Enhanced Key Cryptography Protective Technique In Wireless Sensor Networks

Dr.J.R.Arunkumar, Mr.Amanuel Bahiru

Abstract: In emerging trends of networks, wireless Sensor Networks is playing vital role for data communication and transmission. In that communication different types of attacks are notices during data transfer from sink to another node as well as sink node to base station. However different type of security needs and required for message and data transfer. Even single key encryption is not enough to secure the above statement give. This is the issue forced to design the efficient protective technique in order to secure the data. This paper describes some study about the basic key cryptographic protective technique in wireless sensor networks. . The security of WSN plays a vital role in the WSN, as sink node often store important information with base station but these base station may be unsafe. The main issue of sensor storage is to secure the data. Many of the security algorithms are available in the Sensor networks environment. This proposed algorithm is also to ensure the data key generation very important. In this proposed method Cryptographic table is used to generate key and perform several versatile operation used to secure the data in WSN. Finally, this paper show of the proposed scheme is investigated from the characteristics of computational effectiveness, storing condition and communication cost, and its protective techniques used to protect WSNs is discussed under different attack.

Index Terms: Wireless Sensor Networks, Security, Sensor nodes, security algorithm and protective techniques

1. INTRODUCTION

Wireless sensor networks consist of sensor nodes to show the location of the altitude and used for the some real time natural applications like weather forecasting, temperature. In WSN's, the nodes are moving in omni-directional and communication between the nodes like Multi and Bi-Directional. It is also the combination of large number of nodes and communicate each node. Finally the node information are worked with sink. It use the wireless communication technique for transferring the data among the sensor node and sink. Wireless sensor networks uses the different methods and techniques for sending the data from sensor nodes to sink and investigating the route to propagate the data to other nodes. It maintains the different protocols to leads the route very well. Even WSN has different node fault tolerance functionality, route failure, path failure, and security aspect also. This issues may causes to reinvestigate the route or node failure. In this paper, security issues are focused very well and describe the types of security attacks in wireless sensor networks data transmission. This research keeps major concern about the secure the data and efficient communication. In figure 1 describes the different concepts of WSN. There are many sensor nodes are associated together based on the location of the sensor node and these nodes are clustered by
different cluster algorithm and elected the cluster head based on cluster election algorithm, and each cluster has one cluster head[18]. Each node in cluster has to send the retrieve data to cluster head [18] and cluster head forward that data to sink or base station of the WSN[1].

- *Dr.J.R.Arunkumar, Assistant Professor, Faculty of Computing and Software Engineering, Arbaminch University, Ethiopia.*
- *Mr.Amanuel Bahiru, Lecturer, Faculty of Computing and Software Engineering, ArbaminchUniversity, Ethiopia*
- *E-mail: arunnote@yahoo.com*

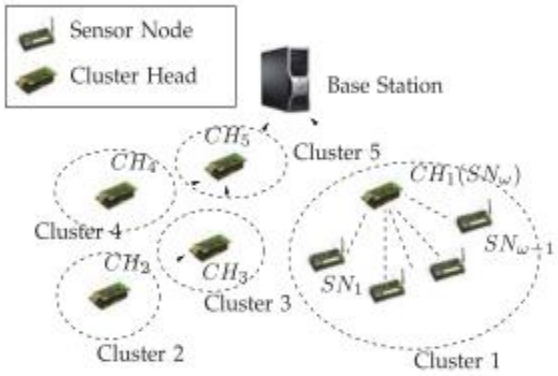

Figure 1: *Categorized Sensor networks*

Besides, [1] there square measure WSNs having no base station by any means, and thus, the combined methodology isn't proper. Also, the combined methodology is inefficient, Non versatile, and energy loss [20, 21] against some possible attacks on the long communication way [1]. Then again, as showed up inside the above Figure 1, a communication on approach are often used for reconsidering in WSNs. It permits various showed compose nodes to at the same time and truly update code pictures on completely startling cluster head while excluding the base station. Another piece of cluster of passed on recreating is that extremely astounding embraced nodes may be assigned completely sudden advantages of reworking to find the path to reach the sink. The security issues are working in between the sensor node and sink[19,22].

