International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 05, 2020
ISSN: 1475-7192

Sequestration Security in A Remote Sensor Network

Niketha Anand, Sibi Amaran and R.S. Preyanka Lakshme

Abstract--- *The implementation of identifying a malicious node in a system and then removing the malicious nodes detected to prevent errors that might occur due to them. An effective Security Program is one that does not have any malicious nodes. Few techniques and as viruses, spyware, and trojan horse. Message authentication and checksum are involved in the implementation of identifying malicious nodes. The tools used are Network Simulator 2, Cryptography, GSTEB algorithm. Network Simulator is an open-source designed specifically for research in computer communication networks. The proposed work can solve Sequestration Security in a network and detect any intruder detections on a cluster of data in a network, it not only detects attacks but also handles them.*

Keywords--- *Wireless Sensor Network, Network Simulator 2, GSTEB Algorithm, LEACH Algorithm, Source Node, Base Station, Clusters.*

I. INTRODUCTION

The data communication across the nodes in the WSN network faces with high traffic intensity and high information measure while transferring in the problem statement. The WSN tends to communicate by sending data across the nodes from the base station where the sensor nodes reverts back with the solution. This process is extremely energy consuming and requires all sub networks within the limited communication range. The sensors in one arena may not be available to be accessed in the other neighboring arenas. Thus, communication becomes a plot of challenge for the nodes. Accumulating knowledge or data from various nodes is tedious task. Wireless transfer of data constantly requires the maximum energy for the sensors to draw out information. The information that is processed by the sensors may not be important and the head sensor always requires high amount of energy to get the information from the alternative sensors. The unapproved aggressors screens, listens to and alters the information stream in the correspondence channel are known as dynamic attack.

Each and every node cluster and assigned to the region. Source node send the message to the destination node to the other region in the multicasting way. Each and every node movement updating to the cluster table. In every cluster assisting to send data to the destination. Every cluster stores the information and check the polynomial to other clusters. En-route filtering separate the false message in the way of node based on the key.

A. Leach Algorithm

The LEACH algorithm is an algorithm commonly used for reducing the energy consumption. LEACH stands for low energy adaptive cluster hierarchy. It consists of a base station, cluster head and nodes. Cluster head is selected based on a few criteria's, we do not consider energy consumption during this. Though we use it to lower the energy

Niketha Anand, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu.
Sibi Amaran, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu.
R.S. Preyanka Lakshme, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu.

DOI: 10.37200/IJPR/V24I5/PR201927
Received: 20 Feb 2020 | Revised: 14 Mar 2020 | Accepted: 28 Mar 2020

it leads to data sink at times. LEACH makes use of CSMA message authentication, TDMA scheduling. After the cluster heads are assigned comes the next task where nodes decide which cluster they want to join [3,4] and form a cluster which consists of the cluster head along with the nodes.

All the nodes belonging in a particular cluster send and receive data from the cluster head. The cluster head is connected with the base station. There are several methods to decide how the nodes are allotted to the cluster. One such way is K means.[1,5]

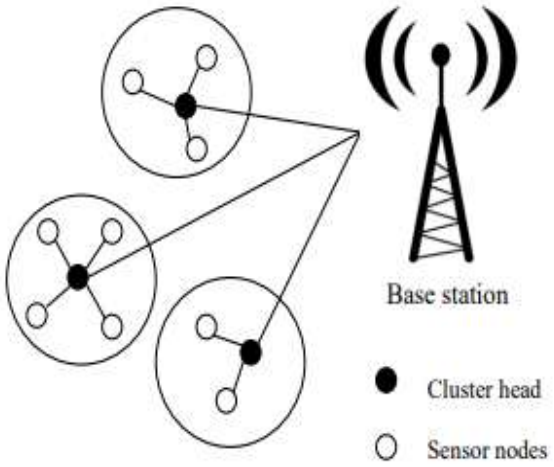

Fig. 1: Architectural diagram of LEACH

B. GSTEB Algorithm

GSTEB algorithm stands for general self organised tree based energy balancing routing protocol. This algorithm is capable of further reducing the time and consuming less energy. This method consists of three phases which consists of the cluster head selecting phase, cluster building phase and the cycle phase. The first step in this algorithm is broad casting, so every node will send a packet to each and every neighbouring node, within a particular radius in a particular time slot. GSTEB algorithm follows the architecture of a tree. So the routing tree will be rebuilt after each round. The root node which is the cluster head has to be assigned so overall which node has the highest weight will be chosen.

