International Journal of Advanced Science and Technology
Vol. 29, No. 8, (2020), pp.4142-4150

Crypto-Mechanism To Enhance The Data Security İn Wireless Sensor Networks

Parli B. Hari[1] , Dr. Sandhya Tarar[2], Dr. Shailendra Narayan Singh[3]
[1]*Research Scholar, Dept of CSE, ASET, Amity University, Noida (UP) INDIA*
[1]*pbhari@gmail.com*
[2]*Assistant Professor, School of ICT, GBU, Greater Noida (UP) INDIA*
[3]*Professor, Dept of CSE, ASET, Amity University, Noida (UP) INDIA*

Abstract

In the recent research under the field of wireless sensor networks has led to a number of security schemes to secure the data of the sensor nodes. As we know that the resource constrained is big problem so we need efficient security in WSNs. WSNs have thousands of potential applications in various fields and activities because a WSN has a distributed communicable nodes over an area to receive and transmit the data freely in secure way and send it to the connected base station that is connected to the Internet or satellite. Since the wireless sensor networks nodes are with various constraints like as restricted battery life, limited operations of sensor's computation and the small memory size. We proposed the various appropriate algorithms that provide the battery energy for minimal key sizes, fast transmission of data, reducing the computational power, minimum size of storage, low bandwidth rate consumption. The proposed algorithm is best to secure data transmission in wireless sensor networks

Keywords: *Algorithms, Security, Cryptography, security analysis and Wireless Sensor Networks*

1 Introduction:

A WSNs also known as the network of many sensor nodes those are connected via any topology and every node can sense the data and control the surroundings of the network field. Each connected sensor node sense the data and send it to the gateway via wireless medium. Since the wireless sensor nodes are with various constraints like as restricted battery life, limited operations of sensor's computation (CPU) and the small memory size [1]. With rising concerns in regards to the wireless networking and security of information the noticeable security calculations particularly symmetric calculations can be generally utilized in WSNs applications administrations which include encryption systems. Cryptography is a procedure which is being utilized in putting away private data in a cryptographic structure with the goal that lone those whom it is wanted can understand it and can convey data within the sight of adversary. The security calculations limit security issues by utilization of cryptography, verification and circulation of key safely, it is in this way the study of creating message safely modifying the information. The cryptography algorithm can resolve the issues in regards to WSNs end node data security, record framework and gateway security [2]. The concept about sensor node and wireless sensor network is shown in figure1.

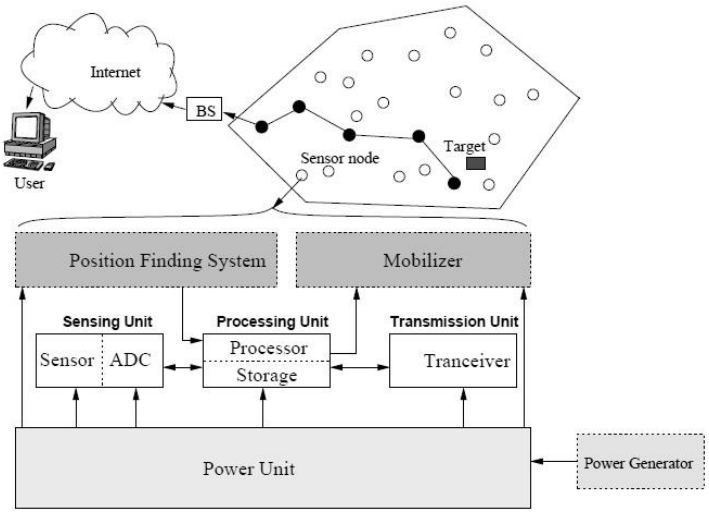

Figure1. (Wireless Sensor Network)

Encryption is the major device for ensuring touchy data. The primary motivation behind utilizing encryption is protection (forestalling exposure of secrecy) in correspondence. This paper presents the presentation assessment of symmetric key cryptographic calculations which could be utilized for improving security of distributed computing devices conditions [3]. Single key, one key and private key encryption known as symmetric key calculations utilizes a private and an open calculation to execute encryption/decoding process. Because of the utilization single key for encoding the enormous amount of information can be handled at a quick speed [4]. There is no characterized procedure inside the network specialist organizations for shielding and making sure about information from dangers and attacks [8]. The objective of the digital assailants is sensors data which is being made sure about by the wireless network utilizing cryptographic calculations whose fundamental objective is to make it unimaginable for the aggressor to unscramble the figure content. The security in WSNs create an attention to prevent the data from attackers as well as life of the sensor and designing of the sensor node because every sensor in an tiny device on selected OS based so there are many problems in node like as memory, calculation i.e. computation, RF device and battery etc. In Symmetric cryptography a shared key is used to encrypt and decrypt the data between the communicating sensor nodes. This technique used because it wants limited hardware and low energy [3].

