© 2017 IJSRSET | Volume 3 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Detection of Blackhole Nodes for Securing Wireless Sensor Network Using MATLAB

Prof. Parikshit Tiwari, Raj Kumari Kushwaha
Rewa Institute of Technology, Rewa, Madhya Pradesh, India

ABSTRACT

Wireless Sensor Networks consists of hundreds and thousands of micro sensor nodes that monitor a remote environment by data aggregation from individual nodes and transmitting this data to the base station for further processing and inference. The energy of the battery operated nodes is the most vulnerable resource of the WSN, which is depleted at a high rate when information is transmitted, because transmission energy is dependent on the distance of transmission. In a clustering approach, the Cluster Head node loses a significant amount of energy during transmission to base station. So the selection of Cluster Head is very critical. An effective selection protocol should choose Cluster Heads based on the geographical location of node and its remaining energy. In this work a centralized protocol for Cluster Head selection in WSN is discussed, which is run at the base station, thus reducing the nodes energy consumption and in- creasing their life-time. The primary idea is implemented using a trust model based selection of Cluster Head from among the nodes of network, which is concluded depending on two parameters, the current energy of the node and the distance of the node from the base station. The protocol is named TR-LEACH based on Energy and Distance, and is run periodically at the base station where a new set of cluster heads are selected at every round, thus distributing the energy load in the network and increasing the network lifetime. The simulation results show that the proposed approach is more effective than the existing AODV protocol.
Keywords: Wireless sensor networks, Cluster Head, micro sensors, network lifetime, TR-LEACH, AODV.

I. INTRODUCTION

1.1 Introduction Wireless Sensor

Networks (WSNs) are networks that comprise of sensors that are distributed in an ad hoc fashion over a defined geographical area, aimed at sensing some predefined information from the surrounding, processing them and transmitting them to the sink station. The sensors work with one another to capture some physical event. The data assembled is then transformed to get important outcomes. Remote sensor systems comprise of protocols and algorithms with self-arranging capabilities. WSNs can be widely divided into two types-Unstructured WSN and Structured WSN. While Unstructured WSN have a large collection of nodes, put up in an adhoc fashion; Structured WSN have few, scarcely distributed nodes with pre-planned deployment. The Unstructured WSNs are difficult to maintain, but it is relatively easy to maintain Structured WSNs.

1.2 Comparison of WSN with ad-hoc networks

i. Wireless sensor networks primarily use broadcast form of communication while ad-hoc networks use point − to −point communication.
ii. Wireless sensor networks are restricted by sensors limited power, energy and computational capability; whereas ad-hoc networks are not.
iii. Sensor nodes may not have global ID owing to the huge volume of overhead, tremendous number of sensors and geographically constrained dosage.

Figure 1. Uses of Wireless Sensor Network [4]

II. METHODS AND MATERIAL

The Sensor Node

Wireless Sensor Networks mainly consists of nodes known as sensors. Sensors are devices with low energy as they operate on battery, having limited memory and processing ability and are designed to survive extreme environmental conditions. These are mostly due to their small size. They are also featured with self-organizing and self-healing power. Three basic parts of a SENSOR NODE can be seen as:

A sensing subsystem that is used for data capturing from the real world.

A subsystem for processing that is used for local data processing and storage.

A subsystem consisting of wireless communication to be used to for data receiving and transmission.

Related Work

Survey Literature

In designing routing protocols for WSNs, it is necessary to deploy advanced routing algorithm for decreasing the consumption of any node's energy, thus be able to extend network life. Wireless Sensor Network routing algorithms are primarily classified as follows hierarchical protocols protocols and flat routing. While flat protocols employee an overhead of delay and management complexity which leads to excess power consumption, in hierarchical protocols-node that is the cluster head is selected, that are responsible towards handling all nodes contained in the cluster and establishing communication with the Base Station. This prolongs the network life [5].

A hierarchical clustering based architecture has many advantages. The network is scalable and components are task oriented. The algorithms are of distributed type, light weight and energy efficient; which makes the network reliable and less granular with clusters. Every node also has data aggregating capability [6].

The advantage of this architecture [6] are as follows:

i. The cluster membership change is limited to at most two clusters. Thus the clustering algorithm is not processed for entire network. This is an important feature for sensor networks, which will help in scaling the network.
ii. Sensor networks, unlike general internet networks, are task specific at time. The architecture is based on combining neighbor list information. The task data object helps in choosing the cluster data, based on the task. Thus network performance is optimized for specific task.
iii. In this clustering algorithm, the nodes furnish the information, does the complicated computation, while clustering algorithms run on the base station (BS). Also cluster algorithm runs at the start of/updation of the cluster.

