International Journal of Pure and Applied Mathematics
Volume 118 No. 20 2018, 861-875
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue
ijpam.eu

An Efficient Light Weight Cryptography Algorithm Scheme for WSN Devices using Chaotic Map and GE

[1]Aakash Dutta, [2]K. Naveen Kumar, [3]N. Sai and [4]Radhika Rani Chintala

[1]Department of Computer Science and Engineering,
KLEF, Vaddeswaram, Guntur, India.
aakashdutta73@gmail.com

[2]Department of Computer Science and Engineering,
KLEF, Vaddeswaram, Guntur, India.
naveenkumarkodeboyina@gmail.com

[3]Department of Computer Science and Engineering,
KLEF, Vaddeswaram, Guntur, India.
namburisaikumar1@gmail.com

[4]Department of Computer Science and Engineering,
KLEF, Vaddeswaram, Guntur, India.
radhikarani_cse@kluniversity.in

Abstract

The Wireless Sensor Network (WSN) is an accumulationof variety of sensor nodes. All the Remote sensors that are organized by a network are monitored and protected by various lightweight cryptographic schemes. The main focus is to provide a better lightweight encryption system without overloading the pre-existing bandwidth of the network and computational sources of the sensor nodes. Based on both the genetic operations and the chaotic map, a lightweight block cipher is implemented to address these limitations. The communicating nodes are being verified by the chaotic map parameters in this cryptographic scheme and also output the bit sequence pseudo randomly. To encrypt the data blocks, mutation, crossover operations and XOR are used in this sequence. Chaotic map and genetic operations is mechanism used in sensor networks to provide confidentiality and security for data.

Key Words: Chaotic map, WSN, light-weight block cipher, security, and confidentiality.

1. Introduction

Software accomplishment depends upon on the proficiency of providing a fast and accurate output that is expected by the end user. The WSN consist of different hundredsof sensor nodes, where every node is linked to one or many sensors. Figure 1.1 represents the functionality of sensor nodes.

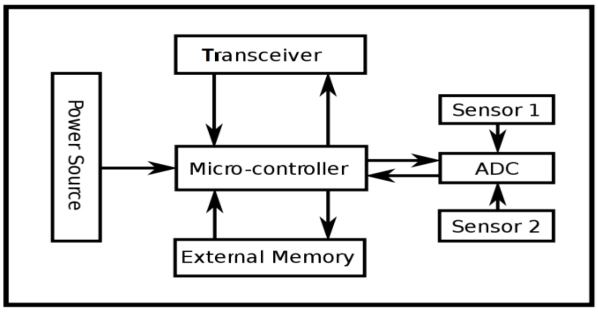


Fig. 1.1: Sensor Node of Architecture

A sensor node might differ in itssize. In spite of functioning modes, Size and economic limitations of the sensor nodes may result in restrictions of the resources likespeed, memory and bandwidth and power. Cluster Heads (CHs) are responsible for transferring messages from normal nodes to the Base Station (BS) [14]. Figure 1.2 represents CHs can communicate very easily with the Base Station, that can be found anywhere in the network at any given time and changes which occurs at every definite length of time and also improves network's energy ratio.

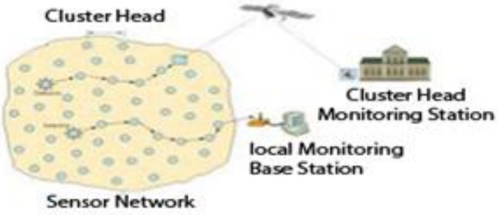

Cluster Head
Cluster Head Monitoring Station
local Monitoring Base Station
Sensor Network

