumed by the intermediate node using the hybrid scheme, and it saves more than 84% of the energy consumed by the intermediate node using ECC. Additionally, the sink node uses RC5 to save about 72% of the energy consumed by the hybrid scheme and 82% of the energy consumed by ECC. As a result, the network energy in this scheme will be drained very slowly after a very large number of interactions which makes this the symmetric scheme, RC5, the most suitable and viable one for WSN.

3.3 Computational Overhead

High efficiency is strongly demanded for data security in WBANs, not only because of the resource constraints, but also for the applications. Wearable sensors are often extremely small and have insufficient power supplies, which render them inferior in computation and storage capabilities. Thus, the cryptographic primitives used by the sensor nodes should be as lightweight as possible, in terms of both fast computation and low storage overhead. Otherwise, the power and storage space of the nodes could be drained quickly[1]. Study in [6] investigates the computational requirements for a number of popular cryptographic algorithms and embedded architectures. The measurements obtained cover a wide class of commonly used encryption protocols such as MD5, SH1, RC4, RC5, and IDEA. The symmetric key encryption of RC5 performs better than IDEA. The initialization overheads are significant for all encryption algorithms (RC5, IDEA and RC4), especially for small plaintexts. Thus they are suitable for large data size. [2] presents a methodology for the evaluation of the computational cost and energy

efficiency of two block ciphers, Advance Encryption Standard (AES)- Rijndael and RC5, that have been published as potentially suitable for WSN security. From [2] analytical model, RC5 is faster compared to AES-Rijndael and therefore more energy-efficient under memory constraints for both encryption and decryption, but it suffers from a relatively costly key expansion. As per [2] RC5 is a potential candidate for encryption of large amounts of data since in this case the costly key expansion does not fall into account. Conversely, AES Rijndael will normally be preferred for the encryption of small amounts of data or medium-sized messages.

Experimentation in [15] suggests using encryption service with RC5 algorithm. As per comparison in [15], RC5 has the following advantages: 1) The design of RC5 is concise and it does not need a lookup table with large storage. The memory cost of RC5 is significantly smaller than that of AES. 2) We can customize the group size, secret-key length, and the number of iterations of RC5, which can be used flexibly in systems with different resource configurations.
In WBSN the size of data varies for different medical (health parameters such as ECG, EEG, Blood pressure, Blood Sugar etc) or nonmedical (video, audio etc) applications. RC5 is a highly efficient and flexible cryptographic algorithm, for which many parameters (key size, block size, number of rounds) can be adjusted to tradeoff security strength with power consumption and computational overhead. Thus RC5 with suitable parameters may perform well for WBSN applications with different data size.

4. IMPLEMENTATIONS OF RC5 ALGORITHM

Although prototype modules for WBSN applications are becoming available; these devices are multi-chip solutions with excessive power consumption. Recent advances in embedded systems, microelectronics, sensors and wireless networking enable the design of wearable advanced health monitoring systems. The development of a custom ASIC can deliver improvements to the patient's quality of care through miniaturization and power consumption reduction. However prototype models of such ASIC (Application Specific Integrated Circuit) or SoC (System on Chip) implementations for WBSN nodes are in evolving stage. This section presents implementation issues of RC5 algorithm for WBSN nodes. RC5 algorithm can be implemented in software as well as hardware. Even though the software implementation of encryption algorithms has the advantages of portability, flexibility, and ease of use, it provides a limited physical security and agility compared to hardware implementations. Major advantages that lead to the hardware implementation include less power consumption, small circuit size, hardware reconfigurability, cost efficiency, high operating speed and security [8]. There are various platforms for hardware implementations, such as, embedded architecture based, reconfigurable platforms such as Field Programmable Gate Array (FPGA) and Programmable System on Chip (PSoC) based and VLSI implementation in the form of ASIC (Application Specific Integrated Circuit). This section describes various hardware implementations of RC5 algorithm in literature.
Study in [6] assesses the feasibility of different encryption schemes for a range of embedded architectures. Measurements were obtained for six different architectures, ranging in word size from 8 (Atmel AVR) over 16 (Mitsubishi M16C) to 32-bit width (StrongARM, XScale) to cover low-end, medium and high-end embedded processors. This study includes RC5 as one of the popular encryption algorithm for mobile devices such as nodes in a sensor network. A comparison of RC5 and RC4 on Atmega 103 reveals that the encrypt times are close to each other. In fact, RC4 is slightly faster. However, a similar comparison on StrongARM indicates RC5 is three times faster than RC4. This can be attributed to the fact that RC5 operates on 32-bit words while RC4 operates on 8-bit words. A comparison between RC5 and IDEA on the Atmega 103 reveals that RC5 is 1.5 times faster than IDEA, although they both work on 64-bit blocks. Further from given set of algorithms RC4 and RC5 are found the most efficient in terms of code memory size over all the given architectures.

