Available online at: https://ijact.in

Date of Submission	25/02/2019
Date of Acceptance	08/04/2019
Date of Publication	30/04/2019
Page numbers	3117-3125 (9 Pages)

Cite This Paper: Srikanth, N. & GangaPrasad, M.S. (2019). Green comp based energy efficient data aggregation algorithm with malicious node identification (geed-m) for lifetime improvement in wsn. 8(4), COMPUSOFT, An International Journal of Advanced Computer Technology. PP-3117-3125.

ISSN:2320-0790

compusoft
An International Journal of Advanced Computer Technology

GREEN COMP BASED ENERGY EFFICIENT DATA AGGREGATION ALGORITHM WITH MALICIOUS NODE IDENTIFICATION (GEED-M) FOR LIFETIME IMPROVEMENT IN WSN

Nandoori Srikanth[1*], Muktyala Siva Ganga Prasad[2]

[1, 2]Department of Electronics & Communication Engineering, KoneruLakshmiah Educational Foundation, Green fields, Vaddeswaram, India.

Abstract: Random deployment of sensor nodes, energy limitations, interference of wireless links, and exposed nodes, are the major reasons of performance degradation in WSN. Energy efficiency, Lifetime improvements are the key research areas from last few decades. Even a high level of research is going on; still there are several issues which reduce the network lifetime and its throughput. For diminishing the energy consumption, the sensor nodes are driven into sleep mode once they finished their sensing round. Introducing mobile nodes in sub clusters is an efficient technique to make the network energy efficient in irregular terrains like plateaus. The energy limitations of mobile nodes, and malicious behaviour are big issues in mobile node based sub clustered sensor networks. These issues can be clear up by introducing a Green CoMP based energy efficient data aggregation algorithm with malicious node identification is proposed, which exchange messages to the cluster head through a mobile node. Malicious behaviour of mobile node is also identified by using Built-in self-Test based technique to improve network throughput. The proposed algorithm gives better results compared with existing algorithms with a lifetime improvement of 56%, energy consumption 44%.

Keywords: Data aggregation; Green-CoMP; Malicious node; Built-in self-test; Lifetime;

I. INTRODUCTION

WSN is a collection of group of sensor nodes which communicate through wireless links, and can work together to sense environmental conditions. WSN has changed the way of living, and reduce the complexity situations, and giving attractive solutions to various problems in various fields. The wide range of applications of WSN includes military, medical, communication, industrial, wild life, environmental applications etc. The drastic development of WSN changed the entire communication system in many applications with high end security, throughput. The data gathered from various sensor nodes are aggregated and send to the Base station through a cluster head. The smart sensors nodes works on command controlled strategies that have one or more memory unit, sensors, processor, an actuator and power supply [4]. In WSN, sensor nodes are controlled w.r.t communication bandwidth, processing power and storage space which are mandatory to be very efficient as a source of operation. In Wireless sensor networks, the sensor nodes are organized into clusters. It is more advantageous to use clustering in WSNs, Due to clustering, reducing the complete energy consumption and decreasing the interferences between sensor nodes. The major issues of WSN are Energy efficiency, lifetime, and security. There are several clustering and routing approaches have been proposed to make the network more energy efficient. From the past few decades, there is a rapid growth in WSN, and technologies in various fields which are associated with WSN. Even a high level of research is going on; still there are several issues to make the network energy efficient. Depends on application of WSN, there are several issues which degrades the performance of WSN.

Election of cluster head and formation of clusters and sub clusters are basic steps to design and implement WSN. Traditional approaches make the network into groups of clusters, and each cluster is assigned with a cluster head, each cluster is divided into sub clusters, and each sub cluster is assigned with a sub cluster head. Every sensor node in sub cluster sense the data and forward to the sub cluster head, and sub cluster heads forward data to the Cluster head. Cluster head is the gateway of particular cluster.

A. Motivation of the paper

In plateaus or grid based networks, sensor nodes are randomly deployed in various places like valleys, hills, under water, etc. In these types of applications some sensor nodes may place in valleys and these nodes head, or cluster head (CH) may place in hills or in other places. So it is a difficult task to send data from node to cluster head. Sensor nodes has to use more energy to send data from nodes to the cluster head, due to these limitations some of the mobile nodes are assigned to move around each sub cluster in order to collect data from each node and send it to the cluster head after the data aggregation. The selections of mobile nodes are based on threshold level, due to Energy limitation, sometimes there is a chance of each sub cluster may have only one mobile node, or none after some rounds of data sensing. To overcome this problem, a Green CoMP based energy efficient data aggregation algorithm is proposed. Due to malicious activities of nodes, wireless sensor network faces the critical problems like behavioural change, Throughput failure, Improper QOS. In these types of applications, Mobile node plays a key role in each sub cluster operations. Therefore if a mobile node is malicious in the network, then entire performance of the network degrades, Hence this paper proposed a Built in Self-Test (BIST) based Algorithm, for finding which mobile node is malicious.