Fig.1.2: Architecture of Wireless Sensor Networks

Networks Many intensified secure hierarchal routing protocols are there to attempt and achieve both efficiency and security for WSN. Many routing protocols are susceptible to a large number of security breach attacks. Attacks which are most destructive are the one which involves CHs. Due to the limitation of resources of the network, cryptographic algorithms based upon the public keys like Diffie Hellman[11] and RSA are too energy-consuming and complicated for WSN. However compared to public key cryptography, the symmetric cryptographic technique has its own high grade which is much more efficient. Moreover, to provide security in WSN, encryption keys must be accomplished among sensor nodes. The Key distribution is a phenomenon of distributing several keys among the sensor nodes and the Key management often receives more attention in data authentication and encryption in WSN security. A sensor hub may shift in a measure, and may provoke financial constraints on sensor hubs due to its expensive security which result in confinements on assets, for example, vitality, memory, and speed, transmission capacity. As matter of fact keeping the game of economics in point no institution would not like to invest more for its security than actual cost for the machine i.e. the sensor nodes, but providing security to this nodes in this integrated wireless network is the real challenge in this modern world, as to make sure that it does not decrease the nodes working potential without creating high dependencies on its computational resources.

2. Literature Review

The algorithms that are utilized for security reasons might be arranged into three fundamental classifications, they are minimal equipment based cryptographic plans, regular square figures, and lightweight piece figures. The information transmission conventions including group situated conventions are presented to various security assaults. Particularly, assaults to CHs in WSNs could bring substantial harm to the system since information transmission and information accumulation relies upon the CHs in a general sense. In the event that a programmer figures out how to act like a CH, it can incite assaults, for example, sinkhole and particular sending assaults, subsequently disturbing the system [14].Accordingly, the momentum inquiries about spotlights on outlining secure and lightweight square figures.

In actualizing an encryption calculation by utilizing AES (Advanced Encryption Standard) has been recommended to accommodate information classification in a remote sensor arrange. It concentrated on an AES-based symmetric key waywhich offers a similar key for encoding and decoding between the two sides of correspondence. The calculation brings plaintext by figuring 10 adjusts numerically to deliver the cipher text in a brief timeframe.

In a convention in light of open key cryptography for outside specialist confirmation and session key foundation has been recommended. An outer specialist imparts through an open key encryption system with a base station, which communicates with the sensor hubs through sharing of a private key. The procedure for the given convention is separated into three stages: enrolment, verification and session key foundation.

In a productive cryptographic approach for information security in WSNs utilizing the Modern Encryption Standard Version-II is presented. MES V-II proposes a kind of symmetric key encryption. This calculation, created by Nath et al., utilizes the TTJSA and DJSA calculations in a randomized strategy. In this given method, a summed up and altered Vernam figure technique is being utilized with various keys for each square and piece sizes. As an extra security calculation is standardized, criticism is additionally given to this technique. After the immediate stage encryption is finished, whole record is being isolated into two traded parts and the altered Vernam figure technique with input and another key will be rehashed. Rehashing this whole operation under various circumstances brings a framework that is profoundly secure.

3. Security Issues

The essential elements and a portion of the security assaults were featured with a review of security answers to set up a safe foundation for WSNs. This started accompanying security necessities like:

Data Authentication: Message confirmation is a basic measurement for sensor systems. And the capacity of the every corresponding host to confirm the other's data [2].

Data Integrity: these spotlights on the accuracy of the information to guarantee that no progressions are made by including, changing or erasing data amid the transmission.

Data Confidentiality: This guarantees any message is known by the sender and recipient as it were. The standard approach for accomplishing this requires utilization of encryption systems.

Availability: This guarantees that information is accessible consistently at the season of any demand. Some security assaults, for example, the dissent of administration will influence information accessibility, however feeble system outlines and security instruments can likewise bring about the inaccessibility of information. Securing accessibility requires evading a solitary purpose of substantial calculations that prompt vitality utilization of the sensor hubs.

Data Freshness: This guarantees no old messages have been replaced by a vindictive performing artist. Timestamps can be connected to accomplish this objective. What's more, the accompanying terms are utilized to depict remote sensor assaults:

Denial of Service (DoS): This kind of assault expects to decrease transfer speed and stultify assets. Such assaults on WSNs can show up as different sorts set in various system layers [18].

Sybil Attack: This kind of assault subverts a notoriety framework by distorting personalities.

Blackhole/Sinkhole Attack: In this kind of assault, a malicious hub goes as a dark gap that controls the activity of WSNs. This happens when a malevolent gadget is presented between any two hubs and controls correspondence between them.

