Intelligent Systems and Computer Technology
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC200147

Efficient Cluster Head Selection in WSN Using Secure Mobility Cluster Based Algorithm

Sampoornam K P [a,1], Hemavikasini S[b], Vidhya S[b], Vakula V[b], AndDharani S [b]
[a]*Associate professor, BannariAmman institute of technology, India*
[b]*PG Scholars, Dept of ECE, BannariAmman institute of technology, India*

Abstract. Wireless Sensor Networks (WSNs) are widely adopted by various civilian/military applications for implementing real-time monitoring or long-term surveillance task. Considering sensor nodes with mobility has emerged as a major application in environmental monitoring or surveillance. Due to the limited battery lifetime, the network in the deployed region is divided into clusters and the clusters are controlled by their Cluster Heads (CH). But selecting CH in WSNs (considering the network with both static and mobility nodes) is a challenging task because security is significant. To prevent the malicious sensor node from becoming CH, Secure Mobility Cluster Based Algorithm (SMCBA) is proposed. This algorithm considers only static node among mobility node for selecting CH with efficient parameters such as trust criteria, selection time and mobility. The simulation results show that the proposed algorithm works effectively compared with the existing clustering algorithms.

Keywords. wireless sensor networks, SMCBA, cluster head, mobility

1. Introduction

With the fast improvement in wireless innovation, the WSN have got significance in most recent decades. WSN are spatially conveyed self-governing sensors to screen physical or ecological conditions and to agreeably forward their information through the network to a fundamental area. The WSNs are made of a few hundreds or thousands of nodes, each outfitted with a radio handset, a microcontroller and a battery. size and cost limitations on sensor systems brings about comparing requirements, for example, vitality, memory, computational speed and transmission capacity [1].The topology of a WSN can differ from a straightforward star system to a progressed multi jump wireless mesh organize. The propagation method between the hops might be directing or flooding. Past assessments [2] had exhibited that communication is the costliest action for a WSNs to the extent power use. In this manner, the life-cycle of a WSN, is upgraded by restricting the exchanges between sensor nodes, for instance by grasping data blend procedures [3]. Additionally, portable nodes were deployed in certain territories because they are more flexible than the static hubs.

[1]Sampoornam K P, associate professor, Bannari Amman Institute of Technology, India;
E-mail: sampoornam@bitsathy.ac.in

2. Related Works

The authors [4] proposed logical classification and request of normal data bundling plans and laid out distinctive gathering calculations for WSNs considering course of action for variable coverage time shows. Filter Mobile (Low Energy Adaptive Clustering Hierarchy for Mobile), in shortLEACH-M [5], is a variety of LEACH (Low Energy Adaptive Clustering Hierarchy), which support node portability. In LEACH-M, clusters are continuously limited by respective time the sensor moves, offering high danger of overhead in the cluster arrangement.The author [6] had proposed LEACH-TM (Low Energy Adaptive Clustering Hierarchy Trust Transmission) and shaped LEACH-TM custom by using trust outlines in which CH sets up multi route thereby exchanging CHs that are going as switches. The exhibition of this plan was found to be better than LEACH with respect to vitality usage and number of nodes alive in the system however has no worry about node versatility. A portion of the adjusted LEACH calculations are LEACH-C, F-LEACH, TLLEACH, M-LEACH and V-LEACH which are explicitly intended for static sensor organizes and are not portability adjusted.

In this manner LEACH-M and LEACH-ME [7] calculations are proposed for versatile condition. The author [8] had proposed ALM, improving the system dependability and sparing the vitality utilization while keeping the system, yet the security of CH gains no consideration. The executive's framework for trust dependent on neighbor checking is proposed for MWNW. In the trust executives' structure, the trust quality of the node is registered by the neighbor observing the component, the prompt trust criteria and indirect trust quality are merged to arrange the appropriated trust model for perceiving the malevolent nodes. This plan doesn't concentrate on node grouping and CH determination. The authors [9] has proposed an innovative method of demonstrating wireless sensor network using fuzzy graph and energy effective fuzzy based k-Hop clustering algorithm which considers the dynamic nature of network, physical layer uncertainty and volatile aspects of radio links.

3. Proposed Work

The proposed fuzzy k-hop centrality metric considers residual energy of individual nodes, hop distance between the potential cluster head, and particular member nodes to let us assume that the quantity of sensor nodes s= {N_1, N_2, N_3… … Nn}are dispersed over a locale of checking territory inorder to gather data and send them to the base stationor sink node. Here the WSN are thought to be with mobility (MWSN). The network is divided into cluster and the cluster head isselected based on the proposed Secure Mobility Cluster Based Algorithm (SMCBA).For enhancing the security, only static nodes are considered for CH selection.

3.1.Drawbacks of Selecting Mobility Node as CH

The location of the node changes often, hence there is often cluster reformation. Due to frequent cluster reformation, some of the static nodes are left out.There may be collision in data forwarding to CH resulting in loss of sensed data, thereby reducing the throughput. There is high possibility of malicious node becoming CH.