B. Contributions of the paper

The main contribution of the paper is to make the network more energy efficient and also to improve lifetime of the network. To achieve this, a novel green comp based energy efficient data aggregation algorithm with malicious node identification (GEED-M) is proposed.

The Major contributions of the proposed work are:

- This algorithm concentrates on sub clusters which does not have a mobile node, and which sub clusters has only one mobile node with low energy.
- A novel BIST based algorithm is proposed to find which mobile node is malicious. There are three cases in malicious nodes Identification, and this algorithm makes the network to identify the malicious nodes automatically and immediately, and moreover network itself takes the action according to the case.

The proposed method section of the paper explains how GEED-M algorithm enhances the network lifetime, throughput, PDR, energy efficiency of the network.

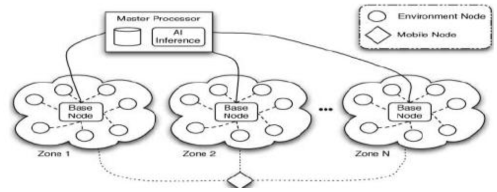

Fig. 1 General scenario of WSN

II. RELATED WORKS

Generally data sensed by the each sensor node is very important to the cluster head to know the event happening, malicious attacks, hidden nodes, and fault nodes status. Majorly data aggregation techniques are classified under five strategies.

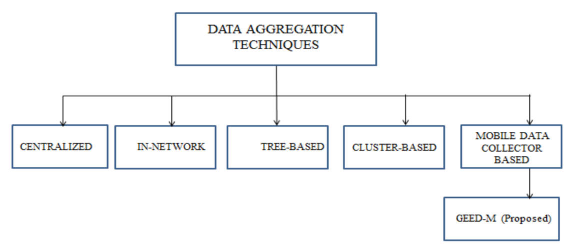

Fig. 2 Data Aggregation Methods in WSN

2.1 DATA Aggregation Strategies

In centralized data aggregation methods, each sensor node sends its sensed data to the highest energy node in their ambience. This highest energy node is also called as head node, which aggregates data based on average of the all sensor nodes data in particular region. In network processing aggregation methods have two approaches, without size reduction, with size reduction. This process is carried out with intermediate nodes in multi hop networks. in size reduction phase, the intermediate nodes perform data aggregation by combining and compressing the data packets and reducing the size of packets for forwarding to the sink node. In without size reduction method, all packets from neighbor nodes are merged into a packet without processing. In tree based approaches [2, 14], spanning tree structure is created with every node, and each node has its parent node for data transmission. In this type of approaches leaves nodes are less loaded, and nodes near to sink node are heavily loaded for aggregation.

In cluster based routing [13], entire network is partitioned into clusters, and each cluster is assigned with a cluster head. This cluster head collects data from every node in the cluster, and aggregates the data and finally forward to the base station. Due to this technique, bandwidth for data transmission is reduced due to reduction in number of data packets. in mobile data collector based aggregation methods [14, 15 16], various new algorithms are proposed for efficient data aggregation. In conventional methods, entire network is divided into clusters, and assigned with a cluster head. The mobile data collector collects data from each cluster head, and aggregates the data and forward to the base station. The mobile data collector move among clusters and aggregates the data collected from cluster head nodes. The major problem in this type of algorithms is every node’s data can be easily accessed at cluster head.

Guoxing Zhan et al., [7] For dynamic wireless sensor networks, to provide a trustful and efficient scale routing without time synchronization, a robust trust-aware routing framework is designed and implemented. To overcome the misdirecting of multi hop communication, and also to provide security for WSN, authors proposed this algorithm.

B. A Mohan, H. Saroja Devi, [8] proposed an efficient hybrid data collection algorithm, for data collection from multiple mobile nodes. In this technique, the cluster head will be elected by the base station for first two rounds using centralized algorithm, after that CH selection is based on previous cluster heads selection in distributed way. Here a mobile node is introduced between CH, and Base Station. For this type of applications, Mobile nodes are assigned with unlimited resources to increase lifetime of Network.

J. Luo and J.-P. Hubaux, [9] presented an energy efficient and conserving routing protocol for the purpose of improving lifetime, by managing the concentration of data traffic at small number of base stations. In WSN, sensors which are nearer to BS have to relay high amount of data traffic, then those nodes batteries ends up quickly. To overcome this problem, the BS should be a mobile, and then automatically sensors nearer to BS changes timely and no more data traffic burden would be on same nodes.

Atakli et al. [10] developed a scheme based on weighted-trust estimation in order to detect and isolate the compromised nodes in hierarchical clustered WSN structure. In this scheme, they select some nodes as forwarding nodes to give a trust values for all of the cluster nodes. Afterwards, they decrease the node's trust level for all nodes that sent malicious information. D. Tolba, W. Ajib, and A. Obaid, [11] proposed an energy efficient algorithm, for mobile WSNs, It is a distributed clustering algorithm, and it is named as ALM. This algorithm enhances network lifetime, and it also improves the stability, and network connectivity.