Field programmable gate arrays (FPGA) are becoming a commonly used technology for digital systems implementation due to their fast manufacturing turnaround time, low startup costs, and ease of design changes [9]. FPGAs are an array of programmable logic cells interconnected by a matrix of wires and programmable switches. Each cell performs a simple logic function defined as per the user instructions. An FPGA has a large number (64 to over 20,000) of these cells available to use as building blocks in complex digital circuits. The potential features of Field Programmable Gate Arrays (FPGA) implementation is that it allows SoC modelling.

[10] describes area optimized architecture and an FPGA implementation for RC5 is introduced. The proposed implementation allocates less area resources, with a range between 28 to 33%, compared with the conventional architecture. The proposed architecture has been designed with a pipeline technique, which achieves high speed performance.

[8] presents the design and analysis of various hardware reconfigurable models of RC5 Encryption algorithm to determine the effects of loop-unrolling design concept on improving the encryption performance in terms of throughput. Loop unrolling is a used generally in system design to improve throughput and optimize critical parts of the system by duplicating hardware components. Results revealed that while no-loop-unrolling provided the least circuit size, the 3-loop-unrolled approach provided the highest encryption throughput. Further, a throughput speed up of 24% was achieved as compared to a reference system implemented. Although this design approach could succeed in achieving throughput, there is no significant improvement in power consumption. Thus it is a serious issue of concern as far as WBSN is concerned and hence needs to be explored in this context.

[11] experimented high performance RC5- integrated architecture with variable key registration, enhanced security and improved encryption throughput. The proposed architecture is synthesized to FPGA device similar to the related work for comparisons. The proposed architecture shows an improvement in the speed of operation as compared to the conventional architecture and related work. The deliverable encryption throughput of the proposed RC5-SoPC (System on Programmable Chip) design is from 300 Mbps to 450 Mbps, depending on the choice of the clock frequency (i.e. 24 MHz or 35MHz). However this work does not reveal the power consumption of hardware implemented.

[12] presents a half-run RC5 cipher architecture with low power dissipation for transmission security of biomedical systems. The proposed architecture uses a resource-sharing approach utilizing only one adder/subtractor, one bi-directional barrel shifter, and one XOR with 32-bit bus width. Therefore, two data paths are switched through four multiplexers in the encryption/decryption procedure. A prototype chip is fabricated by a standard 0.18 μm CMOS technology. The size is 704*697 μm^2, where a total of 1.64k gates are used. The proposed architecture consumes 5.87 mW@50 MHz system clock. Though power consumption is less compared to that of implementations in [8], a more research is needed to investigate ways to reduce power consumption in such implementations as power requirement in WBSN nodes is very less compared to this.

Thus RC5 algorithm can be implemented on various platforms. Each implementation platform has its own advantages and disadvantages. One may choose the platform based on its application. ASIC and SoC based implementations are best suitable for WBSN sensor nodes considering various performance metrics such as size, weight, power consumption etc.

5. CONCLUSIONS

There has been very little study done for encryption scheme for WBSN. Thus lot of scope lies in study, experimentation and investigation of suitable cipher solution for WBSN. This study

initiates to propose RC5 as a potential cipher solution for Wireless Body Area Networks. It provides a satisfactory balance between energy consumption, security strength, and computational time. RC5 is a highly efficient and flexible cryptographic algorithm, for which many parameters (key size, block size, number of rounds) can be adjusted to tradeoff security strength with power consumption and computational overhead. Thus RC5 with suitable parameters may perform well for WBSN applications with different data size. Study included survey of RC5 implementations on various platforms. This theoretical discussion may further be supported with experimental results in near future.

REFERENCES

[1] Ming Li, Wenjing Lou, Kui Ren, "Data security and privacy in Wireless body area networks" IEEE Wireless Communications, Volume 17 , Pp 51 – 58, Feb 2010

[2] M. Razvi Doomun and KMS Soyjaudah, "Analytical Comparison of Cryptographic Techniques for Resource-Constrained Wireless Security" International Journal of Network Security, Vol.9, No.1, PP.82–94, July 2009

[3] Saleem, Shahnaz, "Towards Security Issues and Solutions in Wireless Body Area Networks" 6th International Conference on Networked Computing (INC), pp 1-4, 2010

[4] Kyung Sup Kwak1, M. A. Ameen1, Daehan Kwak1, Cheolhyo Lee2, Hyungsoo Lee2, "A Study on Proposed IEEE 802.15 WBAN MAC Protocols" 9th International Symposium on Communications and Information Technology, 2009. ISCIT, pp 834 – 840, 2009.

