Classical Number Theory based Vs. Chaos based Cryptography for Wireless Sensor Networks: A Research Perspective

Shantala Devi Patil[1] Dr. Vijaya Kumar B P[2]
[1,2]Department of Computer Engineering
[1]REVA, ITM, Bangalore [2]MSRIT, Bangalore

Abstract— Wireless Sensor Networks (WSN) have fascinated the whole world with their capability to connect to the inhabitable regions. Their applicability to almost every possible area makes it more interesting. Needless to say, that there are certain shortcomings of these tiny devices (sensors) in terms of their memory, processing and battery and hence classical network practices are inapplicable to these networks. Security is a major concern in WSN as they are deployed in hostile regions. Classical security techniques based on number theory are not suitable to energy constrained WSN. This paper aims to discuss the advantages and drawback of introducing the chaotic and fractal based security schemes to WSN. Application of security techniques based on Chaos and Fractals is first of its kind in the field of WSN and expected to revolutionize the field of Sensor Networks.

Key words: Fractals, Chaos, PKC, WSN, Public Key, Private Key, RSA

I. INTRODUCTION

Wireless Sensor Networks may be deployed in dangerous and hostile environments and still it's expected that they transmit the information securely across the network, among the nodes. This requires security measures such as confidentiality, authentication etc to be imposed on to the network. The very fact that wireless sensor nodes [23, 24] are severely constrained in terms of their energy, computation and communication capabilities creates a need to develop security mechanisms that can consider these limitations.

Cryptography is a study of providing information security with mathematical and computation techniques [1]. Current cryptographic techniques are based on the number theory and the strength of such a technique is assessed with the difficulty of solving number theoretic problems [2-4]. These techniques also depend heavily on the huge key size and key space.

Another new paradigm which is more promising than that of the number theory based approach is the Chaos and Fractals based technique part of non-linear dynamics field [5]. This technique is highly robust to attacks as infinite space needs to be searched for a fractal key in a Brute Force Attack and also even if part of key is obtained by the attacker, it will be impossible to extract the rest of the key [6].

This papers aims at exposing the latest application of chaos and fractal functions in cryptography. The paper aims to discuss the advantage of these new type of cryptosystems based on chaos and fractals. In the subsequent section security and performance analysis of both the methods is carried out, followed by discussion of applicability of the new technique to Wireless Sensor Networks. The Conclusion is drawn in the last section.

II. CRYPTOSYSTEMS

The cryptosystem is designed to reduce common attacks and is supposed to possess two cryptographic properties 1: Confusion and Diffusion. The first property is intended to make the relationship between the key and the cipher text as complex as possible. The second property refers to rearranging or spreading out the bits in the message so that the influence of individual plaintext or key bits is spread out over as much of the cipher text as possible. Based on the mathematical functions involved the cryptosystems can be broadly classified into Number Theory based cryptosystem and Chaos and Fractals based Cryptosystems.

A. Number Theory Based Cryptosystem:

The number theory based cryptosystem includes the DES, AES, RSA, ECC algorithms [26].

B. Chaos and Fractal Based Cryptosystem:

The theory of chaos and fractals give us a very different perspective of seeing the world in a new chaotic way and not the Newton way and also not use the Euclidean geometry but use the fractal geometry [25]. A system is called chaotic if it's not possible to make long term predictions of the systems behavior. The properties of chaos include high sensitivity to initial conditions, mixing properties of confusion and diffusion as required by Shannon and long term system behavior unpredictability ergodicity.

Many cryptosystems based on Chaos and Fractals have been proposed in the recent years to include into symmetric and asymmetric (Public Key) Systems, due to its computational efficiency and ease with the public-private key pairs can be generated. [8] Proposed a public key encryption algorithm based on Chebyshev's chaotic maps.[6] Proposed the analysis of fractal structure for the information encrypting process.[9] Explored the relativity of Julia and Mandelbrot fractals and developed a new Public Key Cryptosystem. [10-22] study shows that many cryptosystems, encryption algorithms, key exchange protocols and digital signature algorithms have been proposed incorporating the chaos and fractals.

C. Advantages, Shortcomings and Differences

The advantages of the Chaos and Fractal based cryptosystems include,

1) Complexity of these systems is due to extreme sensitivity to initial condition and no closed form of solutions exists. This type of problems in cryptography is considered to be very hard. This eliminates one of the fundamental drawbacks of the Number Theory Based Cryptosystem.
2) Some Fractal and Chaos equations values grow very rapidly and hence very secure against attacks.

