IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Simulation of Traffic and Energy Aware Routing (TEAR) Protocol for Efficient Data Transfer in Wireless Sensor Networks

SARAGADAM ANURADHA [#1], KOTHAPALLI SAMEER[#2],

K PRAMEELA[#3]

[#1] M.Tech Student, Department of Computer Science and Engineering,

[#2] Head & Assoc. Prof, Department of Computer Science and Engineering,

[#1,#2] Gonna Institute of Information and Technology &Sciences

Gonnavanipalem, Aganampudi,Visakhapatnam,530053.

[#3] Assistant Professor, Department of Computer Science and Engineering,

Vignan Institute of Information Technology, Visakhapatnam.

ABSTRACT

Now a day's lot of information is send from one location to another location with the help of some dedicated path with a substantial IPaddress and port number inside the system. During this data communication there may be some type of assaults that happen in the field of information technology, which may lead to delay and data loss. In general there are lot of attacks which occur in the network during data communication either in wired or wireless networks, one among them is Energy attack or Packet Dropping attack. This is one in which the attacker try to reduce the energy or bandwidth of the wireless node and try to make the node into off state. This will mainly increase in packet delay and sometimes lead to data loss. In the primitive algorithms there is no single method to detect and prevent the energy loss nodes and send the data under best path without having such low energy nodes. In this proposed paper we try to design a model known as TEAR Protocol (Traffic and Energy Aware Routing) Protocol in wsn for identifying the nodes which is having high energy among a set of nodes and then try to choose one which is having highest energy as cluster head (CH).In this way if we try to form a best path with all high energy nodes the data will be send under no packets loss from one location to another location.

Key Words:

Traffic and Energy Aware Routing, Cluster Head, Wireless Sensor Networks, Bandwidth Attacker, Data Communication.

1. INTRODUCTION

Internet of Things (IoT) has become one of the main source for interoperability of heterogeneous gadgets to help differing applications, and WSN is becoming as one of the most prominent among those IOT gadgets. Although it is having a lot of heterogeneity (e.g., vitality, connect and computational heterogeneities) [1] this can greatly increase the ability of fast data sending,calculated,increase in quality,accuracy,long distances and a lot more. The vitality heterogeneity in WSN is mainly classified in very broad manner and hence the vitality heterogeneity, are moderately less investigated regions. In the primitive methods of WSN accurate calculations for identifying data heterogeneous is unstable. One of the method which is used in the existing networks is Stable Election Protocol (SEP) [2] and another is Low-Energy Adaptive Clustering Hierarchy (LEACH) ,which is clearly seen in figure 1 [3].