2 Related Work

With ascend in the attacks, accentuation given by the mists specialist co-ops are at end sensor information to be as secure as could be expected under the circumstances. Because of conflicting determination of encryption decoding calculations there has been given the low need to the sensor network execution [5].

To give progressively planned about the presentation of symmetric key cryptographic calculations this paper will examine the outcomes got by different assets. The vitality utilization of various symmetric key cryptographic calculations on dealt with gadgets was that after 600 encryption of a 5MB record utilizing triple DES the rest of the battery power is 45% in this way encryption are unrealistic as the battery dies[6]. AES is effective and quicker than different calculations, increment in key size by 64 bits prompts increment in vitality utilization by 8% and diminishing the quantity of rounds prompts power sparing however it can bargain the security of the convention. Present execution investigation between calculations utilizing c# programming language and AES requires all the more handling power. This paper examines the essential points of interest of AES as for other encryption strategies and was inferred that AES can be very acceptable in both high and low level dialects. The parameters were diverse for all

calculations as various key sizes of data squares, various information, life of the batter or battery energy utilization, key size and speed of the encryptions. Blowfish indicated preferred execution over others and it was presumed that higher the key size higher the battery and time utilization [7]. A great cryptographic calculation finds some kind of harmony between what is conceivable and what is accepted. It was finished up for both uniprocessor and network, RSA is the most expending and Md5 is least.

3 Proposed securıty

(i) ES for record Encryption (ii) Blowfish calculation for making sure about correspondence (iii) SHA3 hashing to make sure about tables (iv) One time secret key for validation

WSNs security has gotten one of the best difficulties to specialists everywhere to give answers for these issues. Each time the node needs to active state it will require a onetime secret key. Once secret key keeps the node secure from unapproved get to, the onetime secret key is finished randomly in light of the fact that the client characterized passkeys can be no problem at all traded off [8]. The recently produced secret key naturally deletes the more seasoned secret key from the framework and one secret key is for one time utilize as it were. The principle motivation behind this strategy is to make framework progressively secure and not to give any escape clauses to the unapproved get to. The client would first be able to time just transfer the data subsequent to associating to the WSNs yet thereafter it can both transfer and download the document [9]. The login procedure ensures whether the client is bona fide or not. At the point when client need to recover a document from the framework, the principle gateway serves the key which at that point coordinates the account which is as of now being spared in the database made sure about with SHA3 hashing. The area of the scrambled document is as it were known to the principle gateway.

4 Securıty Algorıthms

In wireless sensor network we want secure data transmission or communication with applying the cryptography to ensure the CIAA (confidentiality, integrity, availability and authentication of data). Confidentiality means the hiding of the data, integrity (to prevent the data from alteration) and the proof of the identity are known as authentication of data. Such type of the goals can be achieved with the help of AES,DES, RC4.

4.1 AES (Advanced Encryption System) is a fast and secure form of encryption to secure the data. This algorithm symmetric key structure which uses plain text of 128 bits. A 10, 12 and 14 rounds variable, and a permuted key length of 128, 192, 256. In addition 10 sub keys are used each with a length of 128, 192,256 bits. Single S-box and same algorithm are used to decrypt cycle in reverse. Rijndeal are square attacks, enhanced square attacks, impossible denial attacks, and reverse key schedule attack are some of the attacks that are being carried out on AES, but none of these attacks were feasible [10].

4.2 DES is a symmetric-key square Cipher dependent on Feistel structure. It utilizes 16 rounds of Feistel Structure. It was created in the mid 1970s and was endorsed as a government standard in November 1976. It was reaffirmed as a standard in 1983, 1988 and again in 1999. It was uniquely in 2002 when AES (Advanced Encryption Standard) was at last received after an open rivalry. It's a square figure which utilizes a 64 piece plain content with 16 adjusts and key length of 56 piece. 1 piece has been chosen as equality bit however initially the key length is 64 piece and this bit isn't utilized for encryption process. The 56 piece key size creating 7.2*1016 potential keys invigorates DES in run of the mill danger conditions [11].

4.3 3DES Presented in 1998. 3DES is named precisely it is as it is ought to be and as the name recommends, 3 cycles of DES encryption are performed on each square. It depends on a feistel structure with a key length of 168 pieces which is permuted in 16 sub keys 48 piece length each likewise

containing 8 S squares. It utilizes a similar calculation for unscrambling. That is utilized in maintaining a strategic distance from supposed man in the center assaults [12].

