# Cluster Head Selection based Energy Efficient Technique for Defending against Black Hole Attack in Wireless Sensor Networks

Snehal P. Dongare
M.Tech. (Computer Science and Engineering),
Department of Computer Engineering,
B. D. College of Engineering,
Sevagram-442102, Wardha (M.S.) India

Ram S. Mangrulkar
Associate Professor and Head,
Department of Computer Engineering,
B. D. College of Engineering,
Sevagram-442102, Wardha (M.S.) India

## ABSTRACT
Wireless Sensor Networks (WSNs), besides its huge application areas, is prone to various types of attacks and security threats. Due to its dynamic topology, highly decentralized infrastructure and resource constraint sensors, proper energy utilization becomes a challenging issue. These entities are responsible to make WSNs susceptible to various types of denials of service attacks which results in disastrous consequences like energy-hole creation in the network.Various cluster head selection based energy efficient protocols have been proposed to improve the lifetime of WSNs. In mostof the energy efficient techniques, different approaches for energy utilization by sensors are proposed to extend lifetime of WSNs. The proposed scheme is defend against cooperative Gray-Hole and Black-Hole attacks that lead to performance degradation in WSNs containing mobile sensors. In order to overcome this, energy efficient technique is presented in this paper to mitigate the impact of both attacks simultaneously, on improving cluster head selection mechanism. Proposed protocol implements a energy efficient technique, on detecting and preventing compromised node to be a part on network communication in WSNs. It also determineshonest nodes to become cluster head during packets transmission phase in WSNs. NS2 simulation result compare proposed protocol with LEACH proves that implemented scheme effectivelyminimize the chance of compromised node to become cluster head and significantly achieves better network performance related to packet delivery ratio(PDR), throughput ,end-to-end delay and energy utilization in WSNs.

## Keywords
Black-Hole Attack; Cluster Head Selection; Delay; Energy Efficiency; Gray-Hole Attack; LEACH; Network Lifetime; Packet Delivery Ratio; Throughput ;Wireless Sensor Networks.

## 1. INTRODUCTION
Wireless Sensor Network (WSN), is a distributed system consists of Base Stations (BS) and large number of mobile Sensor Nodes (SN) that integrate micro sensing, computing and wireless communication capabilities, which are capable of detecting various events related to its surrounding environment such as speed, temperature, pressure, difference in displacement, light, etc. [1] as shown in Fig. 1 .

These nodes operate in ad-hoc manner and have limited hardware and energy recourses due to its small size.The data sensed by the sensor node in the network gather data in form of electrical signals that are further converted to digital form and wirelessly transmitted to BS where the information can be accessed. As a new technology for information collecting and processing, there are wide range of applications of WSNs in military, health, commercial applications, and agriculture and so on. In WSN with single or even cooperative compromised nodes, energy consumption becomes a critical issue.

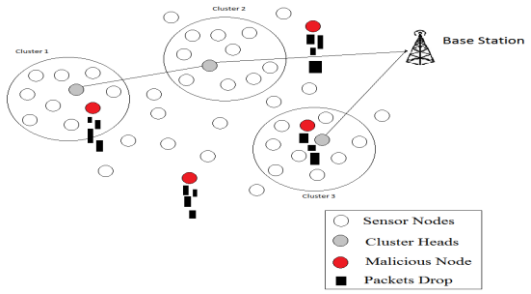


**Figure1. Wireless Sensor Networks Communication**

This paper proposes multi-hop inter-clustering protocol that selects most optimal Cluster Head (CH) with maximum residual energy at each round of CH selection mechanism along with preventing compromised node to become CH, which leads to better performance than LEACH. The rest of the paper is organized as follows. Section II provides an overview of the original LEACH protocol. Section III explains the security constraints in WSNs introducing Gray-Hole and Black-Hole attacks, whereas other previous enhancements of LEACH related to mentioned attacks along with their performances are discussed in section IV of related work. In section V implemented work on detecting attacks and its impact on WSNs is elaborated. The conclusion is presented in section VI.

## 2. LEACH PROTOCOL
LEACH (Low Energy Adaptive Clustering Hierarchy) is a common clustering algorithm that allows dynamic selection of cluster heads for distributing energy utilization among all of the sensor nodes in WSNs. LEACH is divided into number of rounds for selecting cluster heads. LEACH uses one hop inter-clustering to reach the faraway BS which misses the cooperation among cluster heads which is a major drawback of LEACH as more energy is consumed by the sensor nodes that are far away from the BS. Multi-hop inter-clustering algorithm leads to better performance in terms of energy conservation that leads to increase in lifetime of WSNs.