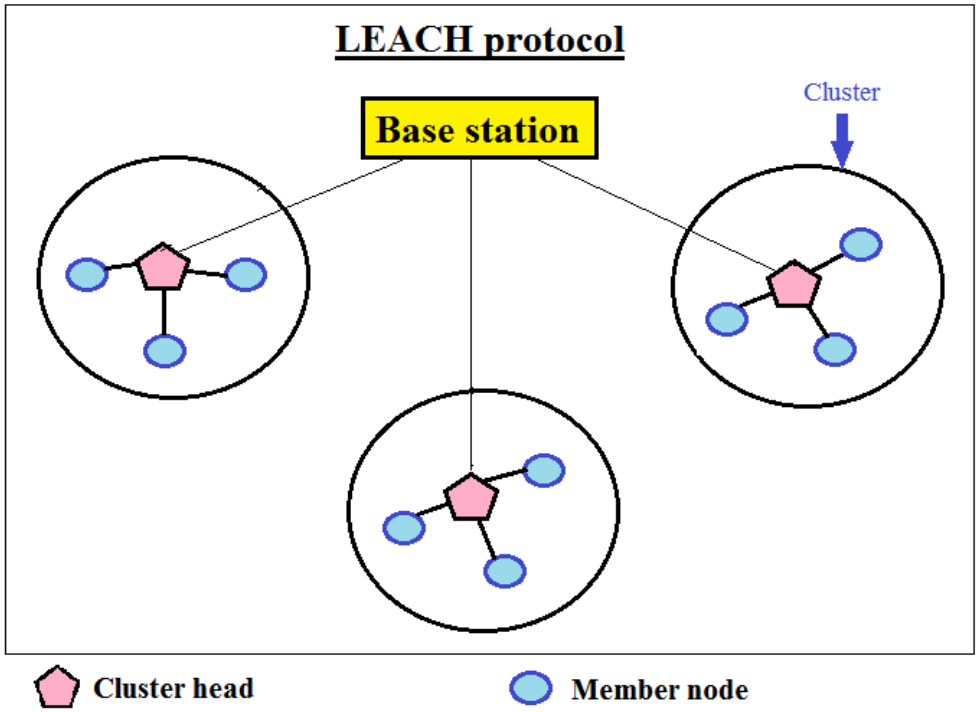


Figure 1. Represent the Leach Protocol in the Existing System

SEP is mainly deployed by gathering all the participating nodes information and try to conduct an election on set of nodes which are present within the networks. In this the node identification is mainly done based on the node which is having high number of connected nodes all together attached with this appropriate node and hence there is a very less probability in finding the best nodes. If the node which is having more number of connections is got off then all the other ways will also be terminated by that node failure, hence this method is failed to achieve the principle of data integrity. Another method which is used is LEACH in which this will be finding all the energies which are underlying inside the cluster and try to regenerate the energy for those low energy nodes and then send the data according to those best nodes. But this is failed to identify the failure nodes prior to data transfer, and hence this is also not accurate in data transfer. Hence in this proposed application we came with a new concept like TEAR protocol in which the TEAR shows enhancements as far as solidness period over existing calculations (LEACH, SEP) under the situation.

2. BACKGROUND WORK

In this section we will mainly discuss about the related work which is already some by some of the previous authors in WSN domain. Now let us discuss about them in detail

MOTIVATION

1) **E. Alami and Najid et al.** [8], have composed a paper on "Stable Election utilizing three Fuzzy Parameters (SEFP) to build the system lifetime and solidness time". In this proposed paper the creators for the most part focused about the various remarkable boundaries like hub power, base station separation and absolute separation between all the hubs and individual proximity separation between any two hubs. By considering every one of these boundaries we can ready to distinguish the exactness about the system life time and we can get the solidness of that current system, yet this is having one confinement like the proposed strategy is neglected to recognize the sink hub good ways from each group and its unwavering quality nature to distinguish the traffic as one of the most critical factor.

2) **Lee and Kao et al.** [9] , have composed a paper on "Semi-conveyed grouping technique by considering a half and half of brought together gridding for the upper-level CH choice and dispersed bunching for the lower-level CH selection". In this proposed paper the creators principally focused on the bunching strategy by taking an example of cross breed organize which contains a ton of hubs for sending the information under substantial way. This paper is essentially separated the system into a few groups and each bunch will contain two fundamental hubs one is upper level group head and another is lower level bunch head. The proposed creators is accomplishment in distinguishing those two boundaries in unique way with exact outcomes. Yet, the fundamental restriction with this current paper is there is no honesty and dependability for recognizing the best CH hub to convey the parcels from source to goal hub.

3. EXISTING METHODOLOGY

In the existing system almost all the routing methods are normal routing technique for sending the data from one location to another location. All the primitive methods try to identify the best path based on shortest path algorithms like Prims, Krushal and so on. But there is no single method which can identify the best path based on energy or high bandwidth and then try to send the data under that best path.

LIMITATIONS OF THE EXISTING METHODOLOGY

The following are the limitation of existing system. They are as follows:

1. The existing system didn't concentrated on the property of cost (I.e. In terms of Energy).
2. In the existing system if there was any node failed in the network entire architecture need to be changed and hence it is a delay process.
3. If the node which has very shortest distance to reach the destination has less energy or bandwidth, the same data may be transferred in the estimated time to the destination.

4. There is no concept to identify the less energy nodes dynamically and choose a best path based on high bandwidth or energy nodes.