3.2 .Secure Mobility Cluster Based Algorithm (SMCBA)

The fact is to develop a totally scattered clustering calculation with a particular ultimate objective to upgrade the energy proficiency, stability in cluster, and safe CH determination in an adaptable area.The trust metric is definitive and permits the proposed CH choice calculation to stay away from any malignant node in the area to turn into a CH. In the event that a portability sensor node enters the group, the confirmation dependent on the versatility and trust criteria is determined. If it fulfills the criteria, it is one of the individuals from the cluster or else disposed of. As referred, only static nodes can compete for CH selection. The static hubs screen its one hop neighbor in all directions and rate them dependent on its node id, parcel sending, effective bundle conveyance proportion and its productive force utilization during detecting and information sending. The rating is shared among every one of the hubs with its neighbors and the choice is made. In the event that the rating is more prominent than the 0.85 likelihood esteem, it can go after CH determination. When a hub is chosen as CH, the "SOLICITATION FOR CH" is sent to the comparing node. On accepting the solicitation, the node gives the affirmation "ACK" to its individuals and cluster is framed. After selecting the CH, all the data sensed by the cluster members are forwarded to the CH by CDMA inorder to avoid collision among data transmission.The WSN nodes and the mobile nodes should be synchronized for better utilization of CDMA. The CH after collecting the data from its member nodes, it transmits the data to the nearby base station.

3.3 Selection Time(ST)

The time taken by the sensor nodes during rating one another and picking CH is called selection time. All nodes need to hold up before communicating CH declaration messages to avoid extraordinary accident and strife among the nodes. The selection time is determined as

$$TC = R^*[1\text{-}PF_{m,n}(T_{tot})] + R\,[RSD_{m,n}(T_{tot})] + R\,[EP_{m,n}(T_{tot})] + \text{node id} \quad (1)$$

Where ST_{max} is the maximum selection time, R_n is the rating of the neighboring node,R_o is the checking the rating of own node itself, $E_{residual}$ is the residual energy of the node, $E_{initial}$is the initial energy of the node and V_m velocity of node with mobility.

3.4 Trust Criteria(TC)

The trust estimation is done in explicit time which is called periods. Specifically, node m will monitor and process complete trust of node n as follows in the given condition

$$ST = ST_{max} * (R_n * R_o) * [1\text{-}(E_{residual} / E_{initial})] * V_m \quad (2)$$

Where R is the rating given, PF m,n is the packet forwarding of the m,n nodes, RSD m,n is the successful packet delivery ratio of the nodes m,n, EP is the efficient power usage of the nodes m,n and Ttot is the total time taken by the nodes. By evaluating the trust criteria,the rating is performed by the nodes to its one hop

neighbor. The distance(D) calculated for a node n to its one hop neighbor is given by,

$$D_n = \sum_{m \in s}^{N_n} dis\,(n,m)_t \quad (3)$$

From the trust criteria, the rating of the node is calculated as, Normal node: $0.85 \leq TC \leq 1$, suspect node: $0.5 \leq TC < 0.85$, malicious node $0.1 \leq TC < 0.5$

3.5 Calculation of Mobility(M)

The main purpose of calculating mobility is to form a stable cluster. Considering the node K with mobility,

$$M = \max \sum \sqrt{(\Delta s/\Delta t)2k - 2(\Delta s/\Delta t)2k \cos\,(\Theta_k)} \quad (4)$$

Where $\Delta s/\triangle t$ is the change in position with respect to time Cos Θ_k is the angular movement of node k.

3.6. Algorithm for Cluster Formation

Step 1: select static node from the deployed sensor nodes
Step 2: for s=1
If $E_{\text{I static node}} > 0$, thenEvaluate TC // 2 equ
Check = rating R > 0.85 probability = true
If R < 0.85 probability = false (discard)
Evaluate ST//1 equ
Step 3: Sort the static nodes
    Select CH
    If CH = True
    Send = SOLICITATION FOR CH by its one hop neighbor
    Send = ACK by CH for other nodes
Step 4: Cluster formation request from S nodes
Step 5: CH accepting the nodes that satisfying TC.
Step 6: checking the request of mobility nodes to join cluster
Step 7: Check = mobility M of a node // 4 equ
    Evaluate TC // 2 equ
    TC true = add into cluster
Else
TC false = discard
End

4. Simulation Parameters

Table 1. Parameters used in simulation

Parameters	Description
Mobility	Randomly assigned
Total sensor nodes	100
Total mobility nodes	30
Field size	150*150
Data packet length	612 bytes

Inference queue type	drop tail
Speed	1-30m/s
Communication model	bidirectional
BS position	Fixed

5. Results and Discussions

From fig.1, the efficiency in cluster head selection is compared with the existing algorithms. The proposed algorithm has 48%, 38% and 24% higher efficiency then LEACH-M, ALM and DCA in selecting the CH for 100 nodes. from fig 2, the existing algorithm has no trust and security in selecting the CH. Hence the proposed SMCBA algorithm has detected almost 16 malicious nodes among 100 nodes. Fig 3 explains the packet delivery ratio to CH. The proposed algorithm shows that it has the highest packet delivery ratio to CH than other algorithms. Hence sensed packets reach the CH without issues.Also, for the increased number of nodes, the packet delivery ratio also increases resulting in high throughput.