This information will be broadcasted again. It is an efficient algorithm and saves a lot of time and well as reduces energy consumption. It consists of a parent node, root node and a primary node. One important rule to be maintained is the distance between the parent node and primary node should always be lesser than the distance between the node and the root node. Transmission delay is short followed by improved efficient packet delivery to every node present in the wireless sensor network. Each and every node cluster and assigned to the region. Source node send the message to the destination node to the other region in the multicasting way. Each and every node movement updating to the cluster table.[6] In every cluster assisting to send data to the destination. Every cluster stores the information and check the polynomial to other clusters.[15] En-route filtering separate the message in the way of node based on the key.

DOI: 10.37200/IJPR/V24I5/PR201927
Received: 20 Feb 2020 | Revised: 14 Mar 2020 | Accepted: 28 Mar 2020

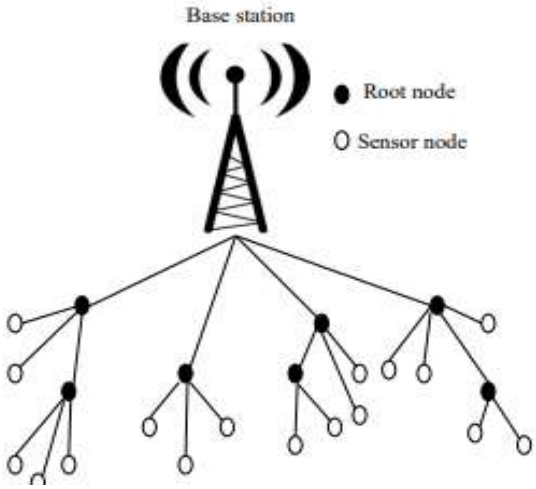

Fig. 2: Architectural diagram of GSTEB

C. Load Balancing

Load Balancing is an approach that is used to control and balance traffic. There maybe times when one cluster overlaps over another cluster this is one reason that leads to data link. There may also be some confusion in order to handle this we use load balancing. It handles the traffic effectively when few nodes are stuck. Each and every node cluster and assigned to the region.

Source node send the message to the destination node to the other region in the multicasting way. Each and every node movement updating to the cluster table. In every cluster assisting to send data to the destination. Every cluster stores the information and check the polynomial to other clusters. En-route filtering separate the false message in the way of node based on the key.[12,13]

Catch of a hub might uncover its data including exposure of cryptographic keys and accordingly trade off the entire sensor system. A specific sensor may be caught, and data (key) put away on it may be gotten by a foe. A breaking down hub will create incorrect information that could uncover the uprightness of sensor system particularly in the event that it is an information totaling hub, for example, a group pioneer Hub blackout is the circumstance that happens when a hub stops its capacity. For the situation where a group pioneer stops working, the sensor system conventions ought to be strong enough to moderate the impacts of hub blackouts by giving a backup course of action. Attacks: Packets can be defiled or indeed, even misrouted.

This can bring about a separated system, false sensor readings, and so forth. On the off chance that an assailant can increase physical access to the whole system he can duplicate cryptographic keys to the imitated sensor hubs. By embeddings the imitated hubs at particular system focuses, the assailant could without much of a stretch control a particular section of the system, maybe by detaching it by and large.

D. Disadvantages in Existing System

The Existing system has some limitations cannot be used efficiently to deal with those attacks. The data transmission protocols in the WSNs, which includes the cluster-based protocols are prone to variety of security

DOI: 10.37200/IJPR/V24I5/PR201927
Received: 20 Feb 2020 | Revised: 14 Mar 2020 | Accepted: 28 Mar 2020

attacks and they cannot achieve optimization or reduction in the energy involved[9,17]. Data compression techniques needs huge volume of storage capacity and high machine power and are ineffectual to deal with the divided network in the system. And additionally it causes request flooding problem. Using centralized cluster algorithm does not help in the decrease of energy consumption since it uses greedy formula. Mobile sink may fail at times to collect data from all nodes where sensors are connected and as a result of it we may have the communication variation.