In WSNs number of nodes with small amount of energy, which does not enable them to reach the nearest intermediate node, dead spots occur. LEACH is not concerned with energy distribution in the wireless sensor networks for cluster head selection, number of dead spots would appear.

At the beginning of each round of CH selection normal node chooses a random number x between 0 to 1 and checks if it is less than a certain threshold value T (n)[20],then it is converted from normal node to CH node, where the threshold function is defined as follows:

$$T(n) = \begin{cases} \frac{P}{1-P*\left(r \bmod \left(\frac{1}{P}\right)\right)}, n \epsilon G \\ 0, \quad otherwise \end{cases} \quad (1)$$

where P is the desired percentage of CH which is a predefined value (e.g. P=0.01), r is the current round number, and G is the set of nodes in the last 1/p rounds, that has not been selected as CHs.

The main purpose to design and develop an energy efficient technique for WSNs is to improve the network lifetime and to increase the overall performance of network. In order to achieve this goal, there are number of energy efficient techniques available based on different parameters like, to improve CH selection approach, to reduce energy consumption of individual nodes, on improving inter cluster communication mechanism along with an optimal technique of cluster formation, residual energy based approach ,on calculating threshold value to select optimal set of CHs on considering various network topological parameters like average distance between sensor nodes and BS, area of the field and number of sensor nodes deployed over field.

LEACH is better than conventional routing protocols as the responsibility of CH is distributed around all the sensor nodes, and also data aggregation by CH from member nodes reduces energy dissipation of the network. But LEACH still ignores the residual energy at each node during the CH selection stage and also the impact of malicious attacks encounter in the WSNs. The energy dissipation models for the transmitter and the receiver along d distance are respectively given by:

$$E_{TX}(l.d) = \begin{cases} lE_{elec} + lE_{fs}d^2, \ if d \le d_0 \\ lE_{elec} + lE_{mp}d^4, \ if d > d_0 \end{cases} \quad (2)$$

$$E_{RX}(l) = lE_{elec} \quad (3)$$

where Eelec is the energy required to transmit or receive one bit and 1 is the length of the message. The cost of data aggregation is modeled by TDA, Efs is the free space model power loss, while Emp is the power loss of the multi path model. The used model depends on the acceptable bit-error rate chosen and the distance to the receiver. The threshold distance d0that determines which model to use is provided in [5] and is given by-

$$d_0 = \sqrt{\frac{E_{fs}}{E_{mp}}} \quad (4)$$

Several clustering algorithms proposed for energy efficient technique for WSNs consisting of fixed sensor nodes improve the CH selection approach to extend the lifetime of networks. In WSNs, there are some applications, where some sensor nodes may require moving and changing their location. In the traditional clustering algorithms for CH selection in WSNs is based on the decision taken from the residual energy and certain threshold value of the respective nodes. The threshold is set as –

$$T(n) = \begin{cases} \left(\left(\frac{P}{1-P*(r \bmod (\frac{1}{P}))}\right)\frac{E_{residual}}{E_{initial}}\right) * K_{optimal}, \\ 0, \quad otherwise \end{cases}$$

$$T(n) = \begin{cases} \left(\left(\frac{P}{1-P*(r \bmod (\frac{1}{P}))}\right)\frac{E_{residual}}{E_{initial}}\right) * K_{optimal}, \\ 0, \quad otherwise \end{cases}$$

(5)

Using this threshold, each node will be fairly selected as CH at some point within 1/P rounds of the CH selection mechanism.

Where Koptimal is the optimal number of CH during the state of cluster formation and is defined as follows:

$$K_{optimal} = \sqrt{\frac{N}{2\pi}} * \sqrt{\frac{E_{fs}}{E_{amp}}} * \sqrt{\frac{M}{d^2_{toBS}}} \quad (6)$$

Where, N is the number of nodes, M is the network area, and Efs and Amp are the amplification power losses and d is the distance between the selected CH and BS.

## 3. SECURITY CONSTRAINTS IN WSNS

WSNs encounters number of security threaten attacks .A Gray-Hole (Packet Drop) attack or Black-Hole (False Report) attack is a type of denial-of-service attackaccomplished by dropping packets. The attack can be accomplished either selectively by dropping packets for a particular specified networkdestination, a packet drops for every n packets or for every t seconds, or for randomly selected portion of packets, which is called Gray-Hole attack or in bulk, by dropping all packets.A malicious node may falsely route and drop all the packets on the way and thus consume much of energy available, unnecessarily, such attack is referred as Black-Hole attack.

