ISSN (Online) : 0974-5645
ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(3), 216–221, February 2015* DOI : 10.17485/ijst/2015/v8i3/59585

A Survey on Cryptography using Optimization algorithms in WSNs

Swapna B. Sasi[1,2*] and N. Sivanandam[3]

[1]Department of CSE, Karpagam University, Coimbatore, India; swapna@jecc.ac.in
[2]Department of CSE, Jyothi Engineering College, Thrissur, Kerela, India
[3]Department of CSE, Karpagam College of Engineering, Coimbatore, India

Abstract

Objective: The main intent of this research is to provide the secure communication in the wireless sensor networks. For that, several cryptography using optimization algorithms is investigated. **Methods:** In this manuscript, a survey has been made on the cryptography using optimization methods for secure communication. Several optimization algorithms are presented for cryptography to create the keys for the encryption. One of the suggested techniques is ant Colony Optimization Key Generation based image encryption method that is used to create the keys for encryption of text. The ant colony optimization method is used to generate the keys for encryption. **Results:** This survey comprehensively studies the issues in the cryptographic optimization methods for providing security in the wireless sensor networks. The performance of the different methods is compared with various parameters such as maximum number of keys stored, battery capacity, and runtime. The maximum number of keys store in the Ant Colony Optimization based key generation is 52, for Novel stream cipher cryptosystem 256, for fast and secure stream cipher 256, and also for RC4 256 keys. **Conclusion:** This survey investigates the several cryptographic optimization methods and provides the idea for efficient methods for future work.

Keywords: Cryptography, Encryption Algorithms, Information Security, Optimization Methods, Wireless Sensor Networks

1. Introduction

Secure communication in wireless sensor network is an important concern. In order to provide secure data communication in the wireless sensor networks, cryptographic techniques are used. Key plays a vital role in Symmetric key encryption method. The size of the key is very significant in the symmetric key encryption. There are various examples of cryptographic algorithms[1] such as RC2, DES, 3DES, RC6, Blowfish and AES. RC2 and DES use one 64-bit key.

Various cryptographic methods using the optimization methods are suggested in this survey. The performance of the numerous optimization algorithms used in cryptographic techniques is also analyzed. Some of the suggested methods include Ant Colony Optimization based Cryptographic techniques, Genetic algorithm based key exchange, Binary Particle Swarm Optimization for cipher method etc.

The remainder of this survey is organized as follows: Section 2 describes the security objectives and challenges in the wireless sensor networks. Section 3 presents the various cryptography using optimization methods and analyzes the comparison the performance. Section 4 gives the conclusion of this survey.

2. Security Objectives and Challenges

Each and every security system presents a collection of security functions which guarantees the secrecy of the system[2]. The functions are generally referred as the objectives of the security system. To consider the security in the wireless sensor networks, some of the security services are mainly focused to accomplish the problem:

**Author for correspondence*

2.1 Confidentiality

Confidentiality is also called as secrecy which is used to make the information unapproachable to unlawful users[3]. A confidential message is challenging to exposing its meaning to an eavesdropper.

2.2 Service Reliability

The secure systems generally get intruded by adversaries in which influence the availability and type of service to their users. This type of systems provides a way to grant their users the quality of service they expect.

2.3 Integrity

This security factor makes sure that the received data is not modified in transit by an attacker. It verifies the content of the communicated data is ensured to be free from any type of alteration between the end points[4]. The essential form of integrity is packet checksum in IPv4 packets.

2.4 Authentication

Authentication is a significant security factor which verifies the receiver and sender identity before the sender and receiver communicates.

2.5 Non-Repudiation

This factor indicates that neither the sender nor the receiver can incorrectly reject that they have sent a certain message.

2.6 Authorization

These metric guarantees that only certified users can be accessed to network services or resources.

Furthermore, suppose new sensors are deployed in the wireless sensor network and old sensors are working to defect regularly. In order to provide security the following forward and backward secrecy are also imperative to security:

2.7 Forward Secrecy

Forward secrecy is nothing but a sensor should be not permitted to know the future messages after it leaves from the network.

2.8 Backward Secrecy

Backward secrecy is nothing but newly entering sensor should not be capable to know the formerly transmitted message.

To accomplish the objectives of the security system, the encryption methods are suggested which provides adequate strength with high security. Also, the optimization algorithms are used in the cryptographic methods to analyze how the performance in terms of security is improved.

The survey is conducted[5] for various popular secret key methods like DES, 3DES, AES, and Blowfish. The performance of the methods was evaluated by encrypting input files of modifying contents and sizes on two dissimilar hardware platforms.

