Trust Based Secure and Energy Efficient Clustering in Wireless Sensor Network: A Bee Mating Approach

Rashmi Ranjan Sahoo[1], Abdur Rahaman Sardar[2], Moutushi Singh[3], Sudhabindu Ray[1], and Subir Kumar Sarkar[1]

[1] Department of ETCE, Jadavpur University, Kolkata, India
[2] Department of CSE, NITMAS, West Bengal, India
[3] Department of IT, IEM, Kolkata, India
{rashmi.cs2005,abdur.sardar,moutushisingh01}@gmail.com,
sudhabin@etce.jdvu.ac.in, su_sircir@yahoo.co.in

Abstract. In this paper we have proposed a trust based secure and energy efficient clustering algorithm in wireless sensor network using Honey Bee Mating Algorithm (TBCR-BMA). The proposed TBCR-BMA deprives the malicious node to act as cluster head, thus prolong the life time of the network. Moreover, we reveal that this proposed scheme outperforms the most popular hierarchical Low Energy Adaptive Clustering Hierarchy (LEACH) and Advertisement timeout driven bee's mating approach to maintain fair energy level in sensor networks (TBCMA) in terms of average residual energy of nodes and total energy of the network.

Keywords: Wireless Sensor Network, Clustering, Trust, HBMA.

1 Introduction

Energy consumption is one the foremost factor for wireless sensor network (WSN), which is inversely proportional to the life span of the WSN. By clustering the nodes and reducing the number of transmission, its lifetime is enhanced [1]. In our proposed work we have considered a trust based secure and energy efficient clustering algorithm using Honey Bee Mating Algorithm (HBMA) inspired by the conduct of social insects. HBMA is used to find the most appropriate cluster head (CH) in WSN. The clustering architecture of WSN localizes the route set up within the clusters, reduces size of the routing table of individual sensor nodes, eliminate the transmission redundancy and data aggregation from multiple nodes [2–4]. We have calculated trust value on each node for ensuring selected CH_s trustworthiness and highest remaining energy.

2 Proposed Honey Bee Mating Based Clustering

This section presents the proposed clustering method. The operation of the protocol is broken up into cluster head(CH) selection and cluster creation process.

P. Maji et al. (Eds.): PReMI 2013, LNCS 8251, pp. 100–107, 2013.

Further CH section consists of premiere phase and steady-state phase. Details procedure for finding the trustworthiness of a node can be found in section 3.

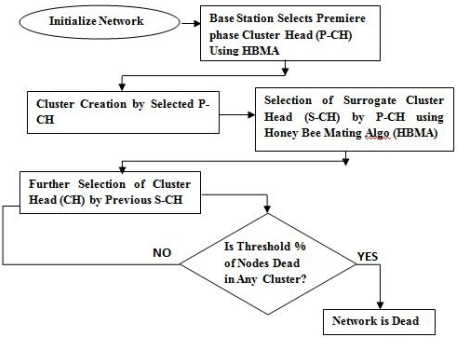

Fig. 1. Flowchart of artificial honey bee mating based clustering

2.1 Cluster Head Selection Process

The mechanisim of CH election mechanism is carried in two different phases. In first phase (Premiere Phase) the entire CH election process is govern by base station (BS) where as in subsequent phases (Steady Phase) the election is carried by the CH of previous phase.

2.1.1 Premiere Phase Secure Cluster Head Election Process

In this phase, as the entire CH selection process will be carried by BS so there will be less over head on different sensors node in terms of energy consumptions.

Algorithm Premiere Phase Secure Cluster Head Election Process

1. BS broadcast a $START - ELECTION$ message to find out the expected premiere Phase cluster head (CH_{EPP}).
2. The node which wishes to be a candidate for CH will send a *WISH_FOR_CH* packet to BS with its Node id (N_{id}), Residual Energy (R_E), Distance from BS (D) and Neighbor node list present within its transmission range.
3. BS multicast a message to all the neighbor of each CH_{EPP} for Direct Trust (DT_{EPP-CH}) [Discussed in section 3].
4. BS compares the direct trust of each individual expected cluster head with supplied trust thresh hold value, if BS found $DT_{EPP-CH} > T_{th}$ then consider that node as expected premiere Phase cluster head $(CH_{EPP})list$.
5. BS executes Honey Bee Mating Algorithm (HBMA) on expected premiere Phase cluster head (CH_{EPP}) list by preparing chromosome structure1 (Discussed in section 2.3) and finds the $P - CH : CALL\_HBMA()$
6. BS station declare that node as premiere phase cluster head ($P - CH$) and broadcast a message PCH_ADV_MSG with N_{id} of CH across the network