Wormhole Attack: In this kind of assault, organize bundles at one area in the system are borrowedto another area in the system. Retransmissions then come back to the beginning area. At last, the writing audit concentrated on some WSN security arrangements, for example, the accompanying [2].

Shared Keys: This is an ordinary assurance composition that gives a similar key to both encryption and decoding blueprint.

Protected Grouping: This includes countless hubs in a WSN in which a few hubs are assembled together to finish particular assignments. [7]

Encryption: This includes applying distinctive cryptographic methodologies, for example, message confirmation codes, symmetric keys, and open key encryption.

Secure Data Aggregation: Sensor hubs ordinarily assemble data in perspective of the end goal to transmit it to the base station. To diminish the vitality devoured by sensor hubs, this data ought to be totalled at a middle of the road sensor level by utilizing a fitting accumulation work. [7,8]

Security Protocols for Sensor Networks (SPINS): This is a gathering of different security building squares intended to accomplish diverse security prerequisites. [8]

Link Layer Security Architecture (TinySec): This is a modest security bundle introduced in the uses of a sensor organizer. It is a piece of the official arrival of Tiny OS. Its security inclinations are verification encryption (TinySecAE) and validation just (TinySecAuth). [8]

A multilevel security system is presented by utilizing information situated in arbitrary number generator to encode a tag of casings. The principal level will be begun with an interleaving strategy. Second, the estimation of a pseudo-arbitrary number generator is seeded. Third, a numbered bank is appropriated at first. The last level is begun by applying operations to the number bank. Cryptographic blueprint utilizing riotous guide and hereditary operations have been recommended for WSNs. Generation of Pseudorandom Bit Sequence: In this stage, pseudorandom bit successions are created by utilizing confused guide capacities.

The Encryption Process: Disarray and dispersion are the fundamental ideas used to plan a square figure. To accomplish perplexity, a clouding connection between the cipher text and the symmetric key must be connected. Dispersion is again accomplished by spreading the diffused redundancy of the plaintext over the cipher text. Three unique operations can be actualized by this cryptographic method: XOR, change, and hybrid.

4. Usage of the System

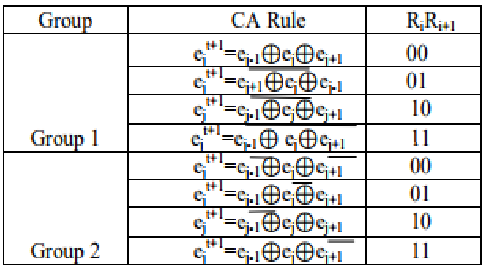
These days, utilizing exchanged data incorporate pictures has expanded because of expanding utilization of PC requests. Large noise based picture encryption technique is a standout amongst the most productive strategies which is utilized to cover up visual data amid transmission. This paper displays another picture encryption technique in light of Logistic and Tent disorganized maps and stage dispersion design, in which, clamorous maps will change the pixels of the plain-picture to scramble that. At last, the scrambled picture will be decoded to change the plain-picture [21]. With the advancement in cryptic system, concealing the data has developed too and discovering its position as a capable instrument in perspective of the end goal, to keep up the data. These days, correspondence through media transmission gears has expanded drastically at various levels, so there is a danger of listening in and altering by adversary or profiteering that undermines this data. The security of picture as a standout amongst the most widely recognized interchangeable information is thought about with the advance of innovation in the previous decade to anticipate unapproved access at arranging level. So analysts are searching for an approach to back off the rate of connection between the pixels in the pictures. Thus, the high relationship between the pixels of the pictures will ease speculating the first one [14]. Encryption systems from key point of view are divided into two categories as symmetric systems or safe key and asymmetric systems or public key. In symmetric encryption systems, encryption and decryption operations is dependent on a secret key agreement called private key and the safety and validation of the message is dependent on a safety of this key [8]. Symmetric systems are divided into Block Cipher and Stream Cipher or the sequence systems. In Block Cipher (cryptographic) systems, the sequence of information is divided to the templates with specified length and each Block is encrypted under a certain algorithm that is dependent on a key. But in Stream Cipher, encryption will happen for the entire data. The ideal mode in a Stream encryption, is applying a completely random sequence as a key. In Block Cipher systems to regenerate a key sequence by decoder, we should necessarily use definite and specific methods for the production of sequences. In fact we can use Pseudo Random Sequences rather than Random Sequences. One way to generate a Pseudo Random Sequence is using chaos systems. Encryption methods based on chaos has two stages: Turbulence and influence (distribution). In turbulence method, the pixels of image will find permutation by some chaos mapping and in influence stage the pixels value will change in a way that a minute change in the original picture will cause a great changes in a relevant Cipher image [20]. In techniques based on chaos, the designing of change function is challenging, so designing an effective and easy change function can lead us to cryptography. In this we are trying to reach a new approach in image encryption adopting Tenet and Logistic chaos functions. These functions using generation of random numbers will produce Cipher image.

