Security and Privacy in Wireless Sensor Network Using RC6 Algorithm

Shailesh N. Sisat, Prof. Shrikant J. Honade

[1]Department of E&TC, G H Raisoni College of Engineering, Amravati, Maharashtra, India

Abstract— *With the widespread growth in applications for resource limited Wireless Sensor Networks (WSN), the need for reliable and efficient security mechanisms for them has increased manifold but its implementation is a non-trivial task. Limitations in processing speed, battery power, bandwidth and memory constrain the applicability of existing cryptography algorithms for WSNs. Several security mechanisms have been introduced to address the need for security in WSNs. To provide a better understanding of these security mechanisms, two encryption algorithms RC5 and RC6 have been studied and implemented in WSN environment.*

Keywords— RC5, RC6, WSN, Security.

I. INTRODUCTION

Wireless Sensor Network is continuously gaining popularity as a communication media due to vast applicability in military as well as in commercial purpose. It is necessary to protect the sensitive data transferred through the wireless sensor network. Different techniques have been studied to achieve secure communication in the WSN. Use of cryptography ensures the security of data in the wireless sensor network but also introduces severe resource constraints due to low sensor power and limited data storage capability. The paper states the comparative study of RC5 and RC6 cryptographic algorithms while implemented in the smart sensors. Security requirements in wireless sensor network such as Data Confidentiality, Data Authenticity-integrity and Availability are achieved by using RC5 and RC6 cryptographic algorithms and smart sensor's IMEI number. The influences of cryptographic security on the sensors have been studied in terms of obstacles such as sensor energy, memory requirement and time delay. To achieve the reliable and secure communication in wireless sensor network it is necessary to study the obstacles in WSN. Main obstacles are,

1. Limited Memory and storage space.
2. Power limitation

Figure 1 shows the basic architectural components of smart sensor.

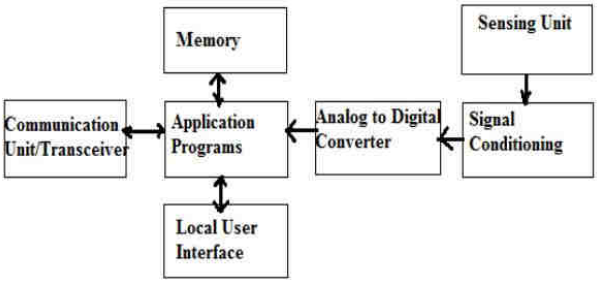

Fig. 1: Basic architectural components of smart Sensor node [25]

II. WSN SECURITY SOLUTIONS

Cryptography and secure routing protocols provides the defense against the security in WSN [23]. Rivest et al. (1998) proposed RC6 block cipher based on RC5 symmetric key approach [23].

Details of RC6: RC6 can encrypt 128-bit data blocks by using 128, 192, or 256 bit keys [3] [23]. RC6 can support various word/key sizes and number of rounds and it can be defined as RC6-w/r/b where w stands for bit size of word, r stands for the number of rounds, and b stands for key size in bytes [3]. The most fundamental difference between RC6 and RC5 is that RC6 uses an extra multiplication operation to perform bit rotations in each word.

The operations used in RC6 are defined as followings [3].

- ✓ A+B integer addition modulo 2^w
- ✓ A-B integer subtraction modulo 2^w
- ✓ A $\oplus$ B bitwise exclusive-or of w-bit words
- ✓ A*B integer multiplication modulo 2^w
- ✓ A<<<B rotation of the w-bit word A to the left by the amount given by the least significant lg w bits of B
- ✓ A>>>B rotation of the w-bit word A to the right by the amount given by the least significant lg w bits of B
- ✓ $f(x) = x(2x+1) \bmod 2^w$

Encryption process in RC6 algorithm is described in figure 2 and figure 3. Encryption and Decryption process are vice versa.

Input:
Plaintext stored in four w-bit input registers A, B, C, D
20 rounds
32-bit round keys S [0,…. 43]
Output:
Ciphertext stored in A, B, C, D
Procedure:

```
B = B + S [0] //Pre-whitening
D = D + S [1]
for i = 1 to 20 do
{
 t = (B x (2B + 1)) <<< 5
 u = (D x (2D + 1)) <<< 5
 A = ((A ⊕ t) <<< u) + S[2i]
 C = ((C ⊕ u) <<< t) + S[2i+ 1]
 (A, B, C, D) = (B, C, D, A)
  }
A = A + S [42] //Post-whitening
C = C + S [43]
```

Fig. 2: RC6 Encryption for AES with RC6-32/20/ [23]