2.2 Cluster Formation Process

In cluster formation, cluster size is very important for network lifespan. With a big cluster size and distant between CH and BS, the overhead for data transmission is more; hence energy consumption by that CH will be more as compared to large cluster with small distance from BS. Same thing happens for small cluster with large distance from BS than small cluster with small distance from BS. So our proposed cluster formation process considers the equipoise size of cluster. For balancing the CH load across the network, cluster size (SC) is considered the as a function of distance between CH and BS i.e.$SC = f(D(CH, BS))$. When the $D(CH, BS)$ is large the corresponding CH will accommodate small number of nodes. Hence our proposed method ensures stable cluster in terms of load and energy dissipation across the network. The entire cluster creation process is as follows:

1. Every recipient of $P_{CH\_ADV\_MSG}$ message expect P-CH decides which cluster it will Join as a cluster member depending upon its own R_E and distance from premiere cluster head.
2. Every non-cluster member calculates value of $P-CH$ as ($VP-CH$), present within its radio range in order to join as cluster member. $VP-CH_i = W_1 * RE_i + W_2 * D(P-CH_i, BS) + W_3 * D(P-CH_i, Nc_i)$, where $D(P-CH_i, BS)$, is the distance between $P-CH$ and BS. $D(P-CH, NC_i)$ is the distance between $P-CH$ and non-cluster member.W_1, W_2, W_3 are different weights such that $W_1 + W_2 + W_3 = 1$.
3. Each non-cluster members decides $P-CH$ depending upon the minimum value of $VP-CH_i$ and uses CSMA to inform $P-CH$ which it belongs.
4. After $P-CHs$ received messages from all nodes, it will create Time Division Multiple Access(TDMA) scheduling table and send it to all nodes, which contains the time allocated to each node for transmitting data to the $P-CH$.
5. To avoid the collision $P-CHs$ will issue new TDMA slots to all nodes in their clusters when thresh hold allocated time elapsed.

2.2.1 Steady Phase Cluster Head Selection

After the selection of $P-CH$ by BS and cluster formation by $P-CH$, it elects a surrogate cluster head ($CH_{surrogate}$) as spare CH before it run out a thresh hold energy. Also, $CH_{surrogate}$ finds another CH before its energy level reaches to a certain threshold level and so on. This procedure will continue until a certain percentage of sensor nodes run out their energy completely within any cluster. The detail description of $CH_{surrogate}$ election is as given below.

1. Cluster Head selected at premiere phase (act as CH) compares its own residual energy level with supplied Residual Energy Threshold (TH_{R-E}) value. When the residual energy level reaches at supplied TH_{R-E} value at that point of time, $P-CH$ starts the election of $CH_{surrogate}$.
2. CH broadcast a message within its cluster members to get the R_E, TRUST (Direct and Indirect) and cluster head counter (CH_C) value.

3. CH compares the TRUST value of each cluster members with supplied total trust threshold (Th_{total_trust}) value, if TRUST value of each individual member is greater than the Th_{total_trust} then that node will be considered as a candidate for $CH_{surrogate}$ otherwise will be considered as malicious one.
4. CH execute the Honey Bee Mating Algorithm (HBMA) on surrogate cluster head list by preparing chromosome structure 2 (Discussed in section 2.3), in order to select the $CH_{surrogate} : CALL\_HBMA()$

2.3 Problem Mapping

In this section we have modeled the proposed clustering algorithm of wireless sensor network as per the honey bee mating algorithm. Various controlling parameters of HBMA are mapped with the proposed clustering algorithm are as follows The parameters of real honey bee mating such as Nodes in the Network, Random selection of Expected cluster Head, Queen, Drone Bee, Worker Bee and Mating are mapped onto Bees in hive, Initial Population (Chromosome), Best Bee (Selected by Fitness Function), Expected cluster head list (initial population) - Best bee (Queen), Heuristic Search Function and Cross Over respectively of artificial bee.

