International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:10, No:2, 2016

Dominating Set Algorithm and Trust Evaluation Scheme for Secured Cluster Formation and Data Transferring

Y. Harold Robinson, M. Rajaram, E. Golden Julie, S. Balaji

***Abstract*—**This paper describes the proficient way of choosing the cluster head based on dominating set algorithm in a wireless sensor network (WSN). The algorithm overcomes the energy deterioration problems by this selection process of cluster heads. Clustering algorithms such as LEACH, EEHC and HEED enhance scalability in WSNs. Dominating set algorithm keeps the first node alive longer than the other protocols previously used. As the dominating set of cluster heads are directly connected to each node, the energy of the network is saved by eliminating the intermediate nodes in WSN. Security and trust is pivotal in network messaging. Cluster head is secured with a unique key. The member can only connect with the cluster head if and only if they are secured too. The secured trust model provides security for data transmission in the dominated set network with the group key. The concept can be extended to add a mobile sink for each or for no of clusters to transmit data or messages between cluster heads and to base station. Data security id preferably high and data loss can be prevented. The simulation demonstrates the concept of choosing cluster heads by dominating set algorithm and trust evaluation using DSTE. The research done is rationalized.

***Keywords*—**Wireless Sensor Networks, LEECH, EEHC, HEED, DSTE.

I. Introduction

WSN became a pillar of surveying environment in real time agricultural survey. Initially small number of nodes was used for the purpose of surveying. The technique used chunk direct transmission to the base station from each node in WSN. This did not work for larger areas. It is modified to MTE (Minimum Transmission Energy), where the data is transmitted through intermediate nodes in the network. This approach is efficient when the average transmission distance is large. Static clustering technique is used to upstream traffic routing by transmitting data from cluster member to all cluster heads. The cluster heads are responsible for forwarding the messages to the base station.

The concept of homogeneous environment is introduced in LEACH where cluster heads were chosen among homogeneous nodes. Energy Aware Routing (EAR), Sequential Assignment Routing (SAR) are network based algorithms whereas, Multi path and Multi speed (MMSPEED) Sensor Protocols for Information via Negotiation (SPIN) are operation based routing protocols.

Cluster head selection is the demanding job to be done in any type of topology of WSN. Energy consumption of cluster heads is up for cogitation for WSNs. The cost induced for maintenance came in control. The existing research targets on equitable cluster head selections. In this paper we talk about the concept of dominating set algorithm which efficiently chooses the cluster heads and save energy as well.

Security of network is defended by preventing infiltration of suspicious nodes. Earlier in the part of security the invasion into nodes are detected through the signal strength of the messages based on their location in the network. State-of-the-art trust and group based trust management scheme are the protocols used to evaluate the trust of network nodes. Our system uses Dominated Set Trust Evaluation (DSTE) [12] to secure the network. Mobile data sink has been proposed for future work.

II. Related Work

The nodes reside under certain region sends their data to the cluster head. The cluster head agglomerates it and passes them to the sink [5]. The former cluster formation is based on the velocity of the nodes in a connected dominated set (CDS) to be a part of the cluster [7], [10]. The cluster head selection was either done based on the average network energy [3] or based on balancing the energy consumption throughout the network [9]. The network delay and distance from the base station or the mathematical calculation between them [6] was contemplated for cluster head selection.

The hierarchal steering protocol LEACH proposed the notion of cluster head selection to conserve energy than other routing protocols [4]. LEACH is further modified with genetic algorithm for better performance [11]. When they sensed the significance of energy conservation in WSNs a number of researches were done. An energy efficient Ant based routing algorithm where an ant moves in a path and tracks the energy of the nodes in that path and returns in backward direction of the same path [9].

