International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 6, ISSN No. 2455-2143, Pages 188-192
Published Online October 2020 in IJEAST (http://www.ijeast.com)

SECURE REPROGRAMMING EXPLOITATION M-RSA TECHNIQUE IN WIRELESS SENSOR NETWORKS

Dr. Mallikarjunaswamy N J
Professor, Dept of CSE,
M.I.T, Thandavapura,
Mysore

Dr. Keshava Prasanna
Professor, Dept of CSE,
C.I.T, Gubbi,
Tumkur

Latha Yadav T R
Assistant Professor, A.I.T, Tumkur
Research Scholar, Visvesvaraya
Technological, University,
Belgaum

Abstract: **Wireless sensor networks are self organized, autonomous, automatic discovery of services, extremely ascendable, reliable, Infrastructure less service. Mainly applicable in the field of defense, healthcare. A previous affair of encryption and decryption technique gives the confidentiality to the text data. In this conversion plain text is the composition of only the text characters, some of the application's like reprogramming in the air technique uses encryption of program data. The encryption of program data is differing compare to the text data. Proposed method uses m-RSA for the effective encryption/decryption of program data. This gives more accurate results compare to existing method. To demonstrate that, the execution time and the security achieved by the proposed method are more effective than the RSA.**

Keywords - RSA, private key, public key, encryption, decryption, m-RSA.

I. INTRODUCTION

Wireless sensor network (WSN) is Associate in Nursing Ad-hoc like infrastructure less network and distributed system, during which every node organize itself to come up with the new system. Every node requires its own fixed frequency range to communicate with its neighbor one.

Wireless sensor networks (WSN) is the widespread technology which is contributing effectively in various application domains. Though it is a popular technology there are some issues to be solved before it can become a complete technology. The main issue in this technology is the energy requirement by the nodes and its utilization based on its functionality. The main source of energy in these networks is battery power. This research work focuses on the variety of techniques which can be utilized for saving the power in the network components. It constitutes the approaches for reducing the energy at different layers varying from physical to network. It is indeed a tedius task for the design engineer to find the reliable solution which has to be taken into consideration for the design of an application specific WSN architecture. The below section presents the trade off between the application specific requirement and methods to increase the lifetime of the nodes in the network.

The prime requirement in the WSN is the security specifically for few applications like medical, military or transportation etc. the WSNs are more prone to the third party attacks specially when deployed at the hostile environment.

Authentication is one of the primary requirements in securing any communication networks. This requirement is very much essential in the field of the wireless communication due to its characteristics. The medium used in wireless communication is very much affected for the attacks by external agents. And the wireless medium is open in nature and is operated in hostile environment most of the time, thereby requiring the authentication features in the network.

Usually this authentication features is achieved in any network by using the Message Authentication Code (MAC). This MAC is a code derived by a symmetric scheme of authenticating the data using a secret key. The secret keys used are only known to centralized or authenticated agencies. This can also ensure the data integrity in the network.

In order to secure the transmission WSN uses security needs reminiscent of authentication,

integrity, and confidentiality plays important role in infrastructure less network. During this association confidentiality is that the conversion of original information into cipher text. Reborn information is not within the variety of user clear kind. Which intern composition of hexadecimal values, numbers and special characters.

This paper is organized as follows: Section II presents the related work and section III presents the proposed methodology. Section IV presents the Experimental analysis. Section V contains the conclusion and future work.

II. RELATED WORK

Wireless device networking could be a wide technology to extract knowledge from the outside surface setting and process according to the user instruction and acquire the results in a memory device. On demand node sends the information in to the air for the betterment of the network. However, these edges go along with numerous limitations, vulnerabilities, and risks.

To distinguish legitimate data from intruder's data, confidentiality techniques are frequently used to verify the received data in a communication system. There are several message confidentiality schemes in wireless sensor networks have been proposed. The confidentiality techniques used in the severely constrained wireless sensor network environments.