Gong et al. [12] presented a routing protocol for the purpose of energy efficiency and security in WSNs, named, secure and energy aware routing protocol (ETARP). The main contribution point in ETARP is route discovering and selection based on both the maximum utility concept. ETARP scheme takes into consideration the energy efficiency and the trustworthiness in routing protocol, which may sustain more complexity and overhead compared to AODV routing protocol. For hybridized networks like some nodes are fixed and others are mobile, a CBR-MOBILE routing is proposed. It is a traffic adaptive routing protocol, which gives a re-assigned time slot to the mobile nodes which are moving into the network by removing the timeslots of nodes which are moving out of the network [13].Authors proposed a novel secure mobile data routing to the mobile nodes while collecting the data. For secure data collection they proposed three protocols with a tree based connection management among them [14].

S. Deng ; J. Li ; L. Shen proposed a Mobility based clustering protocol for wireless sensor networks, with mobile nodes. Based on its residual energy and mobility of the sensor node, it can decide itself as a cluster head. Based on connection time estimation, the sensor node aims on link stability which is connected between sensor node and cluster head. Each sensor node can send its data in assigned time slot in an ascending order (TDMA).During mobility condition; sensor node sends a joining request message to the new cluster head, about its joining when it lost its connection with previous cluster head [16].

III. RESEARCH METHODOLOGY

3.1 Network model

The network model should have randomly deployed sensor nodes in distributed way with non-uniform manner. Sensor nodes are arranged as sub clusters, and each sub cluster is assigned with one or two mobile nodes randomly. The cluster head (CH), should be at centre of sensing sub regions, and it has to be in communicate with only Mobile nodes. All sensor nodes are homogeneous, and equipped with a unique ID.

1. The sensor nodes are always static and that nodes never change its location.
2. These nodes are used to accumulate surrounding data and forward this data to the cluster head, through Mobile node by wireless communication.
3. The unique identifier (ID) is assigned to each and every sensor node to avoid redundant data, these sensor nodes won’t work when their energy is less than threshold level.

4. Power level can be adjusted dynamically when node's transmitting energy level decreases.

Every sensor nodes calculates their position based on the received signal strength instead of GPS equipment based position finding in the sensor region

3.1.1 Energy consumption model:

The energy spent for transmitting an m-bit message over distance n is, $E(Trans)_{m,n} =$

$$\begin{cases} m \times E(elec) + n \times \propto (fs) \times n^2, & n < n(0) \\ m \times E(elec) + n \times \propto (mp) \times n^2, & n \geq n(0) \end{cases} \quad (1)$$

The energy spent to receive m-bit message is

$$E(rec)_{\mathbf{m}} = m \times E(elec) \quad (2)$$

Amount of energy consumption to aggregate k messages with m-bit is denoted by,

$$E(agg)_{\mathbf{k,m}} = k \times m \times E(da) \quad (3)$$

Where E(da) is the energy dissipated per bit to aggregate message signal.E(elec) is the energy consumed by the sensor node for a bit of data transmission.

The residual energy (RE) of proposed algorithm is measured in each round, which starts from the current round, round+1 and round+ 2 until final node is reached. The energy consumption rate of proposed system is shown in the following equations. The energy consumption measured in various rounds is as follows,

In current round, the energy consumed by CH is given in equation 1.

$$\text{Residual energy} = RE + S(i) * E \quad (4)$$

From this, the average residual energy (ARE) is calculated using,

$$ARE(Round + 1) = \frac{RE\,(Round\ +1)}{2} \quad (5)$$

The Total Energy Consumption (TEC) on each rounds are calculated using the following equation.

$$TEC(Round + 1) = E_0 * n - RE(Round + 1) \quad (6)$$

In case are 'n' layers available in the network, the average energy consumption of node can be defined as

$$AEC(Round + 1) = \frac{TEC\,(Round\ +1)}{n} \quad (7)$$

The AEC is calculated with respect to the total energy consumption. TEC consists of the average of all transmitted energy, received energy, idle energy and sleep mode energy. The result shows the total dead and alive nodes present in the system.

3.1.2 Energy Consumption model for proposed algorithm

The Energy consumption for the mobile data collector, and in the system for data transmission when CH is located at centre of the cluster, can be calculated as

To send 'R' bits of data to the cluster head from mobile data collector, its energy consumption is

$$E_{(MDC)} = m \times E_{(elec)} + m \times E_{(s)} \times r_h^2 \quad (8)$$

Where $E_{(MDC)}$ is the energy consumed by mobile data collector node, and r_h is the average distance between mobile data collector and cluster head.

$$r_h^2 = \frac{L^2}{2\pi K} \quad (9)$$

RE is the residual energy consumed by the cluster head for R bits of data transmission in particular round, and it is expressed as

$$RE = \left(\frac{T}{K} - 1\right) \times m \times E_{(elec)} + \frac{T}{K} \times m \times E_{(d)} + m \times E_{(elec)} + \propto (fs) \times r_d \quad (10)$$

Where,

T is the number of nodes equally dispersed over the square area L × L.