CDS for collection of data traffic, partition of network zones and integrating CDS and clusters are the steps followed in virtual topology design [1]. In [2], the author has proposed a CDSEP algorithm to optimize the broadcasting of data using

Harold Robinson Y. and Balaji S. are Associate Professors with the Department of Computer Science and Engineering, SCAD College of Engineering and Technology, India (e-mail: yhrobinphd@gmail.com, sbalajiphd@gmail.com).

Prof. Dr. M. Rajaram is the Vice-Chancellor, Anna University Chennai, India (e-mail: rajaramgct@rediffmail.com)

Golden Julie is an Assistant Professor, Department of Computer Science and Engineering, Anna University, Chennai, India (e-mail: goldenjuliephd@gmail.com).

dominating set algorithm to choose energy dominated node in a heterogeneous environment.

In the phase of trust, the malicious nodes were detected based on the signal strength of the messages [8]. The nodes were attacked by disseminating probes throughout the network either by sending the probe to single node or by sending to set of nodes in the network. The nodes of the network are not aware of the information about the neighbour nodes. The nodes are expected to be trustworthy [3]. The cost and overhead in the trustworthy management system is high. The VAR trust model improves the network performance along with the malicious nodes within the network [12].

III. Proposed System

Best in the lifetime of a network is crucial. Our research presents dominating set clustering schema which increases the life time of the network. Security and trust is achieved through secured trust model. The energy consumption is reduced in the network by all means.

A. The Dominating Set Algorithm

The dominating set can be formed by scanning the network in the form of tree. Fig. 2 demonstrates the dominant set creation.

Calculating dominated set in a network takes negligibly less time. For a network G=(V,E) with N nodes the dominating set can be found by scanning all the nodes in $O(2^n n)$ time to form a minimum connected dominating set.

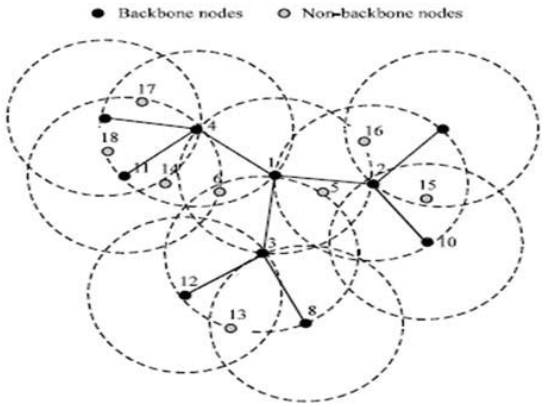

Fig. 1 Dominating set nodes Formation

The backbone nodes are the members of the dominating set and they are adjacent to each other. They are chosen as cluster heads.

B. Overhead in Each Node

The package transmission rate and collision rate at each node is decreased rapidly. Overhead has been calculated by using

$$OH(x) = 1 - e(x) \quad (1)$$

C. Energy Consumption of Each Node

As the energy and overhead cost is low, the CDS reorganization is also a negligible burden. Implying reorganisation is required only after the death of the cluster head. Thus, the impairing of networks operations is impossible. The energy consumption can be estimated by using

$$E(x) = A(x) + D(x) \quad (2)$$

D. CDS Size

A minimal CDS minimizes the routing overhead. The sensor networks go to sleep mode when they are not required. This saves the energy of the nodes. The nodes are awakening when a transportation of data or messages is needed.

E. Cluster Formation and Cluster Head Selection

In WSN, the clusters are formed based on the dominating set algorithm. The cluster head is selected in the following way,

1) In a connected network of 'n' nodes the dominating set of nodes are chosen where each node in the set is neighbour to any one of the other connected nodes.
2) Among the cluster nodes which are also is dominating set compete to act as cluster head.
3) The node with high energy level is chosen to be a cluster-head.

```
If (node x fit in with the set of dominant)
{
If (power(x) >= L_power and trust (x) >= L_trust)
{
Set status (x) = Dominant
Licentious (x) = ON
}
Else if (power (x) >= A_ power and trust (i) >= M_trust)
Set status (x) = Best
Else
{
Set status (x) = good
}
Else
Set status (x) = Average
}
```