[5] Juha Kukkurainen, Mikael Soini, Lauri Sydanheimo, "RC5-Based Security in Wireless Sensor Networks: Utilization and Performance" WSEAS TRANSACTIONS on COMPUTERS, ISSN: 1109-2750, Issue 10, Volume 9, October 2010

[6] Prasanth Ganesan, Ramnath Venugopalan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu, "Analyzing and Modeling Encryption Overhead for Sensor Network Nodes", Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, pp 151 – 159, 2003

[7] Mohammad AL-Rousan, A. Rjoub and Ahmad Baset, "A Low-Energy Security Algorithm for Exchanging Information in Wireless Sensor Networks" Journal of Information Assurance and Security 4 (2009), pp 48-59

[8] Omar Elkeelany, "Design and Analysis of Various Models of RC5-192 Embedded Information Security Algorithm" International Journal Of Applied Mathematics And Informatics, Issue 1, Volume 2, pp 18-27, 2008

[9] Yongming Yang , Xiaobo Huang , Xinghuo Yu , "Real-Time ECG Monitoring System Based on FPGA" The 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON), pp 2136-2140, 2007

[10] Sklavos, N, Machas, C.; Koufopavlou, O. "Area optimized architecture and VLSI implementation of RC5 encryption algorithm " Proceedings of the 10th IEEE International Conference on Electronics, Circuits and Systems, pp 172 - 175 Vol.1, ICECS 2003

[11]Omar Elkeelany, Adegoke Olabisi, "Performance Comparisons, Design, and Implementation of RC5 Symmetric Encryption Core using Reconfigurable Hardware" Journal Of Computers, VOL. 3, NO. 3, pp 48-55, 2008

[12] Yain-Reu Lin; Chia-Hao Hsu; Rieger, R.; Chua-Chin Wang, "Low power RC5 cipher for ZigBee portable biomedical systems " IEEE International Conference on Consumer Electronics (ICCE), pp 615 – 616, 2011

[13] Rivest, R.: The RC5 Encryption Algorithm. In: Proc. 1994 Leuven Workshop on Fast Software Encryption, Springer-Verlag (1995) 86–96

[14] Perrig, A., Szewczyk, R., Wen, V., Culler, D., Tygar, J.: SPINS: Security Protocols for Sensor Networks. In: Proceedings of the 7th Ann. Int. Conf. on Mobile Computing and Networking, ACM Press (2001) 189–199

[15] Meikang Qiu, Wenzhong Gao, Senior Min Chen, Jian-Wei Niu, and Lei Zhang," Energy Efficient Security Algorithm for Power Grid Wide Area Monitoring System" IEEE Transactions On Smart Grid, Vol. 2, No. 4, pp 715-723 DECEMBER 2011

[16] Kumar.J, Ezhilarasi.M, "Adaptive security mechanism for PEAS in Wireless Sensor Networks" International Conference on Computing and Control Engineering (ICCCE 2012), ISBN 978-1-4675-2248-9 © 2012

[17] Y. W. Law, J. M. Doumen, and P. H. Hartel. Benchmarking block ciphers for wireless sensor networks (extended abstract). In 1st IEEE Int. Conf. on Mobile Ad-hoc and Sensor Systems (MASS), page electronic edition, Fort Lauderdale, Florida, Oct 2004. IEEE Computer Society Press, Los Alamitos, California.

Authors

Dhanashri Gawali received Bachelor degree in Electronics engineering from Pune University in 2001, Master degree in Electronics-VLSI engineering from Bharati Vidyapeeth University in 2005. She is currently working as an Assistant Professor at an engineering institute affiliated to Pune University, India. She is member of ISTE, VLSI Society of India, ACEEE and IACSIT.

Her area of interest includes hardware design using reconfigurable platform and its applications in various domains such as computing, communication and control. She is currently doing research in Wireless Body Area Network Node.

Dr. Vijay M.Wadhai received his B.E. from Nagpur University in 1986, M.E. from Gulbarga University in 1995 and Ph.D. degree from Amravati University in 2007. He has experience of 25 years which includes both academic (18 years) and research (7 years). He has been working as Principal & Professor of MIT College of Engineering, Pune (since 2011) and

simultaneously handling the post of Director - Research and Development, Intelligent Radio Frequency (IRF) Group, Pune (since 2009).

His research interest includes Deductive Databases, Knowledge Discovery and Data Mining, Cognitive Radio and Wireless Communication, Spectrum Management, Wireless Sensor Network, ASIC Design - VLSI, Advance Network Design. He is a member of LMISTE, MIETE, MIEEE, MIES and GISFI (Member Convergence Group), India.