Chandrakant Naikodi, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 10, October- 2017, pg. 27-35 **ISSN: 2321-8363**
Impact Factor: 4.123

POWER AWARE LOAD BALANCING IN SECURED CHARACTER DIVERSE WSN

Chandrakant Naikodi
Visiting Professor, CSE, CiTech, Bangalore, Karnataka, India
Email: nadhachandra@gmail.com

Abstract: ***A Wireless Sensor Network (WSN) is a vitality and security limitation ad-hoc network. This paper is endeavoring to apply proficient systems of load, vitality and security to such an extent that network life can be expanded with security. Vitality powerful load compromise in a WSN needs to spread workload over numerous sensor hubs in view of its character of usefulness, for example, temperature, light identification, guardianship as a primary concern of security. Accordingly, vitality successful load compromise can be accomplished and improvement of asset utilization, augment throughput, augment network lifetime, limit reaction time and maintain a strategic distance from overload by appropriating work among indistinguishable sort of sensor hubs with vitality and security proficient courses. This will make utilization of different sensor hubs to compromise of load instead of a solitary sensor hub consequently this may expand unwavering quality through excess. Network is partitioned logically, one is Physical Group(PG) which speaks to an arrangement of hubs which are physically neighbors to a hub, another is Logical Group(LG) which speaks to an arrangement of hubs which grouped in light of its sort of usefulness. Vitality productive courses can be assessed in virtual groupings(PG,LG), course will picked in light of the cost of vitality inspite of the course belongingness. Since every hub in this network require not comprehend security strategies of different hubs, in light of the fact that, there could be distinctive encryption procedures, parcel measure, convention and so forth, subsequently header(cluster header) can have regular security layer where security related things are assessed.***

Keywords: Secure, WSN, Energy Efficient, Load Balance, Heterogeneous, Logical Group, Physical Group

1. Introduction

A WSN is a gathering of sensor hubs that impart through wireless connections, and these cannot have an exceptional topology. These hubs agreeably go their information through the WSN to a primary area.

Load adjusting in WSN includes the dissemination of all PC and correspondence exercises in at least two network hubs. This load adjusting can enable us to lessen the execution to time of exercises and to guarantee that all assets in the framework are utilized ideally.

In a perfect world, the load adjusting algorithm chooses the hub to process execution in light of accessible data about every one of the assets in the network.

Load adjusting algorithms can be static, dynamic and adaptive. Static algorithms settles on choices by from the earlier learning of the network, therefore, overheads caused in static algorithms is just about zero. On account of dynamic algorithms, choices depend on the data of framework status (loads on hubs), therefore, bring about overhead in the gathering, stockpiling and examination of network status. Adaptive Algorithm is a sort of powerful algorithms that adapt their exercises to progressively change the parameters of the algorithm to adapt to network conditions.

WSNs require suitable algorithm to make prudent utilization of limited vitality assets of heterogeneous sensor hubs, therefore, we need to legitimize the cost count before running the load on it!

2. Literature Survey

Load adjusting in heterogeneous WSN hubs can be accessed through bunch hubs, it is an original thought, however few paper utilized as contribution to this idea.

Paper [8] proposed a load-adjusted grouping algorithm [14] for Wireless Sensor Networks on the premise of their separation and thickness dispersion. In the group, hubs can join the bunch head by considering the bunch size and correspondence radius.

Further, load adjusting with vitality efficiency[10][1] involves two sections [12]. The initial segment being Determining the quantity of bunch heads in view of the dissemination and correspondence radios of the hubs and the second is to choose the group heads as indicated by the lingering vitality, portability, the group number single hub to group and separations of their heads and part hubs server bunch heads.

Paper [7] proposed to design where new applications can be created through an adaptable administration Rapidly arrangement. This engineering clog Helps to Control Which load-adjusting and adaptively adjust the work load over multipaths. In this algorithm, an assessment metric and way empty proportion is utilized to assess and locate an arrangement of connection disjoint ways from every single accessible way. Over this algorithm, an edge is connected sharing algorithm to part the packets into different fragments will be conveyed by means of That multipaths to the goal way empty contingent upon the proportion.

