Secure and Improved Lifespan Routing Protocol for Wireless Sensor Network

V Vasanthi[1] V Vinuraja[2]
[1]M.E. (Applied Electronics) [2]Assistant Professor
[1,2]Department of Electronics and Communication Engineering
[1,2]Sri Eshwar College of Engineering, Coimbatore

Abstract— Wireless Sensor Networks (WSNs) are pertinent in numerous arenas where WSNs may be used for sensing, ciphering, and communication elements that give a administrator the ability to instrument, observe, and retort to events and phenomena in a specific environment. For these requirements of WSNs necessitate high efficient routing protocols design ought to energy efficient as feasible to extend their lifetime, and secure data delivery without any time delay. But sensor devices are resource curbed, positioned in an open and unattended environment, different types of attacks and conventional techniques against these attacks are not desirable due to the resource constrained nature of these kinds of networks. An energy-balanced routing method based is designed with change of cluster head for each round of data transmission. This energy efficient algorithm is proposed with verification algorithm which ensures that the secure data transmission is achieved without releasing private sensor readings and without introducing significant overhead on the battery-limited sensors. Additionally different power levels are used to reduce immobile node breakdown in WSN.

Key words: Data aggregation, Energy efficient routing, Verification algorithm, wireless sensor networks

I. Introduction

Holocene technological debuts made in electronics and wireless communications have fostered the enlargement of WSNs [1], [2]. A WSN is a self-organization wireless network system typically dwells of many small, low cost, low-power communication devices called sensor nodes. Each sensor node has restricted on-board processing, inadequate storage and radio capabilities [3]. Owing to the limited communication ability and Non-rechargeable energy supply (e.g. battery), WSNs have rigorous requirements about power consumption. Therefore energy-efficient protocols are vital to save energy and protract network lifetime [4]. Micro sensors are deployed to monitor the sensing field and collect information from physical or environmental condition and to co-operatively pass the collected data through the network to a main location. Traditionally there are two approaches to accomplish the data collection task: Single-hop and Multi-hop forwarding. In single hop wireless communication (Direct), the sensor nodes upload data directly to the sink, which may result in long communication distances and degrade the energy efficiency of sensor nodes. But in multi-hop forwarding, data are transferred from the nodes to the sink through multiple relays, and thus communication distance is reduced. However, since nodes closer to the sink have a much heavier forwarding load, their energy may be exhausted quickly, which degrades the network performance [4] – [6].

Clustering is an effective technique to reduce energy consumption in WSNs. In clustering algorithm, a number of nodes in a network will be chosen as the cluster heads (CHs) and the remaining nodes will be regarded as the cluster members (CMs). CMs will form connections with the CHs. A head node will collect data from its CMs and the actual data transmitted to the base station (BS). In WSN clustered hierarchical routing protocols, at times CMs are closer to the sink than CH, but it should transmit data to CH earliest. This backward transmission result in waste of energy.

In paper [10] a new energy-balanced routing protocol is used which uses forward transmission area (FTA) based on position of sink and final data flow direction to avoid backward transmission [6]. In other words, FTA define forward energy density which constitutes forward-aware factor with link weight, and propose a new communication protocol based on forward-aware factor, thus balancing the energy consumption and protracting the network function lifetime. In the BBV weighted network model is created by Barrat, Barthelemy, and Vespignani; this model defines the strength of connections, which also takes the change of connection strength into consideration, which makes the model closer to real network of any application. Nevertheless, most of the existing in-network data aggregation algorithms have no provisions for security. A compromised node might attempt to thwart the aggregation process by launching several attacks, such as eavesdropping, jamming, message dropping, message fabrication, and so on [8]. This paper focuses on one of the most troublesome attacks: the falsified sub aggregate attack, in which a compromised node relays a false sub aggregate to the parent node with the aim of injecting error to the final value of the aggregate computed at the base station.

II. Related Work

A. Low Energy Adaptive Clustering Hierarchy (Leach) Protocol

In LEACH, all the nodes in a network organize themselves into local clusters. The protocol is divided into a setup phase when the clusters are organized and a steady state phase when CH receive data from all the CMs, perform data aggregation and transmit data to the remote base station.