5. Chaotic Logistic Mapping

The polynomial mapping of degree 2 is calculated guide which is regularly referred to as an original case of how perplexing, disordered conduct can develop from extremely basic non-direct dynamical conditions. The guide was advanced in an original 1976 paper by the scholar Robert May, to some degree as a discrete-time statistic display practically equivalent to the calculated condition initially made by Pierre Francois [11]. Scientifically, the calculated guide is composed as given in (Eq.1).

$$X_{n+1} = \mu X_n(1 - XX_n)\text{- Eq.1}$$

Here X_n is a number in the vicinity of zero and one that speaks to the proportion of the current populace to the greatest conceivable populace. The μ=4 instance of the strategy guide is a nonlinear change of both the bit-move delineates the μ=2 instance of the guide. The conduct of the calculated guide is reliant on μ which is a consistent, the guide produces complex connection between the present and next state when 3.5699456<μ [16].



Group	CA Rule	R_iR_{i+1}
Group 1	$c_j^{t+1}=c_{j-1}\oplus c_j\oplus c_{j+1}$	00
	$c_j^{t+1}=\overline{c_{j+1}\oplus c_j}\oplus c_{j-1}$	01
	$c_j^{t+1}=\overline{c_{j-1}\oplus c_j}\oplus c_{j+1}$	10
	$c_j^{t+1}=\overline{c_{j-1}\oplus c_j\oplus c_{j+1}}$	11
Group 2	$c_j^{t+1}=\overline{c_{j-1}}\oplus c_j\oplus \overline{c_{j+1}}$	00
	$c_j^{t+1}=c_{j-1}\oplus \overline{c_j}\oplus c_{j+1}$	01
	$c_j^{t+1}=\overline{c_{j-1}}\oplus c_j\oplus c_{j+1}$	10
	$c_j^{t+1}=c_{j-1}\oplus c_j\oplus \overline{c_{j+1}}$	11

Fig. 5.1: Table Explaining CA Rule

At first, we change over the permuted picture I' MxN(Image Matrix) into lines of twofold arrangements to get the double stream picture BMxN(Image Matrix). Here, N is even. If not, an arbitrary line of pixels could be included toward the finish of the picture. The length of every paired grouping is L=MXT bits, where T is the quantity of bits per pixel. In our encryption plot, there are two rounds of encryption. The key K1 and run selectors r1 are utilized for first round while key K2 and principles r2 are chosen for the second round. We get a decent execution by the encryption conspire. The encryption plot has appeared in Fig.1.4.The first round: Step 1: Take first two rows of binary stream image and key K1 and XOR them to get C1 and C2. Iteratively apply the CA(Certificate authority) diffusion rule selected according to first two rows values of r1 to obtain C`1 & C`2. Then again XOR C`1 & C`2 with first two rows of key K1. Step 2: Take the third and fourth rows of the binary stream image and XOR with next two rows of key K1 and previous two encrypted rows. Then similarly apply iterative CA rule depending on third and fourth rows of rule selector r1. Then again XOR with key and previous two rows of the encrypted matrix. Repeat the step 2 until step N/2. The second round: Then flip the first round encrypted matrix upside down and perform the steps similar to first round with key K2 and rule selector r2. The encrypted matrix is converted back to decimal values ENCMxN(Encrypted Matrix) from binary streams.