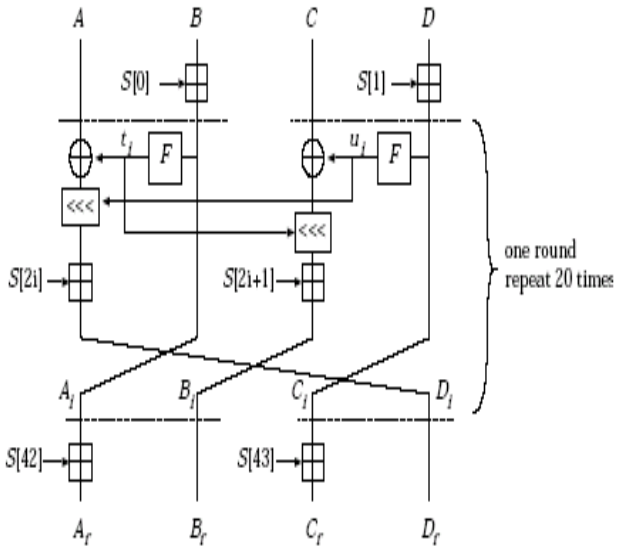

Fig. 3: RC6 AES Encryption Diagram [3][23]

III. METHODOLOGY

System Architecture: An integrated platform for wireless sensor network allows nodes to communicate using WLAN. There are several challenges associated with connecting nodes to each other using server.

- A network to connect nodes
- Discovering and accessing services, which require software service that can run on server.
- Storing data produced by nodes, which requires a storage location on server.

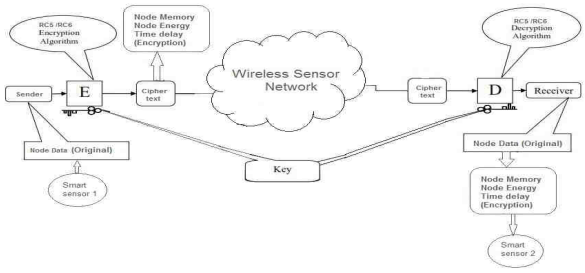

Fig. 4: System architecture

IV. RESULTS ANALYSIS

The research is focused on the implementation of RC5 and RC6 algorithm that provides a better security and observes the results in terms of energy, memory and delay. The main design for such approach is as following,

1. The methodology of the work requires the implementation of RC5 and RC6 algorithms which are used to provide security for uploading, downloading sensor data and then this algorithm will perform their encryption and decryption of data.
2. Use java platform to implement algorithm.
3. Calculated and analyzed parameters which are described as: Energy, Memory and Delay required for encryption and decryption.

The implementation of the work goes through various steps which are described as follows.

Step 1: Activation of Wamp Server: the very first step of the work is to run the Wamp server which is used as backend to store the database and SecurityRC5_RC6 IDE as a front end where algorithms are implemented in java language.

Step 2: Initiate the Servers: In this phase, we have to initiate all the servers that are used to process the node requests.

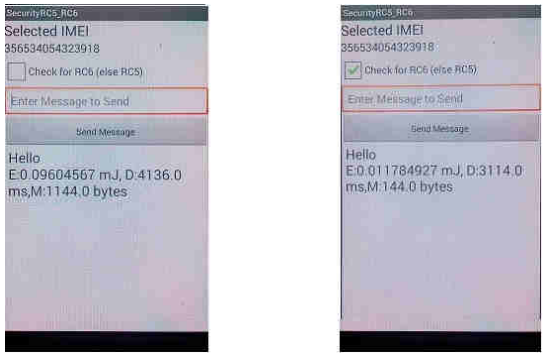

Fig. 5: Encryption parameters for two different algorithms

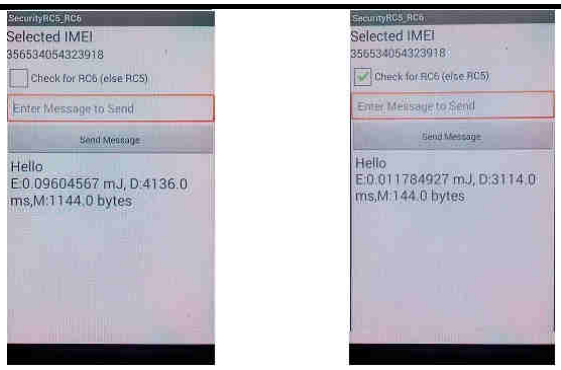

Fig. 6: Decryption parameters for two different algorithms

Step 3: Node Connections: In this phase node discovers the other nodes in the network by fetching IMEIs number of respective node and by selecting particular IMEI number, connection get established.