2. LITERATURE REVIEW

Actually, Sensor networks are based on battery life and power, communication and computation unit like processing unit and transmitter unit. Therefore wsn focus on power consumptions and critically looking the life time of wsn.In data aggregation was used for practical implementation for power computation.[17,18] The first idea is to total different detecting information by performing logarithmic or measurable tasks, for example, expansion, duplication, middle, least, most extreme, and mean of an informational index, and so on. Typically, information collection is performed by bunch heads if the entire system

is separated into a few gatherings known as groups. For instance, in military fields, sensors are sent to gauge radiation or substance contamination. The base station (sink) may require the most extreme estimation of all detecting information to generate the quick reaction; hence, every group head chooses the greatest estimation of different detecting information of its own bunch individuals and sends the outcome to the base station. Clearly, correspondence cost is diminished since just totaled outcomes arrive at the sink. [16] Unluckily, an opponent has an aptitude to detention sensor CHs. It may create the negotiation of the entire sensor cluster; so, numerous systems, such as ESPDA [4] and SRDA [5], been proposed. However, these systems restrict the files form of collection or root extra communication overhead. Also, an opponent can silently get the detecting data of its cluster associates after capturing a cluster head. To tackle above issues totally, two concepts are utilized in ongoing exploration [6], [7], [8]. To start with, information are cryptography during transmission. Second, group heads legitimately total cryptography. A notable methodology named Concealed Data Aggregation (CDA) [6] has been planned reliant on these two opinions. CDA gives both start to finish encryption and in-systems administration handling in WSN. Since CDA applies security homomorphism (SH) cryptography with added substance homomorphism, group cluster heads are equipped for executing option procedure on cryptography numeric information. Afterward, a few PH-based information accumulation plans [7], [8] have been proposed to accomplish higher security levels. In the above SH-based plans [6], [7], [8], the base station gets just the amassed outcomes. In any case, it brings two issues. To start with, the use of collection capacities is obliged. For instance, these plans just permit bunch heads to perform added substance procedure on figure writings sent by sensors; consequently, they are incapable if the sink wants to question the most extreme estimation of all detecting information. Second, the base station can't confirm the respectability and credibility of each detecting information. These issues appear to be settled if the sink can get all detecting information moderately. This paper presents a supportive direction-finding structure by XOR network coding. The data feature of sensor network coding was presented [5] [13] have projected their system for arbitrary direct

***Figure 2**: XOR network cryptography*

Sensor network cryptography that realizes packet based ability for together solo unicast and solo multicast communication networks in wireless networks.[17] have planned a technique to include net cryptography into a non-cryptography localized procedure that attempts to optimize the coding improvements given a set of natural packets and the subsection of packets each adjacent neighbor obtains. Also, a WSN cryptography scheme for mobile ad hoc network (MANET) using guiding antenna has been planned [18],[19] have projected an efficient broadcasting techniques for energy efficient in wireless ad hoc networks. An elementary system that uses XOR of packets for applied net cryptography has been proposed [20]. They have shown a significant bandwidth improvement in wireless network. However,[11] have designed a communiqué procedure that finds the trade- off between energy efficiency [23] and consistency in WSN. Disparately existing methods, the focus of this paper is on the analysis of the reliable wireless transmission problem in a Node to Node and Node to Sink in WSN, wherever vitality and power consumption is an significant constraint for this research.