3. Different Cryptographic Methods using Optimization Algorithms

3.1 Vernam Cipher Method

In [6] Pfleeger Charles suggested Vernam Cipher method which is considered as a perfect cipher and a category of a one-time pad cipher. Here keys are generated by utilizing the random stream generator. The receiver requires the similar group of keys as the sender to decrypt the image. Long non-repeating sequences of arbitrary numbers representing the keys are integrated with the bits which denote the binary image. The encrypted image is the XOR function of the bits illustrating the binary image with the corresponding stream of arbitrary numbers. The main disadvantage of this method is it requires the limitless number of keys and the dissemination of a large number of arbitrary keys causes a problem. Also, another drawback is if the arbitrary number sequence is found, then the keys used for encryption can be traced effortlessly.

3.2 Stream Cipher Cryptosystem

Martin del Rey[7] has proposed a novel cryptosystem for encrypting binary images. According to this approach, a stream cipher cryptosystem is used whose cryptographic secure pseudorandom bit generator is a hybrid boolean cellular automaton. The drawback is that the secret key of the cryptosystem is formed by 256 cells, which have to be sent to the receiver. Also the characteristic vector distributed to the receiver has 256 cells.

3.3 Fast and Secure Stream Cipher

In [8]Biham and Seberry presented a fast and secure stream cipher which is called Rolling Arrays. This method contains variable rotations and permutations. The security declares of the cipher are that no key revival attacks can be carried out with less difficulty than that of comprehensive exploration, and discriminating attacks are also not practical with a analogous difficulty. When compared to the RC4 algorithm, the speed of the cipher is imposingly fast. The disadvantage is that total of 256 keys has to be accumulated for initial permutation. The maximum internal state memory is 4164 bytes. The key stream created does not depend on the plain text to be encrypted. Also the plain text is not encoded.

3.4 RC4 Stream Cipher

Kim et al. suggested an effectual RC4 stream cipher method[9] which is called key-pooled RC4 for secure transmission of multimedia files in the wireless mobile network. In this technique, a 1MB-sized key stream pool is taken which includes 048 or 8192, or 32,768 key stream frames is generated exclusively for every client device in the registration step. This method is more time proficient when compared to the normal RC4 and more secure than normal RC4. The main disadvantage of this method is that the number of keys to be accumulated and disseminated is huge. Also the plain text is not encoded.

3.5 Swarm Intelligence Based Approach

In [10]Sreelaja and Vijayalakshmi Pai suggested a method which is called Swarm Intelligence [11]based approach for the purpose of text encryption. At this time, an autonomous agent is a subsystem which cooperates with its environment, which possibly consists of other agents, but acts comparatively independently from all other agents.

3.6 Ant Colony Optimization Key Generation Based Image Encryption Algorithm

In [12]recommended Ant Colony Optimization Key Generation Based Image Encryption (AKGBE) method which is used to create the keys for encryption of text. Ant system is a Swarm Intelligence method which is used to resolve the problem of optimization. Artificial Ants [13]have some distinctiveness which does not discover counterparts with real ants. They live in a discrete world and the movement consists of transitions from discrete state to discrete states. These ants have an internal state. The private state includes the memory of the ant agent's past action. They deposit a specific amount of pheromone, which is a function of the quality of the solution found. An Artificial Ant's timing in pheromone deposition is problem dependent and frequently does not reproduce real ant's performance. The main intent of this method is to create the key stream which is used for encryption based on the distribution of characters in the plain text denoting the binary image so that the keys in the key stream are encoded using a mutated character code table which would enable to increase the security of the system.

3.7 Binary Particle Swarm Optimization for Attacking Knapsack Cipher Algorithm

In [14]suggested a method which is called Binary Particle Swarm Optimization for Attacking Knapsacks Cipher Algorithm. The main idea of the Merkle-Hellman knapsack algorithm is to hide a binary message as a solution to knapsack problem. A block of plaintext equal in length to the number of items in the pile would choose the item in the knapsack and cipher text would be the resulting sum. Actually, there are two knapsack problems, one solvable in linear time and the other supposed not to be. There are some modifications done in the easy knapsack to generate the hard knapsack. The public key is the hard knapsack, which can effortlessly be utilized to encrypt but cannot be used to decrypt messages. The private key is the easy knapsack, which gives a simple mode to decrypt the message.