Step 4: Encryption of Sensor Data: This phase includes sending sensor data by selecting particular algorithm such as Rc5 and RC6 which is to be encrypted and saved in the database server. Server receives the data and sends to the respective node by comparing the key. At the same time detail report for the energy, memory and delay is generated at the sender node.

Table 1: Calculated encryption parameters

Size of I/P (bytes)	Memory (bytes)		Energy (µj)		Delay (µs)	
	RC5	*RC6*	*RC5*	*RC6*	*RC5*	*RC6*
40	1112	88	0.057	0.004	6968	5932
64	1119	102	0.055	0.005	6899	5827
80	1120	219	0.057	0.012	6837	5870

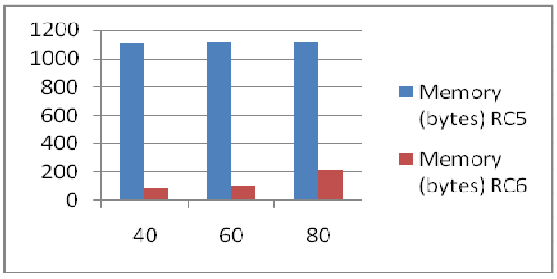

Fig. 7: comparison graph of required encryption memory

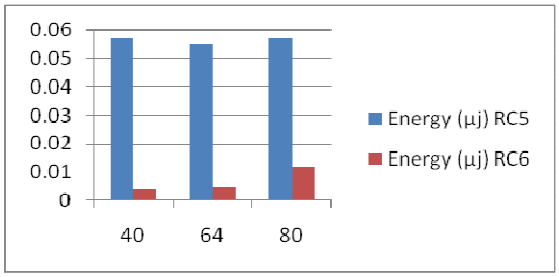

Fig.8: comparison graph of required encryption Energy

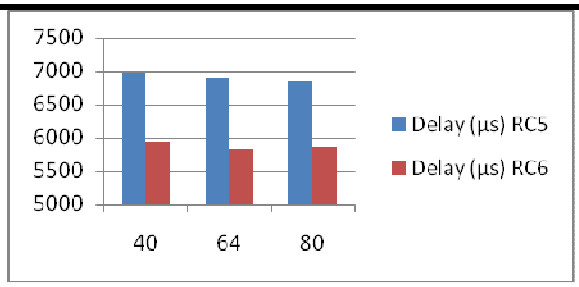

Fig. 9: comparison graph of required encryption delay for RC5 and RC6 algorithm

Step 5: Decryption of Sensor Data: This phase includes the decryption of received data by using particular algorithm and generating the detail report for the parameters.

Table 2: Calculated decryption parameters

Size of I/P (bytes)	Memory (bytes)		Energy (µj)		Delay (µs)	
	RC5	*RC6*	*RC5*	*RC6*	*RC5*	*RC6*
40	1028	135	0.083	0.001	4239	3197
64	1132	127	0.107	0.004	3990	3304
80	1136	120	0.106	0.009	3954	3297

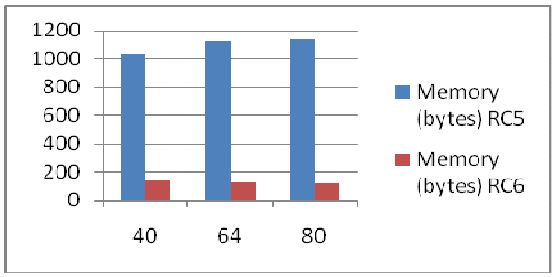

Fig. 10: comparison graph of required decryption memory

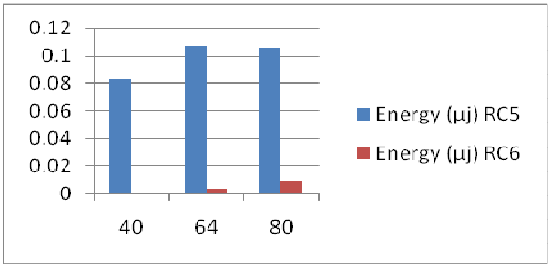

Fig. 11: comparison graph of required decryption energy

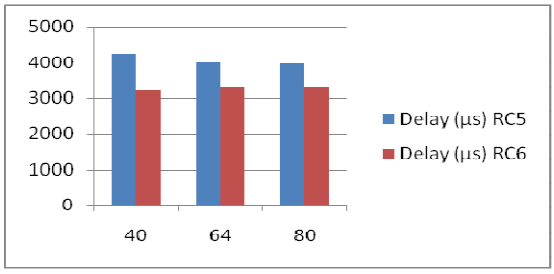

Fig. 12: comparison graph of required decryption delay for RC5 and RC6 algorithm

The table No.1 and 2 describes the output of each operation performed during encryption and decryption on different files of size 40, 64, and 80bytes. In this we show the comparison of two algorithms in terms of parameters by graphs.