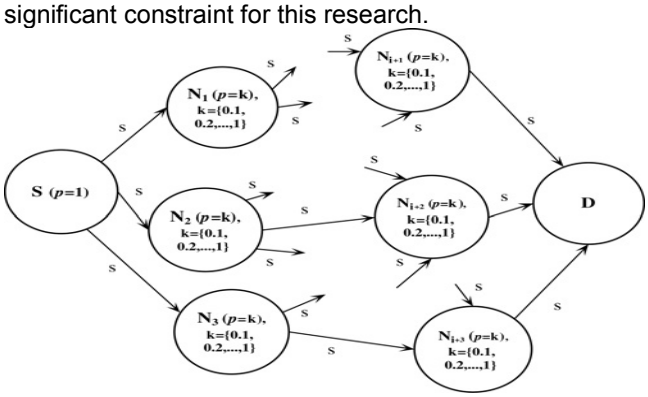

***Figure. 3** Transmission method in WSN*

Data broadcasting state in WSN using the dynamic and probabilistic path directing arrangement. Actually the source sensor node (A) transmits a packet, says, with probability Pr ¼ 1. When in-between nodes (such as B1, B2,B3 and B4 in Fig. 2) will get the first packet of transmission , that node will again transmissions the packet to its around neighbours with probability Pr ¼ k (where k ¼ 0.1, 0.2, 1). The packet is unwanted with probability (1/2 Pr) by the in-between nodes. In occasion, a sensor node gets similar packet all over again, it is unwanted. So, each node again transmissions or forwards an agreed data packet at maximum once. The packet is distributed through the net and eventually extended at the target sink node C. Here occurs a main cavity in executing network cryptography for m-m communication model in WSN. This paper presents a probabilistic transmitting system using net cryptography with XOR-based processes in WSN. While maximum of the previous effort accepts the analysis of network congestion for either many-to-one or one-to-many communication, a many-to-many model of two-way congestion traffic flow is measured in this research paper. This paper that notwithstanding the topological deviations due to link failure, the WSN performance increases.

3. PROPOSED METHODOLOGY

The Proposed method to increase the traditional cryptography by combination of multiple cryptography techniques for cipher Text (CT) and Transposition cipher. This Hybrid methods applied by letters for CT.

3.1 Notation used in proposed technique:

Notations are specified in table 1. In proposed algorithm, principal step the PT is converted into corresponding Hexadecimal ASCII code of each letter in alphabet. In classical cryptography method, the key value ranges are

from 1 to 256 or key can be string (Hybrid alphabets). Then this paper is proposed algorithm, key value range from 1 to 127. The specified steps are the cryptography technique and encryption algorithm steps.

Symbol	Description	Symbol	Description
BS	Base Station	CH	Cluster head
SNi	Sensor Node i	T	Transformation
(Pi,.Ki)	Public and private key of input text	M[I,k]]	Substring of m from index I to k
di	Sensing data of SNi	mi	Encoded result of di
Φi	Bits of transfer from sensor node	L	Length of data
Ci	Aggregated Cipher text	δ	Signature of aggregated data
C	Concatination of Pi and Ki	X	Scalar multiplication

3.2 Proposed Encryption Method

Step 1: Check and Count the Number of letters (L) in the plain text input value without any space.
Step 2: Change the plain text input value into equivalent Hexadecimal code. And arrangement a matrix with value (NXN >=L).
Step 3: Apply the transformed Hexa-Decimal code value form the Transposition Matrix (A=AT)
Step 4: Accumulation the values of AT values in ascending order. (A[0],A[1],A[2],…..A[N])

Table 1 Notation in WSN

Step 5: Apply to Shift row transformation
Step 6: Key generation. To construct Encryption table
Step 7: Find out the place of PT in the Encryption key table. Take the equivalent value of plain text in which the row, column intersect.
Step 8: Form a matrix (NXN >=L) for the key value (the key value contain decimal values) the maximum key size 64(8X8), if plain text is more than 64 characters the same key will be appended.
Step 9: Add the matrix A with key value is 64
Step 10: Read the message by, column by column using the key value 2431
Step 11: Find the modulus value of the matrix
Step 12: If the value <64 the add value+64
Step 13: Convert the Hexa decimal ASCII code into output character value

This proposed encryption algorithm is used in demand to encode the numbers of the Node in the wsn. Node can store data on demand or for the data without protection any local copy of the data on node memory. Subsequently the node has no control above the data after the node data transmission session transmitted out, the encryption key production the very significant role and its main verification for the node. Projected procedure is defined below. The key is produced by expending Encryption Table. The Encryption table concept by using 8X8 matrix and rows and columns are numbered from 1 to 8 and it contains alpha, numeric, two special characters. Alphabet uppercase A-Z and lowercase a-z, number 0-9, special character $, #. It shows the encryption algorithms.