$E_{(d)}$ is the energy consumed per bit report to the base station, and r_d is the distance between cluster head to the base station.

3.2 Proposed method

In Wireless sensor networks, even there is a tremendous work going on to make the network more energy efficient and also to improve the lifetime of network. In this paper each sub cluster is assigning with two to three mobile nodes to move among sub clusters for data gathering from each sub cluster nodes and finally they forward data to cluster head. When mobile node (MN), moves around the sub cluster nodes, then they gets off from sleep mode and they forward data to mobile node. Once the MN moves away from Sub cluster nodes, they again go to sleep mode until next event comes. This paper introduces a Green CoMP based energy efficient data aggregation algorithm (GEED-M), to make the network more energy efficient, and also to improve lifetime of the network.

3.2.1 Objectives and Advantages of Proposed Aggregation Algorithm

The main advantages of proposed algorithm, compared to conventional algorithms are listed below.

- Conventional clustering and data aggregation algorithms are unsuccessful to give optimum results in plateaus and military applications. But this algorithm gives better results in network loss, lifetime, and energy efficiency.

- Mobile data collector collects data from sensor nodes independently, without any neighbour node interferences
- Mobile data collector can identify low energy sensor nodes, and keep them in sleep states, to reduce energy consumption.
- Less loaded and heavily loaded sub-clusters can take decisions dynamically to share the mobile node energy resources.
- Tree structured data aggregation algorithms are avoided to reduce more load in ends of the branch nodes. Therefore unwanted overhead is also reduced in this algorithm.

3.2.2 Green CoMP based Energy efficient Data Aggregation Algorithm (GEED-M)

In green comp based cellular networks, the less loaded cell (during night times) is switched off up to some time, and traffic of that cell is shared by neighbour cells by increasing their coverage to cover switched off cell users. This efficient technique reduces power wastage very well in cellular networks [4]. In the same way, due to random deployment of sensor nodes, some sub clusters may less loaded and some sub clusters may heavily loaded. Heavily loaded sub clusters need more than one mobile node to cover the entire sub cluster quickly, less loaded sub clusters do not require more than one number of mobile node. to make the load balance, one sub cluster's mobile node is handover to another sub clusters (neighbour clusters) in following conditions.

1. If one of the sub cluster has less number of nodes.(less loaded sub cluster)

2. If one of the sub cluster has more number of nodes (heavily loaded) but assigned with less number of mobile nodes (<2)

3. If the energy of mobile nodes is less than the threshold level.

As mentioned in first condition, less loaded sub cluster does not require more than one mobile node, therefore remaining mobile nodes of sub cluster are switch over to another sub clusters which are heavily loaded. If a sub cluster is loaded with very few nodes (SC3), then that sub cluster is assigned with neighbour sub cluster mobile nodes as green comp technique in cellular networks. As per next two conditions, if heavily loaded sub cluster has less number of mobile nodes (SC2), or if the energy of mobile node is less than the threshold level after some rounds, then neighbour mobile nodes are switch over from other sub clusters. From implementation, the sub cluster 3 has less number of sensor nodes with a single mobile node, sub cluster 2 has large number of sensor nodes but it is also assigned with a single mobile node (MN 30).

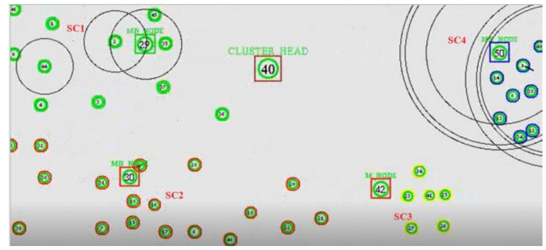

Fig .3 Implementation of Green CoMP (Initial Rounds)

In sc3, sensor nodes send their data to the MN 42, once the data transmission is completed, those nodes goes into sleep state, and MN 42 moves towards to the SC2 for data gathering (in fig. 4). Similarly in SC1, MN 29 moves towards to the SC2, after SC1 nodes moves into sleep state.

In SC2, some nodes, like 24, 22, and 20 send their data to the MN42, and other nodes 15, 18, 42, 28 etc. send their data to MN 29. Based on distance, nodes send their data to nearest MNs. Depends on energy level network can decide whether MN 30 has to be switch off/on.