II. PROPOSED SYSTEM

In this project, we propose a model that will be able to solve privacy and security problems in a network [2]The current in transit separating plans depend on T authentication validation : a genuine estimation report convey in any event T substantial message verification codes (MACs). T - limit and predefined before CPNS is conveyed. At the point when a report is transmitted from a sensor hub to the controller, every sending hub checks whether the sending reports really convey T substantial MACs. If not, the report is considered as a false one produced by the foe dropped. Something else, the report is sent to the following sending hubs along the course. Considering the above scenario, in this paper, we propose a model that works based on paper we propose Polynomial-based Compromise-Resilient En-route Filtering scheme to filter the false injected data effectively downside of traditional method is the lack of communication between different ends which might get destroyed in terms of failure and during crucial times[7,8].One of the key issues in Wireless Sensor Networks (WSN) is the hot-spot problem The model will be divide clusters into different groups by using different shortest path routing protocols such as OSPF.[11,16] Each cluster head will have a set of data grouped and they will all be executed at the same time. This reduces the time to 10 milli seconds.Some nodes may misbehave, the cluster head will recogonise all those nodes and protect other nodes from malicious nodes.[10] Message authentication and the use of even parity is used in message detection. LEACH algorithm is implemented which leads to data sink this leads to the implementation of GSTEB algorithm. GSTEB algorithm is implemented and along with that load balancing is performed. Load balancing is a phenomenon where balancing of extra traffic occurs when there is traffic or a clash between two or more nodes. Sometimes when there is to much of traffic it may head to data link.

III. IMPLEMENTATION

First we try implementing leach algorithm in network simulator 2.By implementing both it is easy to compare bpth the algorithm as well as perform filtering [14].Filtering is more like refraining and selecting only the needed data and discarding all the unwanted data.

```
Antenna/OmniAntenna set Gt_ 1 ;
Antenna/OmniAntenna set Gr_ 1 ;
Phy/WirelessPhy set L_ 1.0 ;
Phy/WirelessPhy set freq_ 2.472e9 ;
Phy/WirelessPhy set bandwidth_ 11Mb ;
Phy/WirelessPhy set Pt_ 20          ;
Phy/WirelessPhy set CPThresh_ 100.0 ;
```

DOI: 10.37200/IJPR/V24I5/PR201927
Received: 20 Feb 2020 | Revised: 14 Mar 2020 | Accepted: 28 Mar 2020

```
Phy/WirelessPhy set CSThresh_ 5.011872e-12 ;
Phy/WirelessPhy set RXThresh_ 5.82587e-09 ;
Mac/802_11 set dataRate_ 11Mb ;
Mac/802_11 set basicRate_ 1Mb ;
set ns [new Simulator]
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)
set tracefile [open proposed.tr w]
$ns trace-all $tracefile
set namfile [open proposed.nam w]
$ns namtrace-all $namfile
$ns namtrace-all-wireless $namfile $val(x) $val(y)
set n0 [$ns node]
$n0 set X_ 348.616
$n0 set Y_ 368.451
$n0 set Z_ 0.0
$ns color 0 blue
$n0 color blue
$ns at 0.0 "$n0 color blue"
$ns initial_node_pos $n0 28
set n1 [$ns node]
$n1 set Y_ 305.047
$n1 set Z_ 0.0
$n1 color blue
$ns at 0.0 "$n1 color blue"
$ns initial_node_pos $n1 28
set n2 [$ns node]
$n2 set X_ 187.143
$n2 set Y_ 229.744
$n2 set Z_ 0.0
$n10 set X_ 168.787
$n10 set Y_ 634.381
$n10 set Z_ 0.0
$n10 color blue
$ns at 0.0 "$n10 color blue"
```

DOI: 10.37200/IJPR/V24I5/PR201927
Received: 20 Feb 2020 | Revised: 14 Mar 2020 | Accepted: 28 Mar 2020

```
$ns initial_node_pos $n10 28
set n11 [$ns node]
$n11 set X_ 503.598
$n11 set Y_ 226.327
$n11 set Z_ 0.0
$n11 color blue
$ns at 0.0 "$n11 color blue"
$ns initial_node_pos $n11 28
set n12 [$ns node]
$n12 set X_ 554.745
$n12 set Y_ 312.149
$ns at 0.0 "$n12 color blue"
$ns initial_node_pos $n12 28
set n13 [$ns node]
$n13 set X_ 654.533
$n13 set Y_ 267.84
$n13 set Z_ 0.0
$n13 color blue
$ns at 0.0 "$n13 color blue"
$ns initial_node_pos $n13 28
set n14 [$ns node]
$n14 set X_ 713.857
$n14 set Y_ 153.132
$n14 set Z_ 0.0
$n14 color blue
$ns at 0.0 "$n14 color blue"
set n16 [$ns node]
$n16 set X_ 615.12
$n16 set Y_ 154.424
$n16 set Z_ 0.0
$ns initial_node_pos $n14 28
set n15 [$ns node]
$n15 set X_ 636.614
$n15 set Y_ 52.7309
$n15 set Z_ 0.0
$n15 color blue
$ns at 0.0 "$n15 color blue"
$ns initial_node_pos $n15 28
set n16 [$ns node]
```