### 3.1 Gray-HoleANDBlack-Hole Attacks in WSN

In WSNs, it is not viable to identify and protect each individual node from variety of attacks. To make entire network system unsecure, different types of security threats mostly during packet transmission phase are possible. Attacks on routing data can be done in two phases; in first phase, attack on routing protocol by jamming or flooding of information to a node. For example, Hello Flooding Attack, Acknowledgement Spoofing Attack etc. and second phase belongs to attack on delivery of packet transmission by creating a shortest, predefined path in order to divert traffic towards it. Black Hole attack is one of the examples that falsely advertise a shortest route to the destination and divert entire traffic to go through that compromisednode.

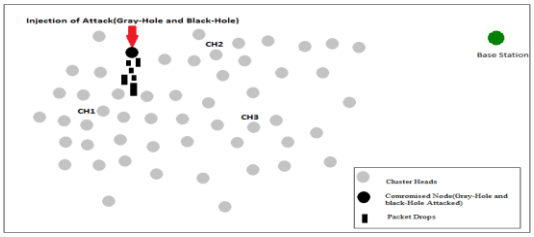

**Figure2. Design Overview of Attacks in WSNs**

Significant research effort has been spent on designing defense mechanisms for Gray-Hole and Black-Hole attack which are complex, energy inefficient and scarce to protect a network when multiple nodes act cooperatively to perform malicious activity and may have devastating impact on overall performance in the WSNs.

In this paper, an efficient and trust based secure routing protocol to detect and defensesingle and cooperative Gray-Hole and Black-Hole attack is presented. The approach is straightforward and trust based to determine trust level of nodes in order to prevent compromised nodes to become CH.

# 4. RELATED WORK

Sheela D. , Srividhya V.R. , Asma Begam, Anjali and Chidanand G. M in their work proposes a technology that uses mobile agent as security solution that will defense against Black-Hole attack for WSNs. The proposedscheme is build to overcome the impact of Black-Hole attack using multiple BS by using mobile agents. The author proposed a mobile agent which is aprogram segment which is self-controlling. They implement in their paper a simulation-basedmodel of their solution to recover from Black Hole attack in WSNs [2].

Ganesh R. Pathak,Suhas H. Patil,Jyoti S. Tryambake ,proposed a secure routing algorithm to mitigate the impact of Black-Hole attack in the overall performance of WSNs[1] They accomplish in their paper, a secure packet transmission. An efficient and trust based secure protocol is proposed to defend against single and cooperative Black Hole attack. They proposed a protocol estimate trust metric to determine honesty of nodes during secure route discovery phase during packet transmission.

Mahmoud M. Salim, Hussein A. Elsayed, Salwa H.El Ramly,proposed in their work,an improved CH selection approach based on selecting maximum residual energy node as CH in their next round of CH selection mechanism and significantly increases the lifetime of each sensor nodes and hence of whole network[7].Jaspreet Kaur, Vinod Kumarin their paper presents a secure routing protocol to minimize the impact of Gray-Hole attack in WSNs [3]. They proposed in their work, technique for local monitoring to defense against the Gray-Hole attack in WSNs.

Yiping Yang, Chuan Lai, Lin Wang, Lin Wang, presented in their work an Energy Efficient Clustering Algorithm (EECA) adapted two steps CH selection mechanism for WSNs, where in first step the node with the highest residual energy is selected as Anchor CH, and the Candidate CHs are determined according to their residual energy as well as the distance from the Anchor CH. In second, The Candidate CHs compete to be the CHs via a delayed broadcast mechanism. After finishing the Optimal CH selection mechanism, the Cluster formation begins. EECA [8] thus not only provides reasonable distribution of CHs with higher energy utilization but also efficiently balances the energy consumption levels of nodes and prolongs the network lifetime.

Van-Trinh HOANG, Nathalie JULIEN, Pascal BERRUET, in their work presents a novel CH selection approach to extend network lifetime and reliability in WSNs by taking obstacle aware criteria into consideration [7]. The approach allows selecting the most appropriate sensor nodes to become CH, reducing 93% the number of lost packets in WSNs, hence improve the network throughput about 53% which extends the network lifetime by 11%.Osama Moh'd Alia, Zyad Shaaban, Ahmad Basheer, Alaa Al-Ajouri, and Ahmed Alsswey, proposed an energy efficient dynamic clustering algorithm for WSNs [8] that automatically organizes the sensors into appropriate number of clusters in network to select best set of CHs.

Itika Gupta, A. K. Daniel, in their paper proposed an efficient clustering algorithm [9] with position based multi-hop clustering technique in which the CH closer to it forward packets to BS using round robin technique which makes network energy efficient to select the CH of minimum energy. The protocol improves the network performance with respect to delay and energy consumption.

