International Journal of Advanced Research Foundation
Website: www.ijarf.com (ISSN: 2394-3394, Volume 3, Issue 9, September 2016)

Detection and Prevention of Malicious Nodes in WSN using DAP Algorithm

Anil Kumar Patil
Dept. of Applied Electronics
Gulbarga University, Kalaburagi, Karnataka, India
anilpatilkbn@gmail.com

Dr. P M Hadalgi
Dept. of Applied Electronics
Gulbarga University, Kalaburagi, Karnataka, India
pmhadalgi@gmail.com

***Abstract*— It is for the most part utilized for correspondence as a part of crisis circumstances. It is worked by sensor hubs and structures a system by interfacing one hub to other hub (a few hubs) it has restricted assets like battery force, correspondence range and handling capacity. WSN is helpless against numerous system assaults. like malevolent hubs in WSN will corrupt the execution by expanding vitality utilization, so Sensor system utilizes Low Energy Adaptive Clustering Hierarchy (LEACH), It is TDMA based MAC convention that adjusts the grouping vitality, so the system lifetime will be amplified. Drain convention, for example, if once the cluster head(CH) passes overall system falls flat. Thus propose another methodology in choice of group head. An adjusted group head choice calculation has been proposed relying upon residual battery life and geological separation of base station, furthermore identification and counteractive action of vindictive hubs by utilizing DAP calculation as a part of a successful way so no assault can destroy the typical system operation.**

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

I. Introduction

Wireless sensor networks are group of sensor nodes. A sensor Remote sensor systems are gathering of sensor hubs. A sensor hubs are thickly conveyed to sense and gathers information from its assigned source, forms that information and sends it back to the characterized base station BS or sink. The base station might be stationary and removed from the sensor hub. The sensor hubs have constraints like battery force, handling limit, scope range and so on. Self-sorting out and Self-designing are the unique elements of this system. This expands the extensive variety of uses particularly in different military and common applications like climate observing, interruption location, security, identifying natural conditions i.e., molecule development, temperature, sound, object recognition, debacle detecting and forecast et cetera. In WSN battery force of the hubs are extremely constrained, supplanting the batteries is impossible. Subsequently legitimate and proficient use of the vitality of the sensor hubs is particularly required to upgrade the lifespan of the entire system. In group based systems, hubs are orchestrated as bunches, with group heads CHs that they in charge of passing on any data assembled by the hubs in its bunch and may total and pack the information before transmitting it to the BSs. As the methodology depends on LEACH convention, It is a bunching based convention that parities vitality utilization in sensor systems. In the working standard of LEACH, addresses this by probabilistically turning the part of group head among all hubs relying upon the leftover vitality of every hub. At the point when new hubs enters in the system so it can demolish the typical system operation by any sort of assault. Various malevolent exercises are caught in WSN, for example, wormhole and DOS and so forth proposed DAP calculation to identify and counteract of pernicious hubs in WSN.

II. Problem Statement

These sensor systems have impediments of framework assets like battery force, correspondence range and preparing capacity. Low preparing force and remote availability make such systems helpless against different sorts of system assaults.

III. Proposed System

Altered Cluster-head CH choice is done on the premise of remaining battery life of applicant hubs and the geological separation from the hopeful hub to the base station.

In existing framework malevolent hubs were not recognized, but rather the proposed arrangement will identify and keeps the pernicious hub.

Existing framework detriments:

1) It doesn't demonstrates that group head development obviously

2) Based on battery life group head choice depended however not working in that

Malevolent hub execution increases

Proposed framework points of interest:

1) In this demonstrates the bunch head choice recently
2) Energy levels measured for individual hubs
3) Decrease the vitality utilization

Discovers malevolent hubs and reduction the execution level.