4.4 Blowfish is a feistel structure symmetric key calculation. It comprises of two sections, information encryption part and key development part. Blowfish is a square figure calculation that uses16 rounds of 64 piece plain content and key length up to 448 bits. There are18 sub keys permuted every one of 32 bits length actualized on both 32 and 64 piece processors. There are 4 S confines blowfish calculation and same calculation is utilized in opposite for decoding. [7].

4.5 RC4 is a stream figure, which implies that every digit or character is encoded each in turn. A figure is a message that has been encoded. The procedure utilizes a similar key for scrambling and decoding the data, another method for saying it is symmetric. This sort of calculation is frequently alluded to as a mutual key calculation. The key length shifts from 40 to 2048 bits. The calculation is computationally straightforward, and in that capacity, fits quick PC usage. RC4 is a common key stream figure Algorithm requiring a safe trade of shared key. It has the limit of utilizing keys between 1 to 2048 bits. The quality of RC4 lies in its trouble of knowing where any worth is in the table and area of the table used to choose each an incentive in succession. A specific RC4 calculation key can be utilized just a single time [13].

4.6 IDEA (International Data Encryption Algorithm) is an encryption calculation. It is a symmetric square figure which accepts 64 piece as an information, 28 piece key and performs 8 indistinguishable rounds for encryption in which 6 diverse subkeys are utilized and four keys are utilized for yield change. Thought under certain speculation is having a solid obstruction against cryptanalysis. It utilizes numerous gathering tasks which builds quality against the majority of the assaults. The 128 piece key size makes it one of the solid security calculations. There is no shortcoming identified with direct or mathematical assaults which have been accounted for yet [14].

4.7 TEA is a particular strategy for scrambling data. Encryption is the way toward changing over data from one structure (generally comprehensible), into another structure (not normally intelligible). The calculation splits the data up into pieces, called obstructs, of 64 bits in size. It utilizes a 128-piece key, which is an outer snippet of data, known earlier, to play out this transformation. It was made in 1994 at the Cambridge Computer Laboratory by Roger Needham and David Wheeler. As the name proposes, the Tiny Encryption Algorithm is little in size. On the whole, it very well may be actualized in a couple of lines of programming code. This is significant in light of the fact that it implies that it very well may be remembered for practically any kind of programming bundle, even those with genuine space imperatives. For instance, the product on your phone, or the product for the GPS in your vehicle. The encryption steps are likewise straightforward, making it easy to execute and keep up.

5 Matrıx For Performance Evaluatıon

The exploratory plan was performed on PC with center i5 processor on windows 10 condition going from 83.3 Kb to 1.54 Mb. The encryption time is viewed as the time that an encoding calculation takes to play out figure content from a plaintext and the throughput of the encryption plot is determined as the absolute plain content in bytes scrambled isolated by encryption time.

The performance parameters are (i) Encryption time (ii) Decryption time (iii) Memory utilization (iv) Flexibility (v) Scalability (vi) Security

6 Methodology

Exploratory research configuration was considered as generally appropriate taking into account the idea of the issue being examined. Information investigation systems are surveyed with anticipated outcomes as

portrayal of the examination. The usage is altogether tried and streamlined to give the most extreme presentation for the calculations. We utilized the Pentium center i5 machine under windows 10 condition through which the exhibition of information is gathered. In the investigation, the machine scrambled diverse document sizes running from 83.3Kb to 15.48Mb. A correlation is directed between the aftereffects of the chose diverse encryption plots regarding encryption and unscrambling time. The objective is to quantify the encryption speed for every calculation for various document sizes. The throughput of the encryption plot is determined by partitioning the all out plain content in Megabytes encoded by absolute encryption time for every calculation. By considering various sizes of information squares (83.3 kb to 1.54 Mb) the calculation were assessed regarding time required to scramble information square. All the usage was careful to ensure the outcomes will be generally reasonable and exact.

7 Result And Analysıs

We utilized java condition for reproduction. We have taken two parameters time and memory for the reenactment arrangement and throughput was determined by isolating the complete plain content encoded on all out encryption time for every calculation. Throughput of the encryption calculation is determined by separating the absolute plain content in megabytes unscrambled on all out encryption time on every calculation. The tables beneath show the outcomes acquired from running the reenactment program utilizing various burdens. The outcome show the effect of changing information load on every calculation and effect on figure mode utilized. The ten content documents of various sizes are utilized to direct ten distinct examinations where the correlation of various calculations of algorithm is performed.