Sushant Miglani, Rajoo Pandey, proposed in their paper a optimize technique of LEACH protocol to extend lifetime of WSNs [11].In the proposed scheme, the optimum number of CHs is determined first by proposed formula for optimum clustering probability.

# 5. IMPLEMENTED WORK

Wireless Sensor Networks is a large network of sensors which have the ability to communicate with each other. Since these sensor nodes are required to transmit the data from one sensor to other,routing and network management are donecooperatively by these nodes themselves. While transmitting sensed information, security is main concern in WSNs along with the energy efficiency approach.

In WSNs of information transmission, AODV is a source initiated Advance On-Demand Vector Routing Protocol. Each sensor node has a routing table that maintains the information of next hop node to route to the destination. When asource node wishes to route a packet to a sink node, it usesthe specified route if a fresh enough route to the sink nodes available in its routing table. If it is not, it will search route discovery phase by broadcasting the Route Request (RREQ) message to its intermediate neighbor nodes, which is further propagated until it reaches an neighboring node with a fresh enough route to the sink node specified in the RREQ, or to the sink node itself.

## 5.1 Gray-Hole Attack Detection Model

In Gray- Hole attack, malicious nodes try to stop the packets in the network by refusing to forward or drop the packets passing through them for considerable periods.Each intermediate node within the range of CHon receiving the RREQ makes an entry in itsrouting table for the node that forwarded the RREQ message,and the source node. The sink node or the next hop node with a fresh enough route to the sink node, uni-caststhe Route Response (RREP) message to the neighboring node from the node where it received the RREQ message. The nodewill update anentry for the neighboring node from which it received the RREP packets, and then forward the same in reverse route. On receiving theRREP, the source node will updates its routing table with an entry forthe sink node, and the node from which it received packets for RREP. The source node starts routing the data-packets to the sink node through the neighboring node that firstresponded with an RREP packets.A Gray-Hole attack is different than that of the Black-Hole attack, in that during the packet transmission phase, it drops the packets for some specified interval of time.

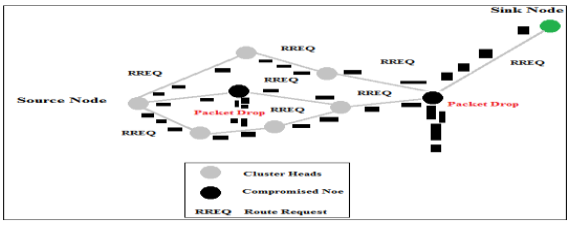


**Figure3. Gray-Hole attack detection model**

## 5.2 Black-Hole Attack Detection Model

In Black-Hole attack, it exploits a trustworthiness of a network by promising routing of data packets to the sink node,reporting falsely that it has a shortest path but in reality it drops all packets and consequently threatens reliability.

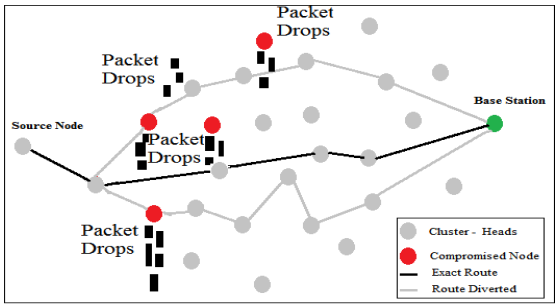


**Figure 4. Black-Hole attack detection model**

A Black-Hole is a malicious node that falsely replies for any RouteRequests (RREQ) without having active route to specified sink and drops all the receiving packets. If suchcompromised node work together as a group then the damage caused willincrease significantly. Such attack is sometime referred as cooperative Black-Hole attack.

The primary goal of the proposed energy efficient technique is to detect the compromised node and prevent it to become a part of network communications.In both of the discussed attacks, if compromised node is selected as an CH that aggregates the data from member nodes of cluster, it may definitely reduce the energy of that node unnecessarily that will seriously affect the lifetime on sensors in each round of CH selection mechanism and hence of the whole WSNs. Also such selection of CH in WSNs significantly affects network throughput, end-to-end delay and packet-drop ratio. It significantly detects the injection of both discussed attacks and also reduces the impact of those attacks in WSNs with respect to the above discussed performance parameters.

In the implemented work presented here, detection and prevention of the above two types of attacks is being carried out on following discussed algorithm. The techniqueworks on a backbone network of trusted nodes and is established over the WSNs network. The source node periodicallyrequests one of the backbone nodes for restrictedIPaddress.