Decryption scheme is a symmetric encryption algorithm thus the keys and rule selectors have to be known at the decryption side. The decryption is the exact reverse procedure of encryption which also has two rounds. The key K2 and rule selector r2 for first round while key K1 and r1 for the second round. Initially convert the encrypted image ENCMxN(Encrypted Matrix). Step 1: Take the last two rows of the encrypted matrix and key K2 along with previous two rows of encrypted matrix and XOR them. Then apply the iterative CA rule selected based on r2. Then again XOR the iterated value with key K2 last two rows and previous two rows of the encrypted matrix. Repeat this step similarly for all rows. Step 2: Flip the matrix after first round of decryption and apply key K1 and rule selector r1 similar to the first round to obtain the decrypted matrix DECMxN. The original image peppers 512 x 512 encrypted by our scheme are shown in Fig 1.4.

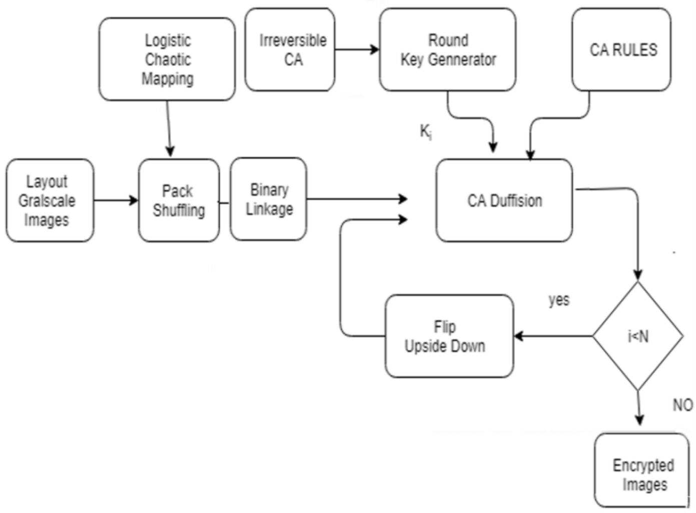


Fig. 5.2: Flow Chart Showing the Image Encryption Scheme

Choice OF ITERATION NUMBER In this calculation, the cycle number d of the reversible CA should be resolved before encryption, in light of the fact that the estimation of the emphasis number is firmly identified with the dispersion property of the picture encryption calculation. A change at a given position in the underlying design of a CA may deliver a change at position r xd far from the given position in the last setup under a sweep r govern iterated d steps. Assume a CA has L cells and the cyclic limit condition is taken, the emphasis number d is required to meet the condition in (Eq.1). With the above talk, the adequate torrential slide impact that a little changes in the original picture can cause an intense changes in the figured picture would be normal when d = L/4 for two-round encryption in our plan.

6. Histogram Analysis

The histogram plot is the graphical representation of the distribution of the grey values of an image where the y-axis corresponds to its frequency while the x-axis represents the grey values [16]. The histogram of the original grey scale image Lena of size 256 x 256 and its encrypted image are shown in Fig 1.5 from which we can see that the histogram of the encrypted image is flat where there is equal probability of occurrences of all grey values. Thus our encryption scheme can be robust against brute force attack and dictionary attacks.

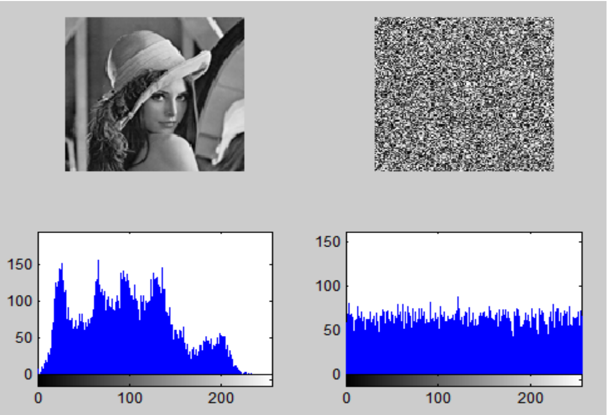


Fig. 6.1: Showing Histogram Analysis for Original Image and Encrypted Image Vice Versa

7. Key Space Analysis

The system has been tested using images of grey level with a scope of 128X128 using in the Matlab Simulator.