In paper [11], creator has examined the impact of load adjusting steering in WSNs stochastic undirected and coordinated with haphazardly set hubs. It reasoned that the stochastic directing does not really accomplish productive load adjusting vitality in undirected networks. They have investigated the execution of the algorithm stochastic steering disseminated and decentralized, i.e. expander steering technique, the strategy for expander steering execution altogether better regarding defer packet transmission, while accomplishing effective load adjusting vitality in coordinated networks.

In Paper [13], proposed convention Secure Load Balancing (SLB), which utilizes the pseudo-sinks that are few hubs sacred uncommon sensors with all the more processing assets, stockpiling, and vitality. This algorithm decreases precision issue securely transmitting information bunches close congested free or pseudo-sinks groups.

In Paper [6], creators have examined the potential parameters of vitality protection and greatest execution of the network by adjusting activity over the WSN. They have demonstrated that the circulation of activity produced by every sensor hub through various ways instead of utilizing a solitary way permits noteworthy vitality funds, therefore, proposed another investigative model for load-adjusted frameworks.

Paper [4] discusses vitality proficient steering in WSN Which isn't simple regardless of having Directed Diffusion directing convention information driven. The information is sent through all the sink hubs force the overhead of sending futile information, subsequently the creator has proposed a multi-Sink Directed dissemination (MSDD) to address this issue by transmitting information towards the closest sink. This convention actualizes a load adjusting by choosing the sink to next hand after the vitality level of the hubs in the first way falls beneath an edge esteem questionable.

3. Proposed Techniques and Implementation

In this work we are utilizing systems of paper [2] with load adjusting algorithms. At first we are thinking about load adjusting factor and the age of the mimicked comes about.

The network is (Logical Group-LG) and physically (Physical Group - PG) isolated on the premise of usefulness and physical, separately presence. In this network, every hub is having a LG (Logical Group) ID that is not quite the same as the bunch group where LG Id is one of a kind and logically grouped in view of the indistinguishable usefulness of sensor hubs, however a hub can have recognizable pieces of proof more than one group to show that you can take an interest in more than one element extraction for instance, the identification of tremors and avalanches perception. At whatever point a sensor hub sends a parcel with LG Id your neighbors, if the neighbors are logically and physically accessible inside the scope territory then those hubs can get this packet or any quick neighbor can pass this packet to his neighbor et cetera, until the point that it achieves LG suitable hubs. This group ID is just logical group ID speaking to the arrangement of hubs practically comparative, therefore, correspondence between various groups depends on the simple group ID. In fig. 1, hub 1 and 5 are in PG (Physics Group) and LG X hub, separately, however the hub 2 is incorporated into the two groups (LG and PG). In each of LG, every hub may get parcels that are recorded for the whole group, however PG hubs are neighbors there intrigued hub can get these packets.