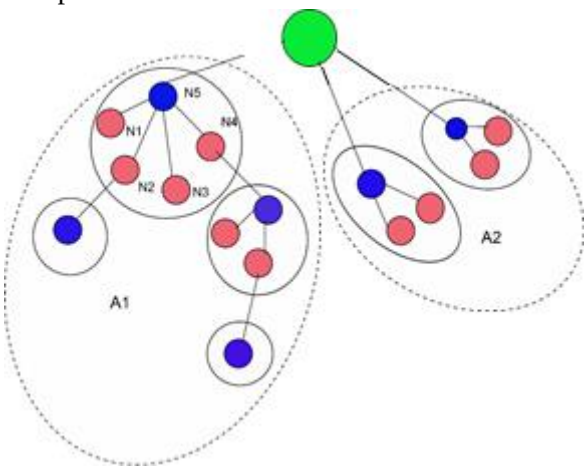


Figure 1. Hierarchical Management Architecture[10]

The dis-advantage of this architecture [6] are as follows:

The architecture does not take care of algorithm for hierarchy one level above, that is, it is single hierarchy.

i. The task orientedness of the algorithm, does not allow it to distinguish on incoming data/input of the nodes.
ii. The algorithm does not mention of fault detection and recovery methods in WSNs.

The architecture of WSNs should to accommodate three features:

i. Scalability: Bigger area based Wireless Sensor Networks depend on hundreds of small sensor

nodes for collecting data from the physical world[7]. All the sensor nodes may not be required to be working continuously, so addition of sensors and removal of sensors from the network can be done dynamically [8]. A long term and extensible design enables alteration in the topology with a reduced of updating of transmitted messages.

ii. Task Orientation: The WSNs correlate with assigned operations at present stage. The operations of WSN vary from the simple data collection, static nodes to complex collection of data, using mobile-node sensor network [9,7]. The structure of the program must be made efficient and enhanced, based on specified task-set of every node, to be adjusted to this specification.

iii. Light Weighting: The processing power and memory – which enables storing data for sensor nodes are very restricted. Tasks like data collection, reducing size of the message, acknowledgement using piggyback, etc. that are lightweight, must be incorporated in the architecture design. Study of Ad-Hoc Mobile Networks

A protocol, that is suitable with SNMPv3-simple network management protocol, version 3; known as Ad-hoc network management protocol (ANMP), is discussed here. It uses same PDU-protocol data units for data collection. This protocol also integrates sophisticated security mechanisms that is improved to fulfill specific requirements [2]. Certain properties of ad-hoc networks pose challenge to manage them. Some of their properties are as following:

- Nodes range in complexity, from simple sensor nodes to complex laptops as nodes.
- In mobile networks, topology changes very frequently.

- Network management overhead should consume minimum energy, as ad- hoc networks run on battery.
- Frequent partitioning of networks, due to switching off/moving out of region should be taken care off.
- Signal quality varies dynamically.
- Frequent attacks from hostile agents – eaves dropping, penetration, snooping, etc. need to be handled.

it is a logical choice in LEACH to adapt clustering of nodes as infrastructure. This enables much less data that is needed to be transferred from the cluster head to the Base Station.

LEACH works with the principle that all the nodes arranges itself into smaller clusters on a local scale and a single sensor node pretends to be the CH. All the other non-CH nodes need to communicate their information to the CH. The CH accepts information from entire cluster, that is the other nodes, it performs data collection, and then sends the information to the sink, the Base Station. Hence, becoming a cluster head (CH) is lot more energy consuming than an on- CH node. When the CH exhausts it energy and it cannot operate any longer, then it affects whole of the network as all the nodes that are belonging to that cluster do not have any means to communicate. So in LEACH there is a system of random rotation of high energy nodes, the CH's position among other sensor nodes, to prevent the emptying the energy of any one node in the entire network. Thus the energy over head in acting as a CH is uniformly divided between all the sensor nodes. LEACH operates by dividing the functioning into rounds. The round in LEACH initiates with a set-up phase. This consists the formation of clusters by selection of cluster head and assignment of each node to a definite CH in the network. This is accompanied by a steady-state, in which information is transmitted from sensor nodes to Cluster Head and then to the Base Station by the Cluster Head. [4]

According to LEACH Protocol for WSNs, the chance of being selected as a Cluster Head is dependent on a node's energy level which is compared proportional to the total remaining energy of the network. The choice of probabilistic method for choosing a CH is developed on the claim that all the sensor nodes will begin operation with same value of energy, and also every sensor node is having information to transmit to CH while each and every frame of a round. In case sensor nodes differ in amount of total energy (or in case an event-driven model is utilized, in which sensor nodes will transmit information only when an event shall happen in the physical surrounding).