- Initial population is a set of random possible solution comprise of chromosome. In this work, we have considered two different type of chromosome structure, one structure for premier phase cluster head selection and other for steady phase.
- Premier Phase Chromosome
  The chromosome structure C_i for premier phase are consists of series of n genes.
  $C_i = \{g_{i1}, g_{i2}, g_{i3} \cdots g_{ij} \cdots g_{ik}\}$ where i=1, 2,3... population size and
  $g_{ij} = \begin{cases} 1, & \forall Premierphaseexpectedclusterhead \\ 0, & \forall Regularnode \end{cases}$
  g_{ij} stands for node n_i associated with chromosome c_i (Shown in Fig. 2.)
- Steady Phase Chromosome
  Fig. 3. shows the structure of steady phase chromosome. First row of the chromosome structure 2 represents node IDs and the values of respective cells are their cluster head ID. In this structure, those nodes which are chosen as cluster head have 0 in their particular cells. Nodes which are not a member of the corresponding cluster head are filled with -1. For example node with id 3, 6 and 8 are not member of cluster head 5.
- Fitness Function
  In this work we have designed two different fitness functions (one for premier and other for steady phase cluster head selection) by considering all the parameters of the problem that affects the fitness of an individual chromosome. The fitness function for premier phase cluster head selection depends on the Residual Energy (R_E), Direct Trust by neighbor node of expected cluster heads (DT_{EPP-CH}) , Distance between expected cluster heads and Base station ($D_{EPP-CH,BS}$).

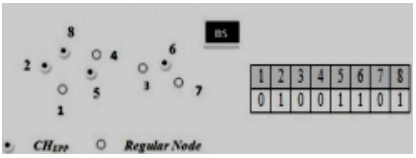

Fig. 2. Chromosome structure 1

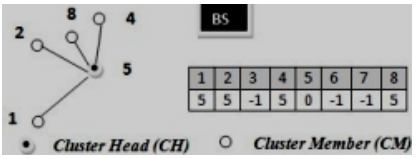

Fig. 3. Chromosome structure 2

$$fitnes(chrome1_k) = \alpha * \sum_{i=1}^{n} R_{EEPP-CH_i} + \beta * \sum_{i=1}^{n} DT_{EPP-CH_i} + \gamma * \frac{1}{\sum_{i=1}^{n} Dist(BS, EPP - CH_i)} \quad (1)$$

Where $fitnes(chrome1_k)$ denotes k_{th} chromosome of chromosome structure 1 and α, β, γ are weighted coefficients, $\alpha + \beta + \gamma = 1$.

During steady phase surrogate cluster head selection following fitness function is used for evaluating the best individual chromosome from chromosome structure 2.

$$fitnes(chrome2_k) = \alpha * \sum_{i=1}^{n} R_{ECM_i} + \beta * \sum_{i=1}^{n} IT_{(CM_i,CH)} + \gamma * \sum_{i=1}^{n} DT_{(CM_i,CH)} + \eta * \frac{1}{\sum_{i=1}^{n} Dist(CH, CM_i)} \quad (2)$$

Where $fitnes(chrome2_k)$ denotes k_{th} chromosome of chromosome structure 2. R_{ECM} is the residual energy of cluster member. $IT_{(CM,CH)}$, $DT_{(CM,CH)}$ are the indirect and direct trust of cluster members calculated by the CH respectively. $Dist(CH, CM)$ is the distance between CH and cluster members.

```
Procedure CALL_HBMA ( )
Initialization
Initialize all the bees (initial population);
Evaluate the fitness (fitness_i) of the population;
Select the bee with highest fitness as Queen and
set fitness_Queen = fitness_Best_Bee;
for Iter=1: Maxiter do
begin
    while  Spermathica_Queen is NOT full do
    begin
        Select a drone depending on depending on
        Prob (Q, D) as in equation (7);
        Store the drone in queens spermatheca;
    end while
for i=1 to no. of brood do
```

```
begin
    Broodi = Dronei + rand (0, 1)*(Queen-Dronei);
    Improve the broods by local search;
end for
Select the brood with highest fitness as best_brood;
if fitness_best_brood  > fitness_Queen then
Q = fitness_best_brood ; %Replace the Queen with best brood
end if
end for
```