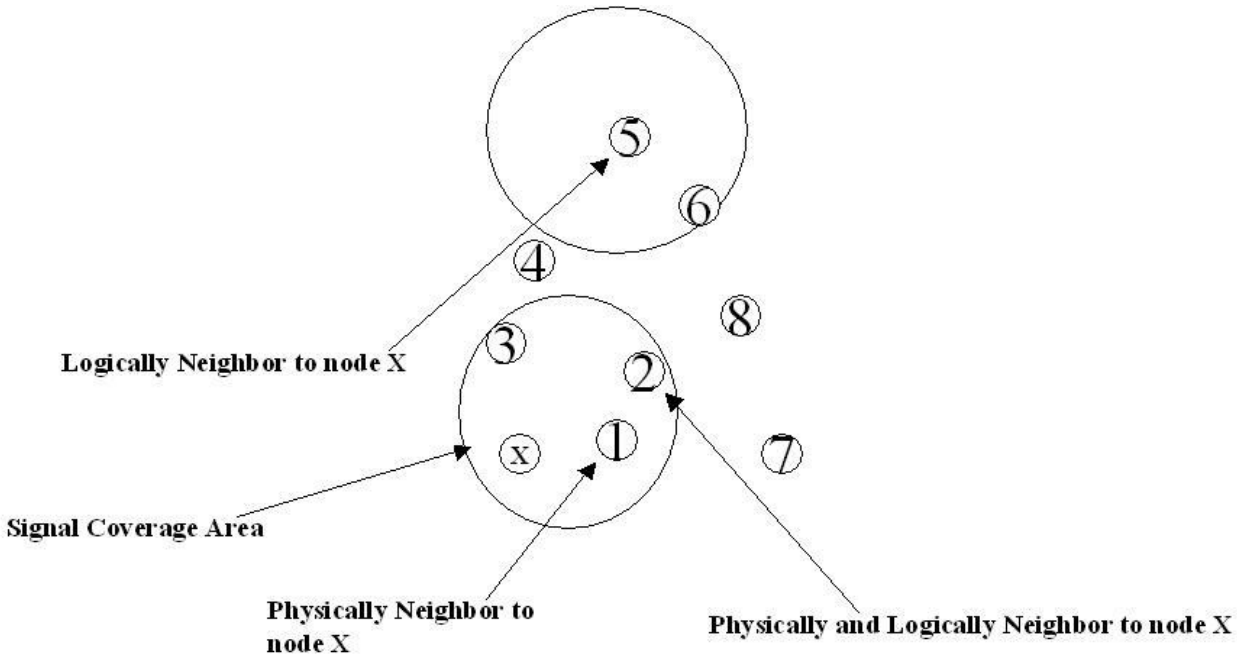

Figure 1. WSN Group Formation

Algorithm 1 Load Balancing in WSN

Require: Initialize N Nodes with L, PG, LG, etc
Require: $L <=$ Number of Work Load Processes(l1,l2,l3...ln=L)

```
while l <= L do
  while i <= N do
    if Type of node i belongs to a LG == Process Type of l then
      Allocate this process l to Node i.
    else
      Allocate load to free node which can belongs to PG.
    end if
  end while
end while
```

Algorithm 1 describes the process of assigning load to nodes in the network. The average amount of energy consumed by node u per unit of time due to the different transmissions within the WSN is denoted by E(u) [5],

$$E(u) = E_{idle}(u) + \sum_{v \in V} \sum_{p \in P(v)} w(p) * A(v) * E(u,p) \quad (1)$$

Here, $E_{idle}(u)$ is the average amount of energy consumed by node *u* per unit of time during its idle state. The lifetime of sensor node *u* is calculated by,

$$T(u) = E_{init}/E(u) \quad (2)$$

Here, E_{init} is the initial amount of energy provided to each sensor node.

Generally, the load balance for a given graph *G* representing the network with *n* nodes where each node contains work load *wi*, the goal is to distribute load across the edges so that finally the weight of each node is (approximately) equal to,

$$\bar{w}_i = \sum_{j=1}^{n} w_j/n \quad (3)$$

Let *f* be the fraction of the total network area covered by a mobile node [8] , then

$$f = \frac{\pi R^2}{A} \quad (4)$$

The average number of neighbours $\bar{n}$ of the network can be obtained by using the following equation,

$$\bar{n} = (N-1)kf \quad (5)$$

Chandrakant Naikodi, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 10, October- 2017, pg. 27-35 ISSN: 2321-8363
Impact Factor: 4.123

where k is a constant, referred to as a connectivity parameter.

The association between the local density, the cover assembly and forwarding Was condensed-through probability equation (6). Assuming that, g be the number of adjacent neighbours of node nI and g_b be the number of nodes of nI that are covered by the broadcast and the forwarding probability at the node nI is as follows,

$$P_{n1} = \begin{cases} \frac{g-g_b}{\bar{g}}; \text{if } g \leq \bar{g} \\ \\ \frac{g-g_b}{g}; \text{if } g > \bar{g} \end{cases} \qquad (6)$$

Adding all the nodes of physical or logical groups are equivalent number of nodes in the network. Say, K,L be the total number of groups of PG and LG respectively and R, S be the size of each group of PG and LG respectively which is specified in the below equation (7) and (8).