The Key space is computed by the entire number of keys utilized in the encryption process. It has large key space so that brute force attack is impossible. As the following proposed encryption has 5.087X10^{135,} hence, the scheme is not feasible for brute force attack.

8. Correlation Analysis

The pixels in a picture are deeply correlated with their corresponding pixels in the directions of vertical, horizontal, diagonal or anti-diagonal .However a secure encryption scheme should maintain an effectively very low correlation of the adjacent pixels, we have computed their correlation coefficient using the illustrated formula given below:

$$Cov(r,s)=E((r-E(r))(s-E(s))) \quad \text{-Eq.2}$$

The archived correlation data are illustrated in the following table:

Table 1: Correlation Table

Input Images	Lena.png	
Horizontal	1.00000000000000e+000 891.522905946749e-003	891.522905946749e-003 1.00000000000000e+000
Vertical	1.00000000000000e+000 949.430039627772e-003	949.430039627772e-003 1.00000000000000e+000
Diagonal	1.00000000000000e+000 853.124830925468e-003	853.124830925468e-003 1.00000000000000e+000

Table 2: Correlation Table

Input Images	Lena_enc.png	
Horizontal	1.00000000000000e+000 4.35117173876768e-003	4.35117173876768e-003 1.00000000000000e+000
Vertical	1.00000000000000e+000 -5.92879335242071e-003	-5.92879335242071e-003 1.00000000000000e+000
Diagonal	1.00000000000000e+000 13.2150704010503e-003	13.2150704010503e-003 1.00000000000000e+000

9. Differential Attack Analysis

The analysis is also taken as to assess the impact of the singular-pixel change in comparison to the original input picture. It helps to determine the unified average changing intensity (UACI) and thenumber of pixel changing rate (NPCR).
Let I1 and I2 be the two encrypted images whose corresponding plane pictures have only single-pixel indifference.

The grey value of the pixel at grid (r,s) in I1 and I2 as I1(r,s)and I2(r,s) are defined respectively. We determine a same size of the input image as a bipolar array M. The NCPR is defined as follow:

$$NPCR = \frac{\sum_{r,s} M(r,s)}{W*H} * 100\% \qquad \text{-Eq.3}$$

Where width and height as W and H respectively, hence UACI is also defined in similar fashion with the following equation.

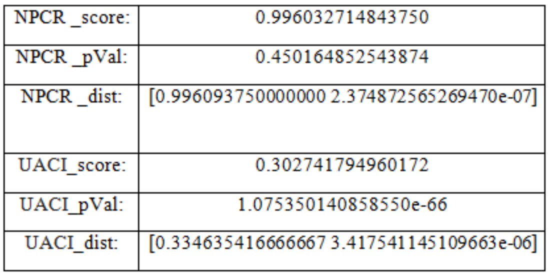
$$UACI = \frac{1}{W*H}\left[\sum\nolimits_{r,s}\frac{|I1(r,s)-I2(r,s)|}{255}\right] * 100\%\text{-Eq.4}$$

NCPR is calculating the percentile difference of different pixels between two pictures and UACI is calculating the mean intensity differences of the twocorresponding pictures.

The results generated by the corresponding cipher images interpreted by the NPCR and UACI tests have been shown in the following table:

10. Result

Table 3: Table for NPCR AND UACI Score



NPCR _score:	0.996032714843750
NPCR _pVal:	0.450164852543874
NPCR _dist:	[0.996093750000000 2.374872565269470e-07]
UACI_score:	0.302741794960172
UACI_pVal:	1.075350140858550e-66
UACI_dist:	[0.334635416666667 3.417541145109663e-06]

11. Conclusion

This paper is presenting a fast, robust, enforced cipher for a WSN application using an encryption scheme of chaos-based on the coupled map lattices. This process makes the encryption scheme harder to break for adversaries. Another major advantage of the proposed system is that it has the ability to encrypt text and images. The encrypted image security for the givendesign is being assessed by the correlation of the two given adjacent pixels, the key space analysis and the differential attack. The encrypted image distribution is very similar to the uniform distribution, which has the ability to protect the image's information which helps to resist the statistical attack probably. Hence, suggesting that this given encryption design iscompactible for the given jobs like online image encryption and safe transmission of confidential data on the internet. The encryption scheme discussed in this paper has some limitations like:- (i) it has been designed to work with predefined block size which means that input images has to be synchronized according to the block size.(ii)Encryption scheme is able to encrypt coloured images has not been verified. In our future works, we will try to implement a protocol for audio and video encryption.