4. PROPOSED METHODOLOGY

In the proposed system we try to design a model known as TEAR protocol for sending the data under best path. In this proposed system the nodes which have high bandwidth will be chosen as transmission node and then data will be sending in that node rather than the nodes which have less energy. Here one node will be chosen as cluster head and this Cluster head node will find out all the other nodes energy dynamically and pick one best node and in the same way all other nodes were chosen under the best path. This will greatly reduce the packet delivery delay and also optimize the data loss.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system. They are as follows:

1. The Proposed system Mainly concentrated on the property of cost (I.e. In terms of Energy) to the destination, and greatly reduced a lot of time delay.
2. In the proposed system if there was any node failed in the network all the nodes need not be changed, the cluster head dynamically picks an alternate node based on best energy and send the data under that node.
3. There is a concept to identify the less energy nodes dynamically and choose a best path based on high bandwidth or energy nodes.
4. It is best in sending the data under wireless medium.

PROPOSED TEAR ARCHITECTURE

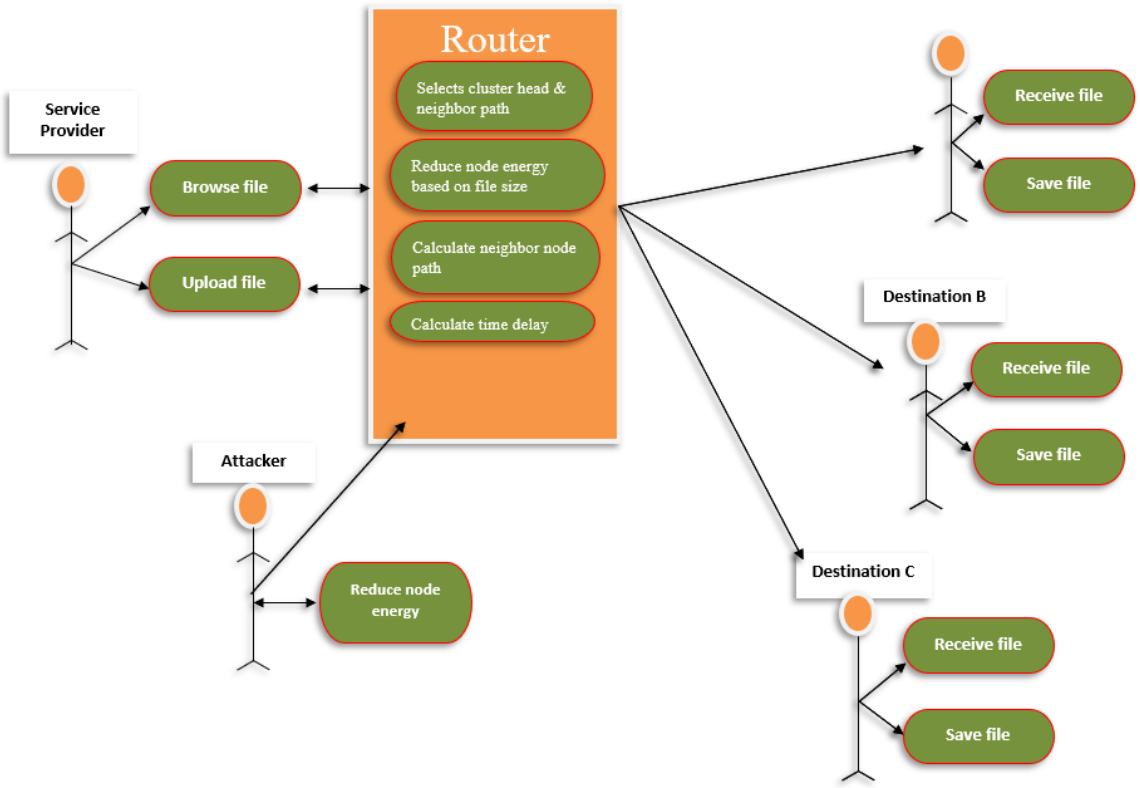


Figure 2. Represent the Proposed TEAR Protocol Architecture

From the above figure 2,we can clearly identify that TEAR protocol main contains following roles such as :