$$\text{N}=\sum_{i=0}^{K} R_i \qquad (7)$$

$$\text{N}=\sum_{i=0}^{L} S_i \qquad (8)$$

Group Relations can be defined as follows, let there is a set of 2 groups like M and W and wanted to express which node of M is communicating with which node of W. Here, one way to do that is by listing the set of pairs (m,w) and recognizing the nodes. The accessing relation can be represented by a subset of the Cartesian Product $M \times W$. In general, a relation R from a set A to a set B will be understood as a subset of the Cartesian Product $A \times B$, i.e., $R \subseteq A \times B$. If an element $a \in A$ is related to an element $b \in B$, we often write aRb instead of $(a, b) \in R$. The set

$$\{a \in A \mid \text{aRb for some } b \in B\}$$

is called the domain of R. The set

$$\{b \in B \mid \text{aRb for some } a \in A\}$$

is called the range of R.

The load balancing [9] in the given a graph G(summation of PG and/or LG) contains N nodes where each node contains work load w_i, here work load is distributed across the edges/nodes so that finally the weight of each node is (approximately) equal to $\bar{w}_i$, i.e.,

$$\bar{w}_i=\sum_{j=1}^{n} w_j/n \qquad (9)$$

We have assumed that WSN is a set of heterogeneous nodes called h_1, $h_2...h_n$ as specified in equation (10), where H is a set of h_1, h_2, ... h_n.

$$H = \{ h_1, h_2,...h_n \} \qquad (10)$$

where each node is having different security techniques i.e.,h_1 is having a security technique called s_1 and so on, therefore equation (11) shows, S is a set of security techniques of all heterogeneous nodes.

$$S = \{ s_1,s_2...s_n \} \qquad (11)$$

here H and S are having one to one relationships. Here also $s_1,s_2...s_n$ can have sub security techniques called $a_1,a_2...a_n$. One important note is [3], in this network each node need not understand security techniques of other nodes because of their own encryption techniques etc, hence this network is fully dependent on central/header node of WSN. The Encryption functionality can include a set of security functions to encrypt, decrypt and sign applicative data,ensuring confidentiality and integrity.

There is a maximum $N(N-1)$ bidirectional communication link can happen between nodes with using a header node (Mk) who is placed with a common security protocol software called M. Integration modulation($i_1..i_m$) is the process of linking together different secured nodes ($n_1,n_2...n_m$) and software applications functionally to act as a coordinated whole. Therefore, M in Mk is set of integration modules is given in equation (12),

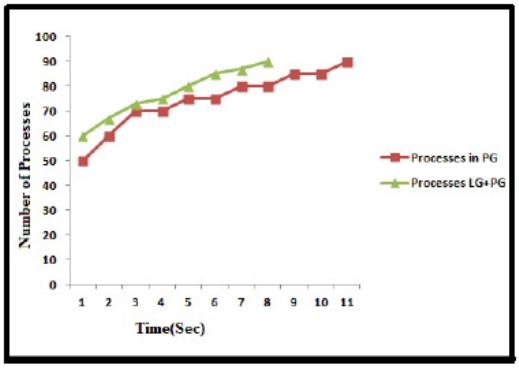

Figure 2. Number of processes in 100 nodes v/s time in load-balancing .

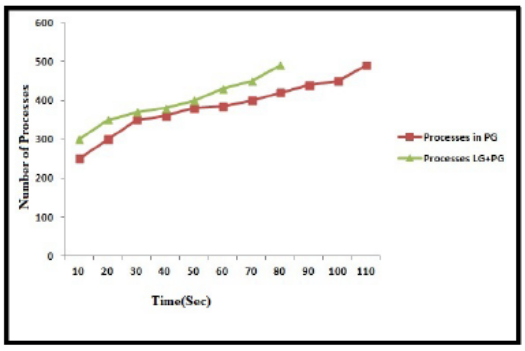

Figure 3. Number of processes in 500 nodes v/s time in load-balancing .