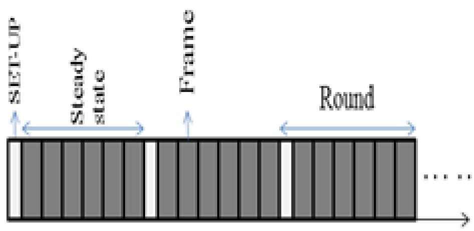

Fig. 1: Time line of LEACH operation

The operation of LEACH in time slots is illustrated in Fig1. In the steady-state phase, operation is broken into frames where nodes transmit their data to the CH at most once per frame during their allocated transmission slot. To reduce energy dissipation, each CM sets the amount of transmission power by using power control. It is based on the received strength of the cluster-head advertisement.

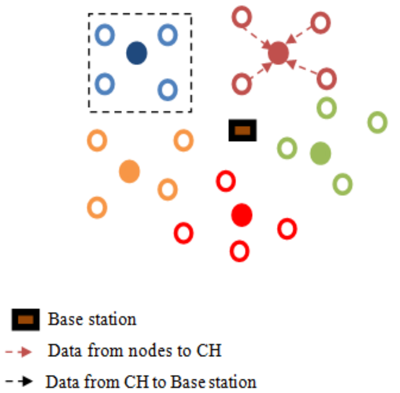

Fig. 2: Data transmission

The CH receives all the data from the nodes in the cluster by keeping its receiver on and then the resultant data are sent from the CH to the base station. In clustering algorithm, CH node is much more energy-intensive than a CM. Thus, when a CH node in a cluster dies, all the CMs inside that cluster lose communication ability.

B. Forward Aware Factor - Energy Balanced Routing Method (FAF-EBRM)

In WSN routing protocol, sometimes cluster members in a cluster are nearer to the sink than the CH, but it should transmit data to CH first. It results backward transmission of data and thus leads to waste of energy. This reliable path method results in reduced energy consumption and the routing model is shown in Figure.3.

In this method, an energy-balanced routing protocol is designed that uses forward transmission area (FTA) based on position of sink and final data flow direction. In other words, FTA define forward energy density which constitutes forward-aware factor with link weight, and propose a new communication protocol based on forward-aware factor, thus balancing the energy consumption and prolonging the network function lifetime.

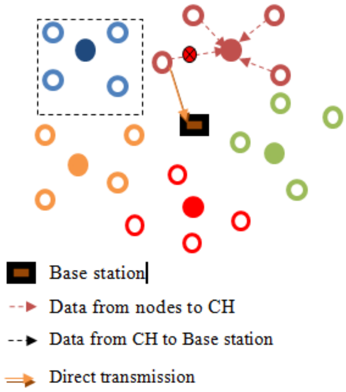

Fig. 3: FAF-EBRM reliable path

C. Local Topology Reconfiguration Mechanism

Nodes with greater signal strength will have more communication link and result in faster energy consumption. So selection CH is necessary after every data transmission. Similarly change of multicast tree node in a path is necessary by choosing alternate path.

The routing algorithm is divided into 3 stages.

1) In FAF-EBRM, every time node finishes transmission, check the point strength of the next- hop node.

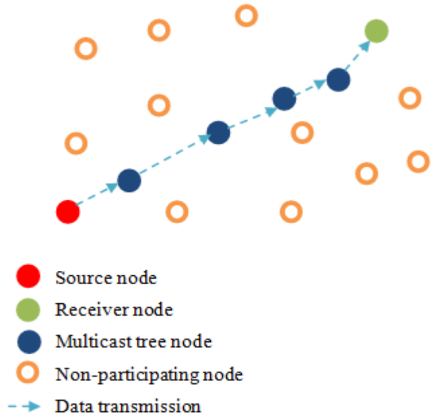

Fig. 4: Data transmission from source node to transmission node

2) If it is less than the average value of all of the sensors' strengths in FTA, remove the link between the nodes.