Nasrin Khanezaei[1]. (2014) aims at having a more solution by The combination of symmetric key cryptography and asymmetric cryptography such as Advanced Encryption Standard(AES) and RSA encryption and decryption methods to distribute the data among different users in cloud system. A combination of symmetric cryptography (AES) and Asymmetric cryptography (RSA) encryption methods was proposed in this approach to provide the assurance of message confidentiality. The proposed approach allows providing difficulty for hackers and it clearly indicates that generating asymmetric key compare to symmetric key is a time consuming process. The main focus is on RSA encryption technique to achieve difficulty for hackers by using symmetric encryption method (AES). The encryption scheme mainly depends on key length and processing speed.

Sangita A[2]. (2015) proposed that modified-RSA method uses 3 prime numbers to provide more security instead of using 2 prime numbers for calculating 'n' (p, q and r) value and (p-1), (q-1) and (r-1) are used to calculating phi value. And it is very difficult to analyze the value of public key e (short bit length) and private key d hence cipher text is vulnerable for attack made by unauthorized users of cloud. Modulus X is used instead of using n and it is used to encrypt and decrypt the original message. The comparison results between existing RSA and modified-RSA algorithms in terms of generating key value, privacy is relatively high compare to existing RSA.

D.I. George [3]. (2017) proposed that algorithm reduces processing or execution speed at the side of both sender (Encryption) and receiver (Decryption). At sender side Encryption technique uses 4 prime numbers to encrypt the original message hence the security is high in the transmission of data in air. At receiver end decryption method uses 2 prime numbers to extract the original message. This gives high processing or execution speed at receiver or decryption end. ERSA divide the file into smaller unit (blocks) and applies the both encryption and decryption techniques hence it provides high speed of execution and security. In this the block size mainly depends on key size. ERSA much suitable in terms of strength of security and makes computation complex. Statistical methods very much suitable to achieve level of security.

Lavanya K[4]. (2016) In this proposed system clearly identified that the cryptosystem security process mainly depends on the design and implementations of the RSA algorithms. The paper also addressed the problem raised by the symmetric key cryptosystem and the solution to overcome the shortcomings of previous affairs of symmetric key cryptosystem. It aims on public key cryptography technique and mathematical properties are identified to enrich the security aspects in terms of providing confidentiality.

Prabhat K[5]. (2017) In this paper the value of private key and public key is depends on product of 4 prime numbers. This gives complex computation at intermediate nodes. The proposed hybrid-RSA (HRSA) algorithm has been implemented using MATLAB platform. To generate *n* bit Modulus, we have chosen two numbers of *n/2*-bit prime numbers for RSA, three numbers of *n/3*-bit prime numbers for ERSA and four numbers of *n/4*-bit prime numbers for the proposed algorithm. hybrid-RSA (HRSA) algorithm was developed to overcome the shortcomings of ERSA. The hybrid-RSA (HRSA) gives high speed encryption and decryption compare to Enhanced-RSA (ERSA).

So, by using the new proposed approach the performance is evaluated and compared with other methods under the same test results to demonstrate the

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 6, ISSN No. 2455-2143, Pages 188-192
Published Online October 2020 in IJEAST (http://www.ijeast.com)

effectiveness of the new approach with regards to enhancement of the run time and security of message in wireless sensor network nodes.

Assumptions

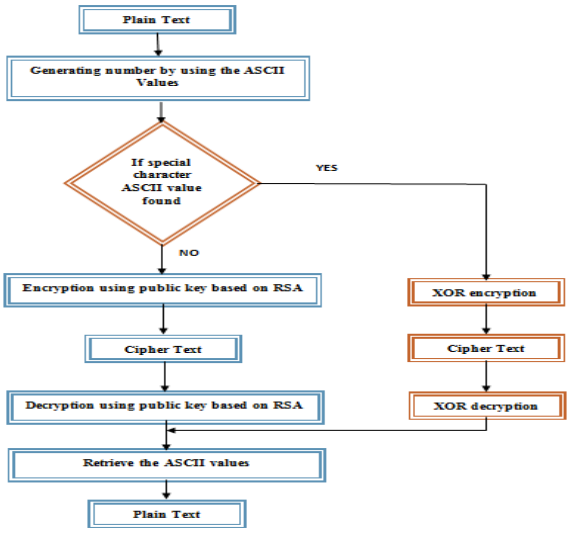
1 The Base station is a powerful node, with unlimited energy.
2 Each sensor node in the network is preconfigured.
3 Each sensor node has its own frequency range.
4 Sensor node captures the data from outside world and process the data according to the user instruction.
5 Each node has predefined cryptographic operation.