F. CM-CM, CH-CH Trust Evaluation

The cluster members' trust assessment is performed through DTD (Direct trust degree) (i.e.) the successful and unsuccessful message transferring rate. The trust of CM's is estimated with the feedback of CH's which eliminates the overhead by neglecting the CM's feedback. The memory consumption level is too lowered significantly. In our light weight Dominated system CH's assessment for trust is done through the feedback from the base station. Applying trust evaluation in the dominated connected set makes the network trustworthy as well as the energy loss of the nodes is reduced. The trust model does not allow any malicious nodes to enter the cluster. Quite a lot of clustering algorithms encompass be projected to decide on Cluster Head that has the highest id, highest node quantity, and highest residual vigour. WSN is less protected than wired network owing to wireless media,

and be short of innermost manage.

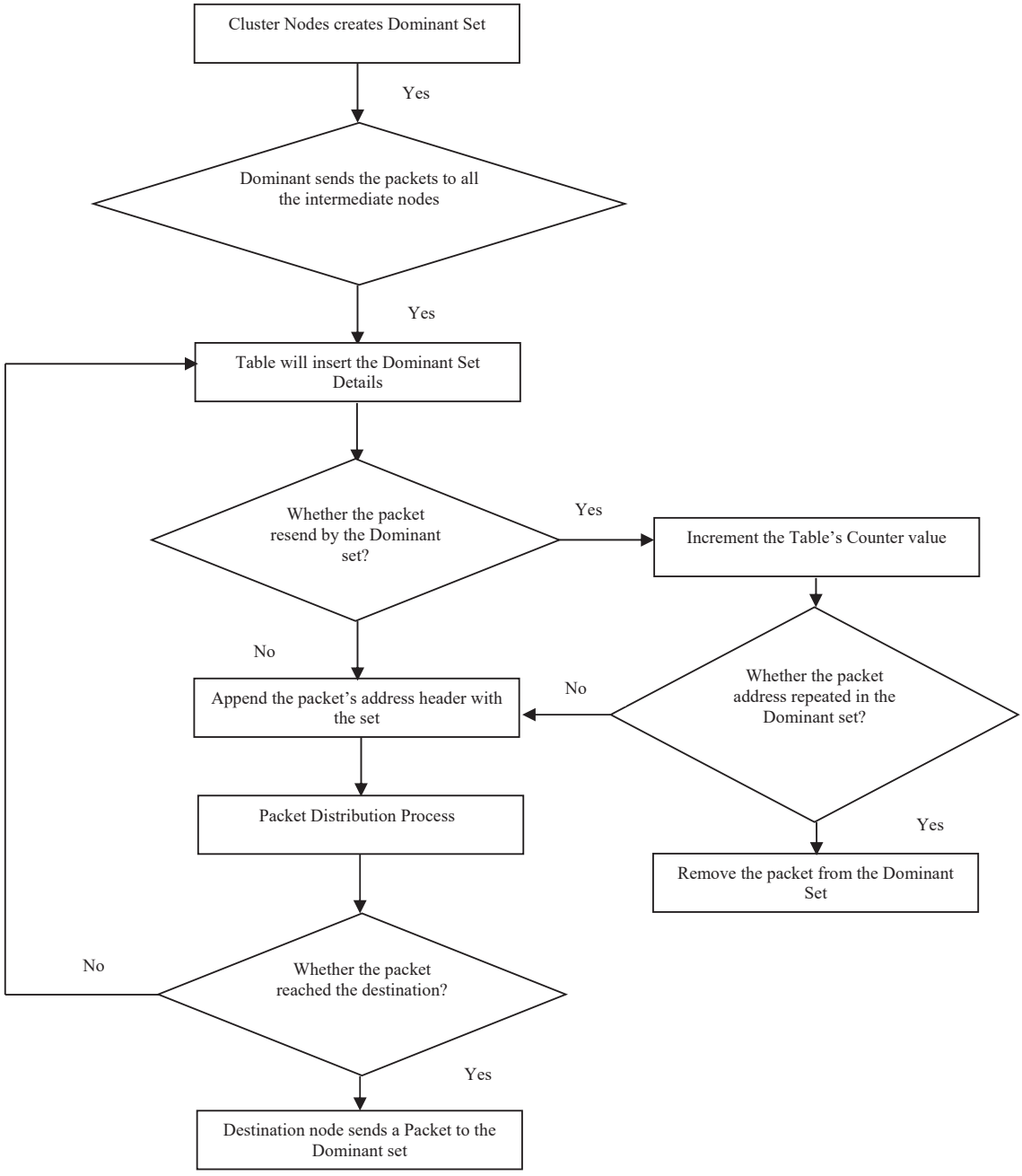

Fig. 2 Flowchart for Dominant Set Creation

G.BEACON Signals

The authentication of cluster heads to the base station is done using the BEACON signals. If the cluster head wishes to communicate with a base station it finds the nearest base station via user level processing. The base station finds the in sequence about Cluster Head and the particular kind of access permission the cluster head consists of in the wireless networks. The domicile site forwards a contradictory confirmation riposte to the support station. Then the cluster is supported or criticized by the support station. The Cluster Head sustains its cluster participator data and metadata about bordering Cluster Heads. Assume node Source node has data to send node Destination node. Node Source sends route appeal to its Cluster Head. The Cluster Head test out for node Destination in its member of the entire node in WSN cluster formation table. If the Destination node is having the exactly same parameters of the particular neighbouring cluster formation, the entire cluster configuration request is requested