IV. SYSTEM ARCHITECHTURE

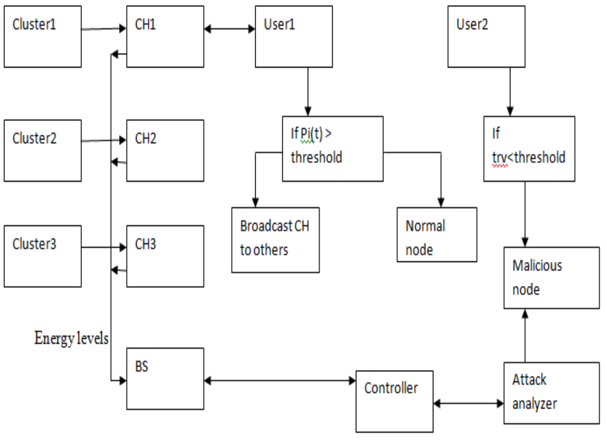


Figure 2: Detection of Malicious Node and CH

The engineering of proposed framework demonstrates that groups are associated with bunch heads, bunch heads are associated with base station so they can impart specifically to base station. in any case, bunches individuals need to speak with BS through the CH. Any bunch can turn into a CH if the hub has more vitality than other hub else it will be dealt with as ordinary hub. In the event that the user2 is new to the system then checking of that hub is finished by some calculation in the event that it comes up short then it will set apart as malignant hub and boycotted by an assault analyzer and the controller will takes out and keeps the vindictive hubs from the system .

V. ALGORITHM FOR DETECTION AND PREVENTION OF MALICIOUS NODES

DAP ALGORITHM

Step 1:

```
Let       G be the Network, where
G={N_1,N_2,’……N_n}’N_i’N
NID(‘Node’_i)=’_(i=0)^(i=n)’I & S is Source Node,
D is Destination Node
```

Step 2:

```
n_r={N_i,N_j,’……N_m}’N_(i,j,m)’the set of intermediate
nodes in the route
```

Step 3:

```
Route={set of all nodes from S to D}
temp(NID,location,pimage)=’_(i=1)^m’retrieve(‘Node’_i(Id,Location,pimage))
```

Step 4:

```
If((NID.valid==true)&&’(N’_i.x,N_i.y
‘max”(x,y))’&&n_i.pimage= =’nr’_nid,pimage)
Then’nr’_i=’nr’_i+node
endif
```

Step 5 :

```
for k=S to D
sendData(S,node(k))
‘end’_for
```

Explanation of DAP Algorithm

There is a Network G which has N no of nodes.In that we find the most trustworthy intermediate nodes to discover a route from the source node to destination node by calculating the trust value of each node. At the time of node creation, node ID, location and one part of image will be assigned for security; the other part of image is stored in the index table with node ID for future verification. When starting to discover a route, the information on each intermediate node is compared with index table ID information stored for the node. For ex if the node ID is 2,this means that node ID 2 and its image are retrieved from the index table and compared. If both are same, this means that the current node is added as an intermediate node and process is repeated until the destination node is reached.

Detection phase:

Phase 1:

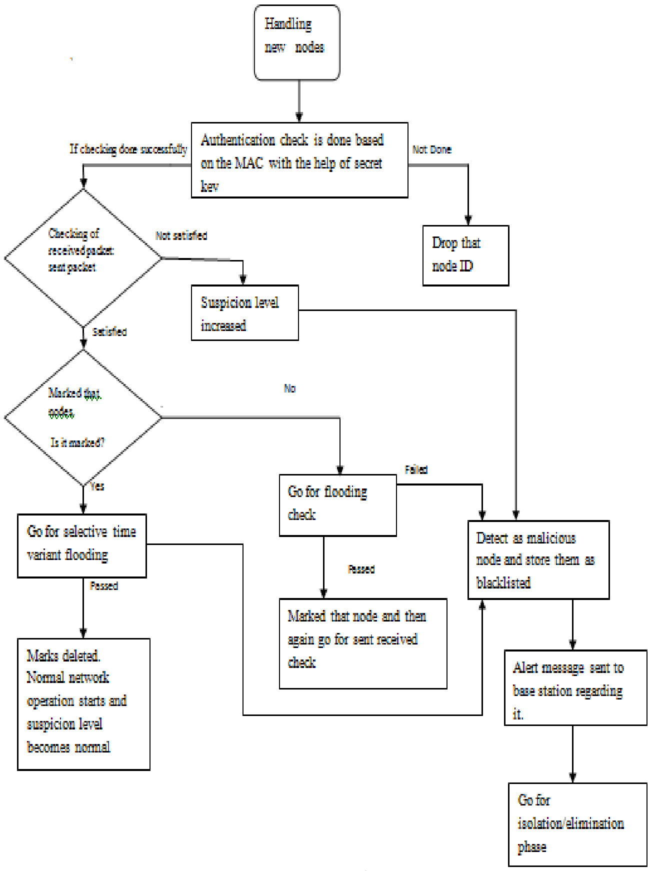
Sender-Receiver Counter: A counter is placed in the base station to check the packets that are sent from the neighboring nodes to the cluster head are received them properly or not and is it further sends them to the base station. If the ratio is proper then we can say that adversary nodes are not there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

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.

