INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 4)
Available online at: www.ijariit.com

Improved LEACH routing protocol for wireless sensor networks

Parvin B. Shaikh
parvin786shaikh@gmail.com
Sinhgad College of Engineering, Pune, Maharashtra

Sachin B. Takale
pb786shaikh@gmail.com
Sinhgad College of Engineering, Pune, Maharashtra

ABSTRACT

In wireless sensor networks (WSNs), the present bunch based information accumulation procedure expends more vitality. Additionally, the secured information transmissions are essential for upgrading the information confirmation and secrecy. Keeping in mind the end goal to conquer these issues, in this review, in this paper, we provide detailed analysis on the relations between clustering and routing, and then propose a Low-energy adaptive clustering hierarchy (LEACH) protocol for reliable and efficient data collection in a large-scale wireless sensor network. LEACH adopts the back off timer and gradient routing to generate connected and efficient inter-cluster topology with the constraint of maximum transmission range. The relations between clustering and routing in LEACH are further exploited by theoretical and numerical analysis. The results show that the multi-hop routing in LEACH may lead to the unbalanced cluster head selection. Then the solution is provided to optimize the network lifetime by considering the gradient of one-hop neighbor nodes in the setting of back off timer. Theoretical analysis and simulation results prove the connectivity and efficiency of the network topology generated by LEACH.

Keywords— *WSN, Data aggregation, Clustering process, Data security, Packet delivery, Energy consumption, Packet drop, Transmission overhead*

1. INTRODUCTION

The wireless sensor network includes small and less cost sensing devices together with a wireless radio transceiver for examining the environment. It involves the data gathering and transmitting the information to one or more sink nodes. The main advantage of this network is that it does not require any infrastructure or external supply for data gathering. The main applications of WSN are wild habitat monitoring, forest fire detection, building safety monitoring, military surveillance and so on.

The characteristics of WSN, which have resulted in challenging issues, are as follows:

(i) Sensor nodes are exposed to maximum failures.
(ii) Sensor nodes utilize the broadcast communication pattern and possess severe bandwidth restraint.
(iii) Sensor nodes hold a scarce quantity of resources.

Owing to the limited availability of resources, the amount of data transmission needs to be minimized. This, in turn, will enhance the network lifetime and bandwidth utilization. This can be achieved through data aggregation.

The process of collecting the data from various sources followed by redundancy elimination thereby minimizing the transmission count is termed as data aggregation. This process leads to energy conservation. Moreover, the inherent redundancy in data gathered from the sensor node can be removed through the process of in-network data aggregation. This is mainly executed for extracting application-specific information. However, in a hostile environment, the aggregated data need to be protected from various attacks for attaining the data confidentiality, integrity, and authentication. Hence, security plays a major role in data aggregation [1].

2. SECURITY REQUIREMENTS

In the hostile environment of WSN, security is a key issue, whose requirements are discussed below:

A. **Data Confidentiality:** The process of safeguarding the transmitted data from passive attacks corresponds to data confidentiality. The process of securing the data from the illegal user is the most challenging task. This can be solved by using an encryption technique such that only the intended user with appropriate key can unlock and read the data.

B. **Data Integrity:** The compromised source nodes or aggregator nodes are prevented from altering the final aggregation value by data integrity. Since sensor nodes lack expensive tampering resistant hardware, they can easily be compromised. Moreover, this tampering-resistant hardware will not be reliable every time. A compromised node can modify, copy or discard messages[2].

C. **Data Accuracy:** The aggregated data need to be provided with more accuracy. As high accuracy requires more memory and high energy, a trade-off among the data accuracy and aggregated data size should be taken into consideration. Availability: This means that the network services need to be available even during the internal and external attacks namely the denial of service (DoS) attack. The technique that involves in offering availability makes use of extra communication facilities among the nodes or central access control system to ensure successful delivery of every message to its recipient.

D. **Reply Attack:** If an attacker records some traffic from the network without any content knowledge and replays those in the later period to mislead the aggregator, then the aggregation results consequently obtain affected.

E. **Node Compromise Attack:** During this attack, the adversary arrives at the node and extracts the data stored in it. With respect to the data aggregation application, once the node has been captured by this attack, the entire secured information can be extracted. This attack is also called the supervision attack.