Table1 (Encryption time)

kb	AES	DES	3DES	BLOWFISH	RC4	IDEA	TEA
83.3	625	41	43	8	15	16	54
108	31	47	47	16	16	125	15
249	468	47	47	47	15	32	16
333	32	47	64	281	15	63	10
416	46	48	94	343	31	127	16
1370	141	110	243	78	47	78	41
2740	62	172	361	93	62	205	97
5480	78	296	749	156	63	325	170
10003	723	484	749	531	141	397	357
15483	798	690	1401	601	198	758	475
average	300.4	198.2	379.8	215.4	60.3	212.66	125.1

Table 2 (Decryption Time)

kb	AES	DES	3DES	BLOWFISH	RC4	IDEA	TEA
83.3	24	10	25	17	5	16	15
108	15	16	31	10	6	94	16
249	16	32	31	15	4	31	10
333	16	46	17	16	7	31	12
416	16	47	125	17	10	47	16
1370	31	78	187	62	12	45	40
2740	47	141	359	78	17	129	96
5480	31	255	687	156	48	218	158
10003	62	484	1346	234	55	351	304
15483	88	680	1988	305	89	597	545
average	34.6	178.9	479.6	91	25.3	155.9	121.2

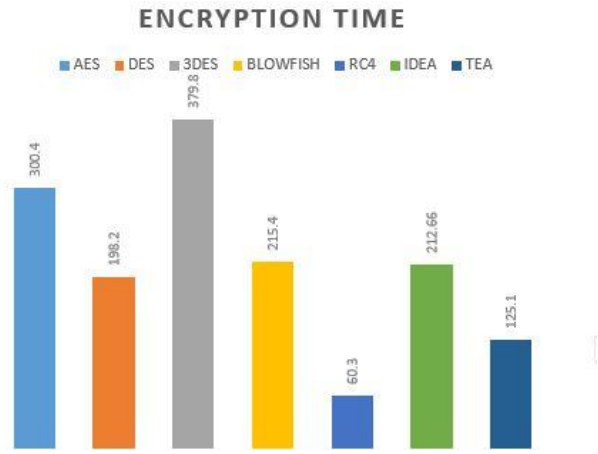

Figure 4 (comparison of encryption time)

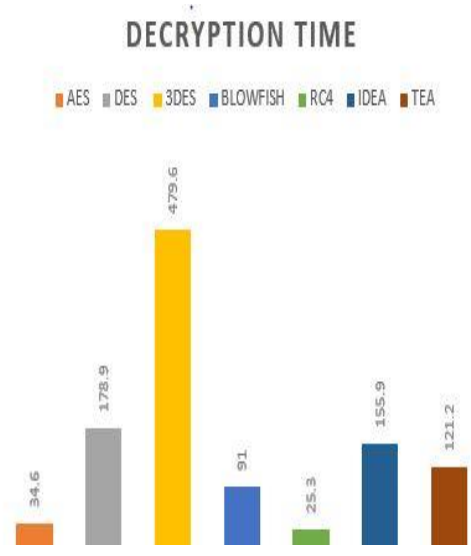

Figure 5 (comparison of Decryption Time)

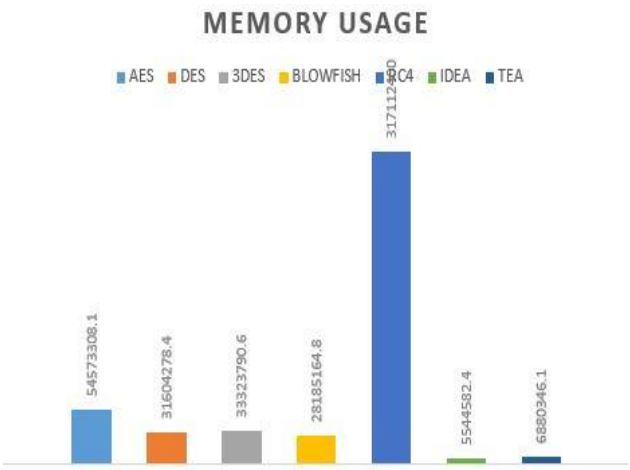

Figure 6 (Comparison of Memory Usage)

Table 3 (level of security)

Algos	DES	3DES	AES	Blowfish	RC4	IDEA	TEA
Plain Text/ Chiper text (bits)	64	64	128	64	40-2048	64	64
KeyLength	56	128	128 192,256	32-448	Variable	128	128
# of round (bits)	16	48	10,12,14	16	256	8.5	32

8 Performance Parameter Of Securıty

8.1 Flexibility

Table 5 (Flexibility)

Algorithm	Flexibility	Modification	Comments
DES	No	None	No modifications are supported by DES
3DES	Yes	168	The DES is iterated 3 times and the key is extended to 168 bits.
AES	Yes	128,192,256	The AES is expandable and support modifications.
BLOWFISH	Yes	32-448	The structure of BLOWFISH is extendable to 448 bits
RC4	Yes	variable	Modifications supported
IDEA	No	128	No modifications supported.
TEA	No	128	No modifications supported.

