Volume 4, Issue V, May 2016
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

ANALYSIS OF VARIOUS CRYPTOGRAPHIC ALGORITHMS FOR SECURITY IN WIRELESS SENSOR NETWORKS

Rajat Soni[1], Deepak Sethi[2], Partha Pratim Bhattacharaya[3]

[1]Mody University, College of Engineering,
Lakshmangarh, India.
rajatsonidss@gmail.com
[2]Mody University, College of Engineering,
Lakshmangarh, India.
deepaksethi@live.in
[3]Mody University, College of Engineering,
Lakshmangarh, India.
hereispartha@gmail.com

Abstract: *A wireless sensor network is a group of dedicated nodes with a computational unit, transceiver and transducer which intends to work in a cooperative manner to achieve a goal in a monitored environment. These networks work for many applications and all of them require some level of security and privacy of the data which make the network worth its implementation. Cryptography is an approach to provide authentication and security to the data provided to the user by the sensor network. In this paper we have studied various cryptographic algorithms for wireless sensor networks like DES, RSA and blowfish. Then the algorithms are simulated and the performance is analyzed on the basis of and time and memory required for their encryption and throughput.*
Keywords: *Wireless Sensor Network, Security, Cryptography, Security Algorithms.*

1. INTRODUCTION

A sensor network is a collection of miniature sensing and signal processing devices working for some specific application [1]. They are low in power and computational strength as compared to other wireless networks. They are used to provide some desired information to the user via the base station. The basic components of any sensor networks are a collection of discrete sensor nodes; a wireless network; a base station (Sink); a set of computational units at the base station (or beyond) to deduce and analyses the received information from the nodes; at times the computing is done by the network itself [2]. The security protocol selection is important issue for the efficient delivery of the packets to their destination with authenticity of the data [2]. Mostly the applied security strategy should ensure the minimum of the energy consumption. Initially WSNs was mainly used by military applications. But nowadays the civilian application of wireless sensor networks has been considered, such as environmental and wildlife monitoring, production, healthcare, smart home [3]. These WSNs may consist of heterogeneous and sensor nodes with mobility, the network topology may be as simple but the scale and density of a network varies depending on the application requirement.

The security in WSNs is to protect the information and resources from attacks and adversity [4]. The security goals encompass both those of the traditional networks and goals suited to the unique constraints of sensor networks. The security requirements include:

A. *Availability:* At the time of attack communication should be available to the sink or base station.

B. *Authorization*: The sensors authorized at network establishment or by base station should be transmitting information to network or the base station [4].

C. *Authentication:* Data communication process in the network should not be encouraged by any misguidance or data tempering done by malicious node/attackers.

D. *Confidentiality:* The communicated data/ message should be decrypted or decoded by the desired node.

E. *Integrity*: The message sent from one node to another should not be tempered or corrupted by malicious nodes or the outside attacker [5].

To provide security, sensor network has many challenges like the channel is open to all, due to lack of energy and constrained resources strong security algorithms cannot be implemented, cost increases as the level of security increases [5]. Due to deployment of network in hostile environment any changes from design aspect cannot be done [4].

2. ATTACKS IN SENSOR NETWORKS

The motive of deploying a sensor network is to get some valuable information. There should not be any alteration in that information by any intruder. Due to the fact that individual sensor nodes are deployed in an isolated environment and they are covert and that communication among sensors is via wireless links, sensor networks are highly vulnerable to security attacks. Thus, these attacks are a major issue that must be resolved in order for the potential of wireless sensor networks to be fully exploited. Some of these attacks are:

1. Physical Attacks

These are attacks where physical destruction, relocation, theft and other related activity could either damage or make a sensor inoperable. In the case of theft, an attacker can learn crucial security information as well as the electronics involved from the sensor itself. The sensor may possess a private or public key, which the intruder can acquire by debriefing the captured node [5].

2. Denial of Service (DoS) Attacks

In these types of attacks, the physical layer effected by deliberate or unintended radio signals. These can either slow a network or make it ineffectual. At the network level and above, there can be an outburst of packets being phony and thus making the nodes spend time handling these packets instead of the real packets and thus decelerating the network [5].

3. Wormhole Attacks

This type of attack is a passive attack and it only takes place near the wormhole or carefully situated trespasser. The attacker archives packets at one place in the network and under passes them to another location so that these messages are replayed. In order to detect a wormhole attack, a distributed algorithm is used, in which each beacon node acts as a detector, each sensor participates in hop counting, while the base station controls the start and end of the detecting process and attempts to locate the intruder based on alarm messages received by nodes near the proximity of the wormhole [5, 6].