DOI: 10.37200/IJPR/V24I5/PR201927
Received: 20 Feb 2020 | Revised: 14 Mar 2020 | Accepted: 28 Mar 2020

```
$n16 set X_ 615.12
$n16 set Y_ 154.424
$n16 set Z_ 0.0
$n16 color blue
$ns at 0.0 "$n16 color blue"
proc finish {} {
 global ns tracefile namfile
 $ns flush-trace
 close $tracefile
 close $namfile
# exec nam proposed.nam &
# exec cat proposed.tr &
 exit 0
}
for {set i 0} {$i < $val(nn) } { incr i } {
 $ns at $val(stop) "\$n$i reset"
}
$ns at $val(stop) "$ns nam-end-wireless $val(stop)"
$ns at $val(stop) "finish"
$ns at $val(stop) "puts \"done\" ; $ns halt"
$ns run
```

Leach Algorithm

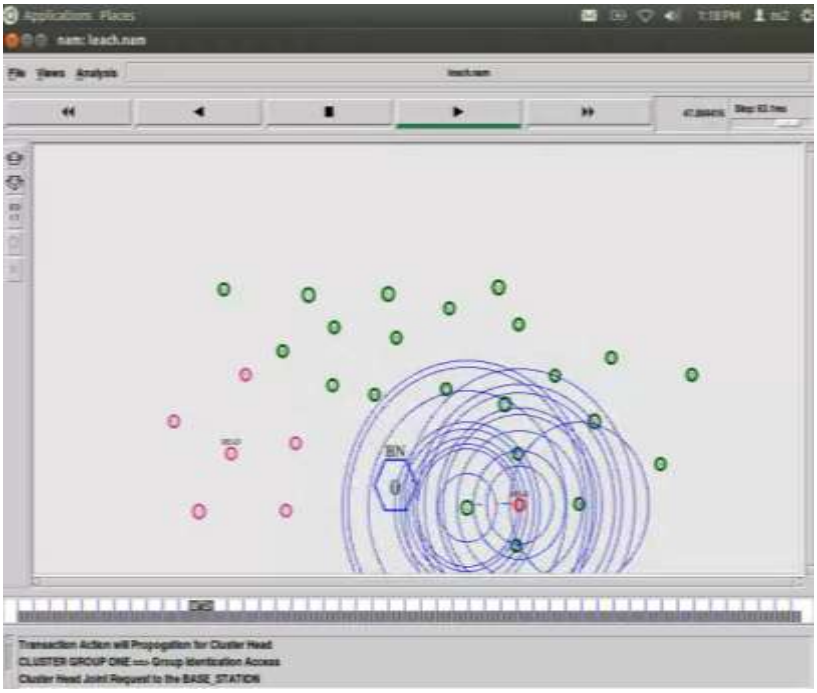

Fig. 3: Cluster head selection

DOI: 10.37200/IJPR/V24I5/PR201927
Received: 20 Feb 2020 | Revised: 14 Mar 2020 | Accepted: 28 Mar 2020

It starts with the assigning of the cluster head followed by the passing of data from cluster head to the other nodes. Once a node becomes a cluster head it cannot become a cluster head again. The red colour circle refers to the cluster head. Clusters are formed with the nodes, we a node that is of different colour that is the cluster head. Clusters are formed continuously.

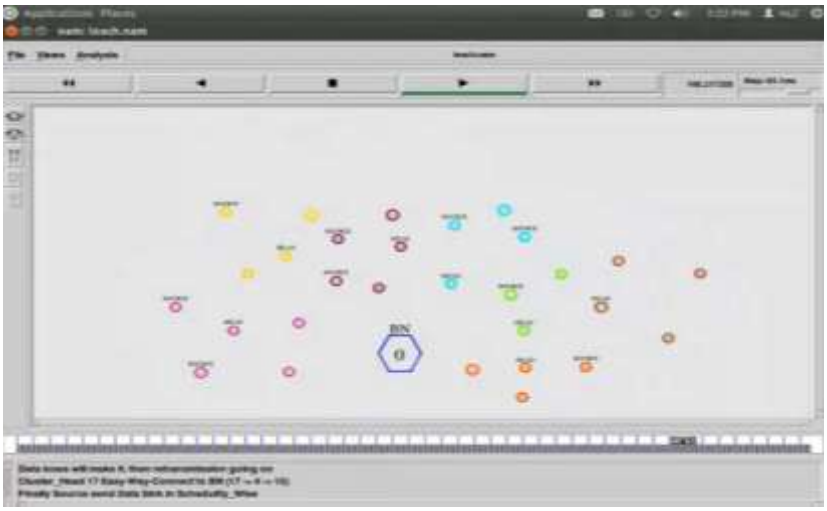

Fig. 4: Data sink

A message occurs telling data sink has occurred so we cannot proceed more than this in leach algorithm. So we try gsteb algorithm.