III. RESULTS AND DISCUSSION

Ad hoc On-demand Distance-Vector Routing (AODV):

Ad hoc On-Demand Distance Vector (AODV) routing is a routing protocol for mobile ad hoc networks and other wireless ad-hoc networks. It is jointly developed in Nokia Research Centre of University of California, Santa Barbara and University of Cincinnati by C. Perkins and S. Das. It is an on-demand and distance-vector routing protocol, meaning that a route is established by AODV from a destination only on demand [4]. AODV is capable of both unicast and multicast routing [1]. It keeps these routes as long as they are desirable by the sources. Additionally, AODV creates trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. The sequence numbers are used by AODV to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes [7] [5]. AODV defines three types of control messages for route maintenance:

RREQ- A route request message is transmitted by a node requiring a route to a node. As an optimization AODV uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. Data packets waiting to be transmitted (i.e. the packets that initiated the RREQ). Every node maintains two separate counters: a node sequence number and a broadcast_ id. The RREQ contains the following fields [6]: -

The pair <source address, broadcast ID> uniquely identifies a RREQ. Broadcast id is incremented whenever the source issues a new RREQ [7].

RREP- A route reply message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.
RERR- Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a ―precursor list", containing the IP address for each its neighbours that are likely to use it as a next hop towards each destination.

In cluster formation phase:
1. Base station decides whether a node will turn into cluster head or not by comparing residual energy.
2. Some nodes with more residual energy turn into Cluster heads and send cluster head information to inform other nodes. The other nodes with less residual energy turn into common nodes, and send cluster joining information to cluster head.

In steady state phase: 1. Nodes in a cluster, sends their data according to TDMA table, and cluster head receives, and aggregates the data. 2. The Cluster head will not sends the data directly to the base station; instead the aggregated data is sends to the base station via Multi-hop transmission with Multi-level aggregation of aggregated data by Cluster heads. The flow chart of LEACH protocol is shown in fig.4

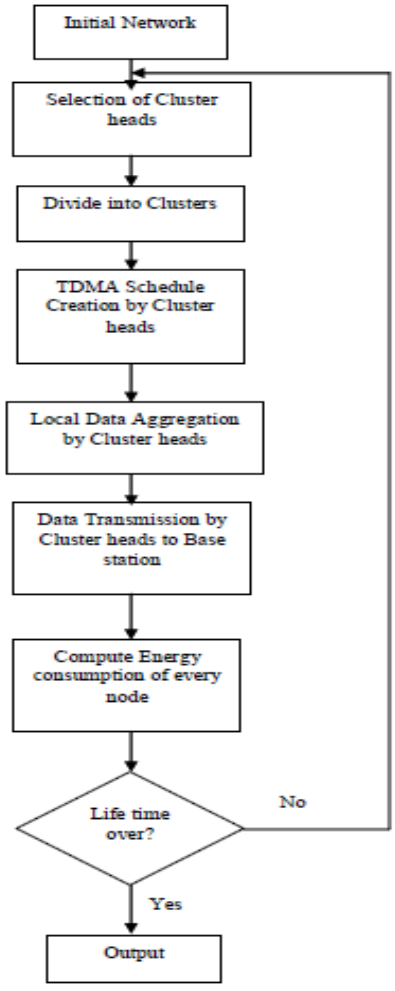
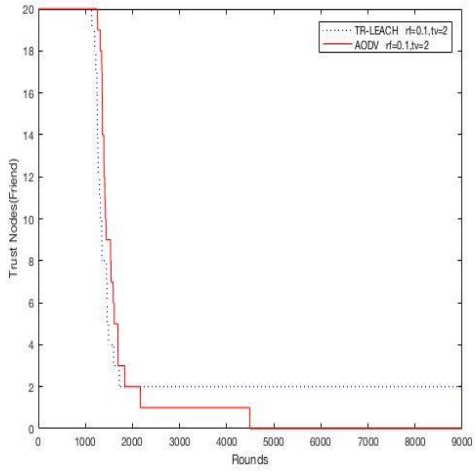


Figure 2. Working of LEACH Protocol

Comparision Graph with Existing AODV Protocol

(a)This graph represent number of packets send to base station using TR-LEACH protocol which shows better performance as compare to AODV.