References

[1] Hara T., Zadorozhny V.I., Buchmann E., Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence 278 (2010).

[2] Wang Y., Attebury G., Ramamurthy B., A Survey of Security Issues in Wireless Sensor Networks, IEEE Comm. Surveys & Tutorials 8(2) (2006), 2-23.

[3] Abbasi A.A., Younis M., A Survey on Clustering Algorithms for Wireless Sensor Networks, Computer Comm. 30(14/15) (2007), 2826-2841.

[4] Yi S., PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks, Computer Comm., 30(14/15) (2007), 2842-2852.

[5] Vineeta P., Pratikkumar Bharti., Ketankumar D., Aishwarya V., Munazza F., UWB Adhoc Wireless Sensor Network for Structural Health Monitoring and Facility Management of Warehouses, International Journal of Engineering Trends and Technology (IJETT) 33 (6) (2016).

[6] Pradeepa K., Anne W.R., Duraisamy S., Design and Implementation Issues of Clustering in Wireless Sensor Networks, Int'l J. Computer Applications 47(11) (2012) 23-28.

[7] Oliveira L.B., SecLEACH-On the Security of Clustered Sensor Networks, Signal Processing 87 (2007), 2882-2895.

[8] Banerjee P., Jacobson D., Lahiri S., Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks, Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA) (2007), 145-152.

[9] Zhang K., Wang C., Wang C., A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management, Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM) (2008), 1-5.

[10] Sharma S., Jena S.K., A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks, Proc. Int'l Conf. Comm., Computing & Security (ICCCS) (2011), 146- 151.

[11] Gaubatz G., State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks, Proc. IEEE Third Int'l Conf. Pervasive Computing and Comm. Workshops (PerCom) (2005), 146-150.

[12] Diffie W., Hellman M.,New Directions in Cryptography, IEEE Trans. Information Theory 22(6) (1976), 644-654.

[13] Shamir A., Identity-Based Cryptosystems and Signature Schemes, Proc. Advances in Cryptology (CRYPTO) (1985), 47-53.

[14] Yasmin R., Ritter E., Wang G., An Authentication Framework for Wireless Sensor Networks Using identity-based Signatures, Proc. IEEE Int'l Conf. Computer and Information Technology (CIT) (2010), 882-889.

[15] Lu H., Li J., Kameda H., A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID Based Digital Signature, Proc. IEEE Globecom (2010), 1- 5.

[16] Sun J., An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks, IEEE Trans. Parallel & Distributed Systems 21(9) (2010), 1227- 1239.

[17] Even S., Goldreich O., Micali S., On-Line/Off-Line Digital Signatures, Proc. Advances in Cryptology (CRYPTO) (1990), 263-275.

[18] Liu J., Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network, Int'l J. Information Security 9(4) (2010), 287-296.

[19] Sivakumar D., SrikiranRao S., Gokula Krishnan S., GuruKarthikeyan V., Case Study: Setting up VOIP Network Over Wireless Mesh Network in Campus, International Journal of Engineering Trends and Technology 34(1) (2016).

[20] Chintala R.R., Rao M.R.N., Venkateswarlu S., Design of a Secure System for Reading Patient's Data Using Medical Sensor Networks, JCPS 10(1) (2016), 673-679.

[21] Nagendram S., Radhika Rani C.H., A Study on Content based image retrieval and storage methods for medical Images, International Journal of Research in Science and Technology 1 (2) (2011), 27–33.

[22] Nagendram S., Rani C., Sharma G.S., A Study on Content Based Image Retrieval and Storage Methods for Medical Images, CLEAR International Journal of Research in Science & Technology 1(2) (2011).