3.8 End-to-End Security Mechanism by using Genetic Algorithm

In [1]presented the end-to-end security approach by utilizing certificate authority et servers for giving digital certificates for particular preferred client nodes by using Threshold Cryptography and Diffie Hellman Key exchange method. Because of the random movement of the mobile nodes and dynamic topology of the network leads to failure of the links. Due to the failure of links, it modifies the network size and also it provides opportunity for the adversaries to enter into the network, which is an important concern. Detection of such unauthorized users necessitates secure key exchange mechanism with the certificate authority node. A genetic algorithm is used for providing a robust security. The combination of genetic algorithm in the secure key exchange mechanism makes the security in an efficient manner to authenticate the client nodes entering into the network.

3.9 Data Encryption Standard (DES)

In [16]presented the Data Encryption Standard (DES) which is a major symmetric-key algorithm for the purpose of encryption. It is a 64-bit block cipher under 56-bit key. The algorithm processes with an initial permutation, sixteen circles block cipher and a final permutation. DES application is very popular in commercial, military, and other domains in the last decades.

3.10 Blowfish Encryption Algorithm

In [16]suggested Blowfish Encryption Algorithm which is a symmetric-key block cipher and comprises of the huge number of cipher suites and encryption products. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. The two parts of this algorithm are: one is key-expansion part and another one are data-encryption part. The main function of the key expansion part is to modify the key of at most 448 bits into a number of sub-key arrays totaling 4168 bytes. The encryption of data happens through 16-round. Each and every round includes a key-dependent permutation, and also a key- and data-dependent substitution. The functions in this algorithm are XORs and additions in 32-bit words.

3.11 Genetic Algorithm to Break a Mono - Alphabetic Substitution Cipher

In [17]presented a genetic algorithm to break a Mono - Alphabetic Substitution Cipher. The main work is to be concentrated on substitution cipher. The principles used in this cipher structure the basis for a lot of the modern cryptosystems. The frequency analysis is used as an important metric in the objective function. The input of this algorithm is the cipher text and the relative character frequencies. The parameter used in this algorithm is the maximum number of generations. After that generate the population keys randomly. Decrypt the cipher text by the generated keys.

3.12 Cryptanalysis of Four-Rounded DES uses Ant Colony Algorithm

In [18]presented a technique which is called as four-rounded Data Encryption method based on Ant Colony Optimization. Ant Colony optimization is a probabilistic technique for resolving computational tribulations which can be diminished to identifying good paths through graphs. The major idea of the ACO is to utilize the repeated artificial ants to create new solutions to the problem at hand. The ants utilize the information which was gathered in the past to direct their search, and this information is accessible and adapted through the environment. To restore the secret key of the DES cipher, a known plaintext attack is used. The directed graph is constructed for the ants which are called as search space is created for proficient searching of the secret key. Also, to develop a heuristic function that evaluates the quality of a created solution. Numerous optimum keys are calculated over dissimilar runs on the basis of routes finished by the ants. These optimum keys are used to recognize every individual bit of the 56 bit secret key which is utilized by DES.

3.13 Network Security Using Genetic Algorithm

In [19]presented network security by using genetic algorithm. The main intent of this work is to send a message in a secure manner to the receiver. So, the third person does not change the original information because they have a cipher text so that the third person cannot understand what it essentially is. This method gives some facilities to sender who enters a complete message and can encode the message by utilizing crossover & mutation of genetic algorithm. This algorithm assists the user and generates new cipher text every time. Receiver on the other hand, will receive the message in the encoded cipher text form and will recover the original message by mapping the cipher text in the decryption algorithm.

3.14 Symmetric Key Encryption Technique Using Genetic Algorithm

In [20]presented Symmetric Key Encryption Technique Using Genetic Algorithm. In this technique, a Genetic Algorithm (GA) is presented according to the symmetric key cryptosystem for encryption and decryption. In this method, the plain text and the user input are transformed into a text matrix and a key matrix correspondingly. By adding the text matrix and key matrix, an additive matrix is created. In the additive matrix, a linear substitution function is pertained to create the intermediate cipher. After that the genetic functions are used in the intermediate cipher to create the final cipher text. This method has two basic steps, substitution followed by genetic crossover and mutation.