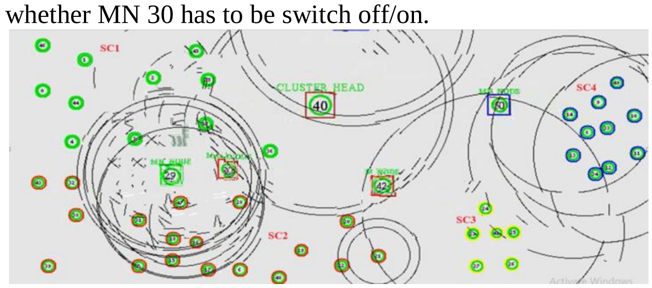

Fig .4 Implementation of Green CoMP (After Few Rounds)

3.2.3 Malicious node identification

The Role of mobile node in these types of applications is very important, especially in data aggregation and data transmission. The entire sub cluster data depends on mobile node of particular sub cluster. Therefore Mobile nodes should have to transmit data perfectly and also within a timeslot. If mobile node is malicious then entire network performance degrades and it is a big issue to the network in some major applications like military and security networks. There are three cases to check or to identify whether the mobile node is a malicious or not.

Case-I: If the mobile node does not able to transmit any data to cluster head (Dead)

Case-II: if the mobile node able to send the data, but it is a fault data. (Fault)

Case-III: if the mobile node able to send the correct data, but it is received as a fault data due to link failure. (Link fail)

In Case–I, if the mobile node does not able to transmit data, then that MN has to remove from the network, and that node is to be considered as almost dead node.

In Case – II, if mobile node transmits data to cluster head, but the data is incorrect in several links, then the network will decide that the mobile node is a fault node, and it has to remove from the network.

In Case – III, if mobile node able to send correct data to cluster head, but it received as a fault data in only one link, then the network will decide that, an error is occurred due to link failure but not due to mobile node.

The above three cases should be check by the network itself and it has to decide which action has to be take according to the case, For this purpose a BIST based malicious node identification algorithm is proposed, In this algorithm the cluster head has to check every mobile node before data transmission initiates. For this the cluster head asks mobile node to transmit a sequence of two bits for checking purpose. The mobile node itself asks neighbour six nodes to send a data bit HIGH, then the mobile node aggregates the data and send it to cluster head, again the mobile node asks another six neighbour nodes to send a data bit LOW, then the mobile node aggregates the data and send it to the cluster head, If cluster head receives two data bits 1, and 0 (Zero) simultaneously from mobile node, then it accepts that mobile node for data transmission. If cluster head does not receive those two bits sequence correctly, then it asks agent node in particular sub cluster to check that mobile node condition. When mobile node sends data to particular agent node, if agent node also does not receive data sequence correctly then cluster head decides, that mobile node is a fault node and it is completely removed from the network. If agent node receives data sequence correctly, but cluster head receives data sequence wrongly, then cluster head decides data received wrongly due to communication link failure. Then it assigns another link to mobile node and check again. Here agent node is the node which node has direct access with cluster head for malicious identification. During this entire process mobile node can identify malicious nodes of sub cluster, when it asks its neighbour nodes to send data HIGH, Low for checking process. Those nodes will remove from the sub cluster by mobile node.

<u>Algorithm of proposed Green CoMP</u>

MN ←collect data from n
Calculation of energy in MN
Threshold (TH) =5J (assigned)
If
TH of MN < 5J
MN of neighbour cluster act as data collector
Else
Present MN act as data collector`
End if

<u>Algorithm of Malicious Node Identification</u>

R = no. of rounds
Sequence formation ←R
No. of bits in sequence= [0, 1]
X falls in the condition
if
MN → $\sum_{n=1}^{N}$ seq[1]
And
MN → $\sum_{n=1}^{N}$ seq[0]
Denote
X = no malicious node is detected
Else
Y= malicious node is detected
End if

IV. PERFORMANCE ANALYSIS

In this section, the proposed green comp based data aggregation algorithm with malicious node identification (GEED-M) is proposed, evaluated and compared its performance with two other known routing protocols: suspicious node information dissemination protocol (SNIDP) and normal Node Behavioral Strategies Banding Trust Evaluation Algorithm (NBBTE). These two algorithms were chosen for being well known in the literature and have the same goals that the proposed algorithm. The TMECA performance is evaluated under the following metrics: (i) Energy efficiency (ii) Energy Consumption (iii) Throughput (iv) Lifetime of network.

Parameters	Values
Simulation Period	100ms
Coverage Area	1320*1032
No of Nodes	51
No of sink node	1
No of mobile node	5
No of Sub cluster	5
No of Cluster Head	1
Traffic Type	CBR
Agent Type	UDP
Routing protocol	AODV
Initial power	100 J
Transmission Power	1 J
Receiving Power	1 J
Queue Type	Drop-Tail

Table-1 Simulation parameters

Network lifetime

The lifetime of network is calculated by data aggregation in number of rounds until sensor node get die. For applications instance, where the time of all nodes operates together, the lifetime can be defined as the first sensor is exhausted of its energy until certain the number of rounds.