F. **DoS Attack:** This is most commonly referred to as jamming attack that transmits the radio signals for obstructing the radio frequencies used by WSN. The increase in adversary capacity can affect the major portion of the network. During aggregation, this attack causes the aggregator node to prevent the data from obtaining transmitted to higher levels.

G. **Sybil Attack:** This type of attacker has a capacity to offer more than one identity within the network. It affects the data aggregation in the following ways:
   (i) The attacker initially generates multiple identities for creating additional votes during aggregator election phase and chooses a malicious node to be the aggregator. If the adversary is able to generate numerous entries with different readings, the aggregated result obtains corrupted.
   (ii) An adversary can launch a Sybil attack and create n or more identities, thus making the base station to accept the aggregation results.

H. **Stealthy Attack:** This attack involves the injection of false data into the network without revealing its presence. In a data aggregation concept, the injected false data value can lead to a false aggregation result.

3. CLUSTER-BASED DATA AGGREGATION

In cluster-based data aggregation, sensor nodes are subdivided into clusters. In each cluster, a cluster head is elected in order to aggregate data locally and transmit the aggregation result to the base station. Cluster heads can communicate with the sink directly via long-range radio transmission. However, this is quite inefficient for energy-constrained sensor nodes. Thus, cluster heads usually form a tree structure to transmit aggregated data by multi hopping through other cluster heads which results in significant energy savings. Figure 1 presents an example of Cluster-based data aggregation[6].

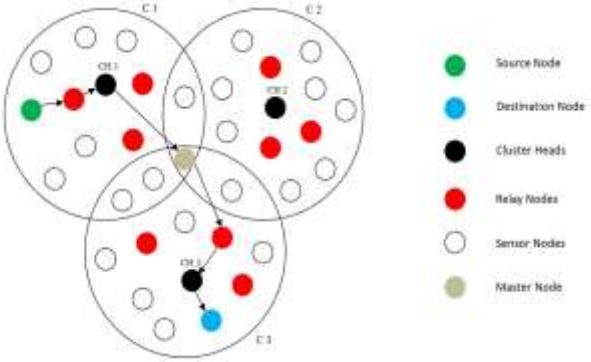

Fig. 1: Cluster-Based Data Aggregation

3.1 Maximum Lifetime Routing in Wireless Sensor Networks

In wireless sensor networks where nodes operate on limited battery energy, the efficient utilization of the energy is very important. One of the main characteristics of these networks is that the transmission power consumption is closely coupled with the route selection. The energy efficiency has been considered in wireless ad hoc network routing, but the conventional routing objective was to minimize the total consumed energy in reaching the destination.

The new problem formulation has revealed that the minimum total energy routing is not suitable for network-wise optimum utilization of transmission energy. The significant improvement can be made by the new routing algorithm in terms of maximizing the system lifetime, which can also be interpreted as maximizing the amount of information transfer between the origin and destination nodes given the limited energy. The routing algorithm is a shortest cost path routing whose link cost is a combination of transmission and reception energy consumption and the residual energy levels at the two end nodes. The simulation results are close-to-optimal performance most of the time with both the fixed information-generation rates and some arbitrary information-generation process of a moving target detecting scenario in wireless sensor networks [8].

3.2 Clustering Mechanism of LEACH Protocol

The selection method of cluster head in LEACH protocol is that the sensor node generates a random number between [0,1] if the random number is less than or equal to the node's threshold $T(n)$, the node is elected as the head node of the cluster.

A. The Problems of LEACH Cluster Mechanism*:* The cluster head election process is completely depended on the random number in the node generates, for other attributes of the nodes, such as the current residual energy, location is not considered, which has the following problems:

(i) Without considering the residual energy of nodes when select cluster head, this may cause low-energy node is selected as a cluster head, which makes the node energy exhausted quickly.

(ii) The location of the node is not considered when the cluster head is distributed, and cannot guarantee the uniform distribution of the cluster head. It may cause some cluster heads are densely distributed, or cluster heads are too sparse, even no cluster head in certain areas.

B. Improvement of Cluster Mechanism: In view of the problem in the LEACH protocol, take the energy and the position of nodes into account to optimize the selection mechanism. The improved algorithm introduces three parameters include energy, the node's number of neighbors, the distance between node and base station to correct threshold.

