International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 3, Issue 6, June 2016)

Detection of Malicious Nodes in WSN Using Improved LEACH Protocol

Santosh Maynal
P G Scholar
Computer Networking and Engineering
Poojya Doddappa Appa
College of Engineering
Kalaburagi, Karnataka, India
Sam.patil2088@gmail.com

Jyothi Patil
Associate Professor
Computer Science and Engineering
Poojya Doddappa Appa
College of Engineering
Kalaburagi, Karnataka, India
Jyothip_2003@yahoo.com

***Abstract*— Wireless Sensor Network (WSN) is built by sensor nodes and forms a network by connecting one node to other node (several nodes) it has limited resources like battery power, communication range and processing capability. WSN is vulnerable to many network attacks. Sensor network uses Low Energy Adaptive Clustering Hierarchy (LEACH), It is TDMA based MAC protocol that balances the clustering energy, so the network lifetime will be extended. LEACH protocol such as if once the cluster-head(CH) dies the whole network fails. Hence propose a new approach in selection of cluster head. A modified cluster head selection algorithm has been proposed depending on remaining battery life and geographical distance of basestation, and detection of malicious nodes in an effective way so no attack can ruin the normal network operation.**

***Index Terms*— Wireless Sensor Network, LEACH, Cluster-head, Malicious Nodes, Base Station etc.**

I. INTRODUCTION

Wireless sensor networks are group of sensor nodes. A sensor nodes are densely deployed to sense and collects data from its designated source, processes that data and sends it back to the defined base station[1] BS or sink. The base station may be stationary and distant from the sensor node. The sensor nodes have limitations like battery power, processing capacity, coverage area etc. Self-organizing and Self-configuring are the special features of this network. This increases the wide range of applications especially in various military and civil applications like weather monitoring, intrusion detection, security, detecting environmental conditions i.e., particle movement, temperature, sound, object detection, disaster sensing and prediction and so on. In WSN battery power of the nodes are very limited, replacing the batteries is not an option. Hence proper and efficient utilization of the energy of the sensor nodes is very much required to enhance the lifespan of the whole network. In cluster-based networks, nodes are arranged in the form of clusters, with cluster-heads [2] CHs that they responsible for conveying any information gathered by the nodes in its cluster and may aggregate and compress the data before transmitting it to the BSs. As the approach is based on LEACH [3, 4, 5, 6, 7, 8] protocol, It is a clustering-based protocol that balances energy consumption in sensor networks. In the working principle of LEACH, addresses this by probabilistically rotating the role of cluster-head among all nodes depending on the residual energy of each node. When new nodes enters in the network so it can ruin the normal network operation by any kind of attack. It can be prevented by detection of malicious nodes by using an algorithm

II. PROBLEM STATEMENT

These sensor networks have limitations of system resources like battery power, communication range and processing capability. Low processing power and wireless connectivity make such networks vulnerable to various types of network attacks.

III. PROPOSED SYSTEM

Modified Cluster-head [9] CH selection is done on the basis of residual battery life of candidate nodes and the geographical distance from the candidate node to the base station [10].

In existing system malicious nodes were not detected, but the proposed solution will detect the malicious node [11].

Existing system disadvantages:

1) It doesn't shows that cluster head formation clearly
2) Based on battery life cluster head selection depended but not working in that

Malicious node performance increments

Proposed system advantages:

1) In this shows the cluster head selection newly
2) Energy levels measured for individual nodes
3) Decrease the energy consumption

Finds out malicious nodes and decrease the performance level.

International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 3, Issue 6, June 2016)

CH Selection

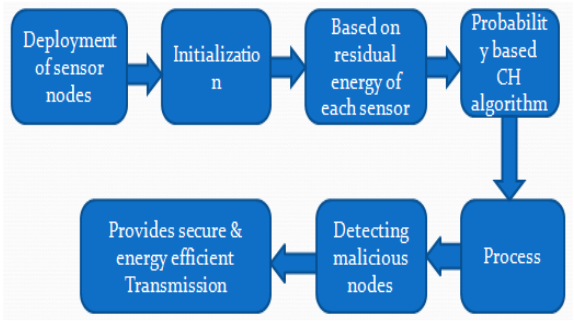


Figure 1: Block diagram of proposed system

In the above diagram shows the deployment block where nodes are arranged in the form of network. In initialization where all the nodes are exchanges there routing information and some related information for communication purpose.CH [12] Selection is based on the remaining energy of the candidate node which are participated in cluster-head selection. Algorithm in which if the probability of the candidate node value should be less than threshold value otherwise it will be treated as normal node. In process phase cluster load will distributes among all the cluster members to perform the task. Node detector phase detecting of malicious nodes[1] by using algorithm. Finally it provides a secure and energy efficient transmission.