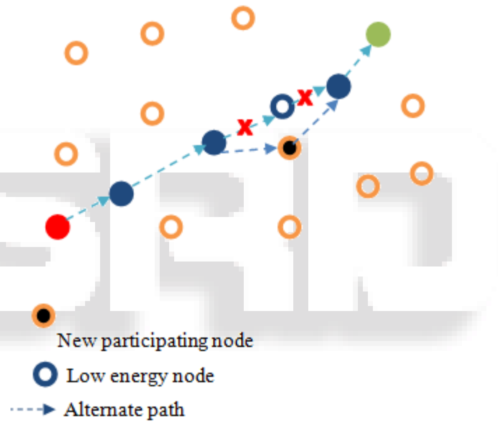

Fig. 5: Data transmission when a node fails

3) The node removed may be the possible next hop node when the next transmission is finished, and the revocation of the edge does not affect the possible reconnection. The node's real-time strength is needed to calculate the sum of strengths.

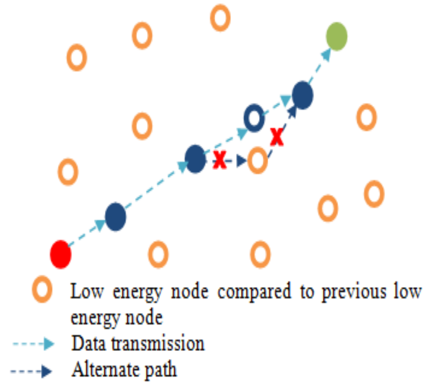

Fig. 6: Recovered data path

So the distribution of Strength of nodes, node degree and weight of edge leads to improved robustness, fault tolerance, reduces the successive node breakdown and enhances the synchronization of WSN.

III. SECURE ENERGY BALANCED ROUTING PROTOCOL

This paper proposes a Secure Energy Balanced Routing Method based on change of Cluster Head or Controller, Verification algorithm.

A. Description of Network Model

Sensor nodes are arbitrarily distributed in a rectangular (WxH) sensing field. Normally data sent to the regional central node (CH), then transferred to the sink node.
The network model descriptions are,

- The entire nodes are isomorphic with inadequate communication ability.
- The energy of sensor nodes is limited with initial energy E0.
- Nodes can vary transmission power according to the distance to its receiver. Cluster Head have more connection, whose degree and intensity are higher than cluster members.

When the data transmission distance is larger than threshold d_0, the energy consumption would rise sharply, so the maximum communication radial of sensor nodes as d_0.

$$d_0 = \sqrt{\frac{\varepsilon_{fsx^2}}{\varepsilon_{mp}}}. \qquad (1.1)$$

Where ε_{fs}- Free space
ε_{mp}-Multipath fading
The function for d(i,sink) is

$$f\big(d(i, sink)\big) \in (0, d_0) \qquad (1.2)$$

B. Cluster Head Selection Phase

The election procedure is as follows.

- The node broadcasts energy request message (ENE_REQ) along with its individual energy level information to the remaining nodes inside cluster.
- The left over nodes its energy level with the nearest elector nodes energy level.
- Then energy reply message (ENE_REP) is send by remaining nodes if any of its energy level is higher than elector nodes energy level, else it hold off for cluster head advertisement message (CH_ADV).
- If energy of elector node is greater than remaining nodes energy level then it becomes cluster head otherwise elector node selects the node with maximum residual energy as the cluster head and successive maximum residual energy as the next elector node.
- The Cluster head selection procedure is repeated for each round of operation that is after each round of data transmission.