3.15 Particle Swarm Optimization in Cryptanalysis of DES

In [21]suggested Particle Swarm Optimization which is used in the cryptanalysis of DES based on their capability to selectively discover the solution space of a given problem. Particle swarm optimization is used to identify the plain text from cipher text. This algorithm is initialized with a population of arbitrary solutions in the search space and searches for optimum solution by regulating potential solutions over generations. The optimized solution will be attained by utilizing the Particle Swarm Optimization. In this algorithm, there are two particles which are called particle best and global best. By utilizing these, the optimized solution will be attained by identifying the least error rate. In the entire particles, the best the error rate will be computed by comparing the generated cipher text. If the error rate will be higher the value of the original text will remain other wise it will be restored

4. Performance Evaluation

In this section, different schemes are compared with the different parameters such as maximum number of keys stored, battery capacity, and runtime. Figure 1. Shows that the maximum number of keys stored is compared for the Ant Colony Optimization based key generation, Novel stream cipher cryptosystem, fast and secure stream cipher, RC4. The maximum number of keys stored in Ant Colony Optimization based key generation is 52, for Novel stream cipher cryptosystem 256, for fast and secure stream cipher 256, and also for RC4 256 keys. In this section, different schemes are compared with the different parameters such as maximum number of keys stored, battery capacity, and runtime.

Table 1. Comparison of Different Cryptographic Methods

Methods	Maximum number of keys stored	Maximum number of keys in the key stream	Maximum internal state memory	Runtime (s)	Remained Battery (%)
AKGBE	52	26	534 bits	Nil	Nil
Novel stream cipher cryptosystem	256	Nil	4164 bytes	Nil	Nil
Fast and secure stream cipher	256	Nil	Nil	Nil	Nil
RC4	256	Nil	Nil	Nil	Nil
DES	Nil	Nil	Nil	2187.50	65%
Blowfish	Nil	Nil	Nil	1696.68	85%

Figure 1. Shows that the maximum number of keys stored is compared for the Ant Colony Optimization based key generation, Novel stream cipher cryptosystem, fast and secure stream cipher, RC4. The maximum number of keys stored in Ant Colony Optimization based key generation is 52, for Novel stream cipher cryptosystem 256, for fast and secure stream cipher 256, and also for RC4 256 keys.

Figure 2. Compares the Battery Capacity for Data Encryption Standard (DES) and Blowfish algorithm. Battery capacity is nothing but the remaining battery level. Battery capacity is represented in percentage. The Battery capacity of the Data Encryption Standard (DES) is 65% and for the Blowfish algorithm is 85%.

Figure 3. Compares the runtime for Data Encryption Standard (DES) and Blowfish algorithm. Runtime is represented in seconds. The runtime for the Data Encryption Standard (DES) is 2187.50 seconds and for the Blowfish algorithm is 1696.68 seconds.

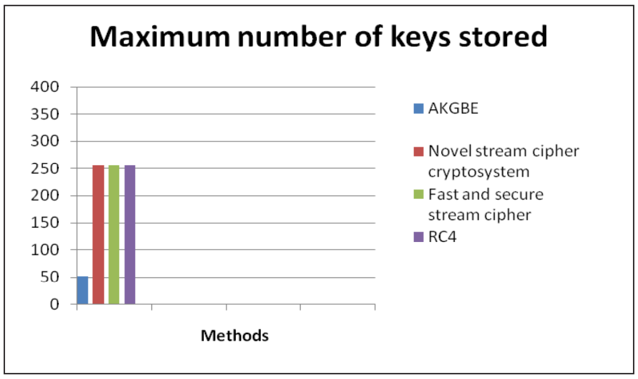

Figure 1. Comparison of Maximum number of keys stored.

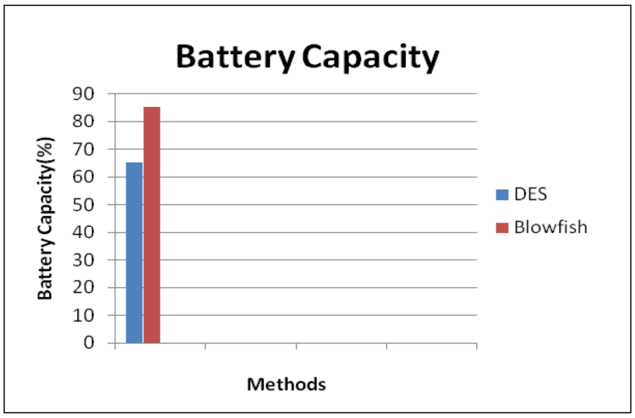

Figure 2. Battery Capacity.