The data aggregation is to perform the uniform energy drainage in the network. The proposed algorithm gives better results compared with SNDP, and NBBTE, GLBD, MLPA algorithms.

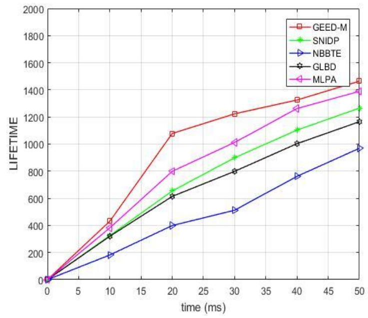

Fig. 5 Network lifetime comparison with existing systems

Energy Efficiency

Energy efficiency is the amount of energy used by the individual node that to be processed. The proposed work shows how much it is efficient than existed protocols. It is an efficient technique which can reduces the energy wastage, and performs the number of rounds within limited energy. Malicious node identification is a good sign for reducing energy wastage of the network.

Energy Consumption

The energy consumption represents energy consumed by the network within assigned data rounds. Energy consumption includes energy consumed by the nodes, processors, transceiver, and all other units used for the network. The energy consumption of the network is greatly reduced by Green CoMP technique. By avoiding malicious nodes in the network, the energy wastage can be reduced. Figure shows comparison results of Green CoMP with existed techniques.

Network Throughput

Throughput is the amount of data transmitted successfully from one place to another in a given time period. It is also referred as overall system performance. The proposed technique can reduce the packet wastage and it can increase the system performance. The comparison results of the proposed method with existed techniques shown below to know how Green CoMP plays a vital role in WSN.

Packet Delivery Ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations which is generated by the sources. Packet delivery ratio is a key parameter in estimation of a network performance. The Packet delivery ratio of proposed method is slightly better than existed protocols. The PDR can be improved by maintaining proper communication links with working sensor nodes.

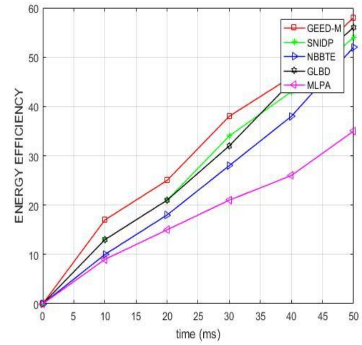

Figure 6: Energy Efficiency comparison graph with existing system

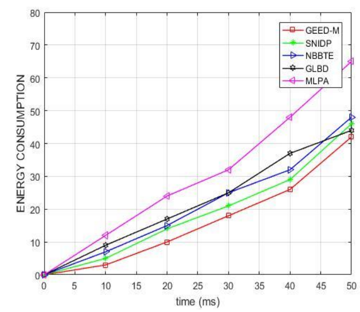

Figure 7: Energy consumption comparison graph with existing system

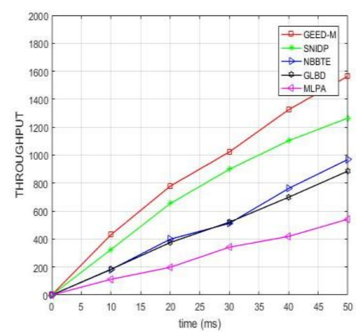

Figure 8: Network throughput comparison graph with existing system

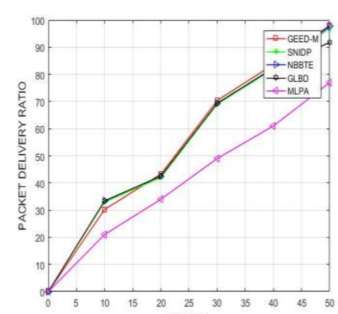

Figure 9: packet delivery ratio comparison graph with existing system

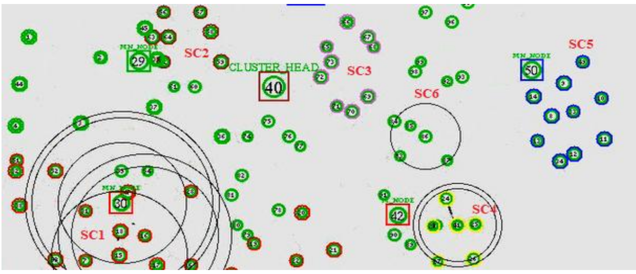

Fig .10: Implementation of Green CoMP with higher nodes (>100 Nodes) at Initial Rounds