## 5.3 Notations used for Implemented Algorithm

1. $SN_{CH}$ : Source Node CH.
2. SeqNo. : Sequence Number of CH.
3. NHN: Next Hop Node.
4. $IN_{CH}$: Intermediate Node CH.
5. TF_GH/TF_BH: Trust Factor for Gray-Hole/Black-Hole.
6. $DN_{CH}$: Destination Node CH
7. FRq_CH: Further Request for CH
8. FRp_CH: Further Reply by CH
9. RIE: Routing Information Entry

## 5.4 Algorithm for Detection and Prevention of Black-Hole and Gray-Hole Attack

1. Select Maximum Energy Node as CH in first Round of CH selection using equations in 5, 6.
2. $SN_{CH}$ broadcast RREQ packet.
3. $IN_{CH}$ receives RREP packet, RIE of $IN_{CH}$.
4. IF

   Received timestamp of RREP by $IN_{CH}$ < TF_GH

   Make current $IN_{CH}$ as Gray-Hole attacked node.

   OR

   SeqNo. Of $IN_{CH}$> TF_BH, make current $IN_{CH}$ as

   Black-Hole attacked node.

   ELSE

   Route Data Packets to $IN_{CH.}$

   Current_IN = NHN_CH.
5. IF $IN_{CH}$ is found Compromised Node,

   Broadcast FRqst_CH to NHN_CH.
6. Receive FRp_CH and RIE of requested NHN_CH.
7. IF NHN_CH is not malicious,

   Route data packets to selected NHN_CH.
8. NHN_CH = $SN_{CH}$.
9. Repeat from step 1 while NHN_CH is not $DN_{CH.}$

Whenever the node wants to make a transmission, it notonly sends a RREQ in search of sink node but also insearch of the restricted IP simultaneously. As the Black-Hole or Gray-Hole nodes send RREP for any RREQ, it replies with RREP for the restricted IP(RIP)also. If any of the routes responds positivelywith a RREP to any of the RIP then the source node start initiating with the detection procedure for these malicious nodes

In the paper presented here, LEACH an energy efficient multi-hop, inter-clustering routing protocol is being implemented to achieve significant increase in the lifetime of network. In this protocol, an inter-clustering communication among CHs is carried out based on the selection of most optimal CH with maximum energy in the clusters along with preventing attacked node from becoming CH.

Algorithm for selection of CH at each round of CH selection is based on detecting compromised node first and preventing such node to become CH in the next round of CH selection mechanism. Such compromised node which may not effectively participate in the WSNs is being prevented from being CH to extend the lifetime of network and always achieve optimal selection of CHs and increases the performance of network related to packet drop ratio, throughput and end-to-end delay in WSNs.

## 6. SIMULATION RESULTS AND ANALYSIS

The implemented work for the proposed protocol has been categorized in three phases; in first phase the performance of WSNs with injection of two types of attacks on some nodes with respect to energy utilization is considered. In second phase, further work is implemented in which, the compromised

node has been detected and prevented to become CH and in third phase, the performance in these two phases has been compared with the presence of Black Holes, performance is measured in terms of Packet Delivery Ratio (PDR), throughput, end-to-end delay at several intervals for existing system.

In this paper NS2 simulator has been used to evaluate the performance of WSNs before preventing the compromised node to become CH and after detecting and preventing of that identified malicious node from being CH. After recognizing the malicious node, the energy efficient algorithm presented here effectively prevents that particular node from being the part of network communication in the WSNs. Hence the network performance is analyzed with different network parameter.

**Table 1. Simulation Parameters**

| | |
|---|---|
| No. of Nodes | 10,50 |
| Simulation Area | 1500*1500 m |
| Initial Energy of Sensor Nodes | 1 J |
| Simulation Time | varies 20s-1000s |
| Transmission Range : | 250m |
| Packet Size | 4000 bits |
| Pause Time | 10 s |
| Maximum Speed | 10,20,40 60 ,100(s) |
| Traffic Source | CBR |
| Channel Type | Wireless |
| Simulation Time | Up to 200s |
| Packet Count | 10000 |
| Routing Protocol | AODV |
| Data Rate | 5Kb/s |
| Channel Range | 11Mbps |

The performance of the proposed protocol is analyzed against Gray-Hole and Black-Hole attack for two cases, first with injecting both attacks randomly and second, on preventing impact of both attacks in WSNs. The performance in both cases is measured in terms of data packets delivered to the sink node and delay caused during this transmissionand also measuring the energy consumption at each node as the simulation time t progress during the communication phase in the WSNs.

For this purpose, these two attacks are assumed randomly deployed in a network and act individually as well as cooperatively. With the presence of both attacks, the performance is analyzedwith respect topacket delivery ratio (PDR), throughput, and end-to-end delay at several intervals for existing system. In the proposed work, the compromised node is effectively prevented from being a part of network communication at each round of CH election mechanism in WSNs.