A) Service Provider
B) Router
C) Router Manager
D) Destination or End User
E) Attacker

Initially the service provider try to choose valid text file as input and divide the file into packets and then send to the router by substituting valid destination IPAddress.Once the router receives the data request from service provider, the router will then find out all the intermediate clustered nodes which are present inside router .This will be identified based on energy assigned for each and every node. Here the node which has high energy or bandwidth is treated as cluster head (CH) and then based on those selection the data will be send from source to destination nodes. If there is any attacker node which is present inside the router, then such attacker is identified by the router manager and immediately this manager will choose alternate route to the router node which is having high energy. In this way the data will be continuously send from source to destination under a dedicated path.

5. IMPLEMENTATION STAGE

Analysis /Implementation Stage is where the theoretical structure is changed over into programmatically way. Here we will try to divide the application into number of modules and then try to code them for deployment. The application is separated essentially into following 6 modules. They are as per the following:

1) Source/Sender Module
2) Router Module
3) Destination/Receiver Module
4) Router Manager Module
5) Attacker Module(Extension Module)
6) Performance Analysis Module

1) SENDER MODULE

In this module, Source browses the file, select the destination and sends to the router. In Source while uploading the file, divide the data into packets and then uploads the file. File content will be initialized to all the nodes. Here the source need to enter the valid IP address for sending the data from source to destination via router.

2) ROUTER MODULE

In this module, router consists of four Networks/Clusters, each cluster contains specific nodes. When Source sends the file initially it comes to the Network1 and passes through the Network1 nodes, if any congestion/Energy attack found in the Network1 node, It automatically selects the another node an moves to Network2 and Network 3 and Network4 and reaches the destination. The energy size also be modified, view the Network details. In the router the router can select one node from each cluster and treated as CH node(Cluster Head) ,and it greatly reduces traffic by omitting other low energy nodes.

3) RECEIVER MODULE

In this module, Receiver will receive the file from the sender via router under shortest path based on energy. Here the receiver can receive file only if he is a valid user and those who don't have permissions cannot be receive the file from the sender.

4) ROUTER MANAGER MODULE

In this module, ROUTER MANAGER views the attacker details by checking the energy details and find attackers. He is the one who acts as a back bone functionality for the router in verifying the attacker node details inside the router.

5) ATTACKER MODULE

This is an extension module in which the external attacker selects the Network and a node, gets the original energy size and modifies the energy size for the node. In this way an external attacker tries to create an attack inside the network and try to disturb the data flow.

6) PERFORMANCE ANALYSIS MODULE

This is an extension module in which the performance of data transfer can be calculated in two ways : One is Time Delay , Another is Throughput .So in this module we can able to find out the time delay and throughput delay for each and every data transfer which is done from source to destination nodes.

6. TEAR ALGORITHM

The CH selection in TEAR is based on the CH role rotation approach [2-4], where the node becomes a CH in the current round , if the random number selected by the node is less than the threshold T(i, r).

$$T(i,r) = \begin{cases} \frac{p_i(r)}{1-p_i(r)\left(r \bmod \frac{1}{p_i(r)}\right)} & if \quad node\ i \in G(r) \\ 0 & otherwise \end{cases}$$

Where P(r) is the CH selection probability for node I during round r .

(r) is a set of eligible nodes for the round , where the rotating epoch for node to become eligible again is 1/ Pi(r).

DEEC considers randomly distributed energy heterogeneity and prefers nodes with higher initial and residual energies for CH role, i.e. an energy-rich node has higher p (r) and higher chances of becoming CH.

As the operations of a CH are energy intensive, preferring nodes with higher initial energies and higher residual energies improves the life of energy weaker nodes and hence it improves the WSN stability period.