IV. SYSTEM ARCHITECHTURE

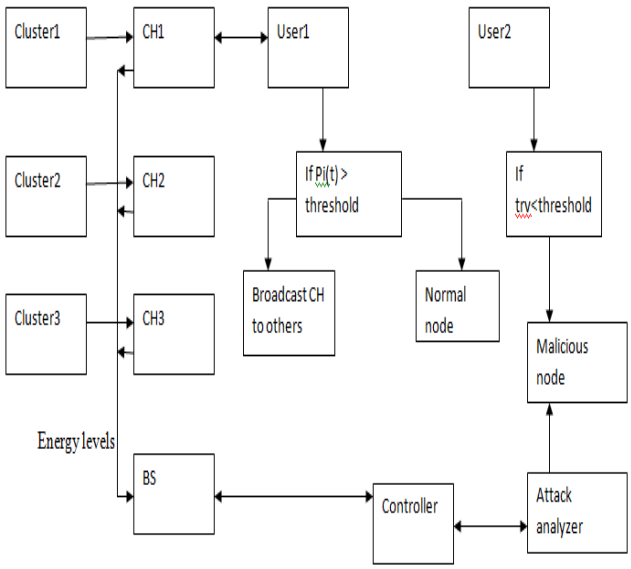
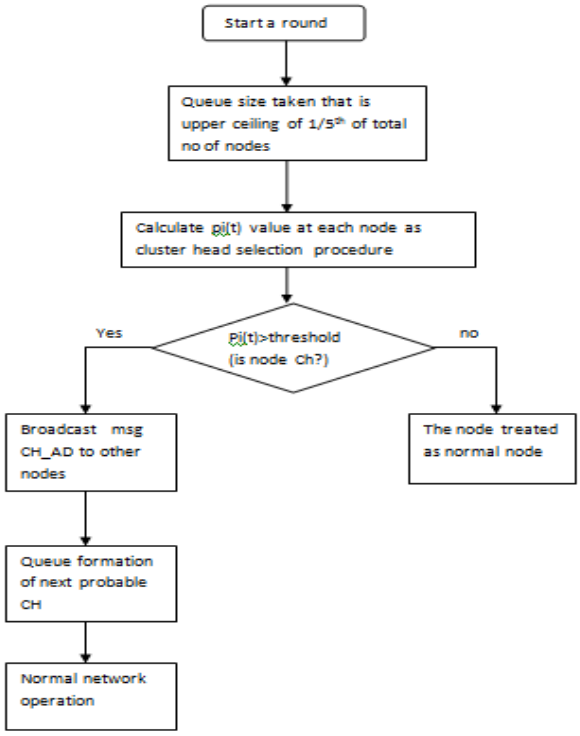


Figure 2: Detection of Malicious Node and CH

The architecture of proposed system shows that clusters are connected to cluster-heads(1,2,3),cluster-heads are connected to base station so they can communicate directly to base station. but clusters have to communicate with BS through the clusters. Any user can became a cluster-head if the node has more energy than other node otherwise it will be treated as normal node. If the user2 is new to the network then checking of that node is done by some algorithm if it fails then it will marked as malicious node and black listed by an attack analyzer and the controller will eliminates the malicious nodes from the network.



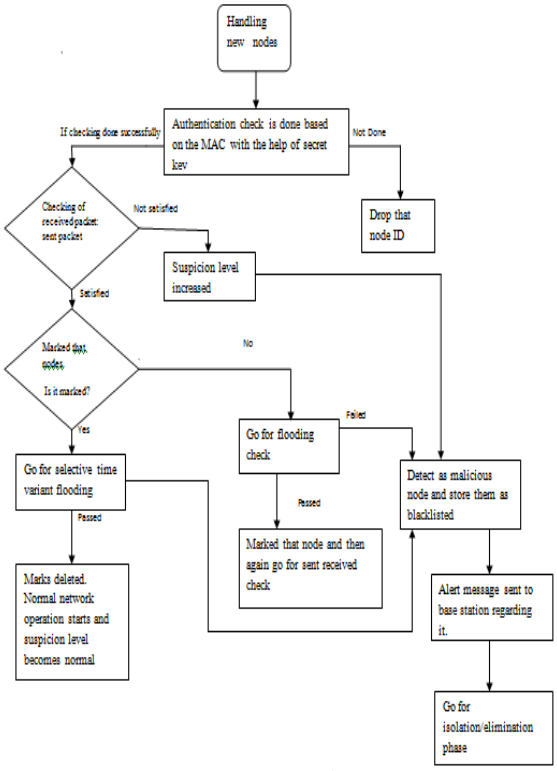
Flow chart1: Cluster Head Selection.

