IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

A Problem Evaluation of Algorithm for Secure Node Authentication in Wireless Sensor Network

Jatinder Kaur[1*], Navroz Kahlon[2]

[1]Department of Computer Engineering Punjabi University Patiala (Pb.) Punjab,
[2]Department of Computer Engineering Punjabi University Patiala (Pb.) Punjab.

Available online at: www.ijcseonline.org

Accepted: 12/Aug/2018, Published: 31/Aug/2018

Abstract- The Wireless sensor is an improved technology for gathering highly sensitive information. Wireless sensor devices are used to gather this information with the help of sensing nodes. These devices are used in various fields but the rapid consumption of energy in wireless network and its usage is still a challenge for researchers. This paper has been designed to provide the security to user credentials as well as private key distribution for the data transmission of secure. We are proposing a new algorithm in this research paper to trim down the consumption of energy as well as to provide security in the network. It will improve the lifespan of the network.

Keywords- WSNs, cluster head, authentication, Homomorphic algorithm, energy consumption, LEACH.

I. INTRODUCTION

Wireless sensor network is a latest technology that plays the significant role in monitoring and tracking the targeted environmental and physical conditions such as temperature, pressure, light, sound and so on to efficiently transfer the data between nodes through its network to main station. The wireless sensor nodes are spatially dispersed and dedicated autonomous nodes.

STRUCTURE: The wireless sensor network is a collection of nodes called sensor nodes which are connecting with each other to build a network to transform the data. WSN may have hundreds or thousands nodes that are connected with single or multiple sensors. These nodes are tiny computers and light in weight as well as portable. Each sensor node has three parts: a microcontroller, a radio transceiver and battery. A microcontroller links the nodes with each other as well as with base station whereas radio transceiver enables the connectivity with external link. There are various topologies formed by network like star topology, ring topology, multi-hop mesh network in which data propagation can be routing or flooding.

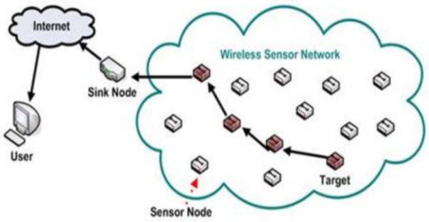

Figure1: Structure of WSN

APPLICATIONS

There are numerous applications of WSN in various fields comprises of area monitoring. WSN is set up in particular area to monitor the physical conditions like enemy intrusion during war, health care monitoring to check overall health of the patient in the hospital as well as home. It is also used to monitoring environmental conditions such as concentration of gases in air, forest fire detection, slight movement in soil, analyze the properties of water in lakes, rivers and oceans. Furthermore WSN applications are used in the industries to track and monitoring the machineries, data logging, building infrastructure and so on.

II. MOTIVATION FOR THE WORK

The advancement of WSN altered the mind of researchers through the globe to search various methods of widening up the scope of WSN at higher levels. The limitations of the previous work have no longer limit the capability of sensors in real applications. However, there is another inflexible need of sensory node which defines the life time of network as well as efficient usage of energy. Although the nodes in WSN communicate with other in isolated environment still these nodes have the external links. All the criteria related to this only depend upon the selection of cluster head. For this lot of researchers have proposed various algorithms for cluster analysis that is the process of grouping the nodes which are in similar in one way. Thus it forms a network of clusters where each cluster has a cluster head along sensor nodes for transmission of data to base station. Cluster heads can be selected randomly or on the basis of decision factor.

The increasing use of WSN emerged some questions in terms of effective and efficient use of energy related to enhancement of WSN lifespan. Although lot of researchers have presented lot of algorithms on how to choose a efficient cluster head to secure a user credentials but still a more needs to be done in this field to get over the limitations of existing work.

III. MAJOR CONTRIBUTIONS OF THE PAPER

Major contribution of this paper is to secure the user credentials through efficient secure base clustering and this is accomplished through LEACH protocol. By taking in mind the various limitations as well as issues while selecting the cluster head based on following criteria:

1. Firstly, it will keep an account of the nodes as well as their energy consumption record.
2. Then put the subjected homomorphic algorithm into execution and will optimally allocate the security in the WSN.

ORGANIZATION OF PAPER

The paper defined and organized as follows: section 1 contain the introduction of wireless sensor networks, section 2 contain the related work regarding to various security algorithms, section 3 contain the information about protocol and algorithm, section 4 explain the methodology with flow chart, section 5 describes the results and discussion and section 6 concludes research work.