An increase in traffic loads increases the effective number of bits to be communicated to the BS and hence increases network energy consumption. In traffic heterogeneous scenario, the rate of energy consumption is higher for the nodes with higher traffic loads. So, it is logical that such nodes should be avoided for energy intensive operation, e.g., CH role. For a realistic WSN model, with the nodes having heterogeneous initial energies and data traffic requirements, the proposed algorithm (TEAR) prefers the nodes with higher energies (initial and residual) and avoids the nodes with higher traffic loads for CH role. In TEAR, the probability of becoming CH for node I during round r is defined as

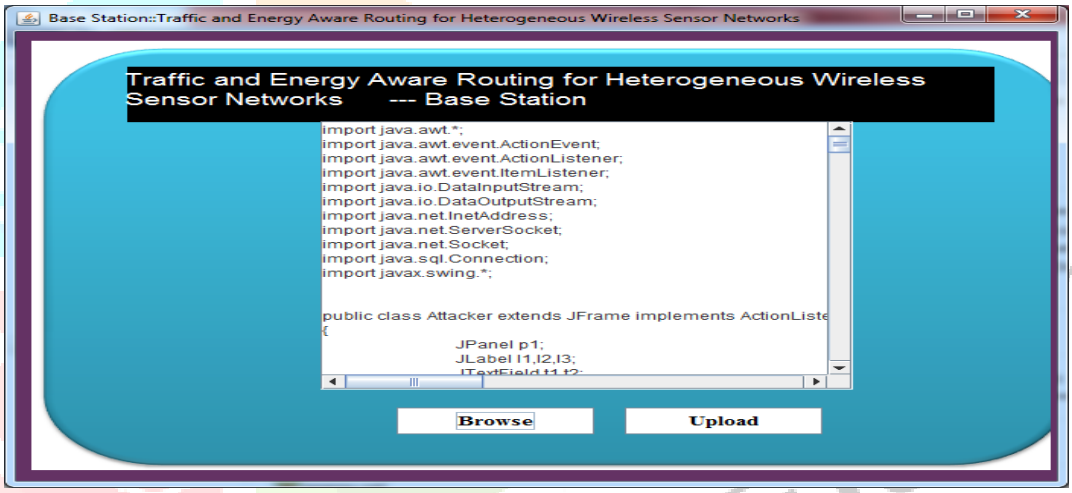
$$p_i(r) = \frac{p_{opt} N(1+\alpha_{ehi}) N(1+\alpha_{th}-\alpha_{ehi}) E_i(r)}{(N+\sum_{i=1}^{N} \alpha_{ehi})(N+N\alpha_{th}-\alpha_{Tot}) E_{Avg}(r)}$$

Where $E_{Av}(r)$ is average energy of the round and *popt* is optimal probability of a node to become CH, given by $p_{opt} = \frac{k_{opt}}{N}$. The remaining functionality of TEAR is similar to DEEC. Further, in the absence of traffic heterogeneity, TEAR falls back to DEEC behaviour.

7. EXPERIMENTAL RESULTS

In this proposed application we for the first time developed a model TEAR in which the traffic and energy is identified by the router and then try to choose the best path for data transfer under the nodes which don't have any high energy or traffic to avoid the data loss. For this we have implemented JAVA as programming language and My-SQL as back end database for storing and retrieving the information.