V. ALGORITHM FOR DETECTION OF MALICIOUS NODES

Authentication check:

1) A sensor node has message M and a pre shared K secret key with base station.
2) A MAC provides message integrity and message authentication using a combination of a hash function and a secret key
3) Sensor node computes MAC with the help of secret key over message M and destination address and then sends it to the Cluster-head.
4) Cluster-head has its own database of keys which are pre shared between its cluster nodes and base station. Cluster-head computes MAC of received message using the common key k with sensor node.
5) Then comparison of two MAC values is needed. If that is same then it can be forwarded otherwise it is not authenticated and sends back again to sensor node.

International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 3, Issue 6, June 2016)



Flow Chart 2: Detection of malicious nodes

Detection phase:

1) Phase 1:

Sender-Receiver Counter: A counter is placed in the base station to check the packets that are sent from the neighboring nodes to the cluster head are received them properly or not and is it further sends them to the base station. If the ratio is proper then we can say that adversary nodes are not there but we marked the nodes for further checking. If it is failed suspicion level is increased on them.

2) Phase 2

Selective Time Variant Flooding: For the marked nodes that go beyond a certain threshold level, then go for a selective time variant flooding. The trusted neighbor nodes are instructed to split their total number of messages into several parts and send them in variant time. If the suspicious node passes this test then its mark will be deleted and it is allowed to participate in normal network operations. If it fails then the node is considered as malicious and stored as blacklisted.

3) Flooding:

The trusted neighbor nodes are instructed to flood a fixed number of messages into in the same time. If the suspicious node pass this test then it is directed to send-received check. If it fails then the node is considered as malicious and stored as blacklisted.

4) Suspicion Level:

To monitor the behavior of nodes introducing a concept of suspicion level of a sensor node to represents its reliability. For a sensor network with n sensor nodes the cluster-head maintains suspicion level respectively and updates them each time a decision on the correctness of their reports is made. If the weight reaches a predefined upper bound the corresponding node is identified as malicious.

Blacklist Storage: If the node is detected as malicious then it should be stored as blacklisted and an alert message sent to the base station informing that the node is blocked and no data can be passed through that.

Isolation phase: In this phase the cluster-head node broadcasts one encrypted message to all the nodes in the network except the blocked node. The message will contain information to delete the blocked node from their neighborhood list and hence the blocked node id isolated and eliminated from the network.

VI. SIMULATION DESIGN

First step is simulating a network to design the simulation. In that users should determine the simulation purposes, network configuration and assumptions, the performance measures and type of expected results. The network performance is depend upon the simulation parameters and logical values.

Simulation setup into the two phases:

1) Network configuration phase
2) Simulation phase

In network configuration phase, network components are created and configured according to the design. Some events are set and data transfer to the setup of simulation and scheduled to start the time.

In simulation phase, starts the simulation which was configured in network phase. It maintains the simulation clock and executes events are continuously and set the parameters. This phase usually runs until the simulation clock reached and threshold value specified in network phase.

1) Post simulation process:

The main task in that process, verifying the integrity of a program and evaluating the performance of the simulated network. The first task is referred to as debugging and second one is properly collecting the simulation results.

VII. RESULTS

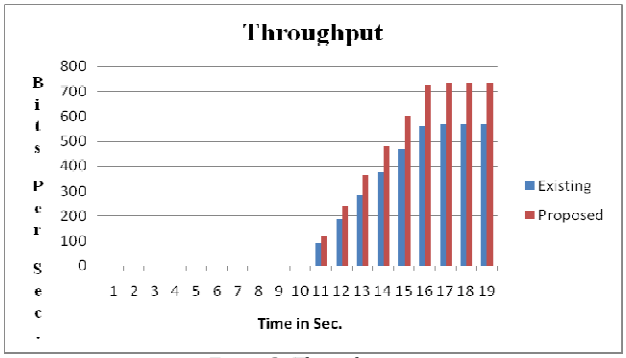


Figure 3: Throughput

International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 3, Issue 6, June 2016)

It is defined as the total number of packets delivered over the total simulation time. The fig.3 shows the throughput, the X-axis represent BPS (Bits Per Second) with respect to time (Y-axis), proposed system achieved transferring more number of packets in a time.