and multipath routed in the network directly to Destination node. Otherwise the Cluster Head sends the route request to all the nearby Cluster Heads. Inter cluster communication and the Intra Cluster Communication is conceded out all the way through the directed virtual path launched within all the intra and the Cluster Heads. The main benefit of all the clustering approaches are diminished the control passage during the self-motivated route detection development. It uses narrow route restore machinery to switch not working links.

H.Trust Evaluation

The trust manager estimates the occurrences accounted by the proposed technique and in order to caution all the other nodes in the particular network regarding malicious nodes for not forwarding from the source node to the destination node with the trust evaluation and then it sends a threshold based distress. The standing system preserves a blacklist of the current network nodes at each node and develops this set of list with the destination nodes in its all other list of the friends list. The Trust Evaluation is based on a castigation format, by not transferring the data packet whose trust level plunges below certain threshold.

IV. Performance Evaluation

The solution for energy consumption and trust evaluation was found using 200 nodes in a certain area. The nodes were clustered using CDS algorithm. The simulation was done in NS2 tool.

The data transmission between CM-Cm and CH-CH is simulated as in Figs. 4 and 5.

The comparison with the LEACH and SEP energy saving protocols were done and illustrated in Fig. 6. The energy consumption is low in connected Dominating set.

The lifetime of network increases as shown above in our system.

The trust in DSTE is shown in Fig. 7 is compared to GTMS. This reduces the overhead in CMs as well as the CHs. This helps energy saving indirectly by reducing the feedback.

TABLE I
Simulation Parameters

Parameter	Value
Number of nodes	160
Transmission variety	225 m
Speed	10, 30, 50, 100 m/s
Network topology	800 x 800 m^2
receiver mold	Omni receiver
Transmitter antenna gain	1.1 dBi
receiver antenna gain	1.1 dBi
System loss factor	1.0
Transmitter indicate power	0.28 watts
Propagation reproduction	Two-ray ground
Simulation time	200 sec