3) The system leads to same set of values with the same function and initial condition, hence said to be deterministic in nature.
4) The system s ergodic in nature and hence robust against statistical attacks.

The shortcomings of the Chaos and Fractal based cryptosystems include,

1) Key exchange must be handled by specialized protocol for symmetric keys.
2) use of floating point arithmetic makes the system slower than that of integer arithmetic.
3) Inefficient to encrypt long messages as the chaos mappings can repeat and go into an orbit for various initial conditions.

The differences between both the cryptosystems include,

Number Theory Based Cryptosystem	**Chaos and Fractal Based Cryptosystem**
Based on Integers	Based on Real Numbers
Used algebraic methods based on rounds	Use analytical method based on iterations
Confusion	Ergodicity
Diffusion	Sensitive to initial Condition
Statistical analysis is applicable	Statistical analysis is not applicable
Known attacks possible	Known attacks not possible.

Table 1: Cryptosystems

III. Performance Analysis

The main purpose of this study is to analyze which cryptosystem performs better. The Chaos and Fractal based cryptosystem seems to be more advantages than that of the number theory based cryptosystem due to key space which helps it to withstand some of the known attacks of Number Theory cryptosystems. The mathematical functions involved Chaos and Fractal based cryptosystem are very complex in nature, they are considered as time consuming to be involved in solving nonlinear system numerically over the definite infinite subfield.

Attackers attempt to break the cryptosystems by using different keys on the messages, investigating the difference between the cipher text and the plaintext. Such attacks can be countered if the *key sensitivity is high*: small change in the decryption key should lead to greatly different plaintexts.

In this performance analysis we consider RSA algorithm based on Number theory and Fractal based Algorithms. We perform evaluation on various parameters such as the Key Space and Key Size.

From the fig 1 and 2 it can be concluded that the fractal based cryptosystems have better performance as compared to other cryptosystems as the time needed for decimal number calculation is less than the time needed for integers as they involve discrete log and factorization operations.

Due to the fast execution and small key size, fractal based scheme is more efficient than other scheme. For any chosen number of bits (n), the fractal key space includes 2^n possible key values, but in RSA the possible key is limited to the number of primes.

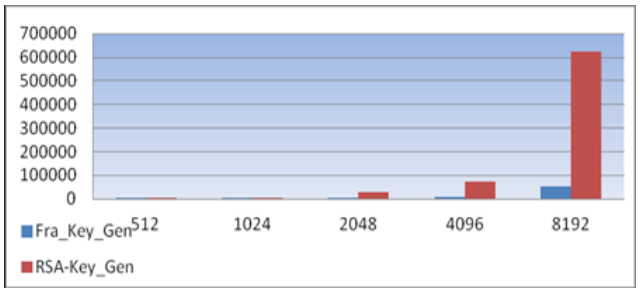

Fig. 1: Fractal and RSA Key Generation Time

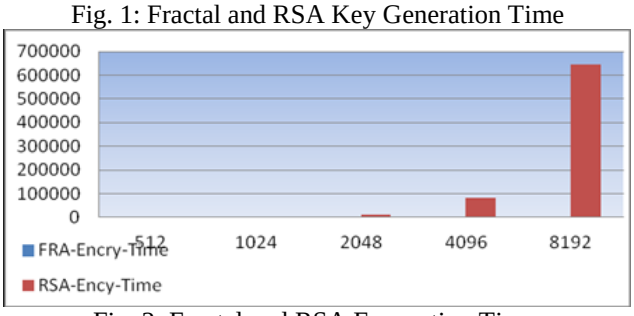

Fig. 2: Fractal and RSA Encryption Time.

The basic requirement of cryptosystems is ease of implementation, Key management and highly secure. It is observed from above facts that fractals and chaos can be applied to cryptographic techniques making the system most secure against attacks.

IV. Application of Chaos Fractal Based Cryptography to Wireless Sensor Networks

Much of research is being done to propose novel techniques to secure WSN as they are deployed in hostile environment. Initially it was assumed that security algorithms based on secret key were only applicable to the WSN nodes due to Static, Homogenous and required less computation. Later it was shown in [26] that PKC based RSA algorithm was found to be more efficient and applicable than the secret key algorithms.