III. PROPOSED METHODOLOGY

The solution we have a tendency to planned is that the m-RSA. This is often the variation of existing RSA technique, which is the combination of hybrid crypto logical technique provides ambiguous output for unauthorized users. in this symmetric key embedded within the asymmetric key cryptography, both use input size 1024 bit and which produces output of 1024 bit information. Transition between RSA to m-RSA gives high security with the key size 1024bit.

Flow chart, as shown in figure 3.1(a), which initially converts original data into ASCII value process according to m-RSA and finally retrieves the plain text.

This proposed approach is more effective compare to RSA. In this, data classified as text data and special character ({, }, [,], *, %, +, -). The following steps indicate the working principle of m-RSA.



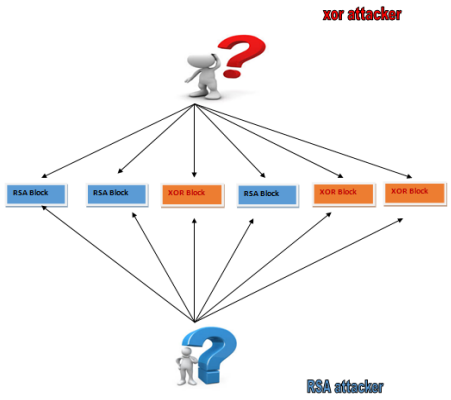
3.1(a) Flow Chart of m-RSA

ALGORITHM:

Step 1: Convert data into ASCII values.
Step 2: if special character found.
Step 3: Compute XOR cipher.
Step 4: Else compute RSA cipher.

Attackers view

Figure 3.1(b) attackers view shows that authorized users of XOR cipher not able to recognize RSA cipher block and authorized users of RSA cipher not able to recognize XOR cipher. Resultant data look like sequential RSA block concatenated with XOR cipher.



3.1(b) Attackers View

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 6, ISSN No. 2455-2143, Pages 188-192
Published Online October 2020 in IJEAST (http://www.ijeast.com)

Table 1: Comparison between RSA and m-RSA

Original Data	RSA	m-RSA
1.Cryptographic Operation	Asymmetric	Hybrid
2.Key Usage	Both public and private	Both public and private
3.Security	Low	High
4.Execution speed	More	Less

Table 1 shows the comparison between RSA encryption and decryption, as well as modified RSA(m-RSA).

IV. SIMULATION RESULTS AND DISCUSIONS

The algorithms were implemented using JAVA programming language. The m-RSA encryption and decryption module uses XOR operation, where as RSA uses mod operation. In the experiment, we clearly demonstrated that the 200000 repeated execution of RSA module consumes 15 ms whereas XOR cipher consumes only 5ms.

m-RSA results the execution speed which lies between the time slots of XOR and RSA. If the program data contains the combination of special characters and the normal text data then it uses the methods of XOR and RSA respectively to calculate the execution speed.

Speed of XOR, RSA and m-RSA Encryption / Decryption

The table 2 shows the time taken for encryption of plain text in to cipher text by both the algorithm.

Table 2 Encryption/Decryption Time in XOR, RSA And m-RSA Algorithm (Time in sec.)