3.3 Proposed Architecture of Encryption

87	111	111	108
109	67	101	101
111	103	108	101
101	99	84	108

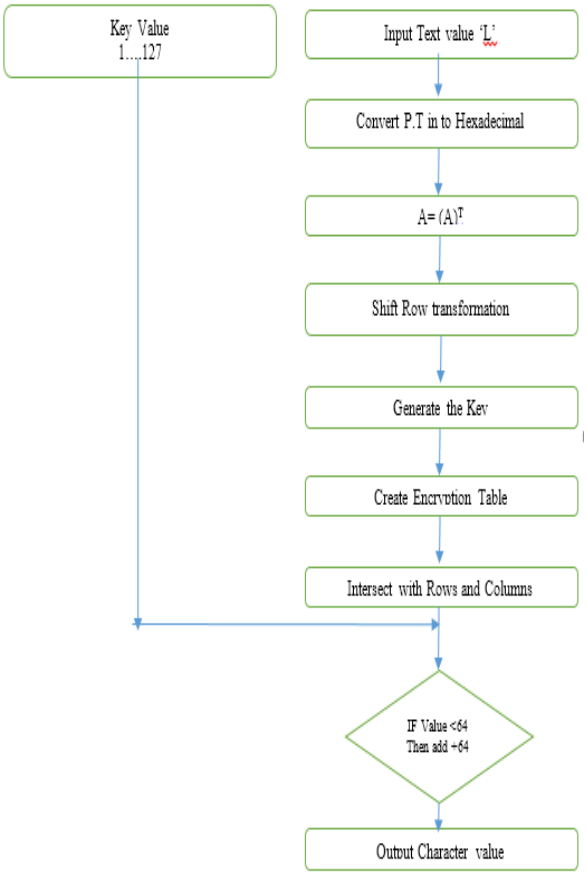

Figure 3: *Encryption Architecture*

The detailed steps of Cryptography encrypted algorithm.
Step 1: Check and Count the Number of letters (L) in the plain text input value without any space Plain text: Temparaturevaleis21. L= 19 (L = No. of Characters in the Message)
Step 2: Change the plain text input value into equivalent Hexadecimal code. And arrangement a matrix with value (NXN >=L). The Encryption table generated by 8X8 matrix. ASCII code value for the plaintext.87,101,108,99,111,109,101,84,111,67,111,108,10 8,101,103,101 To form a square matrix Form a 4 X 4 matrix. Matrix= A

87	101	108	99
111	109	101	84
111	67	111	108
108	101	103	101

Step 3: Apply the transformed Hexa-Decimal code value form the Transposition Matrix (A=AT)

87	111	111	108
101	109	67	101
108	101	111	103
99	84	108	101

Step 4: Accumulation the values of AT values in ascending order. (A[0],A[1],A[2],…..A[N]). Store the values form A[0] to A[15]matrix. A[0]=87,A[1]=111,…..A[16]=101
Step 5: Apply to Shift row transformation
Step 6: Key generation. To construct Encryption table, The Encryption table consists of alphabets, numeric and two special characters. Alphabetic: Upper case A-Z, Lower case a-z, Numeric : 0-9, Special characters: $,#.

	1	2	3	4	5	6	7	8
1	A	a	I	i	Q	q	Y	y
2	B	b	J	j	R	r	Z	z
3	C	c	K	k	S	s	1	7
4	D	d	L	l	T	t	2	8
5	E	e	M	m	U	u	3	9
6	F	f	N	n	V	v	4	0
7	G	g	O	o	W	w	5	$
8	H	h	P	p	X	x	6	#

Step 7: form a square matrix (NXN >=L) for the key value (the key value contain decimal values)
Step 8: Add the matrix A with key value.

+

=

162	163	155	140
183	121	153	146
185	134	182	145
145	151	156	160

Step 9: Read the Plain text by, column by column using the key value 2431 Apply cryptography key 2431

163	121	134	151
140	146	145	160
155	153	182	156
162	183	185	145

Step 10: Find the modulus value of the matrix, Find modulo of 127 and 163 mod 127 =36

36	121	7	24
13	10	18	33
28	26	55	29
35	56	58	18

Step 11: If the value <32 the add value+32; If PT<32 (x=32) 163 mod 127 =36

36	121	39	56
45	42	40	33
60	58	55	61
35	56	58	40

Step 12: Convert the Hexa decimal ASCII code into character value, The encrypted text is: $y'8_*(!<:7=#8:(
The encrypted data is stored in the node and Sink storage. The cryptographic procedure is important for the sink to recover the original data of sensor nodes, Encryption and Decryption is possible distinct with key values which are proposed for encryption algorithm. So the key shows the main and key role in the Cryptography algorithm.