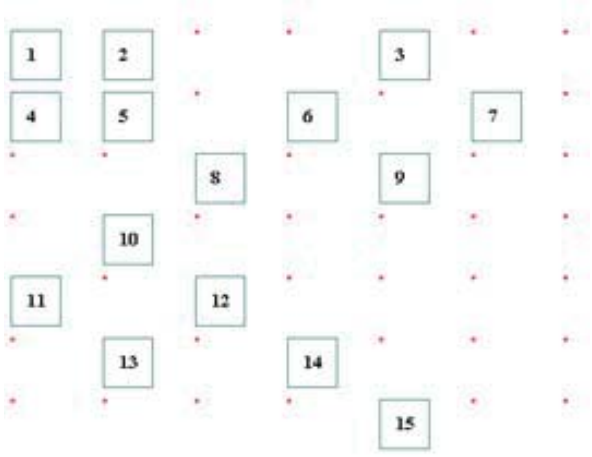

Fig. 3 Cluster head selection

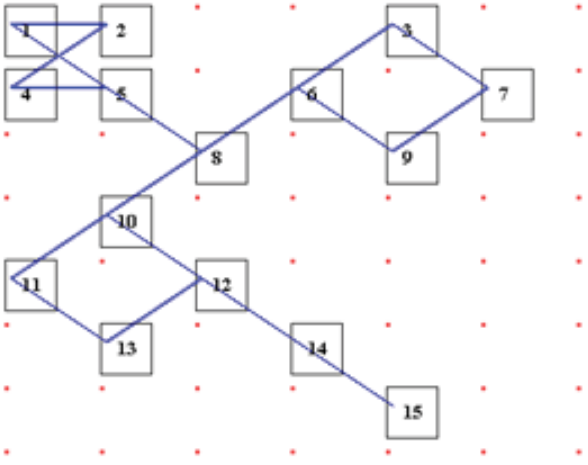

Fig. 4 Data transferring between CM-CM

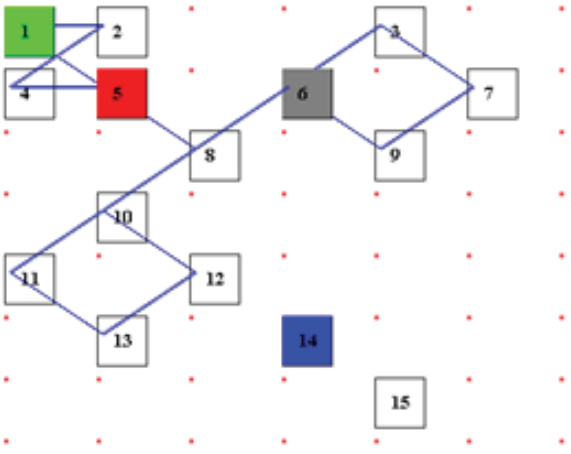

Fig. 5 Data transferring between CH-CH

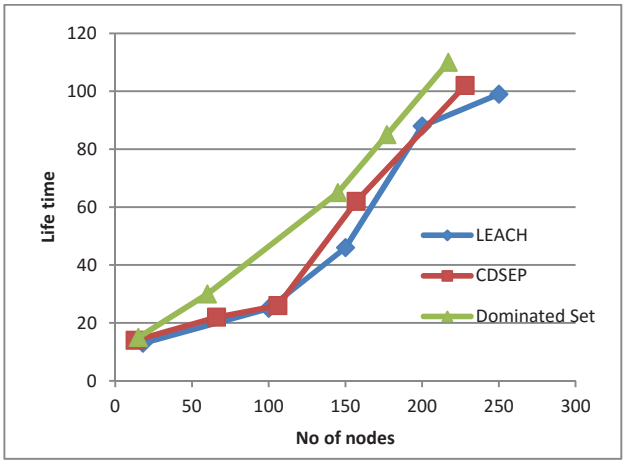

Fig. 6 Lifetime of a Network

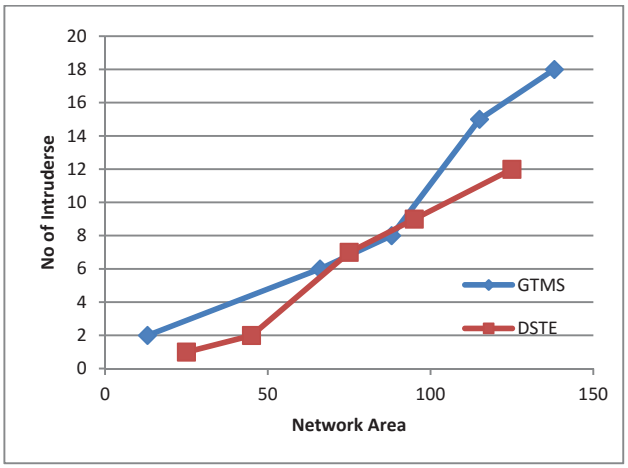

Fig. 7 Trust Evaluation

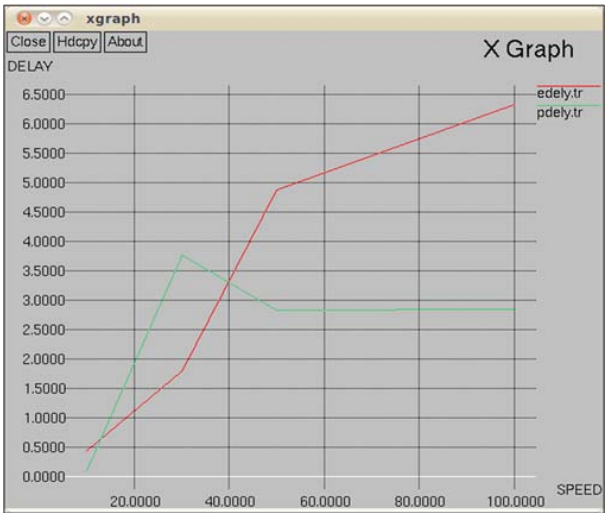

Fig. 8 Comparison graph for End-to-end delay

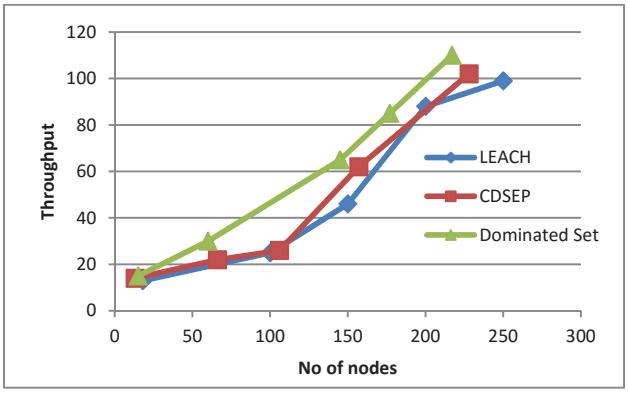

Fig. 9 Throughput

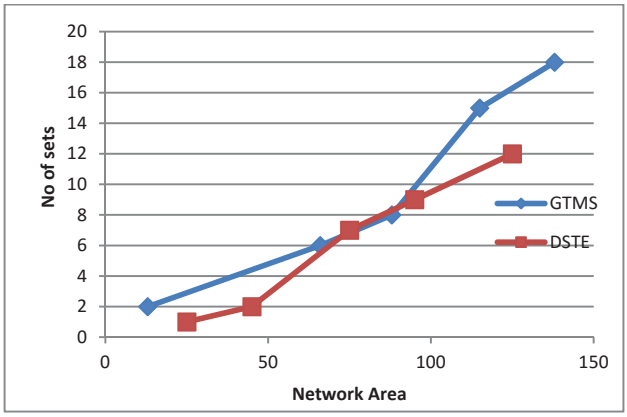

Fig. 10 Dominant Set

As in authentic existence, trust stages are indomitable by the meticulous performance that the trusted gathering can execute for the trustee. Confidence cannot be extravagances as a belonging of trusted arrangements but somewhat it is an evaluation based on understanding that is collective from beginning to end network of individuals. Correspondingly trust levels can be work out based on the endeavour that one node is enthusiastic to enlarge for a different node. The endeavour can be in stipulations of succession expenditure, packet over confident or any other such limitation that helps in establishing a mutual trust levels.