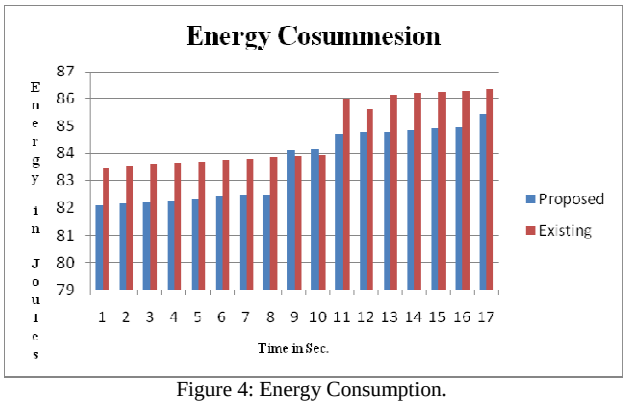


Figure 4: Energy Consumption.

The energy consumption is the sum of used energy of all the nodes in the network, where the used energy of a node is the sum of the energy used for communication. The fig.4 shows comparison between the current and proposed in which the proposed scheme has less energy consumed when compared with the existing scheme.

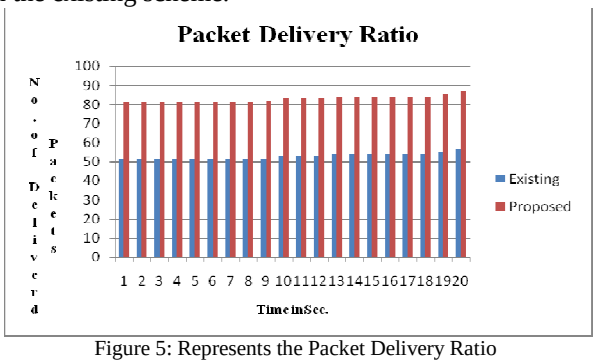


Figure 5: Represents the Packet Delivery Ratio

Packet delivery ratio (PDR) is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as:

$$PDR = S1 \div S2 \quad (1)$$

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source.

The fig.5 shows the PDR Y-axis represent the number of delivered packet and X-axis shows time in sec, the red color line shows proposed work that indicates more packets delivered successfully to the destination. PDR has achieved high compared to the existing system.

VIII. CONCLUSION

Presented as a new mechanism for cluster head selection and set as some rules for the cluster formation and communication between cluster head to base station individually. Enhanced (Improved) LEACH which is balanced energy consumption protocol for wireless sensor network. Through distributing the cluster load overhead over the cluster members, the life time of the entire network extended compared with LEACH protocol. Minimizing energy dissipation and maximizing network lifetime, and detection of malicious nodes by attack analyzer through the communication with controller. The trust value is less than the threshold value then it indicates as malicious node.

REFERENCES

[1] Semanti Das, Abhijit Das, 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) IMS Engineering College, Ghaziabad, India "An Algorithm to Detect Malicious Nodes in Wireless Sensor Network using Enhanced LEACH protocol".

[2] Nirnay and S K ghosh. An approach for Security Assessment of Network Conjurations Using Attack Graph. IEEE Conference on network and communication, pages 283{288, December 2009.

[3] W. Bo, H. Han-yang, F. Wen, "An improved LEACH protocol for data gathering and aggregation in wireless sensor networks," in Proc. Of International Conference on Computer and Electrical Engineering, pp. 398-401, 2008.

[4] W. B. Heinzelman, A. P. Chandrakasan, H. Balakrishnan, "An application-specific protocol architecture for wireless micro-sensor networks," IEEE Transactions on wireless communication, vol. 1, no. 4, pp. 660-670, 2002.

[5] L. Jun, H. Qi, L. Yan, "A Modified LEACH algorithm in wireless sensor network based on ns2," in Proc. Of International Conference on Computer Science and Information Processing, pp. 604-606, 2012.

[6] J. F. Yan, Y. L. Liu, "Improved LEACH routing protocol for large scale wireless sensor networks routing," in Proc of International Conference on Electronics, Communications and Control, pp. 3754-3757, 2011.

[7] S. D. Muruganthan, D. C. F. Ma, B. Rollyi, A. Fapojuwo, "A centralized energy-efficient routing protocol for wireless sensor networks," IEEE Radio Communications, vol. 43, no. 3, pp. 8-13, 2005.

ABOUT AUTHORS

Santosh Maynal, post graduate from Poojya Doddappa Appa College of Engineering Kalaburagi, Karnataka, India. Completed his graduation in electronics & Communication from KCT college of Engineering. His area of interest is in computer networks.

Jyothi Patil, Professor at Poojya Doddappa Appa College of Engineering Kalaburagi, Karnataka, India. Her area of interest is in Computer Science and Engineering.