GSTEB Algorithm

This method consists of three phases which consists of the cluster head selecting phase, cluster building phase and the cycle phase

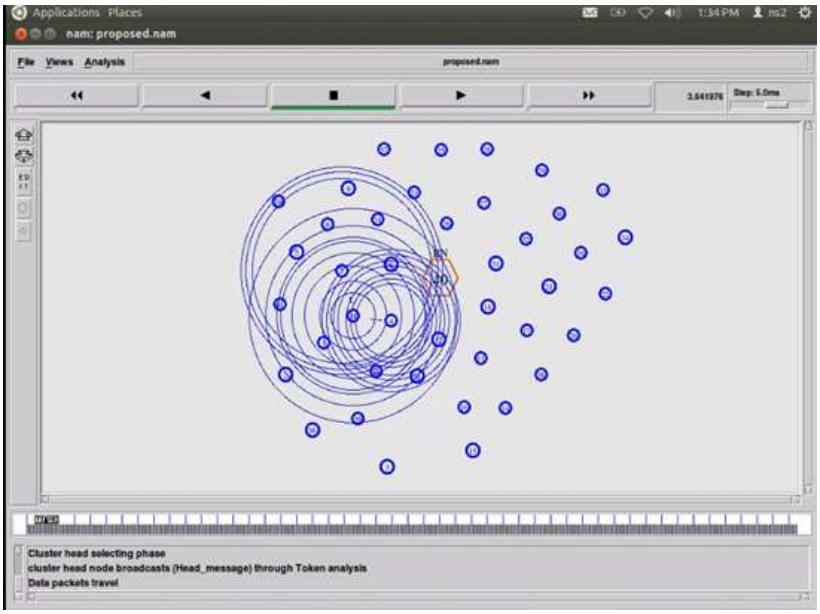

Fig. 5: Cluster head selection phase

DOI: 10.37200/IJPR/V24I5/PR201927
Received: 20 Feb 2020 | Revised: 14 Mar 2020 | Accepted: 28 Mar 2020

This denotes the first step that is the cluster head deciding phase. After this K hop neighbours declare themselves as the cluster head. The weight is calculated and the node which is the heaviest that is the node that weighs the most will be selected. This node becomes the cluster head. After this we have the steady state.

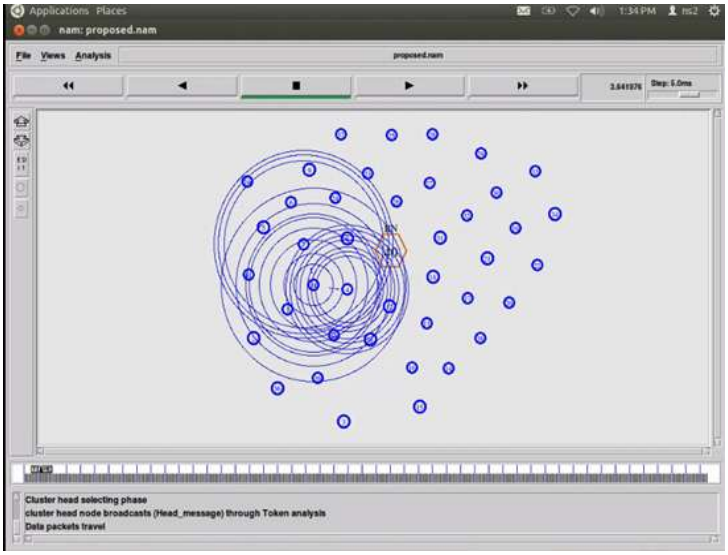

Fig. 6: Cluster building

The steady state is the phase where transferring of data takes from place. Data is transferred from the node to base station and vice versa.

Output

After executing the algorithm, now load balancing and filtering of data takes place.