Decryption algorithm forms with the following steps are given below.
Proposed Decryption Method
Step 1: The Cryptography ciper text or decoded text is converted into Hexa decimal code values.
Step 2: Find and determine the No. of Letters (L) in the Cryptographic cipher text and form a matrix N X N.
Step 3: reverse order of the key value row by column of message matrix A
Step 4: Subtract Encryption table key value with
Step 5: Reverse shift row transformation
Step 5 and 6: Rearrange A [0] to A[15]matrix in decesending, To calculate the Transpose of given Matrix $(AT)T = A$
Step 7: Stop
To run the decryption algorithm the original plain text Temparaturevaleis2 is discovered.

3.4 Proposed Architecture of Decryption

75	52	44	32
74	54	52	45
74	31	74	44
44	52	72	52

87	111	111	108
109	67	101	101
111	103	108	101
101	99	84	108

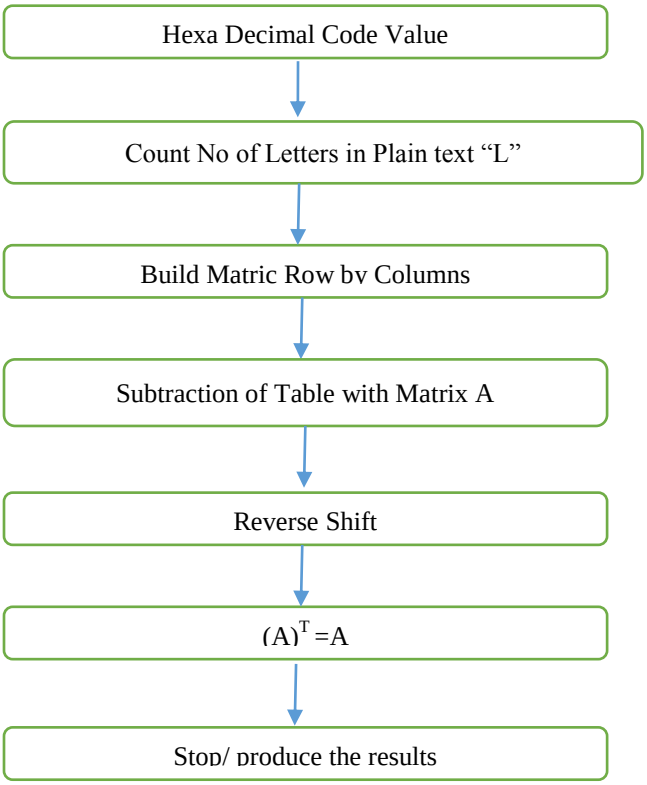

Figure 4: *Decryption Architecture*

Step 1 and 2: The encrypted text is transformed into Hexa code values. The cipher text or decoded text is:$y'8_*(!<:7=#8:(

Step 3: key value with row by column in reverse order with message

163	121	134	151
140	146	145	160
155	153	182	156
162	183	185	145

Step 4: Subtract Encrypt table key value with matrix A

162	163	155	140
183	121	153	146
185	134	182	145
45	151	156	160

-

87	111	111	108
109	67	101	101
111	103	108	101
101	99	84	108

=

Step 5: Reverse shift row transformation

75	52	44	32
74	54	52	45
74	31	74	44
44	52	72	52

Step 5 and 6: A[0] to A[15]matrix will be Rearrange in to ascending order form : Transpose of Matrix of given matrix and find the (AT)T = A

Matrix= A

87	101	108	99
111	109	101	84
111	67	111	108
108	101	103	101

ASCII code value for the plaintext (Decimal Code)87,101,108,99,111,109,101,84,111,67,111,108,108,101,103,101. Original plain text will be recovered by the node as well as sink by using the above proposed algorithm.

4. EXPERIMENTAL RESULTS

The proposed algorithm examined with the aid of the use of 50 pattern phrases with exceptional sorts of characters. In this experiment, out of 100 phrases 80 phrases are efficiently encrypt and decrypt perfectly (100%).