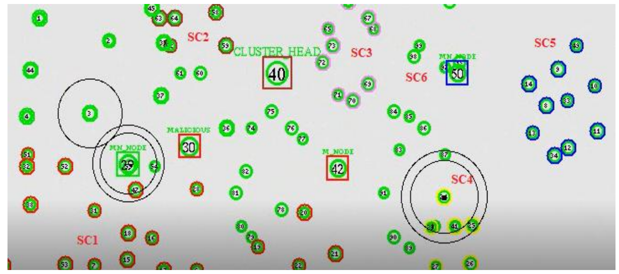

Fig .11 Implementation of Green CoMP with higher nodes (>100 Nodes) after few rounds

PARAMETER	NBBTE	SNIDP	GEED-M (proposed)
Packet delivery rate	77%	72%	97.419%
Control overhead	1265 packets	1564 packets	969 packets
Energy Consumption	65%	80%	44%
Energy efficiency	35%	20%	54%
Throughput	542 Kbps	244 Kbps	886 Kbps
Loss	432 packets	564 packets	207 packets
Lifetime	35%	20%	56%

The major parameters of network are calculated and compared with existing algorithms to show the strength and importance of proposed algorithm. To enlighten the strength of proposed work, simulation has extended with 100 nodes, and various parameters are observed and calculated. The proposed algorithm also gives better results compared with existing algorithms, even at higher number of nodes in a cluster. The entire cluster nodes are organized into sub clusters, and each sub cluster is assigned with at least one mobile node for data collection. The mobile data collector nodes can collect information from sensor nodes individually and given to the cluster head. If the mobile node energy level is reduced than threshold level, then that mobile node, sends a request message to neighbour sub cluster Mobile data collector node, then neighbour mobile data collector node can collect data from sensor nodes and given to cluster head. After few rounds of data collection, MN 42 moves towards to SC6, MN50, moves towards to SC6 and SC3 and MN 29 moves towards to SC1. When one of the mobile nodes is identified, as malicious, then it is separated from data collection, and keep it as dead node, as discussed in the proposed work. From simulation, we can observe in fig.11, The MN 30 identified as malicious, after few rounds of data collection.

V. PARAMETRIC ANALYSIS OF LIFETIME, NETWORK LOSS AND THROUGHPUT BASED ON NODE DENSITY IN A CLUSTER

The parametric analysis of Network lifetime, Network loss and throughput are calculated and analyzed for various node densities 50, 100 nodes per cluster. This analysis shows various changes in parameter values according to the network density. From parametric analysis, the proposed GEED-M algorithm gives better results even the network density increases.

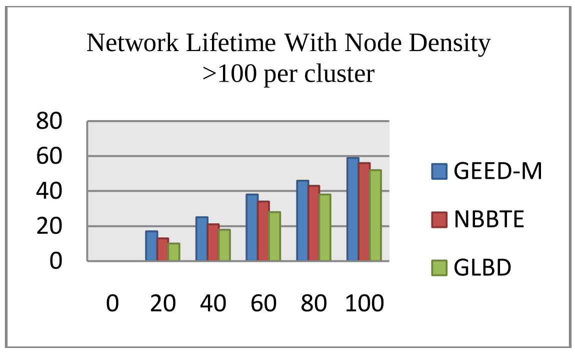

Fig. 12 Comparison of Network lifetime with existing systems

The Network lifetime is calculated by data aggregation in number of rounds until sensor node get die. The proposed GEED-M algorithm is applied at various node densities, and evaluated various parameters. The lifetime is the key parameter which decides the network throughput and usage. So lifetime is calculated at higher node density and compared its results with popular existed algorithms like NBBTE, GLBD.

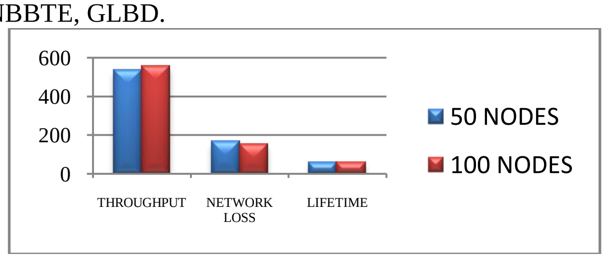

Fig. 13 Parametric Analysis of Lifetime, Network Loss and Throughput

Parametric analysis can be performed, by calculating various parameters at various node densities and analysed at different density levels. The Graph shows comparison and analysis of various parameters like Lifetime, Loss of network, and Throughput of proposed GEED-M algorithm.

VI. CONCLUSION

WSN in plateaus and Military areas has more concern with network lifetime and energy efficiency due to uneven deployment of sensor nodes and due to mobility of data collectors. Due to Energy limitation, Sometimes there is a chance of each sub cluster may have only one mobile node, or none after some rounds of data sensing. To overcome this problem, a Green CoMP Based Energy Efficient Data Aggregation Algorithm with Malicious Node Identification (GEED-M) is proposed. Depending on energy level of mobile node network can decide which mobile node has to be active/sleep, and switch over from one sub cluster to another sub cluster.