IV. RELATED WORK

A lot of researchers provide fool proof algorithms to provide the security in wireless sensor network but no one is successful to provide best method. Lifespan of the WSN is affected by the method of selection of cluster head as well as to secure user credentials. For this reason many researchers have lot of algorithms to select the cluster head and enhance the lifespan of WSN. But a more research needs to be done in this field as majority of the existing methods have their own limitations.

A. SECURITY BASED TECHNIQUES TRUSTED NEIGHBOUR BASED SECURED ROUTING ALGORITHM

Most previous schemes have not considered malicious nodes in the network. The network described in this paper contains black hole nodes and malicious node drop packets. Thus the arrival ratio of the data packet decreases. To improve it, this scheme was proposed. In this, when the source nodes send one data packet to the destination an abstract information is also transmitted to the destination. Thus, if the malicious node in the backbone drop the data packets but the destination receives the information from the source node, the destination will know that the routing path in the backbone contains malicious nodes. It also reduce its evaluation of the trust in the nodes in the routing path. After several rounds of data packet transmission the nodes will communicate each other. If node has lower trust, node will be identified as a malicious node. Thus in the next round of data transmission this node will not be selected in the backbone and with it data packet arrival ratio will also improve. There is one drawback of this scheme is that it unable to calculate the occurring ratio of malicious node. [1]

EFFICIENT TRUST MANAGEMENT SYSTEM

In trusted neighbor based technique one problem is encountered that is the calculation of node communication time with other nodes. To overcome this problem simple and efficient algorithm is implemented. In this algorithm firstly the value of trusted node is calculated to find the malicious node with the help of packet forwarding factor calculated the value of the trusted node and found the malicious node on the basis of packet forwarding factor. It also determined the consistency of clusters and lifespan of the network with only one limitation that is the multi hope communication which increase the overhead cost in WSN. [2]

B. DATA AGGREGATION TECHNIQUES

After finding the malicious nodes in the network is not enough to provide security in the network. So to provide security in WSN various aggregation techniques were based on various parameters such as security principles, prevention of attacks by protocols, aggregation function, and cryptographic techniques but these were failed to judge the accuracy and energy consumption over network and also discussed various security loopholes in wireless sensor network. [3]

TRUSTED AND REPUTATION MODEL

The efficient and trusted model is proposed in WSN to determine the various effects of modes such as static, dynamic, oscillating to judge the accuracy, path length as well as energy consumption in network. Although it comprises various models like Eigen trust, bio- inspired, peer trust, linguistic fuzzy trust as well as reputation but it do not cover all major types of threats arise in WSN. [4]

COLLABORATIVE LIGHTWEIGHT METHOD

In WSN minimal overhead in regard to memory and energy consumption is also introduced. For this a collaborative lightweight method is designed in which works on a threshold value. For instance counselor tracked and send the warning information to that node whose trust fell below a warning threshold. After that the warning message warned the sensor node to check the black node and then sensor node modify the packet forwarding behavior to improve its relation with neighbor node. The limitation of this method is that the all nodes has the same name due to that one node is not reuse for some other. [6]

C. ATTACKS PREVENTING METHOD

Unlike traditional networks, the WSNs are very vulnerable to internal attacks from compromised nodes.

BETA BASED TRUSTED SCHEME

To improve the WSNs' information security as well as to minimize the probability of attacks the efficient technique is used called beta based trust and reputation method. In this research, the only limitation is that researchers failed to consuming energy in WSN optimal manner.[5]

IMPROVED TRUST MANAGEMENT SYSTEM

Above mentioned all the techniques did not specified the relation between nodes, only successful to find the malicious nodes in the network so for this a improved trust management system is proposed which is used to specify the relationship between nodes and also enhancing the utilization efficiency of that information which is coming from other node but the only limitation is that it fails to consuming energy in WSN in optimal manner. [7]

D. DISTRIBUTED ENERGY AWARE TRUST MANAGEMENT METHOD

One more thing is needed to be taken in mind that is the speed. Speed play an important role in WSN to detect the malicious nodes as soon as. To implement this method a distributed energy aware system is proposed in WSN which is routing based method. Its main aim to detect the set of attacks very quickly and also introduced the idea of energy awareness. [8]

E. NETWORK IMPROVEMENT BASED METHOD

The two-tiered network architecture of WSN is also designed for increasing network capacity and scalability, reducing system management complexity, and prolonging network lifetime. The limitation of their research they implement Authentication scheme at one level factor.[9]