Remaining 12 words, phrases are passed off single personality error and three phrases are befell three persona errors. The accuracy of protection is calculated the usage of equation – 1.

Accuracy of Security

S = $\frac{X}{N} X100$ ---------- (1)

X - Number of selected words

N - Total number of words

Input Data (words)	Accuracy (%)		
	100	90	80
100	80	12	07

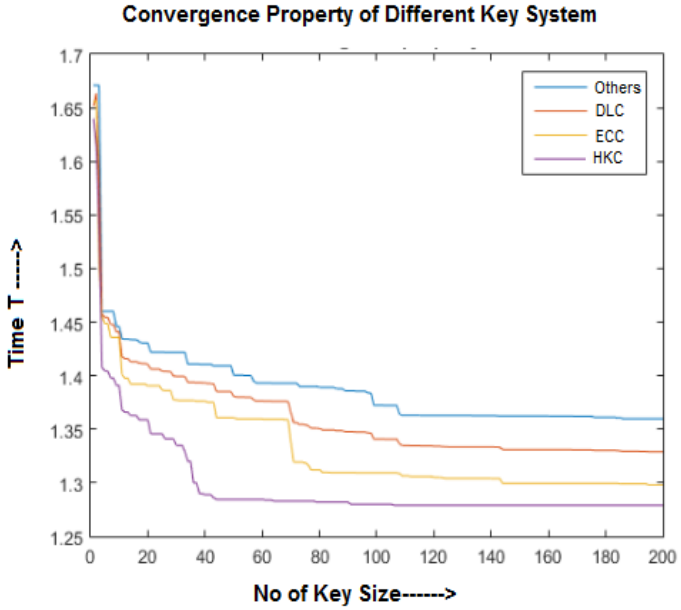

Figure 5: *Convergence Experimental Results*

5. CONCLUSION

The WSN environment Security and Privacy are significant role in keeping of data in that location. So many researchers are effort in that research domain area. Cryptographic techniques are used to maintain the secured communication among the sensor node and the sink in wireless sensor networks. This paper is implemented with a symmetric based encryption algorithm for secure data in sink storage. The produced key performances as the primary validation for the sensor node. By applying this encryption algorithm, data is stored only on secured storage and sensor node guarantees that also and it cannot be accessed by Hackers, administrators or intruders. Based on the experimental results, the proposed algorithm performance is good. We proposed a privacy-preserving efficient framework based on Key cryptography protective technique which provides certain privacy guarantee to sensor nodes in the sink and also sign up facility for the sensor node to communicate in the wsn. We successfully create key exchange facility to sink using simply sharing secret key between the sensor nodes. No one can see or share the data only authenticated sensor node can share the data in the WSN.

REFERENCES

[1] Dr.J.R.Arunkumar. "Enhanced Dynamic Authorized Secured Protocol for Wireless Sensor Networks, "Journal of Science, Computing and Engineering Research, 1(1), 07-11, Mar-Apr 2020.

[2] R. Rajagopalan and P. Varshney, "Data-Aggregation Techniques in Sensor Networks: A Survey," IEEE Comm. Surveys Tutorials, vol. 8, no. 4, pp. 48-63, Oct.-Nov. 2006.

[3] S. Madden, M.J. Franklin, J.M. Hellerstein, and W. Hong, "TAG: A Tiny AGgregation Service for Ad-Hoc Sensor Networks," Proc. Fifth Symp. Operating Systems Design and Implementation, 2002.

[4] J.-Y. Chen, G. Pandurangan, and D. Xu, "Robust Computation of Aggregates in Wireless Sensor Networks: Distributed Rando- mized Algorithms and Analysis," IEEE Trans. Parallel Distributed Systems, vol. 17, no. 9, pp. 987-1000, Sept. 2006.

[5] H. C¸ am, S. O¨ zdemir, P. Nair, D. Muthuavinashiappan, and H. Ozgur Sanli, "Energy-Efficient Secure Pattern Based Data Aggre- gation for Wireless Sensor Networks," J. Computer Comm., vol. 29, pp. 446-455, 2006.