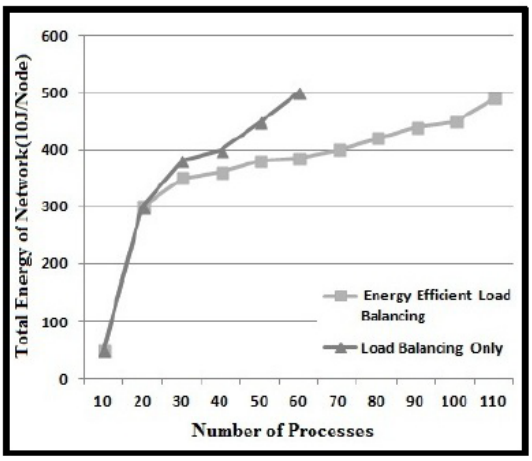

Figure 4. Total Energy of 50 Nodes v/s Number of Processes in the Network.

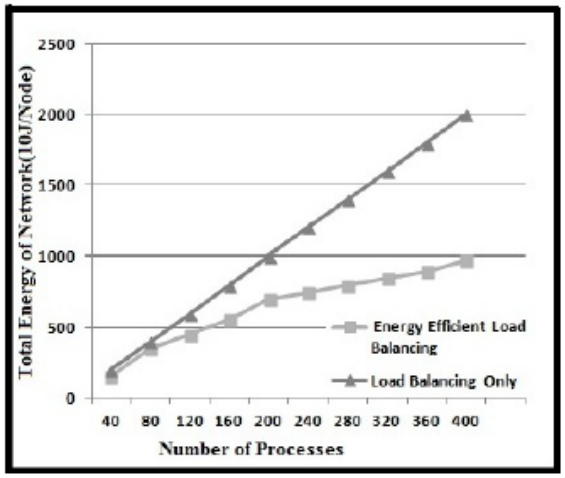

Figure 5. Total Energy of 200 Nodes v/s Number of Processes in the Network.

$$M = \{ i_1 + i_2 \ldots i_m \} \quad (12)$$

Each node's request or response has to reach *Mk*, then *Mk* will process it and delivered to the intendant node(s). As described in earlier paragraph, say security technique s_1 and s_2 is given in equation (13),

$$P(s_1 \text{ and } s_2) = 0 \text{ (disjoint)} \quad (13)$$

As all nodes are heterogeneous in nature, hence we have assumed that $s_1 \neq s_2 \neq s_3 \neq \ldots s_n$.

Say node n_1 wants to send a request R_1 to the node n_2, equation (14) shows the process, here every node has to send their request or response through *Mk*.

$$n_1 \longrightarrow n_2 = n_1 \rightarrow Mk + Mk \rightarrow n_2 \quad (14)$$

and node n_2 sends a response R_2 back to the node n_1, equation (15) shows the reverse process of equation 14).

$$n_2 \longrightarrow n_1 = n_2 \rightarrow Mk + Mk \rightarrow n_1 \quad (15)$$

Here *Mk* is an central node with M which does integration between all nodes in the network. Basically it does mappings and conversions across the network.

This kind of network may suffer from communication failures such as, central mode failure or entry of malicious nodes or network energy lost or natural disaster etc. The header node failure can occur due to non supportive security technology or invalid request/response from nodes.

Considering communication failure due to malicious(L) node(s) entry into the network. However L cannot communicate with other nodes directly, hence this node has to contact *Mk* for request and response. Say node L wants to send a request R_1 to node n_1, equation (16) shows the process of sending a request to *Mk*,

$$L \longrightarrow n_1 = L \rightarrow Mk + Mk \rightarrow n_1 \quad (16)$$

Mk does not forward R_1 to n_1, instead *Mk* will approve the demand whether this hub is enlisted in *Mk*'s registry or not. The coordination should bolster this demand/reaction yet actually this isn't the situation in this situation. On the off chance that it is an enrolled hub then advances the demand to hub n_1 requests legitimacy of hub L out of the blue. On the other hand n_1 will check the genuinity of the same and answer back to *Mk* on the off chance that it is honest to goodness hub or sends acknowledgement(ack_L) bundle to *Mk* in the event that it is malevolent hub.