4. Sybil attack

When an insecure node is stolen to claim clone identities and act maliciously, by either stealing or corrupting information or disrupting communication these type of attack are known as Sybil attacks [6]. Sybil attacks disrupt and manipulate the reliable mechanism of peer-to-peer network. Easily change the overall popularity of an option by providing plenty of false praise, or bad-mouthing [5].

Other types of attacks include Selective forwarding, Sinkhole attacks, Hello flood attacks and Acknowledgement spoofing. Although, here all attacks are not covered, but this gives us a fair idea about type of threats. This information would help when implementing security in a wireless sensor network [5].

3. CRYPTOGRAPHIC ALGORITHMS

Generally, the study of secrets is called Cryptography but in communication it refers to encrypt the data by manipulating it to convert it into a secret or cipher to secure it from possible threats [6]. This process has counterpart where cipher text is decrypted on the other receiver end to acquire the original data. For implementing a cryptographic technique in Wireless Sensor Networks it should follow the limitations of these networks like computational capability, battery power and memory space.

Private Key Cryptography

In this type of cryptography same key is used for the encryption and decryption of data. They use permutation and substitution for the encryption and repeat the same process in reverse for decryption [6]. They are also known as symmetric key encryption. Some examples of private key cryptography are DES, AES and Blowfish.

Public Key Cryptography

In this type of public key cryptography two keys are used for communication one is public key which is common to all devices taking part in the communication and a private key which is known to the devices which are communicating actively. They are also known as asymmetric key encryption. Some of the examples are RSA, ECC and ElGamal.

Data Encryption Standard (DES)

DES is one of the universally recognized cryptographic algorithms. It was developed by Horst Feistel at IBM in the 1970s but was later accepted by the National Institute of Standards and Technology (NIST). This algorithm is designed to encrypt a block of 64 bits data using a key whose length is 64 bit. It is a symmetric algorithm so it uses the same key for decryption [6].

Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits [6]. The algorithm goes through 16 iterations that interlace blocks of plaintext with values obtained from the key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key are used for decryption. There are many attacks and methods recorded till now those exploit the weaknesses of DES, which made it an insecure block cipher. Despite the growing concerns about its vulnerability, DES is still widely used by financial services and other industries worldwide to protect sensitive on-line applications [3, 16]. The flow of DES Encryption algorithm is shown in Figure 3. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation (i.e. reverse initial permutation).

Rivest-Shamir-Adleman (RSA)

RSA was developed by Ron Rivest, Adi Shamir, and Leonard Adleman. It is one of the best known public key cryptography algorithms. It can encrypt variable length data and with variable key length. It is a block cipher system based on number theory. It is used for digital signatures and data encryption. It uses random prime numbers to create two keys used for encryption and decryption purpose. The public key is used to encrypt the data and the private key is used to decrypt the data. There are three steps in its operation; key generation, encryption and decryption [7].

There are many flaws in the design of RSA like when small values of prime numbers are used to generate the key it becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. For larger values of prime number, the computational time is very high which affects the efficiency of the algorithm. Further, the algorithm it also requires of similar lengths of the prime numbers which is practically very tough conditions to satisfy.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Figure 2 illustrates the sequence of events followed by RSA algorithm for the encryption of multiple blocks.

Key Generation Procedure [7]

1. Select two random prime numbers p & q such that $p \neq q$.
2. Let $n = p \times q$.
3. Compute: phi (n) = (p-1) (q-1).
4. Select an integer e such that $1<e<\text{phi}(n)$
5. Compute d to satisfy the congruence relation $d \times e = 1 \bmod \text{phi}(n)$; d is kept as private key exponent.
6. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

Encryption

Plaintext: $P < n$

Cipher text: $C = P^e \bmod n$.

Decryption

Ciphertext: C

Plaintext: $P = C^d \bmod n$.

Blowfish Algorithm

Blowfish is a symmetric encryption algorithm with variable length key of up to 448 bits. It encrypts block length of 64 bits at a time [10]. It is a feistel network in which same process is done for 16 rounds. Encryption is done in two parts key expansion and data encryption. In key expansion the key is converted into a group of sub keys. In data encryption the data is encrypted with the use of sub keys in 16 round feistel network. Every round consists of a key dependent variation, and a key and data dependent substitution. All operation is XORs and additions on 32-bit words after the complex initialization it is a fast and efficient algorithm.

Sub keys

Blowfish uses a large number of sub keys. These keys should be precompiled before any data encryption or decryption.

1. The P-array consists of 18 32-bit sub keys:
$P_1, P_2 \ldots P_{18}$.

2. There are four 32-bit S-boxes with 256entries each:
S1, 0, S1, 1... S1, 255;
S2, 0, S2, 1... S2, 255;
S3, 0, S3, 1... S3, 255;
S4, 0, S4, 1...S4, 255.