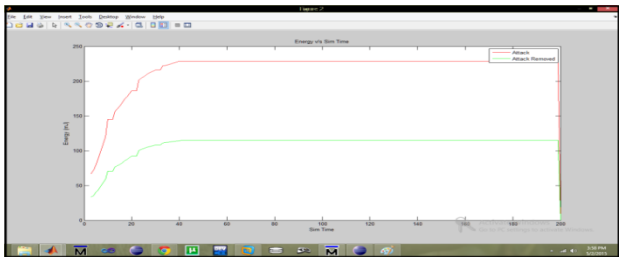

**Figure5. Graph for Average Energy Consumption**

In Fig.5, the average energy at each node is plotted against the simulation time t. Here the comparison is performed about 20 micro seconds of simulation time. Since the possibilities of malicious node to be a CH is prevented in the implemented work that may consume much energy in holding and diverting the packets rather than forwarding to the intermediate or sink node, the energy of each sensor is efficiently save to extend the lifetime of whole network.

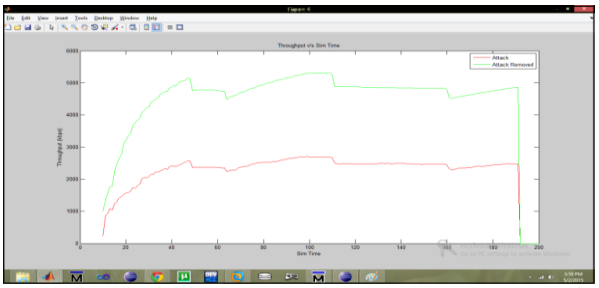

**Figure 6.Graph for Throughput vs. time*t***

In Fig.6, the graph for throughput in the network, where the number of packets on y-axis, per unit time of considered simulation time on x-axis has been plotted. The red lines indicate the performance of network before attack removal, while green line shows throughput in the network after removal of both attacks.

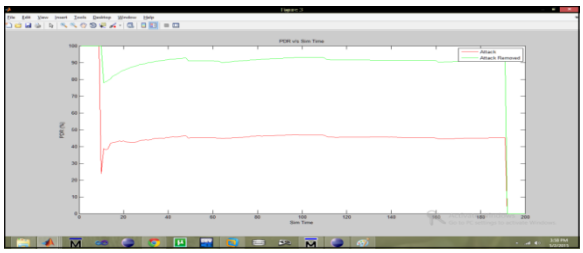

**Figure 7. Graph for packet delivery ratio (PDR) Vs. Time *t***

In Fig. 7, the packet delivery ratio (PDR) before and after attack removal is shown. On y-axis is plotted against simulation time t, along x-axis. The blue vertical lines shows the PDR before the attack removal while green lines shows the PDR plotted after removal of both attacks in WSNs.

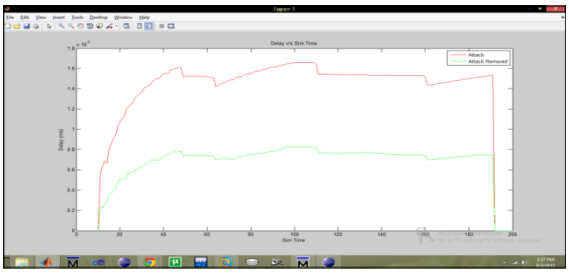

**Figure 8. Graph for end-to-end delay**

Fig. 8, shows the performance of packet transmission among CHs during communication phases in WSNs in terms of end-to-end delay is plotted, where x-axis represents no. of nodes and y-axis considered simulation time t. The blue line shows the result before attack removal and green lines shows after removing both attacks. The graph itself prove that, the energy efficient CH selection algorithm implemented for defense against Gray-Hole and Black-Hole, greatly reduces end-to-end delay as compared to the existing .

**Figure 9. Graph for Good-put in the Network**

The good-put of network is calculated with only real packet transmission that considers only those packets information which actually has been taken part in real data transmission. It does not calculated on retransmitted packets or even packets on considering only either sent or received information is available and not both. In Fig.9, the graph has been plotted for good-put achieved in the network. The red line graph represents the good-put calculated before attack removal, while green line graph shows the same after both attack removal.The output graphs are near about same as like of throughputs graphs.