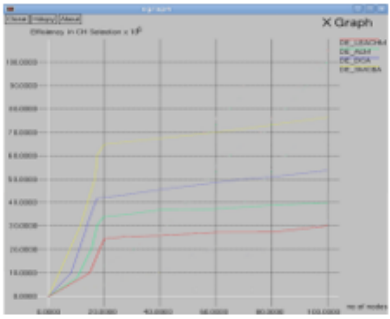

Figure 1. No. of nodes Vs Efficiency

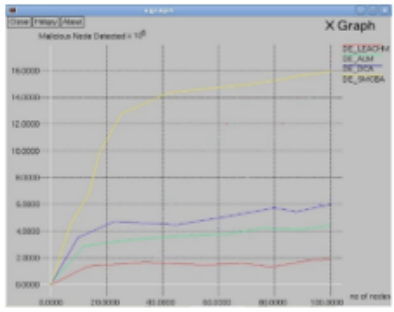

Figure 2. No. of nodes Vs Malicious Node Detected

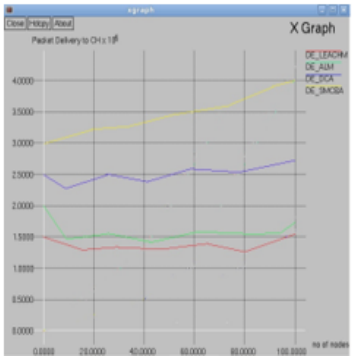

Figure 3. No. of nodes Vs Packet consumption

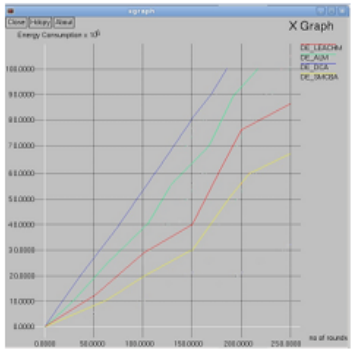

Figure 4. No. of nodes Vs EnergyDelivery Ratio

Fig 4 shows the energy consumption of the network. The No. of rounds denotes the No. of times the sensor nodes transmit the sensed data to the CH. LEACH-M uses 85% energy whereas SMCBA uses 67%, the energy is saved upto

13%, in which another 17 rounds can be completed. The ALM and DCA uses beyond 100%. Hence the proposed algorithm works effective for the taken parameters.

6. Conclusion

To make the WSN more compatible, CH selection is significant. To enhance the security and trust in selecting CH and adding cluster members, a probability value is calculated for normal, suspect and malicious node. The proposed Secure Mobility Cluster-Based Algorithm (SMCBA) has evaluatedthe trust criteria, selection time and mobility criteria to prevent the malicious node from joining the cluster. To make the security effective, only static nodes are considered for CH selection to form a stable cluster.Also, the proposed scheme is compared with the existing algorithms such as LEACH-M,ALM and DCA, the simulation results had found to be more effective.

Reference

[1] Rajesh Kumar Varun, R. C. Gangwar. Hierarchical Energy Efficient Routing in Wireless Sensor Networks and its Challenges; 20192249 – 8958,IJEAT9(1).
[2] Huar, I. Nikolaidis. Balancing energy harvesting and transmission scheduling in aggregation converge cast; 2018 . 17–2; in: Proc. ACM MSWiM
[3] V.F. Marques, J. Kniess, R. Stubs Parpinelli,; An ant colony-based mesh routing protocol for maximizing low power and lossy networks lifetime; 2018 67–73;in: Proc. ACM, MobiWac,
[4] C. Zhu, L. Shu, T. Hara, L. Wang, S. Nishio, and L. T. Yang; A survey oncommunication and data management issues in mobile sensor networks; 2014 19–36;Wireless Communications and Mobile Computing; 14(1)
[5] C.-M. Liu, C.-H. Lee, and L.-C. Wang; Distributed clustering algorithms for data-gathering in wireless mobile sensornetworks; 2007 1187–1200; Journal of Parallel and Distributed Computing67(11)
[6] Xiaoyan Cui; Research and Improvement of LEACH protocol in Wireless Sensor Networks; 2007; IEEE International symposium on Microwave, Antenna, Propagation and EMCC technologies for wireless Communications
[7] F. D. Tolba, W. Ajib, and A. Obaid; Distributed clustering algorithm for mobile wireless sensors networks; 2013;Proceeding of the 12th IEEE SENSORS 2013 Conference; pp. 1–4
[8] Kumar, M V, and Jacob; Mobility Metric based LEACH-Mobile Protocol, ADCOM; 2008; IEEE 78:56
[9] VD Ambeth Kumar, VD Ashok Kumar, M Ramakrishnan, S Malathi, A Govardhan, Efficient routing for low rate wireless network-a novel approach, 2017; International Journal of Image Mining; 2, 208-230.