IV. CONCLUSION

The network life-time, which is dependent on energy remaining in the sensor nodes, is a major factor to be considered when designing WSNs. For an energy efficient WSN, many WSN architectures and clustering algorithms have been proposed among which Leach is a mile-stone. LEACH makes use of the probabilistic model for distributing energy consumption of the CHs among the nodes. The protocol does not guarantee for the placement and count of number for CH nodes. Thus a poor cluster if set-up for a round, may affect the all over performance [38]. LEACH-C is a centrally controlled protocol and produces better cluster forms by spreading the CH nodes all through the network. Along with determining better clusters, the BS also ensures that energy distribution is equally divided among all the sensor nodes.

This work, named TR-LEACH proposes a centralized approach for Cluster Head selection based on Trust model for energy and distance. The main aim of the proposed algorithm is to extend the security of the Wireless Sensor Network by uniforming dividing, to reduce the execution time at the base-station. To accomplish this target, we have concentrated on predicting these nodes eligible for CH selection based on current energy and distance of node from BS, thus reducing the number of iteration random CH selection steps in TR-LEACH algorithm.

V. FUTURE WORKS

As a future work, this protocol can be extended for dealing mobile sensor node networks. Also, future improvements for this work is to integrate this Cluster Head selection approach with multi hop Leach which overcomes the scalability limitation of LEACH and LEACH-C. The Algorithm may require improvement for an event driven network scenario, in which the frequency of event is very Low.

VI. REFERENCES

[1]. Y.G.Iyer,S.Gandham,andS.Venkatesan.Stcp:a generic transport layer protocol for wireless sensor networks. In Computer Communications and Networks, 2015.ICCCN2015. Proceedings. 14th International Conferenceon,pages449–454,Oct2015.

[2]. Yangfan Zhou, M.R. Lyu, Jiangchuan Liu, and Hui Wang. Port: a price-oriented reliable transport protocol for wireless sensor networks. In Software Reliability Engineering, 2015. ISSRE 2015. 16th IEEE International Symposium on, pages 10 pp.–126, Nov 2015.

[3]. ChiehyihWanandShaneB.Eisenman.Coda:Congestion detection and avoidance in sensor networks.pages266–279.ACMPress,2013.

[4]. V.C. Gungor and O.B. Akan. Dst: delay sensitive transport in wireless sensor networks. In Computer Networks, 2016 International Symposium on, pages 116–122, 2016.

[5]. Chieh yih Wan, Andrew T. Campbell, and Lakshman Krishnamurthy. Pump slowly, fetch quickly(psfq):areliabletransportprotocolforsensornetworks.InIEEEJournalonSelected AreasinCommunications,pages862–872,2015.

[6]. O.B. Akan and I.F. Akyildiz. Event-to-sink reliable transport in wireless sensor networks. Networking, IEEE/ACM Transactions on, 13(5):1003–1016, Oct 2015.

[7]. R.A.Santos,A.Edwards,O.Alvarez,A.Gonzalez,andA.Verduzco.Ageographicrouting algorithm for wireless sensor networks. In Electronics, Robotics and Automotive Mechanics Conference,2016,volume1,pages64–69,Sept2016.

[8]. RuiZhang,HangZhao,andMiguelA.Labrador.Theanchor locationservice(als)protocol for large-scale wireless sensor networks.InProceedings of the Firs international Conference on Integrated Internet Ad Hoc and Sensor Networks, InterSense ’16, New York, NY, USA,2016. ACM.

[9]. Xiaojiang Du and Fengjing Lin. Secure cell relay routing protocol for sensor networks. In Performance,

Computing, and Communications Conference, 2015. IPCCC 2015. 24th IEEE International, pages 477–482, April 2015.

[10]. Injong Rhee, A. Warrier, M. Aia, Jeongki Min, and M.L. Sichitiu. Z-mac: A hybrid mac for wireless sensor networks.Networking,IEEE/ACMTransactionson,16(3) :511–524,June2014