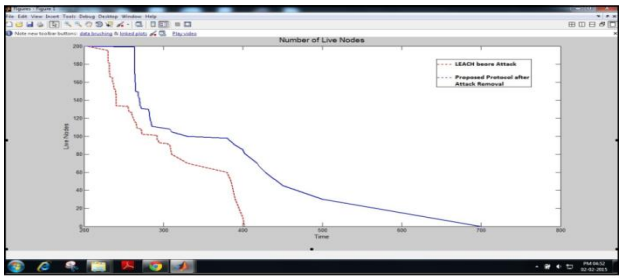


**Figure 10. Graph for number of live nodes**

In the proposed work, the probability of malicious node to become CH is effectively reduced which comparatively increases the lifetime of sensors as the simulation time passes. Fig.10 shows the number of live nodes plotted against the simulation time twith red line indicate the status before removal of attack while blue line shows the status after removal of attack.

## 7. CONCLUSION

Proposed energy efficient technique presented here, provided an effective solution based on some predefined trust values, to detect Gray-Hole and Black-Hole attacks in WSNs and generate a secure routing path from source to the sink node on avoiding detected malicious node during data transmission phase. The implemented scheme prevents the compromised node to become CH during the CH selection mechanism that significantly improves the network performance parameters such as packet delivery ratio (PDR), end-to-end delay. Simulation results in NS2 shows the comparative analysis of energy consumption by the existing LEACH protocol along with injecting malicious nodes in WSNs and the proposed protocol after detecting and preventing compromised node to become CH.

From the research work presented in this paper, it has been concluded thatthe technique proposed here significantly improves the selection of CHs along with Gray-Hole and Black-Hole attack detection, and preventing compromised node to be a part of network communication in WSNs. Hence, it is proved that technique presented here is more energy efficient than the existing techniques. The NS2 simulation results signifies that the performance implementation of proposed technique satisfactorily preventing compromised node to become CH and is robust against both single and cooperative Gray-Hole and Black Hole attacks in WSNs

## 8. FUTURE SCOPE

The research work implemented in this paper can be extended further tomodify the proposed algorithm to increase the communication among sensors on reducing communication overhead and hence to reduce network bandwidth consumption in the whole WSNs and also for to provide security over packet transmission phase along with reducing energy consumption in WSNs.

## 9. REFERENCES

[1] Ganesh R. Pathak,Suhas H. Patil,Jyoti S. Tryambake"Efficient and Trust Based Black HoleAttack Detection andPrevention In Wireless Sensor Networks", International Conference on Computer Science and Business Informatics, ISSN: 1694-2108, Vol.14 No.2. 2014.

[2] Sheela. D, Srividhya.V. R., Asma Begam, Anjali and Chidanand G. M."Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent",International Conference on Artificial Intelligence and Embedded Systems (ICAIES)July 15-16, Singapore,2012.

[3] Jaspreet Kaur,Vinod Kumar" An Effectual Defense Method Against Gray-Hole Attack in Wireless Sensor Networks", International Journal of Computer Science and Information Technologies(IJCSIT),Vol. 3,2012,4523-4528.

[4] Wazir Zada Khan,Yang Xiang,Mohammed Y. Aalsalem,Quratulain Arshad"The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures", I. J. Wireless and Microwave Technologies,2,33-44.Published Online April 2014.

[5] Nidhi Chhajed, Mayank Sharma, "Detection and Prevention Techniques for Black hole Attack in Wireless Sensor Networks: A Review", International Journal of Advanced Research in Computer Science and Software Engineering,Volume-4,Issue-11,November 2014.

[6] Osama Moh'd Alia,Zyad Shaaban,Ahmad Basheer,Alaa Al-Ajouri,Ahmed Alsswey,"Musician Inspired Clustering Protocol for Efficient Energy in Wireless Sensor Networks", Sensor Networks and Cellular Systems (SNCS) Research center, Saudi Arabia,IEEE 2014.

[7] Mahmoud M. Salim, Hussein A. Elsayed, Salwa H.El Ramly," PR – LEACH: Approach for Balancing Energy Dissipation of LEACH Protocol for Wireless Sensor Networks",31st National Radio Science Conference (NRSC), April 28-30, 2014 Ain Shams University, Egypt.

[8] Itika Gupta,A. K. Daniel,"An Energy Efficient Position Based ClusteringProtocol for Wireless Sensor Networks using Round Robin Scheduling Technique",3rdInternational Conference on Advanced Computing and Communication Technologies, 10.1109 ACCT. 2013.59.

[9] Haider N. Javaid,N. Amjad,A. A. Awan,A. Khan,N. Khan," REECH-ME: Regional Energy Efficient Cluster Heads Based on Maximum Energy Routing Protocol for Wireless Sensor Networks " 8thInternational Conference on Broadband, Wireless

Computing,Communication and Applications, IEEE 2013.

[10] Sushant Miglani,Rajoo Pandey,"Optimization of Clustering Probability of LEACHProtocol for Lifetime Maximization of Wireless Sensor Networks "2nd International Conference On Parallel, Distributed and Grid Computing,IEEE 2012 .