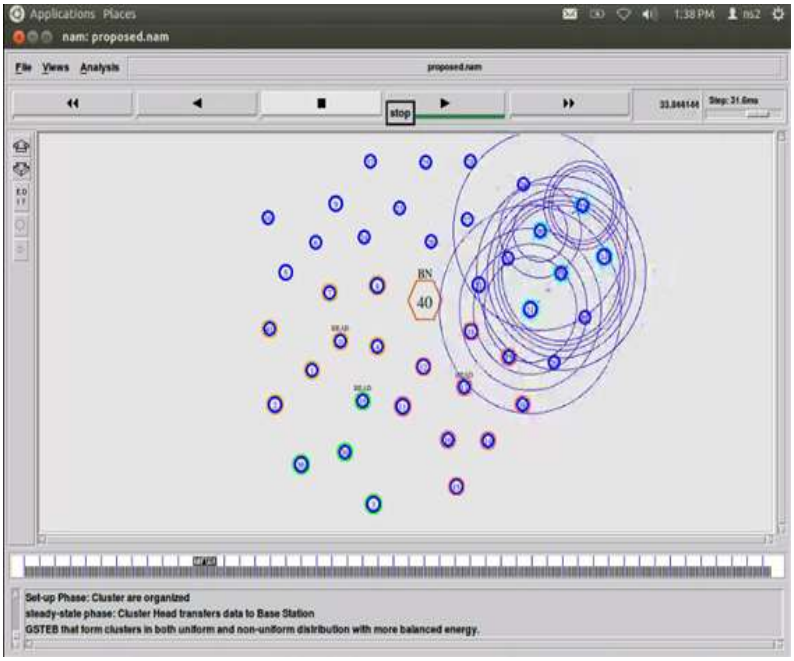

Fig. 7: Simulation output

DOI: 10.37200/IJPR/V24I5/PR201927
Received: 20 Feb 2020 | Revised: 14 Mar 2020 | Accepted: 28 Mar 2020

As we have used GSTEB algorithm there is a uniform and a non uniform distribution but with more balanced energy consumption.

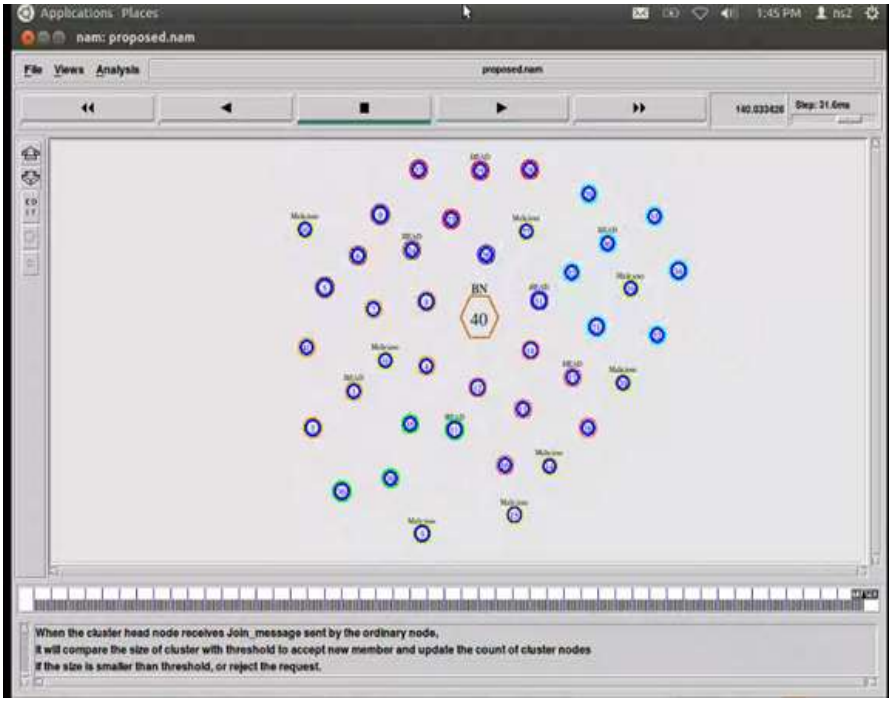

Fig. 8: Simulation output

When the cluster head receives a join message sent by the ordinary node, it will compare the size of the cluster with the size of the threshold. r.It will also be used to update the count of the cluster nodes. If the size is smaller than the threshold then the request maybe rejected.