V. Conclusion

Application of security techniques based on Chaos and Fractals is first of its kind in the field of WSN, and expected to revolutionize the field of Sensor Networks. Chaos and Fractals Cryptography have been used in Image encryption and Decryption. From the above analysis, we can exploit the features of Chaos Fractal Based cryptosystems to secure WSN. In this paper we have shown those fractals are more secure and efficient than that of RSA based techniques widely used in WSN.

References

[1] W. Stalling. Cryptography and Network Security, PHI, 2004
[2] A. MS. Public key cryptography: Applications, Algorithms and Mathematical Explanation, India, Tata Elexi-2007
[3] Diffie W. and M.E. Hellman, New directions in cryptography, IEEE transactions on information theory, IT-22(1976), 644-654.
[4] Neal Koblitz, A course in number theory and cryptography, 2nd edition, springer, pp 235, 1994.

[5] P. R. Massopust, "Fractal functions and their applications," Chaos Solitons and Fractal 8(2): 171-190, 1997.
[6] I. Motyl, R. Jasek and P. Varacha, Analysis of the fractal structure for the information encrypting process, International Journal of Computers, 6(2012), 224-231
[7] B. B. Mandelbrot, Fractal geometry of nature, San Francisco: W. H. Freeman, 1983.
[8] L.Kocarev, M. Sterjev , A. Fekete , G.Vattay , Public-Key Encryption with Chaos, Chaos, Dec; 14(4): 1078-82. 2003
[9] A. Mohammed, A. Samsudin, A New Approach to Public-Key Cryptosystem Based on Mandelbrot and Julia, Ph.D. thesis, Universiti Sains, Malaysia. 2008.
[10] A. Jacquin. An introduction to fractals and their applications in electrical engineering. Journal of the Franklin Institute. 331(6): 659-680, 1994.
[11] V. Rozouvan. Modulo image encryption with fractal keys. Optics and Lasers in Engineering. 47(1): 1-6, 2009.
[12] X. Di,X. Liao,S. Deng, A novel key agreement protocol based on chaotic maps, Information Sciences 177,1136-1142, 2007.
[13] A. Mohammed, A. Samsudin, A New Public Key Cryptosystem Based on Mandelbrot and Julia Fractal Sets, Asian journal of information technology, 6(5): 567-575. 2007.
[14] T.Xiang, K.Wo Wong, X.Liao, "On the security of a novel key agreement protocol based on chaotic maps,"Chaos, Solitons and Fractals. 40, 672-675. 2009.
[15] A. Mohammed, A. Samsudin, Generalized scheme for fractal based digital signature, IJCSNS, vol.7, No. 7, July 2007.
[16] Nadia M. G. Al-Saidi, Mohamed Rushdan Md. Said, Mathematicalchallenges in information age, Math digest,3(1) 2010.
[17] A. Mohammed, A. Samsudin. Fractal (Mandelbrot and Julia) Zero- Knowledge Proof of Identity. Journal of Computer Science 4 (5): 408-414, 2008.
[18] N. AL-Sa'idi, Md. R. Muhammad Said, Improved Digital Signature Protocol Using Iterated Function Systems, International Journal of Computer Mathematics, 88(17): 3613-3625, 2011.
[19] N. AL-Sa'idi, Md. R. Muhammad Said A. M. Ahmed New Direction in Public Key Systems using Iterated Function System. Journal of Computer Science 7 (4): 526-532, 2011
[20] N. AL-Sa'idi, Md. R. Muhammad Said, A new approach in cryptographic systems using fractal image coding. Journal of Mathematics and Statistics 5 (3): 183-189, 2009.
[21] N. AL-Sa'idi, Md. R. Muhammad Said, A New Idea in Zero Knowledge Protocols Based on Iterated Function Systems, World Applied Sciences Journal, 15(3): 364-371, 2011.
[22] S. Kumar, Public key cryptography system using Mandelbrot sets Military Communications Conference, MILCOM 2006. IEEE. 23-25 Oct., 2006.
[23] Gourishankar S et al, "Issues in Wireless Sensor Network", Proceedings in the World Congress on Engineering (2008), vol. I, July 2-4, 2008.
[24] Dr. Manoj Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges", IJCIT, vol. 2, issue 1, pp. 62- 67, 2011.
[25] Q.V. Lawande, B. R. Ivan and S. D. Dhodapkar. Chaos based cryptography: a new approach to secure communications. BARC NEWSLETTER, NUMB 258: 1-11, 2005.
[26] Amin et al," Analysis of PKC for WSN Security", World Academy of Science, Engineering and Technology. International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:2, No:5, 2008.