[11] Yiping Yang,Chuan Lai,Lin Wang, "Energy Efficient Clustering Algorithm for Wireless Sensor Network",10thIEEE International Conference on Control and Automation (ICCA)Hangzhou,China,June12-14, 2013.

[12] Qingwei Liu,Jin Li, Mandan Liu,"A Clustering Algorithm Based on Local Competition and Double Weigh Communication Energy-Consumption for Wireless Sensor Networks",10th IEEE International Conference on Control and Automation (ICCA) Hangzhou, China, June 12-14, 2013.

[13] Lu Gao,Zhongmin Li,"Energy Consumption Balanced Cluster Head Selection Algorithm for Wireless Sensor Networks"International Conference on Computer Science and Applications,IEEE-2013

[14] Ashfaq Ahmad,Nadeem Javaid,Zahoor Ali Khan,Umar Qasim,Turki Ali Alghamdi"(ACH)2: Routing Scheme to Maximize Lifetime and Throughput of Wireless Sensor Networks"IEEE Sensor Journal.VOL.14 No.10 October,2014.

[15] Jin Wang, Zhongqi Zhang, Jian Shen,"An Improved Stable Election Based" Protocol with Mobile Sink for Wireless Sensor Networks " International Conference on Green Computing and Communications and IEEE Internet ofThings An IEEE Cyber,Physical and Social Computing,CPSCom.2013.163.

[16] F. Saleem, Y. Moeen, M. Behzad, M. A.Hasnat,Z. A. Khan, U. Qasim,N.Javaid,"IDDR Improved Density Controlled Divide and Rule Scheme for Energy Efficient Routing in WSNs", 9thInternational Conference on Future Networks and Communications(FNC) 2014.

[17] M. S. Fareed, N. Javaid,M.Akbar,S. Rehman,U. Qasim,Z. A. Khan," Optimal NumberOf Cluster Head Selection for Efficient Distribution of Sources in Wireless Sensor Networks",7th International Conference on Broadband, Wireless Computing, Communication and Application, 2012.

[18] Shalli Rani,Jyotish Malhotra,Rajneesh Talwar,"Energy Efficient Protocol for Densely Deployed Homogeneous Network ", in International Conference on Issuesand Challenges in Intelligent Computing Techniques (ICICT)-2014.

[19] Noor Zaman, Tung Jang Low, Turki Aghamdi, "Energy Efficient Routing Protocol for Wireless Sensor Networks", 3rd International Conference on Advances in Computing Technologies" ,ISBN 978 – 289968650-3-2, February16-19, ICACT, 2014.

[20] Vishnu K. , Amos J. Paul,"Detection and Removal of Cooperative Black/Gray hole attack inMobileADHOC Networks", InternationalJournal of ComputerApplications(0975 - 8887), Volume 1 – No. 22, 2010.

[21] M. Natranjan, R. Arthi, K. Murugan,"Energy Aware Optimal CH Selectionin WSNs", in IEEE 4th ICCCNT, Tiruchengode, India, July 4-6, ICCCNT 2013.

[22] Van-Trinh HOANG,Nathalie JULIEN,Pascal BERRUET,"Cluster Head Selection Algorithm to Enhance-Efficiency and Reliability of Wireless Sensor Networks",International Conference on European Wireless Sensor Networks,ISBN 978-3-8007-3621-8,VDE VERLANG,Berlin,Offenbach,Germany.

[23] Anjali Thampi K.G, L.M. Nithya, "An Efficient ID-Based Scheme For Filtering GangInjected False Data In Wireless Sensor Networks",International Journal of Advanced Research in Computer and Communication Engineering,Vol. 2, Issue 4, April 2013.

[24] S. Sajithbanu, M. Durairaj, "Detecting False Data in Wireless Sensor Networks using Effective Becan Scheme", International Journal of Computer Applications(0975-8887),Volume 43,N0.18,April 2012.

[25] Hyeon Myeong Choi, Su Man Nam, Tae Ho Cho, "A Secure Routing Method for Detecting False Reports and Wormhole Attacks in Wireless Sensor Networks", Scientific Research on Wireless Sensor Networks,2013,5,33-40,PublishedOnline, http://www.scirp.org/journal/wsn, March 2013.

[26] Ebin Deni Raj "An Efficient Cluster Head Selection Algorithm for Wireless Sensor Networks - EDRLEACH ", IOSRJournalof Computer Engineering (IOSRJCE),ISSN: 2278-0661 Volume- 2, Issue-2, and July- Aug. 2012, PP 39-44