Algorithm 1 Cluster Head Selection Phase

```
Cluster ← nil;
Round ← 0;
Better signal ←0;
Set_number ←{};
Last Round CHi ←-1/P;
Advertisement.timeout()
begin
Round i ← Round i +1
  if Round i – Last Round CHi > 1/P then
```

$$Ti \leftarrow \frac{P}{1 - P * (\text{Round i mod} \left(\frac{1}{P}\right))};$$

```
else
    Ti ← 0;
    end if;
rand i ← uniform (0,1);
  if rand i < Ti then
        cluster i < i;
        Last Round CHi ←Round i;
        Set Member i ← {};
        Send ADVi to all nj € N;
  else
    Better signal I ← 0;
End if;
End;
Receive (msg i such that origin i(msg i) =(ni,nj))
begin
 if msg I =ADVj and signali(msgi) > Better signal i then
 Better signal i ← Signali(msgi);
 Cluster I ← j;
 End if;
if msgi = MEMBERj(i) and cluster i = i then
set Member I ← set member i U nj;
end if;
end;
confirmation.timeout()
begin
    if Cluster i ≠ i then
    send MEMBERi(cluster i) to all nj € N;
end if;
end;
```

C. Data Transmission Phase

Once the cluster is formed diffusion of data takes place. Inside the cluster only nodes located in multicast path are in awaken state and only those nodes are involved in data transmission progress. The implementation of this technique also results in reducing the attenuation level of snooping. Also algorithm facilitates for the reception of new node from other clusters when the current cluster is in demand for ordinary sensor nodes. The transmission of data inside each cluster is based on TDMA technique in which time is divided into periodic cycles. This further reduces the collision level of data transmitted from ordinary sensor nodes.

D. Data Accuracy Detection

In this paper verification algorithm is utilized along with Energy efficient algorithm in order to get better level of security. Each cluster head inside definite cluster performs data aggregation of encrypted information being transmitted by ordinary nodes of the corresponding cluster. Each sensor nodes while data transmission, encrypt the data and transmit the cipher text to the Cluster Head. Data aggregators on the other hand does not requires the decryption of cipher text, rather it simply fuse the encrypted data and transmit to the Base station directly.

Algorithm 2 secured aggregation (R, Wx, k)

- Begin
- Receive {(A'x^1, $M^{\times 1}$), (A'x^2, $M^{\times 2}$),……, (A'x^n, $M^{\times n}$)} from ordinary nodes;
- A'x = W' x| A'x^1| A'x^2| ……. |A'x^n; // cipher text aggregation by cluster head;

- Pq^* = index of qth rightmost "1" bit in $A'x$, for $1 \leq q \leq k'$, where k' is largest integer but lesser than k; //
- $A'x$ possibly will have fewer than k "1" bits where k' < k. // generate a MAC bit for Pq^* in Q'x, for 1≤ q ≤ k';
- Assemble the unification of M of the received MAC's; arbitrarily choose M^x = {MI1*, MI2*,……., MIk^* } from M; broadcast (A'x, M^*) to parent nodes;
- End

IV. SIMULATION RESULTS

In this section, the report investigates the simulation cram that examined energy consumption and accuracy of proposed algorithm. The evaluation result shows the better performance metrics for the parameters such as energy, enhanced lifespan and data security.

A. *Simulation Environment*

Simulations were performed by using Network Simulator2 (NS2) environment which is a powerful platform for network research process and it is a discrete event driven simulator tool. In the environment, 50 nodes are randomly deployed in a 300m X 300m area. The performance of our secure energy balanced routing method is evaluated in terms such as the total number of received packets at the BS, network lifetime and the security level of the received packets.

B. *Results and Discussion*

In the proposed technique, secure energy balanced algorithm is used for the transmission and aggregation of the data packets which outcomes with condensed energy consumption and hence protracts the networks lifespan. The verification algorithm works together with previous algorithm to check the accuracy of data packets being ordained to BS from CH.

1) *Energy consumption*

In each simulation of experiment, the energy assign to nodes are changed with number of packets. Energy consumption of each cluster head in the simulation network named node1, node7, node32, node37 is shown in Fig.7.

2) *Data Accuracy*

The accuracy metric is defined as the ratio between the collected summation by the data aggregation scheme used and the real summation of all individual sensor nodes. Data accuracy of nodes node1, node35, node36 is shown in Fig.8.