F. INTERNET BASED SCHEMES

As the Internet market grows, the importance of the WSN which is the network environment on which the Internet is based, is becoming more important. [10]

G. COST REDUCTION METHOD FOR WSN

It is very hard to reduce cost as well as to maintain staff intensity. Furthermore, remote meter reading is also accomplished through WSN. In this abstract the corresponding credits are transmitted over the WSN (Wireless Sensor Network) to the client terminal to recharge on the ESAM and the related data are uploaded to the upper management centre, this way, avoiding the problem brought by IC card as the information carrier and reducing operating costs and staff labor intensity. [11]

H. EFFICIENT TRANSMISSION APPROACH FOR ICN BASED WSN

In this method additional security layer is used to provide data privacy and security in WSN. For this efficient transmission approach for information centric based network (ETAICBWAN) is proposed. This algorithm classify the data into different classes according tom priority (high, normal, low) as well as communication base station buffers the information in the designated queue. Although this method improves the data transmission performance of WBAN but it has one limitation it is not capable for complex network and does not have any specific model. [12]

With the advancement of WSN tools and sensing gadgets, various industries such as electrical, transportation, and other production equipment industries have started installing these devices for smooth functioning. No doubt in coming years WSN sensing devices will gain the popularity however, the biggest challenge is the network reliability to transmit data and power consumption. So for this cluster head requires a proper selection method to secure the user credentials as well as to boost up the lifespan of the network. Although lot of research has been done in this field but no one can proposed the efficient method to secure the user credentials on the basis of cluster head.

V. PROBLEM FORMULATION

In existing research work they have used elliptic curve algorithm to encrypt username and password then send credentials in network. In elliptic curve algorithm, public key elliptic curve algorithm was used. As a result, communication cost was increased. To overcome this issue we will use homomorphic encryption key algorithm using LEACH protocol to encrypt the credentials of user. So that it becomes hard to decrypt by unauthorized users. By using this algorithm authentication cost will also decrease as compare to public key authentication scheme.

VI. PROPOSED METHODOLOGY

In this we first design a framework for wireless sensor network. After designing the network we will check that every node is connected with other node or not. After that implementation of proposed algorithm will be discussed as well as comparison with previous algorithms. To secure the user credentials and to improve the communication cost we will use homomorphic encryption key algorithm. For the formation of the clusters in the network and communication between nodes we will use LEACH protocol.

A. LEACH (LOW ENERGY ADAPTIVE CLUSTERING HIERARCHY)

It is TDMA based MAC protocol which is integrated with clustering as well as simple routing protocol in WSN. The main goal of LEACH is to lower the energy consumption in network to create and maintain cluster head to improve the lifespan of the network. It is a hierarchical protocol, most of the nodes in network are send to the cluster head. LEACH takes the record of nodes that each node has a radio powerful enough to reach at the base station but using this power can lead to wastage of energy.

Nodes that are already the part of the cluster head cannot become cluster heads again for C rounds where C is the desired percentage of cluster head. Each node has an 1/C probability of becoming the part of cluster head. The node which is not cluster head, in the end choose the nearest cluster head and joins the cluster. All nodes that are not cluster head communicate with cluster head in a TDMA fashion. LEACH also uses CDMA to reduce the interference between nodes.

Properties:

- Cluster head
- Cluster membership
- Data aggregation at cluster head
- Cluster head communication directly with user
- Threshold value

B. HOMOMORPHIC ENCRYPTION

It is mathematical approach which allows computation on cipher text, generate an encrypted result. After that result are matches with result of operations when decrypted as if they had been performed on the plain text. The only purpose this scheme is to allow computation on encrypted data. The data in a homomorphic encryption method retains the same structure, identical mathematical operations. No matter, whether they are performed on encrypted or decrypted data. Homomorphic encryption is malleable by design means a system in which anyone can access the information and send to destination. We can say that black hole node can access the information by dropping the packets from the network. So to overcome this problem one method is introduced in this paper that is on the basis of private key distribution. Each user will have its own private key when attempting the login and there will be impossibility of hacker node to access the packet in network.