V. SECURITY REQUIREMENTS IN WIRELESS SENSOR NETWORK

Security requirements in wireless sensor network are achieved in following way.

Data Confidentiality: Data encryption is the standard method that avoids unwanted user interference in the wireless sensor network resulting to the data confidentiality [9] [16]. RC5 and RC6 cryptographic encryption algorithms are used to meet the data confidentiality requirement.

Data Authenticity and integrity: Source authentication provides the truthfulness of originality of the sender which is achieved by using IMEI number to provide the sender as well as receiver authentication. Where, data authentication ensures the receiver that the data has not been modified during the transmission, where the encryption key ensures the data integrity.

Availability: Sensor node must be available when needed. It is observed that the RC6 encryption algorithm avoids unnecessary computations that affect the battery power compared to RC5 encryption algorithm. Data is made available online as well as offline using SQlite database.

VI. CONCLUSION

Now-a-days security has become one of the most important aspects in every field. Information should be secured as any changes in information leads to very serious problem. Data should be secured from malicious attacks and unauthorized access. The aim of the cryptography is to secure the data from intruders. This dissertation mainly deals with the Smartphone sensor network, and solved the security related problems. Security plays an important role in this work as to protect the sensitive information from the unauthorized user. This dissertation has implemented the RC5 and RC6 algorithm in Java platform. In this dissertation, the effect of RC5 and RC6 algorithms used for data encryption, decryption and to improve the reliability of system have studied. With the help of this dissertation the analyzed results for the energy, memory and time delay are obtained. The obtained parameters are compared for both algorithms. Since the algorithm is quite simple, this permits a compiler to produce well-optimized code, resulting in good performance without hand-optimizations. The RC6 is found to be better than RC5 algorithm in terms of memory requirement, energy requirement and time delay.

VII. FUTURE WORK

According to research done in RC5 and RC6 algorithm, modifications are possible in the respective algorithm such as RC5 with LU matrix and RC6 algorithm with an enhance version (RC6e). The new modified algorithms can be used to design a wireless sensor node and parameters can be compared with the conventional RC5 and RC6 algorithms.

VIII. ACKNOWLEDGEMENT

The author sincerely thanks to Prof. Shrikant J. Honade, Assistant Professor, E&TC department, GHRCEM, Amravati, Dr. P. V. Ingole, Principal, GHRCEM Amravati and Prof. N. N. Mandaogade, Head of E & TC Department GHRCEM Amravati for their valuable suggestion, criticism and time to time encouragement.

REFERENCES

[1] Dr Radhika K R, "A Novel Symmetric Key Encryption Algorithm Based On RC5 in Wireless Sensor Network", *International Journal of Emerging Technology and Advance Engineering, June 2013, Volume 3, Issue 6, PP 373-376*

[2] Gil-Ho Kim, Jong-Nam Kim, Gyeong-Yeon Cho, Dept of Computer Engineering PuKyong National Univ. "An improved RC6 algorithm with the same structure of encryption and decryption", *11th International Conference on Advanced Communication Technology, 2009, Volume: 02, PP 1211-1215.*

[3] Harsh Kumar Verma, Ravindra Kumar Singh, "Enhancement of RC6 Block Cipher Algorithm and Comparison with RC5 & RC6", *3rd IEEE International Advance Computing Conference, 2013, PP 556-561.*

[4] Changjiang Li, Yufen Wang, "The Application Research of Wireless Sensor Network Based on ZigBee", *2nd IEEE International Conference on MultiMedia and Information Technology, IEEE, 2010, PP 89-92.*

[5] Vorugunti Chandra Sekhar, Mrudula Sarvabhatla, "Security In Wireless Sensor Networks With Public Key Techniques", *International Conference on Computer Communication and Informatics Coimbatore, INDIA, IEEE, Jan 10 – 12, 2012.*

[6] Shammi Didla, Aaron Ault,"Optimizing AES for Embendded Devices and Wireless Sensor Networks", ICST, Belgium, 2008.