Encryption

1. Feistel network is of 16 rounds.
2. The input is a 64-bit data element, X.
3. Divide X into two 32-bit parts: X_L, X_R.
4. Then, for i = 1 to 16: $X_L = X_L$ XOR Pi $X_R = F$
5. Swap X_L and X_R
6. After the sixteenth round, swap X_L and X_R again to undo the last swap.
Then, $X_R = X_R$ XOR P17 and $X_L = X_L$ XOR P18.
7. Finally, recombine X_L and X_R to get the ciphertext.
8. Decryption is exactly the same as encryption, except that P1, P2... P18 are used in the reverse order.

The comparison of these cryptographic techniques is given in Table 1

Algorithm	Developed by	Key size	Block size	Rounds	Flexibility	Structure	Attacks found	Feature
DES	IBM	64 bits	64 bits	16	no	Feistel	Exclusive Key search, Linear cryptanalysis, Differential analysis	Simple but not enough structure
RSA	Rivest, Shamir, Adleman	1024-4096 bits	Variable block size	1	no	Public Key Algorithm	Brute force attack, timing attack	Excellent Security, low speed
Blowfish	Bruce Schneier	32-448 bits	64 bits	16	yes	Feistel	No attack is found to be successful against blowfish.	Excellent security, high speed

Table 1 Comparison of Various Cryptographic Techniques

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

S. No.	Algorithm used	Data	key	Encrypted data	Data decrypted
1	**Blowfish**	1110001100110011	1011	0000 0010 0101 0110 0101 0011 0000 1001 0000 0010 0001 1010 1101 1001 1110 1010	1110001100110011
2	**DES**	1110001100110011	1011	1011110000111111101001001110011 1010001001010010011100111110000 0101100000010011011011011000110 1011001000001000011111000110011 1110010100101111010001111011000 1100001101011011100001111010111 101000	1110001100110011
3	**RSA**	1110001100110011	7 103	201 201 201 148 148 148 201 201 148 148 201 201 148 148 201 201	1110001100110011

Table 2 Encrypted and Decrypted Data from Different Algorithm Implementation

4. SIMULATION AND RESULTS

In this paper we have analyzed three of the cryptographic algorithm. The simulations have been implemented using MATLAB R2013a for the performance evaluation of three cryptographic algorithms on the basis of encryption/decryption time, throughput and memory space required for encrypted data. Encryption and decryption 2 byte of binary data has been done. The plain data and encryption key used to analyze these algorithms are given in table 2.

- ***Simulation Parameters***

Encryption Time

The time required for transforming plaintext message to cipher text at the time of encryption is defined as Encryption Time

Decryption Time

The amount of time required for transforming the cipher text into the plain text at the time of decryption is defined as Decryption Time.

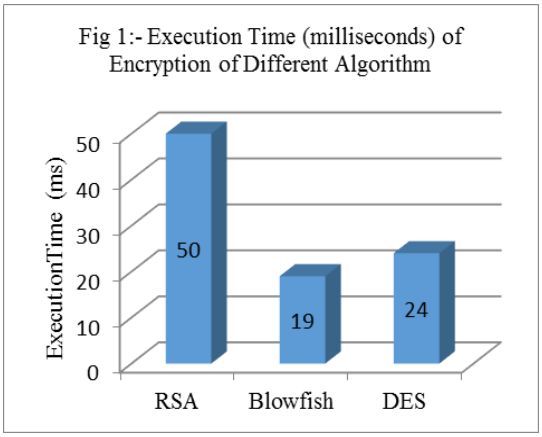
Throughput

The throughput of the cryptographic algorithm is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm i.e.

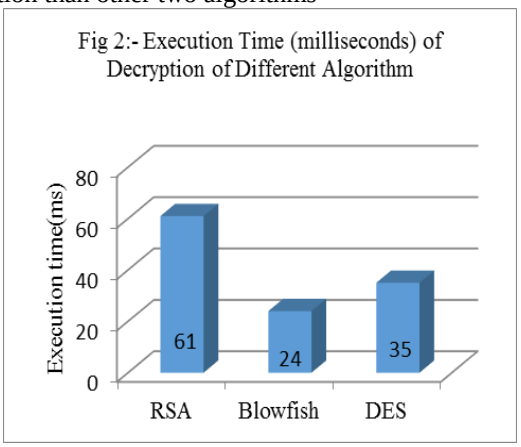
Throughput= Total Plaintext / Encryption Time

The higher the value of throughput more is the efficiency of encrypting any text with an encryption algorithm. All the results are acquired by the data given in table 2.

In fig 1 encryption time required by three algorithms is shown by which we can see that blowfish requires less time for encryption than other two algorithms.