4. SYSTEM ARCHITECTURE

We have proposed a Genetically Derived Secure Data Aggregation in WSN. Initially, the CHs are chosen based on the node connectivity, which acts as a data aggregator (DAG). Then, the clustering process is executed using the genetic algorithm. This technique and thereby enhancing the network lifetime. When the cluster member wants to transmit the data to the aggregator, a data encryption technique are utilized. The crypto module (CyM) utilized offers confidentiality to the data packet (DP), thus ensuring the authenticity and integrity of the sensed data.

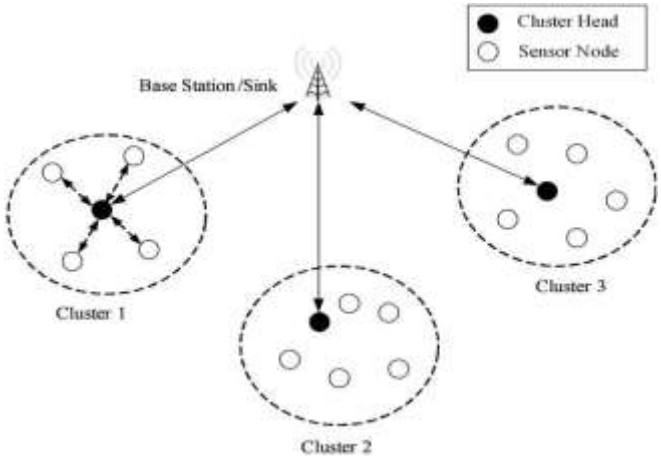

Fig. 2: Proposed cluster creation and transmission process

4.1 Cluster Formation

Figure 2 describes the cluster creation process and transmission between the source and the destination node. At the end of each TS network nodes verifies sensed data and broadcast messages to nodes within the given Cluster Distance (CD) for cluster creation. Cluster creation uses the Relay Node (RN) and CD to group the sensor in the same cluster. Upon accepting the broadcasted message each node verifies the value of RN. If its value is within RN it stores in its memory and compares CD with each node's distance. If the distance between nodes is same or less to CD and sensed value is within given RN then those group of nodes forms a cluster. The nodes NID which are related they will not broadcast message for cluster creation. Nodes which are not participating in the cluster creation process based on *RN* and *CD*.

4.2 Cluster Head Selection

Upon completion of the cluster creation task, each node has its cluster member NID, Node Location (NL), NTE and Sink Location (SL), battery power information in its memory. The node having maximum energy will calculate the minimum distance of each node within the range known as Cluster Head (CH) and broadcast CHID to other network nodes. It also measures the node having a minimum distance from the sink called Cluster Head Transmission (CHT) and broadcast CHTID to CH. This node (CHT) will be used to transmit data toward the sink if the remaining CH energy is not sufficient for data transformation after measurement. Once each node knows its CH it transmits data to CH. Cluster head transmit processed information to the sink, this communication is single hop communication, means it makes direct communication with sink.

4.3 Boundary Node Formation

A dynamic cluster will be built when the target comes close to the boundaries of multiple clusters. A demanding task issue is how the system finds the scenario when the target is approaching the boundaries, especially in a fully distributed way. We use boundary nodes to solve this issue in a fully distributed way.

4.4 Multi-Hop selection

1) The multi-hop planar model: A CH node transmits data to the BS by forwarding its data to its neighbor nodes, in turn, the data is sent to the BS. We have proposed an energy efficient routing algorithm for hierarchically clustered WSNs and it is suitable for the proposed secure data transmission protocols.

2) The cluster-based hierarchical method: The network is broken into clustered layers, and the data packages travel from a lower cluster head to a higher one, in turn to the BS.

4.5 Advantages of Cluster-Based Topology

When we use cluster based on demand dynamic routing protocol for moving target tracking in a given region in a wireless sensor network. This protocol grows the scalability of a sensor network. Throughout energy consumption of the nodes is reduced, leading to a prolonged network lifetime. Sensor nodes organized into cluster network borrow itself for perfect data aggregation, which in turn results in better utilization of the channel bandwidth. Cluster-based routing takes good assurance for many-to-one and one-to-many communication samples those are regnant in sensor networks. With the help of this protocol, we trace out the exact position and path traveled by the target at a given instant of time without any mistake.