[6] H. Sanli, S. Ozdemir, and H. Cam, "SRDA: Secure Reference- Based Data Aggregation Protocol for Wireless Sensor Networks," Proc. IEEE 60th Int'l Conf. Vehicular Technology (VTC '04-Fall), vol. 7, pp. 4650-4654, Sept. 2004.

[7] D. Westhoff, J. Girao, and M. Acharya, "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation," IEEE Trans. Mobile Computing, vol. 5, no. 10, pp. 1417-1431, Oct. 2006.

[8] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks," Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems, pp. 109-117, July 2005.

[9] E. Mykletun, J. Girao, and D. Westhoff, "Public Key Based Crypto schemes for Data Concealment in Wireless Sensor Net- works," Proc. IEEE Int'l Conf. Comm., vol. 5, pp. 2288-2295, June 2006.

[10] H. Chan, A. Perrig, and D. Song, "Secure Hierarchical In-Network Aggregation in Sensor Networks," Proc. ACM 13th Conf. Computer and Comm. Security, pp. 278-287, 2006.

[11] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A Secure Hop-by- Hop Data Aggregation Protocol for Sensor Networks," ACM Trans. Information and System Security (TISSEC), vol. 11, no. 4, pp. 1-43, 2008.

[12] S. Roy, S. Setia, and S. Jajodia, "Attack-Resilient Hierarchical Data Aggregation in Sensor Networks," Proc. ACM Fourth Workshop Security of Ad Hoc and Sensor Networks, pp. 71-82, 2006.

[13] H. Yu, "Secure and Highly-Available Aggregation Queries in Large-Scale Sensor Networks via Set Sampling," Proc. IEEE Int'l Conf. Information Processing in Sensor Networks, pp. 1-12, 2009.

[14] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), pp. 416-432, 2003.

[15] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.

[16] Dr. M.Sundarrajan. "Authentication Scheme Based On Blow Fish Cryptography in Categorized Sensor Networks, Journal of Science, Computing and Engineering Research, 1(1), 12-15, Mar-Apr 2020.

[17] Dr.J.R.Arunkumar, Dr.M.Sundarrajan," An Efficient Greedy Algorithm To Improve The Lifetime Of The Wireless Sensor Network" In CiiT International Journal Of Networking And Communication Engineering ISSN 0974 – 9616, Volume- 8, Issue-10, December 2016.

[18] Dr. M. Sundar Rajan, Dr. J. R. Arunkumar Dr. R. Anusuya," Energy Efficient Cluster Head Selection In Adhoc on Demand Multipath Distance Vector Routing Protocol" in International Journal Of Scientific & Technology Research, ISSN 2277-8616, Volume 9, Issue 01, January 2020

[19] Dr.J.R.Arunkumar, Chaotic African Buffalo Optimization Based Efficient Key Mechanism in Categorized Sensor Networks, International Journal of Engineering and Advanced Technology, Vol-9,Issue-3, February 2020

[20] Arunkumar, J.R., Anusuya, R., Sundar Rajan, M. et al. Underwater Wireless Information Transfer with Compressive Sensing for Energy Efficiency. Wireless Pers Commun (2020). https://doi.org/10.1007/s11277-020-07249-7

[21] Dr. Arunkumar, J.R., Dr. SundarRajan M. And Dr. Anusuya, R.. 2020. "Energy Efficient Algorithm for Wireless Sensor Networks Based On Cluster Head", International Journal of Current Research, 12, (4), April-2020

[22] J.R.Arunkumar, M.Ramkumar Prabhu," Lightweight Extensible Authentication Protocol Based Wireless Sensor Network" International Journal Of Engineering Research And Application ISSN: 2248-9622, Volume-7, Issue- 10, (Part -5) October 2017, Pp.66-74.

[23] Anusuya Ramasamy, J.R.Arunkumar, M.Sundar Rajan "A Secure and Energy Efficient Sensor Nodes in Wireless Sensor Networks using Improved Ant Lion Optimization" (2020). Regular issue, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-9 Issue-1, May 2020

[24] J.R.Arunkumar, DR.E.Muthukumar"Analysis of Energy Efficient Routing Protocols and Data Collection Approaches in Wireless Sensor Networks" Journal of Engineering Sciences, Volume- 2 Issue- 2,2011.