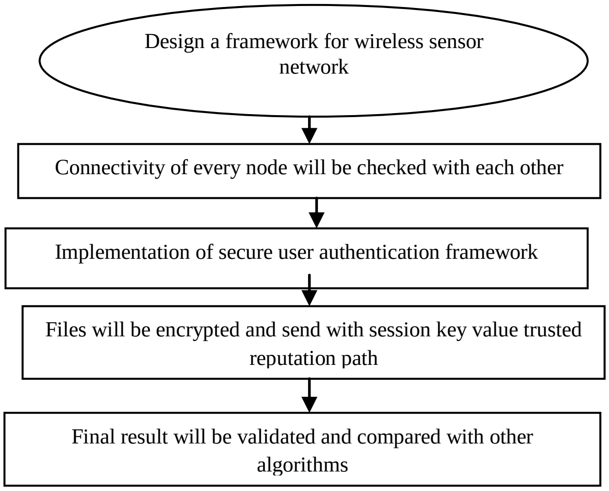
Design a framework for wireless sensor network
Connectivity of every node will be checked with each other
Implementation of secure user authentication framework
Files will be encrypted and send with session key value trusted reputation path
Final result will be validated and compared with other algorithms

Figure 2: Flowchart of Methodology

C. PHASES OF METHDOLOGY INITILAZATION PHASE

In this phase, users of the network will create their accounts by the registration process. For the registration process, there is availability of login form which must be filled with accurate information. There is the various security parameters used for authentication and key agreement are calculated by the control center and the substations.

Table 1**:** Notations used in algorithm

U	user
P	Base point
ID	Identity of user
SID	Shadow identity of user
h(.)	One way hash function
SK	Secret key
e_{pk}	encryption
D	substation
r	Random integer
PSW	password
C	Shared key
||	Concatenation operator

1. First homomorphic equation Hp (a,b): $y^2= x^3+ax+b$(mod p) over a prime finite field F_p is selected by control center. After that control center selects a base point P over H_p (

a, b) and writes P to the temper resistant device of U_i as well as the substations. Here U refers to user.

2. Then control center allocates identity ID for each user and store in memory of the corresponding device. This stored ID is written in data table by the control center and then control center submits this identity table to the substation over secure channel and assigns an identity SID each substation S, substation stored it in memory securely. Finally a one way hash function selected by the control center that is h(.): $\{0,1\}^*$ to $\{0,1\}^k$ is selected by the control center and store the hash function in their memories.
3. Substation selects a random integer $^{s}\in^{RZ^*}{}_{P}$ as a secret key for symmetric encryption/ decryption and then it generates a random integer sk<n as a private key and produce public key pk= skP, where n is the order of base point P. this public and private keys (pk,sk) are used for asymmetric encryption/ decryption.
4. After this substation calculates $C_1 = E_s(ID)$ and C_2 = SID for every user U. furthermore, the substation writes the public key pk and the pair secret (C1,C2) into each corresponding tamper resistant device.
5. If a new user U_j wants to login in network, the control center and the base station should complete the initialization step of the new user by registering. Control server provide the unique id to new user U_j and records it in the database table as well as send this ID to the corresponding base station over a secure channel. After checking the key base station achieve the initialization of the new smart user.

AUTHENTICATION PHASE

After completing the initialization phase authentication process starts .During this phase following steps are performed to realize mutual authentication and key agreement.

- The device of user selects an integer to compute $C_3 = e_{pk}(ID||C_1||r_1)$, where $e_{pk}(.)$ denotes the public key encryption function using the substation S_j's public key pk and $C_{1=}E_s(ID)$ is a secret key stored in the device of U_i sends $C_3 = e_{pk}(ID_i||C_1||r_1)$ to the substation $S_{j.}$
- In this step, substation S_j receives the ID and match it with table stored in database. If not matched or valid, the authentication process stops. Otherwise the login successful and user U_i can start the communication process after verifying its secret key $r_{1.}$
- Here integer r_3 needs not be encrypted because it is only used for freshness of message. It has no connection with final session key in any way.
- After taking the message (C_4, r_3) the user U_i adopts r1 to decrypt C_4. Then also takes r_2 and SID_j. after calculating SID_jP it checks the equation. If equation holds the user calculates the shared session key $SK' = h(r_1 \| r_2)$ as well as authentication message $C_5 = h(SK' \| (r_3 + 1))$ and send it to substation $S_{j.}$ Otherwise authentication process terminates.

In case of any modification if the substation needs to be changed, it submits all the shared keys to corresponding smart appliance and itself. Then deletes the ID's from table and the new session key between the new substation D_l and the smart appliance can be achieved by running the proposed key agreement protocol to realize the secure and easy change of the substation.