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.


Handling new nodes
Authentication check is done based on the MAC with the help of secret kev
If checking done successfully
Not Done
Drop that node ID
Checking of received packet: sent packet
Not satisfied
Suspicion level increased
Satisfied
Marked that nodes.
Is it marked?
No
Yes
Go for flooding check
Failed
Passed
Go for selective time variant flooding
Passed
Detect as malicious node and store them as blacklisted
Marked that node and then again go for sent received check
Marks deleted. Normal network operation starts and suspicion level becomes normal
Alert message sent to base station regarding it.
Go for isolation/elimination phase

Flow Chart 2: Detection of malicious nodes

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.

VII. RESULTS

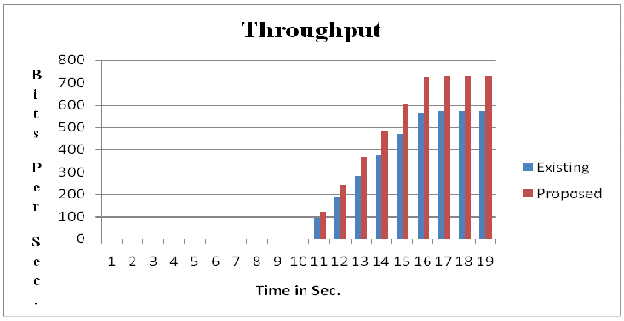


Figure 3: Throughput

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.

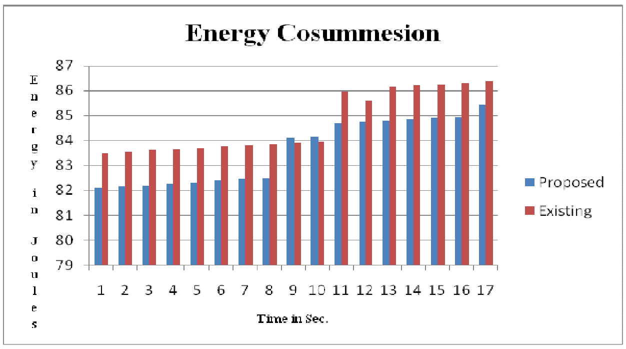


Figure 4: Energy Consumption.

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.

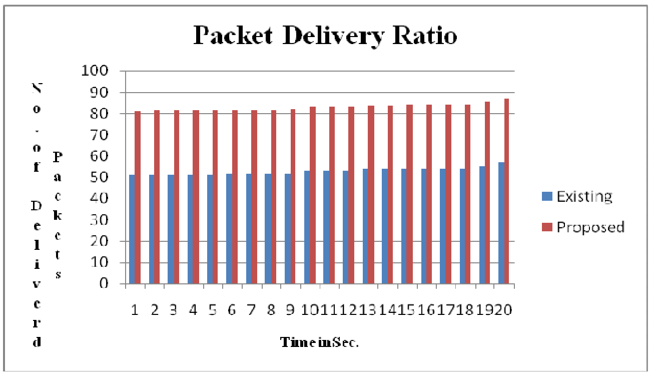


Figure 5: Represents the Packet Delivery Ratio

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:

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

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

In this work Presents another system for bunch head choice and set as a few standards for the group development and correspondence between group head to base station exclusively. Filter which is adjusted vitality utilization convention for remote sensor system. Through dispersing the group stack overhead over the bunch individuals, the life time of the whole system augmented contrasted and LEACH convention. Minimizing vitality scattering and amplifying system lifetime, and Detection and Prevention of vindictive hubs by DAP calculation. The trust worth is not exactly the edge esteem then it demonstrates as noxious hub and averts by checking every hub before correspondence while the proposed calculation displays a practically unimportant loss of vitality, which is essential nature of WSN.

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.

[8]. M. J. Handy, M. Haase, D. Timmermann, \Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection", IEEE MWCN, 2002.

[9]. Zhang, Yu-quan; Wei, Lei, "Improving the LEACH protocol for wireless sensor networks", Wireless Sensor Network, 2010. IETWSN. IET International Conference.

[10]. W.Xinhua, W. Sheng, "Performance comparison of LEACH and LEACH-C protocols by ns2," in Proc. of 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, pp. 254-258, 2010.

[11]. W. B. Heinzelman "An Application-Specific Protocol for Wireless Micro sensor Networks", IEEE TRANSACTIONS WIRELESS COMMUNICATIONS, OCT 2002