Reenacted comes about for the load adjusting is appeared in Figure 2 and 3, PG and PG have considered situations with LG. Load adjusting through PG is an ordinary spread the load among sensor hubs algorithm may traditionally be relegating procedures to the sensor hubs. Applying the algorithm ideas PG LG takes less time contrasted with the ideas of PG.

Figure [9] and [8] demonstrates the reproduction aftereffects of 100 and 500 hubs, individually.

Algorithm 2 Energy Efficient Load Balancing in WSN

Require: Initialize N Nodes with L, PG, LG, etc
Require: $L <=$ Number of Work Load Processes(l1,l2,l3...ln=L)
Require: $N <=$ Number of Nodes in the network(n1,n2,n3...nm=N)
Require: $E <=$ Energy Level of each node in N (e1,e2,e3...en=E), here e1 for n1, e2 for n2....en for nm

```
while l <= L do
  while i <= N do
    if Type of node i belongs to a LG == Process Type of l then
      while Until find a node from i which consumes min. energy e do
        Allocate this process l to Node i.
      end while
    else
      while Until find a node from i which consumes min. energy e do
        Allocate this process l to Node i.
        Allocate load to free node which can belongs to PG.
      end while
    end if
  end while
end while
```

Therefore, the proposed algorithm can be valuable on account of heterogeneous hubs. With the load adjusting algorithm, we likewise actualized an effective vitality procedure, so the web of life can be enhanced/expanded with load adjusting. A short algorithm is given in Algorithm 2, which depicts the way toward appointing workload to hubs with vitality effective. In this network, L is Number of Work Load Processes called l1,l2,l3...ln and N is the Number of Nodes in the network called n1,n2,n3...nm and E is Energy Level of every hub in N called e1,e2,e3...en, here e1 relates to n1, comparably e2 relates n2 et cetera. Re-enacted comes about for effective load adjusting of the vitality is appeared in Figure 4 and 5 50 and 200 hubs, separately, the two charts of recreation comes about are indistinguishable and demonstrate that we can expand the lifetime of the network, while the load designation in the hubs.

4. Conclusion

This paper is endeavoring to apply effective methods of load, vitality and security to such an extent that network life can be expanded with security. Vitality viable load compromise in a WSN needs to spread workload over numerous sensor hubs in view of its character of usefulness, for example, temperature, light identification, guardianship at the top of the priority list of security. Network is logically partitioned, one is Physical Group(PG) which speaks to an arrangement of hubs which are physically neighbors to a hub, another is Logical group(LG) which speaks to an arrangement of hubs which grouped in light of its sort of usefulness. Vitality effective courses can be assessed in virtual groupings (PG,LG), course will picked in view of the cost of vitality inspite of the course belongingness. Since every hub in this network require not comprehend security procedures of different hubs, on the grounds that, there could be distinctive encryption systems, parcel estimate, convention and so on, subsequently header(cluster header) can have basic security layer where security related things are assessed. The reproduction result is empowering and it is worth of utilizing proposed algorithm for vitality productive load adjusting in secure heterogeneous WSN.

References

[1] www.libelium.com
[2] http://en.wikipedia.org/wiki/Agriculture_in_India
[3] Kodali, Ravi Kishore and Rawat, Nisheeth and Boppana, Lakshmi, *Region 10 Symposium, 2014 IEEE*,"WSN sensors for precision agriculture".
[4] Mat I, Kassim, Harun A.N, *2014 Sixth International Conf on Ubiquitous and Future Networks (ICUFN)*, "Precision irrigation performance measurement using wireless sensor network".

[5] Mampentzidou ; Karapistoli, E. ; Economides, *2012 4th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, "Basic guidelines for deploying Wireless Sensor Networks in agriculture".

[6] Jimenez, A.; Jimenez, S. ; Lozada, P. ; Jimenez, C., *Information Technology: New Generations (ITNG), 2012 Ninth International Conference on*, "Wireless Sensors Network in the Efficient Management of Greenhouse Crops".