LOGIN PHASE

- When a user declared as authenticate then login phase starts. In this phase Ui login with his registered ID and Password(PSW) stored in database.
- After login Ui can communicate with other users in the network. This communication can be done in both ways depend upon user's choice whether sending the message in group or particular user.
- It can be done easily but firstly user have to refresh its user list.

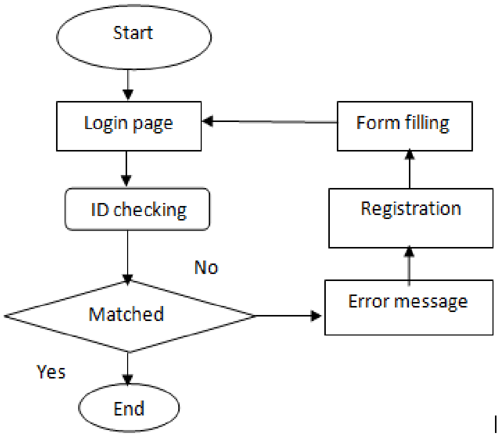

Figure 3: Login process

LOGOUT PHASE

It is the last phase. If a U_i want to stop communication then user can easily leave the network only by clicking the logout button.

- During logout the corresponding data is stored in database by the specific name of that user.

VII. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed system is evaluated using the following performance metrics:

End to end delay (ms): It is also said that one way delay (OWD). End to end delay refers to the time taken by a packet to be transmitted across a network from source to destination. It can be measured between two nodes A and B of an wireless sensor network through the use of synchronized clocks. Such as user A records the timestamp on the packet and then sends it to user B. user B notes the receiving time and calculate the end to end delay as their difference. The most significant point states that transmitted packet should be identified at the end of receiving to avoid from any packet loss.

- It is denoted by E_n the time instant of the n^{th} packet arrival at a network and denote by V_n the time of the n^{th} packet departure from the network. The end to end delay of the n^{th} packet can be mathematically calculated by:

$D_n = V_n - E_n$

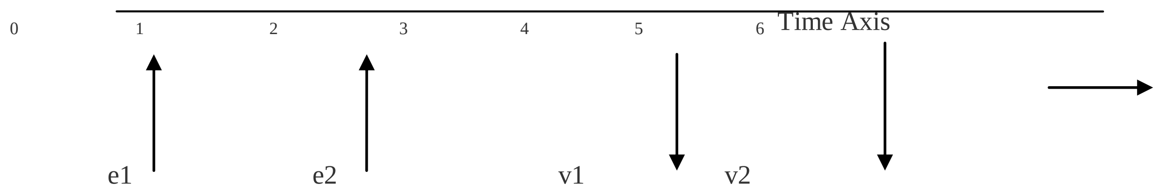

Figure 4: An example of end to end delay

$D_n (1) = 3.5\text{-}0= 3.5$

$D_n (2) = 5.5\text{-}1.5= 4$

Packet arrival rate (%): the arrival rate is the number of arrivals per unit time. The inter arrival time is time between each arrival into network and the next. A router can only process one packet at a time. The average delay can be calculated by given formula:

$$M_n = 1/(\mu\text{-}\lambda)$$

Where μ = no of packets, λ = average rate at which packets are arriving

Table 2: Quantitative results of proposed and other algorithms for various performances metrics

Parameters	**Number of nodes(1 to n)**	**ETAICWBAN(efficient transmission approach)**	**ICN(information centric network)**	**Proposed**
End to end delay (ms)	1	8	9	6
	2	6	5	2
	3	7	4	3
	More than 3(group)	6.5	4.5	5
Packet arrival rate (%)	1	0.93	2.5	0.163
	2	3.52	5.23	0.043
	3	1.34	2.30	0.887
	More than 3(group)	4.20	3.21	0.514

For computing the results of performance metrics stated in above section experiments are implemented in Java, Jdk 1.8 version, Net beans 8.1 on i5 processor. The performance of algorithms is evaluated using both qualitative and quantitative evaluation trends and results of the stated performance metrics are analyzed and compared. Table 2 represents the objective evaluation. An algorithm can deliver satisfactory result for one or more parameters but may not be suitable for the rest of the parameters. Quantitative result in table 2 represents the comparison between different algorithms. ICN is better than ETAICBWAN delivers satisfactory results for both the parameters. But among these algorithms homomorphic delivers the efficient results when tested for both the parameters. The proposed technique has lesser values as compared to others which means it takes lesser time to send packets from source to destination and improves the overall cost of communication.