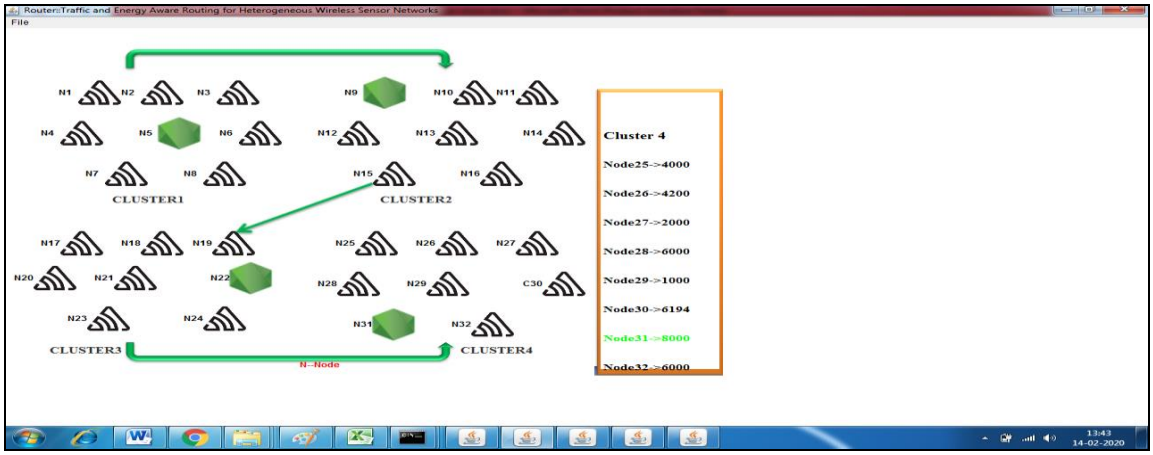
SOURCE WINDOW



Explanation:

From the above window, we can clearly identify the source or service provider try to choose valid text file as input and then try to press upload option to upload the corresponding file.

ROUTER WINDOW



Explanation:

From the above window, we can clearly identify the router node will try to find out the best paths based on energy or bandwidth of all the nodes which are present in the router. Once the router finds the best path, then only data will be sending to the receiver under a dedicated path.

8. CONCLUSION

In this proposed application we for the first time developed a model TEAR in which the traffic and energy is identified by the router and then try to choose the best path for data transfer under the nodes which don't have any high energy or traffic to avoid the data loss. All the primitive algorithms failed to detect and prevent the energy loss nodes and send the data under best path without having such low energy nodes. In this proposed paper we try to design a model known as TEAR Protocol (Traffic and Energy Aware Routing) Protocol in wsn for identifying the nodes which is having high energy among a set of nodes and then try to choose one which is having highest energy as cluster head (CH).BY conducting various experiments on our proposed method we finally came to an conclusion that our proposed method is having the capability to send the data under best path which is having high energy nodes and then try to avoid the nodes which has less energy.In this way if we try to send the data there will be no data loss under any attack conditions

9. REFERENCES

[1] S. Tanwar, N. Kumar, and J. J. Rodrigues, "A systematic review on heterogeneous routing protocols for wireless sensor network," Journal of network and computer applications, vol. 53, pp. 39-56, 2015.

[2] G. Smaragdakis, I. Matta, and A. Bestavros, "SEP: A stable election protocol for clustered heterogeneous wireless sensor networks," in Second international workshop on sensor and actor network protocols and applications (SANPA 2004).

[3] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," Wireless Communications, IEEE Transactions on, vol. 1, pp. 660-670, 2002.

[4] L. Qing, Q. Zhu, and M. Wang, "Design of a distributed energyefficient clustering algorithm for heterogeneous wireless sensor networks," Computer communications, vol. 29, pp. 2230-2237, 2006.

[5] H. Zhou, Y. Wu, Y. Hu, and G. Xie, "A novel stable selection and reliable transmission protocol for clustered heterogeneous wireless sensor networks," Computer communications, vol. 33, pp. 18431849, 2010.

[6] D. Sharma, A. P. Bhondekar, A. Ojha, A. Shukla, and C. Ghanshyam, "A traffic aware cluster head

selection mechanism for hierarchical wireless sensor networks routing," in IEEE Parallel, Distributed and Grid Computing (PDGC), 2016 Fourth International Conference on, 2016, pp. 673-678.

[7] M.-Y. Wang, J. Ding, W.-P. Chen, and W.-Q. Guan, "SEARCH: A stochastic election approach for heterogeneous wireless sensor networks," Communications Letters, IEEE, vol. 19, pp. 443-446, 2015.

[8] J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, “Performance analysis of mesh routing protocols for uav swarming applications,” in *Wireless Communication Systems (ISWCS), 2011 8th International Symposium on*. IEEE, 2011, pp. 317–321.

[9] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” *Wireless Communications, IEEE*, vol. 11, no. 1, pp. 38– 47, 2004.

[10] N. Garg and R. Mahapatra, “Manet security issues,” *IJCSNS*, vol. 9, no. 8, p. 241, 2009.