4.6 Advantages of proposed system

(i) Highly minimizes the energy utilization.
(ii) Ensures data security and reduces the transmission overhead.

5. SYSTEM ANALYSIS

5.1 Procedure: Transmission Using ACO **(Energy)**
Input: Initial source node *sn*, Destination node *dn*, Group of neighbor nodes *nd []*, each node *id*, each node energy *eng*.
Output: Source to destination path when data received success.
Step 1: User first select the sn and dn
Step 2: choose the packet or file f for data transmission.
Step 3: if(f!=null) fd <= f
Step 4: read each byte b form fd when reach null
Step 5: send data, initialize cf1,cf2,pf1,pf2.
Step 6: while (nd[i] when reach NULL)
Cf1=nd[i].eng
Pf1= nd[i].id
Cf2=nd[i+1].eng
Pf2= nd[i+1].id
Step 7: if (cf1>cf2)
Cf2=null
Pf2=null
Else
Pf1=pf2
Cf1=cf2;
Pf2=null
Cf2=null
Step 8: end while
Step 9: repeat up to when reach sink node

5.2 Head Selection

Input: Cluster set with nodes.
Output: Ch selection with remaining sensor node.
Step 1: select all nodes as initial population in same cluster.
Step 2: Select evaluation set
Step 3: Select all nodes in same clusters
Step 4: Apply weighting for on each sensor node.
Step 5: Apply weight scenario on all nodes power
Step 6: select best node using routlet selection.
Step 7: Check overall evaluations
Step 8: Select final max energy node as CH node.

6. SIMULATION

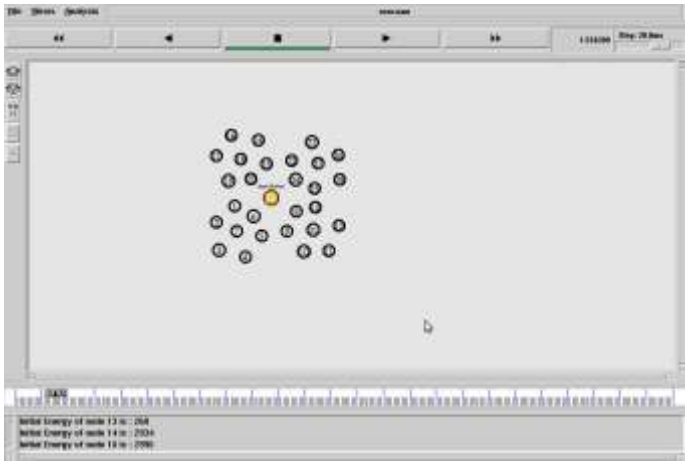

Fig. 3: Cluster creation

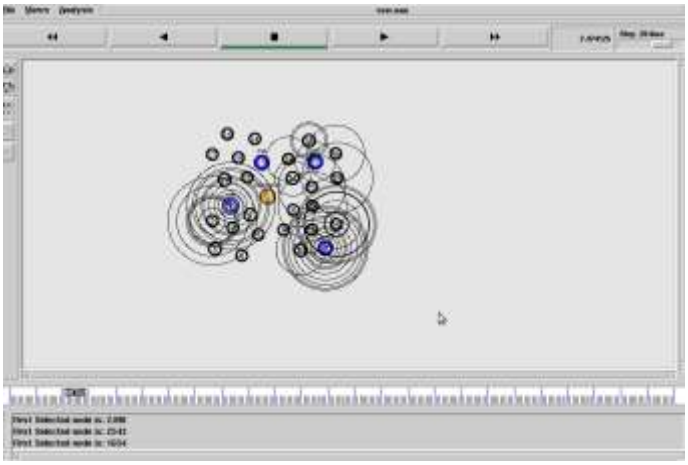

Fig. 4: CHs selection, Data aggregation & data transmission

7. RESULTS AND DISCUSSION

In order to evaluate the performance of the system performed. The network architecture considered is the following:

- A fixed base station (sink node) is located away from the sensor field.
- The sensor nodes are energy constrained with homogeneous initial energy allocation.
- Each sensor node senses the surroundings at a fixed rate and at all times its data to send to the base Station (data are sent if an event occurs).