VIII. CONCLUSION

In this research study, we proposed a new algorithm wherein a cluster head form a wireless sensor network to reduce the consumption of energy in the network and simultaneously boost-up its lifetime. In this experiment, we kept a close watch not only on the energy that was being dissipated after every transaction but also on the number of packets that had been delivered by the nodes as well its neighbor nodes to determine the accuracy and efficiency of selected cluster head more likely to secure the user credentials. In this study, our algorithm succeeded in order to trim down the energy consumption rates of the nodes and improve the lifespan of the entire network.

REFERENCES

[1]. Geetha D. Devanagavi, N. Nalini .”Trusted Neighbors Based Secured Routing Scheme Using Agents.” Springer transactions on routing algorithm,014-1704-4. 2014.

[2]. Monia , Sushma Jain ,Sukhchandan randhava .” An Efficient Trust Management Algorithm in Wireless Sensor Network .”Springer 0287-8_26. 2016

[3]. Mukesh Kumar and Kamlesh Dutta.“.A Survey of Security Concerns in Various Data Aggregation Techniques in Wireless Sensor Networks.” Springer India . 2009.

[4]. Vinod Kumar, Surinder Singh, N.P. Pathak .”Various trusted and reputation models wireless sensor networks.” Springer Science ,1144-4. 2015

[5]. Weidong Fang , Chuanlei Zhang , Shi Qing Zhao. "Evaluation system and reputation Beta-based Trust in WSN" 1084-8045 Published by Elsevier Ltd. 2015

[6]. X Anita , M.A. Bhagyaveni. "Collaborative Lightweight Trust Management Scheme." Published in Springer Science ,014-1998-2. 2014

[7]. Yun Liu, Qing-An Zeng. ".Improved trust management scheme for secure data aggregation" .Springer publications 015-0078-6. 2015

[8]. Yannis Stelios, Sitiris Maniatis, Helen C. Leligoug. ".Routing based Distributed Energy-Aware Trust Management System in Wireless Sensor Networks". Institute for Computer Sciences and Telecommunication 85-92. 2016

[9]. Rong Fan, Ling-Di Ping, Jian-Qing Fu , Xue-Zeng." Two tired architecture of WSN." Pan College of Computer Science and Technology Zhejiang University 5626600.2010

[10]. Gun-Wook Choi . "paired base key distribution scheme in wireless sensor network."IEEE publication 10.1109. 2017

[11]. Karim ZKIK Ghizlane ORHANOU Said EL HAJJI ." Secure framework using ECC".10.1109/ICEngTechnol.2017.8308144 .2017

[12]. longzhe Han , Xin Song, Yi Buz ." province key laboratory of water information cooperative sensing processing" 330099. 2015

[13]. Kamal, L.K. W- LEACH, abdulsalam ." Weighted low energy adaptive clustering hierarchy aggregation algorithm for data stream in WSN". IEEE 1-8. 2010

[14]. Younis, M A, Akkaya. " A survey on routing protocols for WSNs". 325-349. 2005

[15]. ." A survey on sensor networks." IEEE communication. 102 - 14.2016

[16]. Kamal, A.E. "Routing techniques in wireless sensor networks." IEEE, 6-28.2012

[17]. Maja J Matari c, Andrew Howard and Gaurav S Sukhatme ."Mobile sensor network deployment using potential fields". DARS02 425-6788.2010

[18]. Holliday, J,Ding.."A distributed energy efficient hierarchical clustering for wireless sensor network". IEEE conference on distributed computing in sensor networks. 322-339. Fan, X.; Song, Y. Improvement on LEACH Protocol of Wireless Sensor Network. In Proceedings of International Conference on Sensor Technologies and Applications, Valencia, Spain, 14–20 October 2007, pp. 260–264. 2015

[19]. Fereris , Kowshik,N.M. H Kumar. "Fundamentals of large sensor networks." IEEE, 98, 1828-1846. 2010

[20]. A. bestavros, G. Smaragdakis, I. Matta,." A stable selection protocol for herogenous wireless sensor network."1245-1267. 2017

[21]. Halpern, Haas, Z,J, Li, L . "Gossip based adhoc routing in WSN." INFOCOM, New York, pp. 1707-1716. 2016