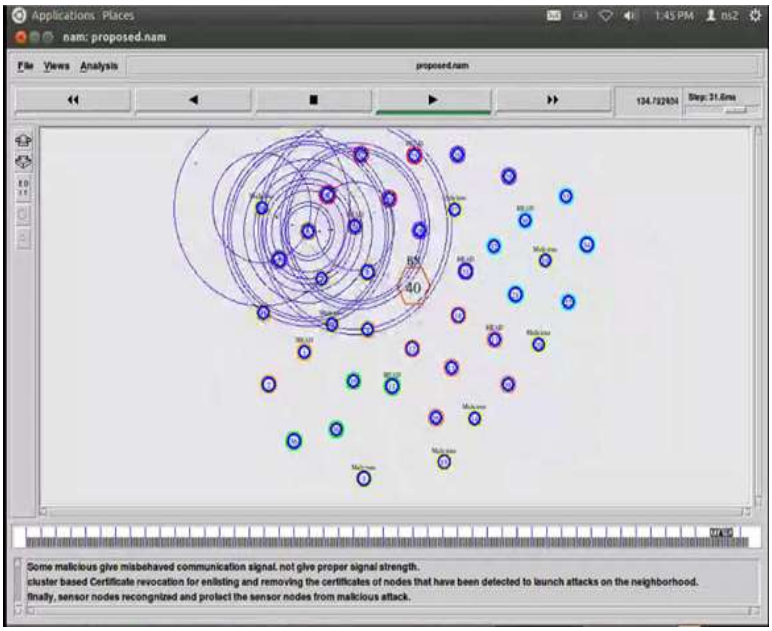

Fig. 9: Simulation Output

DOI: 10.37200/IJPR/V24I5/PR201927
Received: 20 Feb 2020 | Revised: 14 Mar 2020 | Accepted: 28 Mar 2020

The sensor nodes recognize and protect the other sensor nodes from malicious nodes. These malicious nodes are detected by the sensor node and handled by the sensor node itself. Some nodes give a misbehaved communication signal. Because if this signal there will not be proper signal strength. Cluster based certification revocation will be detected so there will a launch in the neighbor hood. This launch is carried out by the sensor nodes.

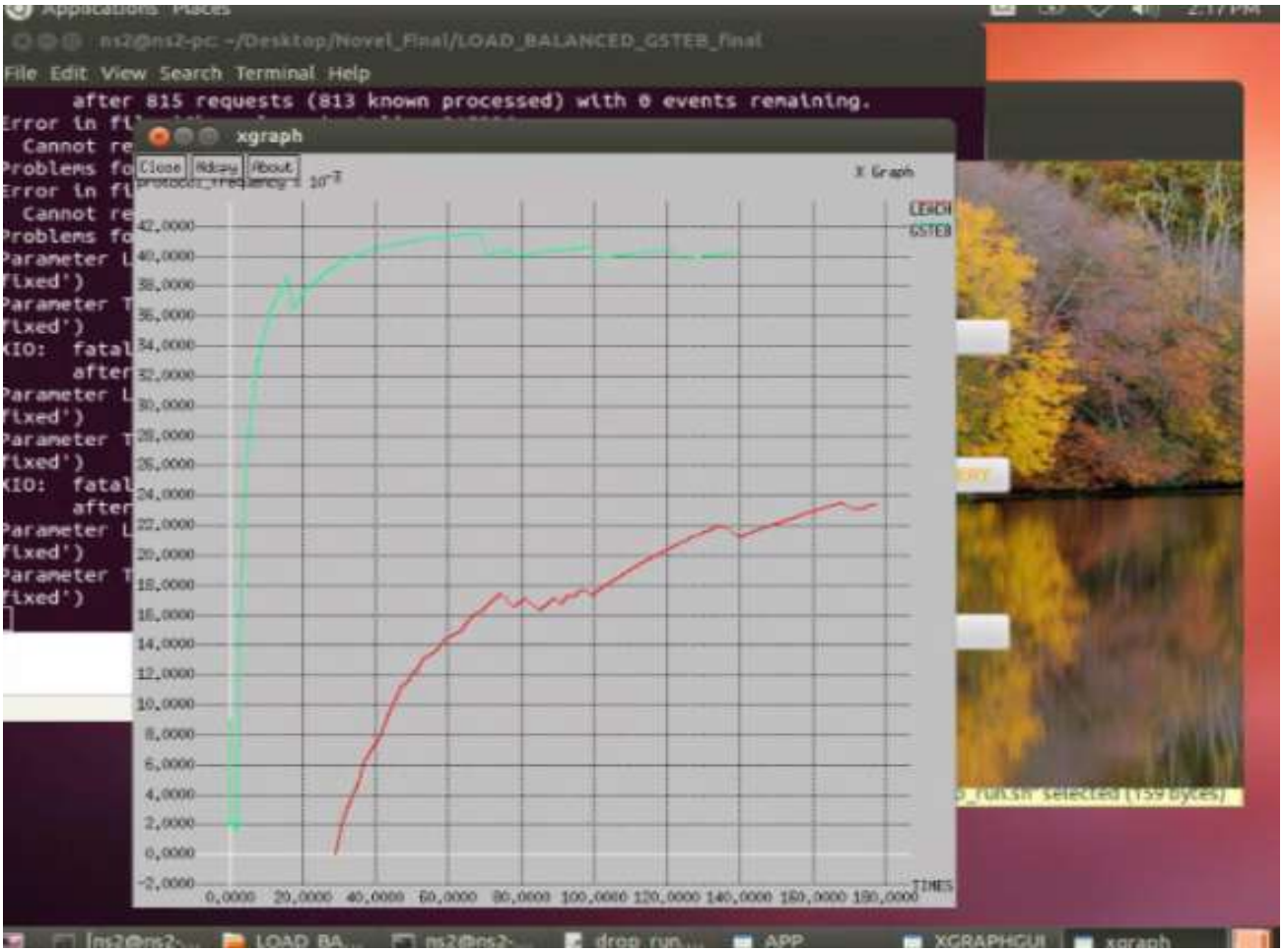

Fig. 10: Simulation Output

We generate a graph between both the algorithms used and we notice that GSTEB algorithm performs better than leach algorithm in terms of energy and the way in works.