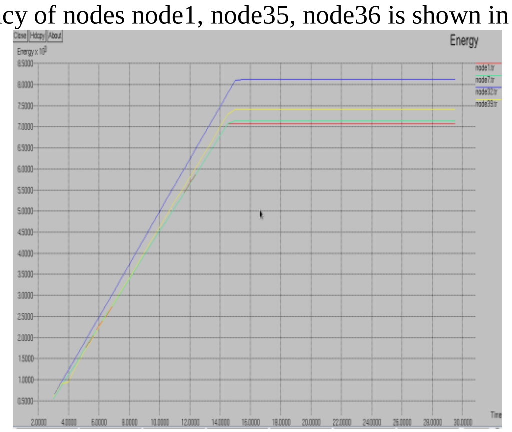

Fig. 7: Xgraph for energy consumption

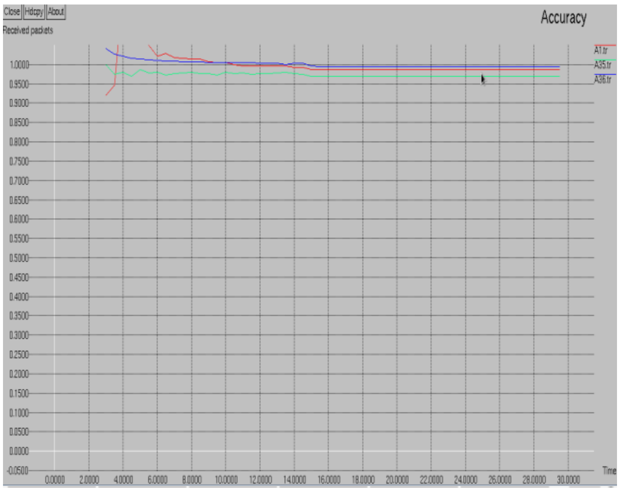

Fig. 8: Xgraph for Data Accuracy

V. CONCLUSION

Secure Energy Balanced Routing Method based for WSN is proposed in this paper. Multi metrics are considered in these algorithms for efficient and secure data transmission. This algorithm provides secure data diffusion, energy efficient by changing the cluster head. The proposed method balances the energy consumption, prolongs the function lifetime and guarantees high QoS.

REFERENCES

[1] A. L. Barabasi, "Scale-free networks: A decade and beyond," Science, vol. 325, no. 5939, pp. 412–413, 2009.

[2] D. G. Zhang and X. D. Zhang, "Design and implementation of embedded un-interruptible power supply system (EUPSS) for web-based mobile application," Enterprise Inf. Syst., vol. 6, no. 4, pp. 473–489, 2012

[3] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application- specific protocol architecture for wireless sensor networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660–670, Oct. 2002.

[4] I. K. Samaras and G. D. Hassapis, "A modified DPWS protocol stack for 6LoWPAN-based wireless sensor networks," IEEE Trans. Ind. Inf., vol. 9, no. 1, pp. 209–217, Feb. 2013.

[5] D.G. Zhang, "A new approach and system for attentive mobile learning based on seamless migration," Appl. Intell., vol. 36, no. 1, pp. 75–89, 2012.

[6] J. Aweya, "Technique for differential timing transfer over packet networks," IEEE Trans. Ind. Inf., vol. 9, no. 1, pp. 325–336, Feb. 2013.

[7] Q. J. Chen, S. S. Kanhere, and M. Hassan, "Analysis of per-node traffic load in multi-hop wireless sensor networks," IEEE Trans. Wireless Commun., vol. 8, no. 2, pp. 958–967, Apr. 2009.

[8] J. Jin et al., "Handling inelastic traffic in wireless sensor networks," IEEE Trans. Sel. Areas Commun., vol. 28, no. 7, pp. 1105–1115, Jul. 2010.

[9] D. G. Zhang and X. J. Kang, "A novel image de-noising method based on spherical coordinates

system," EURASIP J. Adv. Signal Process. vol. 1, p. 110, 2012

[10] Degan Zhang, Guang Li, Ke Zheng, Xuechao Ming and Zhao-Hua Pan, "An Energy-Balanced Routing Method Based on Forward-Aware Factor for Wireless Sensor Networks," IEEE Transactions on Industrial informatics, Vol. 10, no. 1, February 2014.