Through calculating the levels of trust from the intrinsic acquaintance current in the system the dependability of the particular routing tables can be generated in the particular network. The routing tables generated with the help of this technique may perhaps not be in the condition of the parameter of secured communication in the routing network as a replacement for providing dependability. Trust calculation engross an obligation of influences to the proceedings that where monitor and quantify. Based on the evaluated trust, security measures are taken or security conclusions are completed in the network lifetime.

Fig. 9 demonstrates the throughput for the number of nodes using three algorithms like LEACH, CDSEP and dominant set. The result shows that the dominant set algorithm Perform well compared to all the other algorithms of LEACH and

CDSEP with the prescribed number of nodes in the active network of WSN.

Fig. 10 demonstrates the dominant set approach has performed well in the conditions of GTMS and DSTE with the parameters of network area with the number of sets in the particular Network.

Fig. 11 demonstrates the rebroadcasting techniques has been achieved in network. The result shows that the DSTE is performing well compared to GTMS.

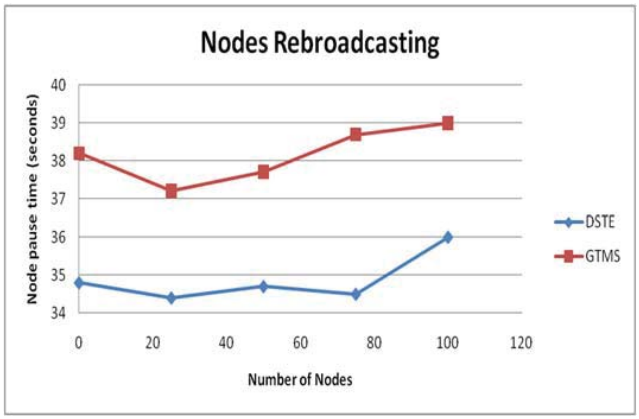

Fig. 11 Nodes Rebroadcasting

V. Conclusion & Future work

Thus the problem of energy consumption is reduced rapidly using CDS-algorithm. The energy deprivation is managed in the network. Adopting the DSTE in CDS allows secured cluster formation and data transferring. This effective method of preventing intruders increases the trust in the network. By eliminating feedback, it reduces the demand for memory and elevated communication cost is reduced. Thus our system is a low cost and energy efficient protocol for WSN.

In future securing of data with WSN with connected dominating set algorithm can be enhanced. The enhancement of security can be done by adding a mobile sink to the clusters which can carry the data from each cluster head to the base station. As the data is replicated in the mobile sink there is no threat of data loss in cluster sites.

References

[1] Shengbo Yang, Chai Kiat Yeo, and Bu Sung Lee, "Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks", *IEEE Transactions on Mobile Computing,* Vol. 11, No. 1, Jan 2012

[2] Harold Robinson, Y., & Rajaram, M. (2015). "Trustworthy link failure recovery algorithm for highly dynamic mobile adhoc networks", World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, vol.9, no.2, 233–236.

[3] Kai Zeng, Wenjing Lou, Jie Yang, Donald R. Brown III, "On Throughput Efficiency of Geographic Opportunistic Routing in Multihop Wireless Networks", *Springer, Mobile Networks Application* (2007) 12:347–357, 2007

[4] Robinson, Y. H., & Rajeswari, S. R. (2011). "Energy-based dynamic encryption for wireless sensor networks. Wireless Communication", vol.3, no.9, pp. 661–663.