IV. CONCLUSION

As discussed, simulated and identified malicious node detection using polynomial we have formulated and sorted the downside issue using the mobility sink and time-based recess which clubs with polynomial technique for the node data transfer across the sensors in various areas. To overcome all the existing techniques of malicious node removal in this technique very effective. This technique remove the malicious node with minimum cost and weight. Its save the energy of node.

DOI: 10.37200/IJPR/V24I5/PR201927
Received: 20 Feb 2020 | Revised: 14 Mar 2020 | Accepted: 28 Mar 2020

REFERENCES

[1] S. Jha, L. Kruger, and P. Mc Daniel, 'Privacy Preserving Clustering', *IEEE*, 2012.

[2] Mina Sheikhalishahi, Fabio Martinelli,'Privacy Preserving Clustering over Horizontal and Vertical Partitioned Data', *IEEE Symposium on Computers and Communications (ISCC),* 2017.

[3] Yanguang Shen, Junrui Han, Huifang Shan,' The Research of Privacy-preserving Clustering Algorithm' *IEEE Third International Symposium on Intelligent Information Technology and Security Informatics,* 22 April 2010.

[4] Jianqing Liu, YaodanHu, HaoYue, Yanmin Gong, Yuguang Fang,' *A Cloud-based Secure and Privacy-Preserving Clustering Analysis of Infectious Disease',* IEEE Symposium on Privacy-Aware Computing 2018.

[5] Hyeong-Jin Kim ; Jae-Woo Chang, 'A Privacy-Preserving k-Means Clustering Algorithm Using Secure Comparison Protocol and Density-Based Center Point Selection', *IEEE* 10 September 2018

[6] Data HuiYin, Jixin Zhan, Yinqiao Xiong, Xiaofeng Huang and Tiantian Deng, 'PPK-Means: Achieving Privacy-Preserving Clustering Over Encrypted Multi-Dimensional Cloud', 8 November 2018 MDPI

[7] H. Yang and S. Lu, "Commutative cipher based en-route filtering in wireless sensor networks," *in Proc. of 60th IEEE Vehicular Technology Conference (VTC'04)*, 2004, pp. 12–23.

[8] H. W. Lee, S. Y. Moon, and T. H. Cho, "A method to control the probability of attempts to verify a report in statistical en-route filtering," *in 2011 7th International Conference on Digital Content, Multimedia Technology and its Applications (IDCTA)*, 2011, pp. 160–164.

[9] Zhijun Li and Guang Gong" Survey on security in wireless sensor network" October 2017

[10] Yao Liu, Peng Ning, Michael K. Reiter" False data against state estimation in electric power grids" December 2017

[11] Yaping Lin, Yu-Fen Kao, Yu- Chee Tseng" From wireless sensor network towards cyber physical systems" January 2018

[12] Alok Kumar, Alwyn "Deterministic En-route filtering of false report: A Combinatorial Design Based Approach".

[13] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injection false data in sensor networks," *IEEE ournal on Selected Areas in Communications (JSCA)*, vol. 23, no. 4, pp. 839–850, 2005.

[14] L. Yu and J. Li, "Grouping-based resilient statistical en-route filtering for sensor networks," *in Proc. of the 28th IEEE International Conference on Computer Communications (INFOCOM'09)*, 2009, pp. 1782–1790.

[15] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking cryptographic schemes based on perturbation polynomials," *in Proceedings of the 16th ACM conference on Computer and communications security (ACMCCS'09)*, 2009, pp. 1–10.

[16] N. Subramanian, C. Yang, and W. Zhang, "Securing distributed data storage and retrieval in sensor networks," *in Proc. of the 27th IEEE International Conference on Pervasive Computing and Communications (PerCom'07)*, 2007, pp. 191–200.

[17] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 2, pp. 52–73, 2009.

DOI: 10.37200/IJPR/V24I5/PR201927
Received: 20 Feb 2020 | Revised: 14 Mar 2020 | Accepted: 28 Mar 2020