[7] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. "A survey on sensor networks", *IEEE Communications Magazine, August 2002, PP 102–114.*

[8] Dirk WESTHOFF, Joao GIRAO, Amardeo SARMA, "Security Solutions for Wireless Sensor Networks", *Nec Technical Journal, 3/2006, volume 1.*

[9] Deepika Thakral, Neha Dureja "A Review on Security Issues in Wireless Sensor Networks", *International Journal of Advanced Research in Computer Science and Software Engineering, July 2012, Volume 2, Issue 7*

[10] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. E. Culler, and K. Pister. "System Architecture Directions for Networked Sensors", *In Architectural Support for Programming Languages and Operating Systems, 2000, PP 93 104.*

[11] Karlof, C.; Wagner, D., "Secure routing in wireless sensor networks: attacks and countermeasures," *International Workshop on Sensor Network Protocols and Applications IEEE, , 11 May* 2003 , *PP113-127*

[12] Z. Tanveer and Z. Albert. "Security issues in wireless sensor networks", *Proceedings of the International Conference on Systems and Networks Communication Washington, IEEE, 2006, page 40.*

[13] John PaulWalters, Zhengqiang Liang,Weisong Shi and Vipin Chaudhary. "*Wireless sensor network security: A survey. Security in Distributed, Grid, and Pervasive Computing", 2006.*

[14] Mayank Saraogi. "Security in Wireless Sensor Networks", In *ACM SenSys, 2004.*

[15] I. Khalil, S. Bagchi, and N. B. Shroff. Liteworp: "Detection and isolation of the wormhole attack in static multihop wireless networks", *Comput. Netw., 51(13):3750– 3772, 2007.*

[16] Ashima single, Ratika Sachdeva, "Review on Security Issues and Attacks in Wireless Sensor Network", *International Journal of Advanced Research in Computer Science and Software Engineering April 2013, Volume 3, Issue 4.*

[17] A.Wood and J. Stankovic. "Denial of service in sensor networks", *IEEE, 2002, volume 35, PP 54-62.*

[18] D. R. Raymond and S. F. Midkiff. "Denial-of service in wireless sensor networks: Attacks and Defenses", *IEEE Pervasive Computing, 2008, volume 7, PP 74–81.*

[19] Piyush Dhule, Girish Talmale, " Secure time synchronization for wireless sensor network", *International Journal of Emerging Technology and Advanced Engineering, April 2014, Volume 4, Issue 4, PP 632-634.*

[20] Prof. Pravin Lakhe,"Wireless sensor network using ZigBee", *International Journal of Emerging Research and Application, VNCET 30 March 2012,PP 292-301*

[21] B.P. Ladgaonkar, A. M. Pawar, "Design and Implementation of sensor node for wireless sensor network to monitor humidity of high-tech polyhouse envirnment", *International Journal of Advances in Engineerinh & Technology, July 2011, volume 1, Issue 3, PP1-11*

[22] Amneet Kaur, Mrs. Meenakshi Bansal, "Secure Distributed Database Communication Using Ntru Algorithm" *International Journal Of Advanced Computing And Electronics Technology (Ijacet),* Issue-6,2015, Volume-2

[23] Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, and Y. L. Yin, "The RC6 Block Cipher" *available at website* http://theory.csail.mit.edu/~rivest/rc6.pdf

[24] Ronald L. Rivest, "The RC5 Encryption Algorithm," *available At website* http://theory.lcs.mit.edu/~rivest/Rivestrc5rev.pdf

[25] Mrs manali chaudhari, Prof. shrinu Dharavath, "Study of smart sensors and their applications", *International Journal of Advanced Research in Computer and Communication Engineerin, January 2014, Vol. 3, Issue 1*

[26] D. Sudharsan, J. Adinarayana, "Dynamic Real Time Distributed Sensor Network Based Database Management System Using Xml, Java And Php Technologies", *International Journal of Database Management Systems (IJDMS), February 2012, Vol.4, No.1*

[27] Revathi Gujjarlapudi, Archana Kakaraparthy, Kalyan Mohan Goli, "Integration of Android Operating System with Wireless Sensor Network", *International journal of computer science and technology, March 2013,vol 3*

[28] William Stallings, "Cryptography and Network Security: Principles and Practices", *Pearson Education, Third Edition*.

[29] Atul Kahate, "Cryptography and Network Security", *Mc Graw Hill, Second Edition.*

[30] William Stallings, "Cryptography and Network Security", Pearson Education, Inc, Fourth edition.

[31] Behrouz A. Forouzan, "Cryptography and Network Security", *Mc Graw Hill, Special Indian Edition 2007.*

[32] Theory and Practice of Cryptography Solutions for Secure Information Systems edited by Elçi, Atilla