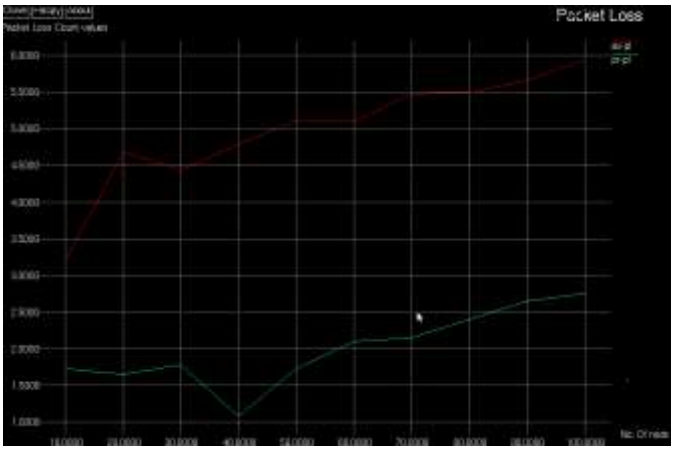

Fig. 4: Packet loss (Proposed vs. Existing)

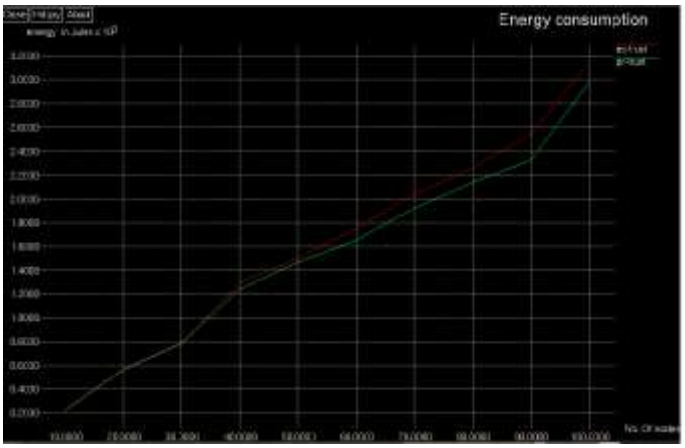

Fig. 5: Energy consumption (Proposed vs. Existing)

We consider energy evaluation for transmission which will conserve the node energy at the time of transmission, the system will select an efficient path for communication with a neighbor node at the same time remaining network will sleep node.

8. CONCLUSION

We have proposed a LEACH protocol to provide reliable and efficient data collection in large-scale WSN. The random backoff and gradient routing schemes are adopted in leach to execute the cluster head selection and multi-hop routing simultaneously with low overhead. Theoretical analysis and simulation results prove that leach can provide connected and efficient inter-cluster topology with limited transmission range. Moreover, the back off timer in leach can be carefully tuned to balance the energy consumption and prolong the network lifetime, we show that the proposed technique minimizes the energy consumption, ensures data security and reduces the transmission overhead.

9. REFERENCES

[1] Nandini. S. Patil, Prof. P. R. Patil, "Data Aggregation in Wireless Sensor Network", 2010 IEEE International Conference on Computational Intelligence and Computing Research.
[2] B. A. Makin and D. A. Padha, "A Trust-Based Secure Data Aggregation Protocol for Wireless Sensor Networks," pp. 7–22, 2010.
[3] Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia, "Secure Data Aggregation in Wireless Sensor Networks", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 3, JUNE 2012.
[4] Priyanka S. Fulare, Nikita Chavhan, "False Data Detection in Wireless Sensor Network with Secure communication", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) Volume-1, Issue-1, 2011.
[5] Hevin Rajesh, D. and B. Paramasivan, "Fuzzy-Based Secure Data Aggregation Technique in Wireless Sensor Networks" Journal of Computer Science 8 (6): 899-907, 2012.
[6] Hani Alzaid, Ernest Foo, Juan Gonzalez Nieto, "Secure Data Aggregation in Wireless Sensor Network: a survey", Information Security Institute Queensland University of Technology.
[7] Ozdemir S, Xiao Y, "Secure data aggregation in wireless sensor networks: A comprehensive overview", Comput. Netw., 2009, 53, (12), pp. 2022–2037.
[8] Jae-Hwan Chang, Leandros Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 12, NO. 4, August 2004.
[9] H. Miao, "Improvement and Application of LEACH Protocol based on Genetic Algorithm for WSN," pp. 242–245, 2015.