This algorithm makes the network more energy efficient and also improves the network lifetime. This work will be extended in future with Trust Node based Data Aggregation. The proposed method achieves 56% of network lifetime and also 54% of energy efficiency.

VII. REFERENCES

[1]. L F. Akyildiz, T.Melodia, and K. R. Chowdhury, ‘A survey on wireless multimedia sensor networks’,*Computer Netw. (ElseVier)*,Vol. No. 51, Issue No. 4, pp. 921-960. 2007

[2]. O. DurmazIncel, A. Ghosh, B. Krishnamachari, and K. Chintalapudi, ‘Fast data collection in tree-based wireless sensor networks’,*IEEE Tran. Mobile Computing*,Vol No. 11, Issue No. 1, pp. 86-99.2012.

[3]. V. Mhatre and C. Rosenberg, "Design guidelines for wireless sensor networks communication: clustering and aggregation",*Elsevier Ad Hoc Networks Journal*,Vol No. 2, Issue No 1, pp. 45-63. 2004.

[4]. Po-Han Huang, Shi-Sheng Sun, and Wanjiun Liao, ‘GreenCoMP: Energy-Aware Cooperation for Green Cellular Networks’,*IEEE Transactions on mobile computing*,Vol No. 16, Issue No 1, pp. 143-157. 2017.

[5]. Syed Muhammad Sajjad, SafdarHussainBouk, and Muhammad Yousaf, ‘Neighbor Node Trust Based Intrusion Detection System for WSN’. *Procedia Computer Science*, Vol No 63, pp. 183-188. 2015.

[6]. R. Ferdous, V. Muthukkumarasamy, and A. Sattar, ‘A Node-based Trust Management Scheme for Mobile Ad-Hoc Networks’. *Proceedings of the 4th International Conference on Network and System Security* (*NSS), 2010*, pp. 275–280.

[7]. GuoxingZhan, WeisongShi, J.Deng, ‘Design and implementation of TARF: A trust-aware routing framework for WSNs’, *IEEE Transactions on Dependable and Secure Computing*,Vol No 9, Issue No 2, pp. 184-197. 2012.

[8]. B. A Mohan, H. Saroja Devi, ‘A hybrid approach for data collection using multiple mobile nodes in WSN (HADMMN)’. In. Proc. *IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*,Vol No. 5, pp. 736-739. 2016.

[9]. J. Luo and J.-P. Hubaux, ‘Joint mobility and routing for lifetime elongation in wireless sensor networks,’ in *Proc. IEEE INFOCOM*, Vol No. 3, pp. 1735-1746, 2005.

[10]. Idris M. Atakli, Hongbing Hu, Yu Chen, Wei-Shinn Ku, and Zhou Su, "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation". *Proceedings of the Symposium on Simulation of Systems Security (SSSS'08), Ottawa, Canada*, April 14 – 17, pp. 836-843, 2008.

[11]. F. D. Tolba, W. Ajib, and A. Obaid, “Distributed clustering algorithm for mobile wireless sensors networks,” in *Proceedings of the 12th IEEE SENSORS 2013*, Conference, pp. 1–4.

[12]. P. Gong, T. M. Chen, and Q. Xu, ‘ETARP: Energy Efficient Trust- Aware Routing Protocol for Wireless Sensor Networks’. Journal of Sensors, 2015, Article ID 469793, 10 pages, 2015.

[13]. Awwad, Samer A. B. and Ng, CheeKyun and Noordin, Nor Kamariah and A. Rasid, MohdFadlee , ‘Cluster based routing protocol for mobile nodes in wireless sensor network’, *Wireless Personal Communications*,Vol No. 61, Issue No 2, pp. 251-281.

[14]. Poornima, A.S. &Amberker, B.B..‘Secure data collection using mobile data collector in clustered wireless sensor networks’, *IET Wireless Sensor Systems*, 2011, Vol No. 1, pp. 85 – 95.

[15]. Sayyed, Ali & Buss Becker, Leandro. ‘Optimizing speed of mobile data collector in Wireless Sensor Network’, 2015, 1-6. International Conference on Emerging Technologies (ICET)

[16]. S. Deng, J. Li and L. Shen, ‘Mobility-based clustering protocol for wireless sensor networks with mobile nodes,’ in *IET Wireless Sensor Systems*,Vol No. 1, Issue No 1, pp. 39-47, 2011.

[17]. Azharuddin, M., Kuila, P., Jana, P.K.: ‘Energy efficient fault tolerant clustering and routing algorithms for wireless sensor networks’, *Comput. Electr. Eng.*, Vol No. , **41**, pp. 177–190, 2015.

[18]. Ip, W., Wang, D., Cho, V.: ‘Aircraft ground service scheduling problems and their genetic algorithm with hybrid assignment and sequence encoding scheme’, *IEEE Syst.* Journal, Vol No.**7**, Issue No 4, pp. 649–657, 2013,