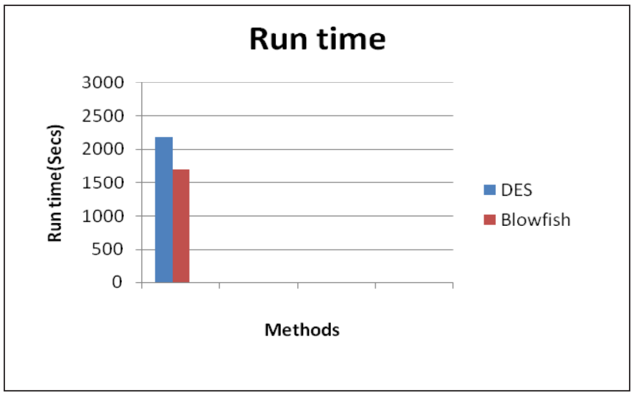

Figure 3. Runtime.

5. Conclusion

Some of the security issues in the wireless sensor network are addressed and the techniques to overcome them are surveyed. While some of the techniques utilized conventional cryptographic methods and others utilized optimization techniques for the cryptography. These various ideas using the optimization methods have been brought out in this paper keeping the advantages and limitations. This survey brings several ideas regarding to the various cryptographic optimization methods and conclude that high storage and high energy is required for storing the keys. So, in the future work a new symmetric system need to be developed for reducing the key size. The other area of interest is the energy consumption and delay caused by the execution time when used in the context of a dynamic security architecture in a wireless sensor network.

6. References

1. Coppersmith D. The Data Encryption Standard (DES) and its strength against attacks. IBM Journal of Research and Development. 1994 May; 38(3):243–50.
2. Earle AE. Wireless Security Handbook. Boston, MA. Auerbach Publications; 2005.
3. Tanenbaum AS. Computer Networks. 4th ed. NJ: Prentice Hall; 2003.
4. Stallings W. Cryptography and Network Security- Principles and Practices. 3rd ed. Upper Saddle River, NJ: Prentice Hall; 2003.
5. Nadeem A, Javed MY. A performance comparison of Data Encryption Algorithms. 2005 IEEE First International Conference on Information and Communication Technologies (ICICT 2005); 2006 Feb. p. 84–9.
6. Charles P, Shari LP, Security in Computing. 3rd ed. Prentice Hall of India; 2003.
7. del Rey AM, A Novel cryptosystem for binary images. International Journal of Studies in Informatics and Control. 2004 Mar. 13(1):5–14.
8. Biham E, Seberry J, Py (Roo): a fast and secure stream cipher. Research Online; 2005.
9. Kim HG, Han JK, Cho S. An efficient implementation of RC4 cipher for encrypting multimedia files on mobile devices. SAC 07 Proceedings of the ACM Symposium on Applied Computing; 2007. p. 1171–5.
10. Sreelaja NK, Pai GAV. Swarm intelligence based key generation for stream cipher,. International Journal of Security and Communication Networks. 2009 Aug; 4:181–94.
11. Liu Y, Passino KM. Swarm Intelligence, Literature Overview, Department of Electrical Engineering. The Ohio State University; 2000 Mar.
12. Sreelajaa NK, Paib GAV. Stream cipher for binary image encryption using Ant Colony Optimization based key generation. Journal of Applied Soft Computing. 2012; 12(9):2879–95.
13. Padhy NP. Artificial Intelligence and Intelligent Systems. Oxford University press; 2005.
14. AbdulHalim MF, Hameed SM. Binary particle swarm optimization for attacking knapsacks cipher algorithm. Proceedings of the International Conference on Computer and Communication Engineering; 2008. p. 77–81.
15. Sahoo D, Rai SC, Pradhan S. Threshold cryptography & genetic algorithm based secure key exchange for mobile hosts. IEEE International on Advance Computing. 2009. p. 1297–1302.
16. Nie T, Zhang T. A study of DES and blowfish encryption algorithm. TENCON Proceedings in IEEE Region 10 Conference. 2009. p. 1-4.
17. Omran SS, Al-Khalid AS, Al-Saady DM. Using Genetic Algorithm to break a mono - alphabetic substitution cipher. IEEE Conference on Open Systems (ICOS). 2010. p. 63–7.
18. Khan S, Shahzad W, Khan FA. Cryptanalysis of four-rounded DES using Ant Colony Optimization. International Conference on Information Science and Applications (ICISA). 2010. p. 1–7.
19. Dutt I, Paul S. Chaudhuri SN. Implementation of network security using genetic algorithm. Int J Adv Res Comput Sci Software Eng. 2013; 3(2):234–41.
20. Sindhuja K, Devi PS. A symmetric key encryption technique using genetic algorithm. Int J Comput Sci Inform Tech. 2014; 5(1):414–6.
21. Pandey S, Mishra M. Particle swarm optimization in cryptanalysis of DES. International Journal of Advanced Research in Computer Engineering and Technology. 2012; 1(4):379–81.