[5] Golden Julie, E., Tamil Selvi, S., & Harold Robinson, Y. (2014). Opportunistic routing with secure coded wireless multicast using MAS approach. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 8, no.7, pp. 1247–1250.

[6] Sanjit Biswas, Robert Morris, "ExOR: opportunistic multi-hop routing for wireless networks", *Proceedings of conference on Applications, technologies, architectures, and protocols for computer communications*, Pages 133-144, 2005

[7] A. Trivino-Cabrera, S. Canadas-Hurtado, "Survey on Opportunistic Routing in Multihop Wireless Networks", *International Journal of Communication Networks and Information Security (IJCNIS),* Vol. 3, No. 2, August 2011

[8] Harold Robinson, Y., & Rajaram, M. (2016), "A memory aided broadcast mechanism with fuzzy classification on a device-to-device mobile Ad Hoc network", Wireless Personal Communications, 1–23, doi:10.1007/s11277-016-3213-0.

[9] Harold Robinson, Y., & Rajaram, M. (2014). "A novel approach to allocate channels dynamically in wireless mesh networks", World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 8(10), 1865–1868.

[10] Stepanov, D. Herrscher, K. Rothermel, "On the impact of radio propagation models on MANET simulation results", *Proceedings of 7th International Conference on Mobile and Wireless Communications Networks (MWCN 2005), Marrakech, Morocco*, September 2005.

[11] Harold Robinson, Y., & Rajaram, M. (2015), "Energy-aware multipath routing scheme based on particle swarm optimization in mobile ad hoc networks", The Scientific World Journal, 1–9. doi:10.1155/2015/284276.

[12] Harold Robinson, Y., & Rajaram, M. (2015), "Establishing pairwise keys using key Predistribution schemes for sensor networks", World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering, 9(2), 608–612.

Y. Harold Robinson is currently working as an Associate Professor, dept of CSE in SCAD College of engineering and Technology, Tirunelveli. He finished ME degree in Anna University, Chennai. He is Pursuing his Ph.D. from Anna University Chennai. His research interests are Wireless Networks Mobile Computing, Wireless Sensor Networks. He has published several Research papers in International Journals. He has presented many papers in National and International conferences in Network security, Mobile Computing and Cloud Computing.

Prof. Dr.M. Rajaram M.E., Ph.D is the Vice-Chancellor of Anna University, Chennai. As a research guide, Dr.M. Rajaram produced 30 Ph.D's and four M.S. scholars in various fields. At present, 10 research scholars are pursuing their Ph.D. under his direct supervision. He has contributed to the areas of Computer Networks, High Voltage Engineering, Measurement and Instrumentation, Adaptive Controller, Electro-Magnetic Theory, and Intelligent Computing with his 157 publications in renowned research journals, 111 research publications in International Conferences, 73 research publications in National Conferences, more than 100 technical reports and six technical books some of which he has co-authored

E. Golden Julie received her B.E degree in Computer Science and Engg in 2005 from Anna University Chennai and ME degree in Computer Science and Engineering in 2008 from Anna University Chennai. Currently she is Pursuing her Ph.D from Anna University Chennai. Presently she is working as assistant professor in Regional centre Anna University, Tirunelveli, India She has published many research papers in various fields. Her research area includes Wireless Sensor Adhoc Networks and Image Processing. She is a member of ISTE.

S. Balaji, M.E, MISTE doing his Ph.D in Anna University, Chennai and currently working as a HOD in dept of CSE at SCAD College of engineering and Technology, Tirunelveli. His research interests are Wireless Networks Mobile Computing, Network Security with apps, Wireless Sensor Networks, Cloud Computing. He has presented many papers in National and International conferences in network security, Mobile Computing, network security, and Cloud Computing. He has organized and conducted various national and international conferences, International Seminars and National Workshops. And also his methodology of teaching about TCP & UDP is hosted on Wipro Mission 10x portal. He is a life time member of ISTE.