Time	Message in byte	XOR	RSA	m-RSA
t1	14	0.0014	0.0042	0.0028
t2	28	0.0028	0.0084	0.0056
t3	56	0.0056	0.0168	0.0112
t4	112	0.0112	0.0336	0.0224
t5	224	0.0224	0.0672	0.0448

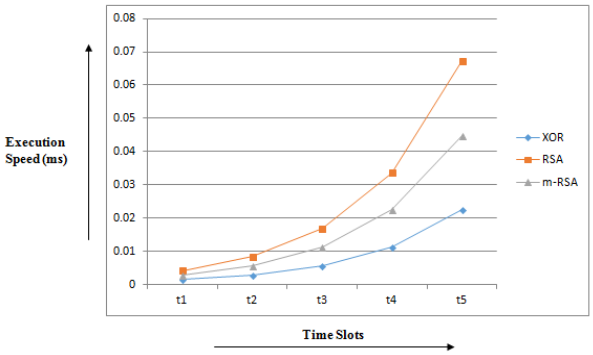


Figure 2: Encryption/Decryption Time using XOR, RSA and m-RSA algorithms.

The m-RSA methodology enhances the efficient way of encrypting the data in secured environment. In order to encrypt data, RSA algorithm uses 3 times more execution speed then XOR cipher, but the new methodology m-RSA is the hybrid approach takes less execution speed compare to existing RSA. Hence, m-RSA consumes less execution time, which gives the better performance.

V. CONCLUSION

The proposed scheme ensures confidentiality of the data and enhances high security. The experimental analysis and evaluation result shows that the proposed scheme is effective and climbable compare to existing RSA. In future we will apply this process for secure communication over public network. Finally conclude that RSA becomes to characters with m-RSA technique in terms of confidentiality.

VI. REFERENCES

[1] Nasrin Khanezaei, Zurina Mohd Hanapi, (2014)'. A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services, in IEEE Conference on Systems, Process and Control (ICSPC 2014), (pp. 58-62).

[2] Sangita A. Jaju, Santosh S. Chowhan, (2015)', A Modified RSA Algorithm to Enhance Security for Digital Signature, in IEEE, (pp. 1-5).

[3] Dr. D.I. George Amalarethinam , H. M. Leena, (2017). Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud, in , (pp. 172-175).

[4] Lavanya K. Galla, Venkata SreeKrishna Koganti, Nagarjuna Nuthalapati, (2016). Implementation of RSA, International Conference on Control,

Instrumentation, Communication and Computational Technologies (ICCICCT), (pp. 81-87).

[5] Prabhat K. Panda, Sudipta Chattopadhyay, (2017). A Hybrid Security Algorithm for RSA Cryptosystem, International Conference on Advanced Computing and Communication Systems (ICACCS -2017) (pp. 1-6).

[6] W. Stallings, (2014) "Cryptography and network security: principles and practice", sixth edition, ISBN: 0-13-335469-5, (pp. 9-60, 253-285).

[7] A.H. Al-Hamami and Aldariseh IA, (2012) "Enhanced method for RSA cryptosystem algorithm", international conference on Advanced Computer Science Applications and Technologies, Kuala Lumpur, IEEE, (pp. 402-408).

[8] R. Minni, K. Sultania and S.Mishra, "An algorithm to enhance security in RSA" , (2013) 4th ICCCNT, IEEE , (pp.1-4).

[9] F.Kong, J. Yu and L. Wu, (2011) "Security analysis of an RSA key generation algorithm with a large private key", Springer-Verlag Berlin Heidelberg, (PP-95-101).

[10] B.R. Ambedkar, A. Gupta,P. Gautam and S.S.Bedi, (2011) "An Efficient Method to Factorize the RSA Public Key Encryption." Communication Systems and Network Technologies (CSNT), International Conference on.
IEEE, (pp.108-111).

[11] W. Rui, C. Ju and D. Guangwen, (2011) "A k-RSA algorithm", 3rd ICCSN, Xi'an, China,IEEE, (pp.21-24).

[12] R S Dhakar, A K Gupta and P Sharma, (2012) "Modified RSA encryption algorithm (MREA)", 2nd ICACCT, IEEE, pp. 426-429.