8.2 Level of security

The level of security of discussed algorithms depends on key size, the greater the key size stronger the algorithm and encryption.

Table 6 (level of security)

Algos	DES	3DES	AES	Blowfish	RC4	IDEA	TEA
Plain Text/ Chiper text (bits)	64	64	128	64	40-2048	64	64
KeyLength	56	128	128 192,256	32-448	Variable	128	128
# of round (bits)	16	48	10,12,14	16	256	8.5	32

8.3 Comparative Study

Table 7 (comparison on various parameters)

Algorithms	DES	3DES	AES	RC4	BLOW FISH	IDEA	TEA
Key size	64 bits	112 or 118 bits	128,192,256 bits	Variable	32-448 bits	128	128
Block size	64 bits	64 bits	128 bits	40-2048 bits	64 bits	64 bits	64 bits
Round	16	48	10,12,14	256	16	8.5	32 cycles
Structure	Feistel	Feistel	Substitution, Permutation	Feistel	Feistel	Substitution-Permutation	Feistel
Flexible	No	yes	Yes	Yes	Yes	No	No
security	secure	secure	Unsecure	vulnerable	vulnerable	unsecure	unsecure

9 Conclusıon

With the WSNs developing new innovation the security despite everything stays probably the greatest test in sensors computing condition. Use of security calculations and ensuring these security calculations are actualized appropriately and precisely utilized so as to defend sensor node security. During the examination it was discovered that AES will be best among all the calculations as far as adaptability, security, memory execution and utilization

References

1. M. Abd and E. Hafez, “Modified Elliptic Curve Cryptography in Wireless Sensor Networks Security,” no. November, 2018.
2. G. Sharma, S. Bala, and A. K. Verma, “SecurityFrameworks for Wireless Sensor Networks-Review,” Procedia Technol., vol. 6, pp. 978–987, 2012.
3. Parli B. Hari, Shailendra N. Singh “Security issues in Wireless Sensor Networks: Current research and challenges” IEEE International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring) Dehradun, 2016.
4. Parli B. Hari and S. N. Singh, “A Wireless Sensor Networks Security Protocol Architecture,” International Journal of Engineering and Advanced Technology no. 2, pp. 400–406, 2019.
5. Parli B. Hari and S. Narayan, “Security Analysis Framework in Wireless Sensor Networks,” International Journal of Advanced Science and Technology vol. 28, no. 20, pp. 823–833, 2019.
6. Parli B. Hari, “Security Attacks at MAC and Network Layer in Wireless Sensor Networks,” Journal of Advanced Research in Dynamical and Control Systems, vol.11, no. 12, pp. 82–89, 2019.
7. Abdul Raoof Wani, Q. P. Rana, Nitin Pandey"Cloud security architecture based on user authentication and symmetric key cryptographic techniques", 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2017

8. Soft Computing: Theories and Applications",Springer Science and Business Media LLC, 2019
9. A R Wani, Q P Rana, N. Pandey "Chapter 24 Performance Evaluation and Analysis of Advanced Symmetric Key Cryptographic Algorithms for Cloud Computing Security", Springer Science and Business Media LLC, 2019
10. Tarek Azzabi, Hassene Farhat, Nabil Sahli. "A survey on wireless sensor networks security issues and military specificities", 2017 International Conference on Advanced Systems and Electric Technologies (IC_ASET), 2017
11. Leili Nosrati, Amir Massoud Bidgoli. "Security assessment of mobile- banking", 2015 International Conference and Workshop on Computing and Communication (IEMCON), 2015
12. Jayvee Christopher N. Vibar, Ruji P. Medina,Ariel M. Sison. "ERC5a – An Enhanced RC5 Algorithm on Bit Propagation in the Encryption Function", 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), 2019
13. Mani Arora, Sandeep Sharma, Derick Engles. "Parametric comparison of EMDS algorithm with some symmetric cryptosystems", Egyptian Informatics Journal, 2017
14. Mihail Sichitiu. "Analyzing and modelingencryption overhead for sensor network nodes", Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications - WSNA 03 WSNA 03, 2003