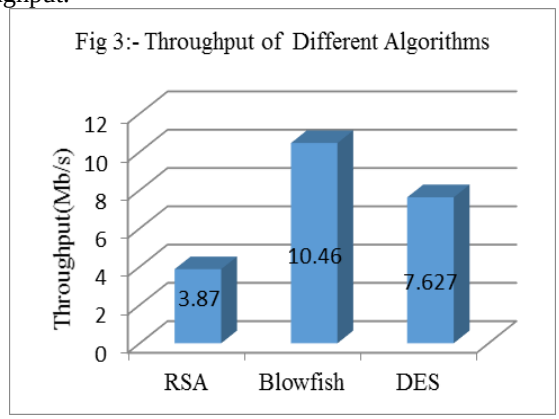


In fig 2 decryption time required by these algorithms is shown by this fig we can see that blowfish requires less time for decryption than other two algorithms



INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Fig 3 shows the throughput of these algorithms which RSA shows the least throughput and blowfish has highest throughput.



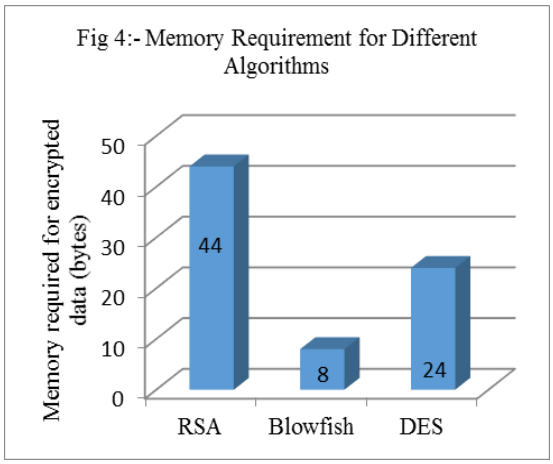


Figure 4 show the memory required for the encrypted data for the plain data of 2 bytes in these blowfish requires 8-byte memory space which is less than others.

5. CONCLUSION

In this paper the performance evaluation of different cryptographic algorithms like DES, Blowfish and RSA has been done on the basis of their memory, time requirement and throughput. From the simulation it is concluded that for Wireless Sensor Network blowfish algorithm is more suitable than others because it is simple, fast, require less memory space and delivers high throughput.

REFERENCES

[1] V. Katiyar, N. Chand and N. Chauhan, "Recent Advances and Future Trends in Wireless Sensor Networks," International Journal of Applied Engineering Research, Vol. 1, No 3, 2010, pp.330-342.

[2] I. F. Akykildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Communication Magazine, Vol. 40, No. 8, 2002, pp.102-114.

[3] T. Naeem and K. K. Loo, "Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks," International Journal of Digital Content Technology and its Applications, Vol. 3, No. 1, 2009, pp. 89-92.

[3] G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009, pp.315-321.

[5] S. K. Singh, M.P. Singh and D.K. Singh, "A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks," International Journal of Computer Trends and Technology, Vol. 1, No.2, 2011, pp. 9-17.

[6] M. Marine, C. Raphael and W. Phan,"Energy-Efficient Cryptographic Engineering Paradigm," Open Problems in Network Security.Springer, 2012, Vol.1, No.1, pp.78-88.

[7] A.S. Wander, N. Gura, H. Eberle, V. Gupta and S. C. Shantz,"Analysis of Public-Key Cryptography for Wireless Sensor Networks," Pervasive Computing and Communications, IEEE International Conference, Vol. 1, No. 2,2010, pp. 324-328.

[8] G. Guimaraes, E. Souto, D. Sadok and J. Kelner, "Evaluation of Security Mechanisms in Wireless Sensor Networks," IEEE Proceedings Systems Communications, Vol. 1, No. 1, 2005, pp. 428-433.

[9] B. Arazi, I. Elhanany, O. Arazi, and H. Qi, ",Revisiting Public-Key Cryptography for Wireless Sensor Networks," Computer Networks, Elsevier, Vol.38, No. 11, 2005, pp.103-105.

[10]G. Guimaraes, E. Souto, D. Sadok and J. Kelner, "Evaluation of Security Mechanisms in Wireless Sensor Networks," IEEE Proceedings Systems Communications, Vol. 1, No. 1, 2005, pp. 428-433.

[11] A. Kaur, "Energy Analysis of Wireless Sensor Networks using RSA and ECC Encryption Method," International Journal of Scientific & Engineering Research Vol.4, No.1, 2013, pp.2212-2216

[12] J. Thakur and N. Kumar,"DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." International journal of emerging technology and advanced engineering 1.2 (2011): 6-12.