3 Trust Evaluations of Sensor Nodes

Trust value of a sensor node is calculated from the history of transactions of the node and from the recommendations given by other neighbor node of the cluster to ensure the sensor nodes trustworthyness. Trust value is the level of confidence of a node N_i on neighbor node N_j depending on the performance of the assigned task [7, 8]. To find trust each sensor node keeps track of the conduct of their neighbors and maintains record of various parameters called as trust metrics. Initially, when a sensor node joins the network, it is assumed that the node N is a Trustworthy (Benevolent) and some trust value is allocated to the node depending upon the threshold trust value (T_{th}). In our proposed scheme Tth is 0.5 [7, 8]. Trust is time dependent. For each of the successful transaction between node N_i and N_j the trust metrics value of corresponding node will increase up to maximum 1, otherwise it will decrease up to as minimum as 0. We considered various trust metrics like Data Packets Forwarded (DPF), Control Packet Forwarded (CPF), Data Packet/message Precession (DPP), Control Packet/message Precession (CPP), Packet Address Modification (PAM), Injection of false Packet ($IOFP$) to measure the trust worthiness of nodes. Direct Trust (DT) of any node is geometric mean of all the trust metrics i.e. DT of node N_i on node N_j can be calculated as shown in equation (3).

$$DT_{Ni}(N_j) = [\prod_{k}(m_k)]^{\frac{1}{k}}. \tag{3}$$

Where $DT_{Ni}(N_j)$ represents the direct trust of node N_i on node N_j and m_k is set of k different trust metrics.

$$IT_{Ni}(N_j) = [\prod_{n}(DT_n(N_j))]^{\frac{1}{n}}. \tag{4}$$

Where $IT_{Ni}(Nj)$ is the indirect trust of node N_i on sensor node N_j, calculated from indirectly given information (i.e. Direct Trust (DT) on N_j) by n neighbor and given to cluster-head (CH).

$$TT_{Ni}(N_j) = W_1 * \sum_{i=1}^{n}(\sum_{j=1}^{n} DT_{Ni}(N_j)) + W_2 * \sum_{i=1}^{n}(\sum_{j=1}^{n} IT_{Ni}(N_j)) \tag{5}$$

Where $TT_{N_i}(N_j)$ is the total trust of node N_i on N_j. Where W_1 and W_2 are the weightage given to DT and IT depending on the applications.

4 Simulation Result and Discussion

Simulation work has been carried in MATLAB and some malicious nodes has been injected intentionally to ascertain the robustness of proposed TBCR-BMA.

Test Bed Setting: Test bed dimension: $500m * 500m$, Initial node deployment: Random, No. of nodes: 150, Node movement: Static, Radio range of node: 30 m, Radio range of base station: Full Network, Sink location: $500m * 500m$, No. of trust metrics: 6, Initial trust metric value: 0.5, Trust value range: 0.0 to 1.0, Broadcast packet size: 25 Byte, Data packet size: 50 Byte, Initial node energy: 3Joule, Transmitter/Receiver circuitry dissipation: 0.5 nJ / bit, Data aggregation Energy (EDA):0.5nJ /bit, Cluster Head Energy Consumption: 0. 7 nJ / bit.

HBMA Parameter Setting: Number of population: 30, No. of drones: 29, No. of broods: 29, Capacity of Spermatheca: 29.

Figure 4 shows the premier phase cluster head selection along with the cluster creation by base station.

A. Alive Node $fig.5$ depicts the percentage of live nodes in the network over 250 simulation rounds.In proposed TBCR-BMA the number of node drained out their energy is less (i.e. more no. of live nodes) as compared to LEACH and TCBMA [5, 6].

B. Average Residual Energy Average remaining energy of nodes in cluster in terms of joules is shown in $fig.6$ over 250 simulation rounds. Here the cluster formation is done only once, so each CH and its members consume less energy as compared to other two methods [5, 6]. Hence our proposed method leaves the CH and its member with more energy.

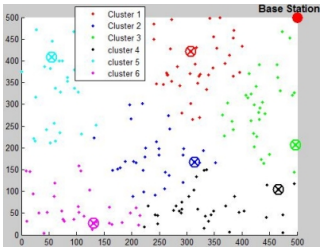

Fig. 4. $P - CH$ selection by base station and cluster creation

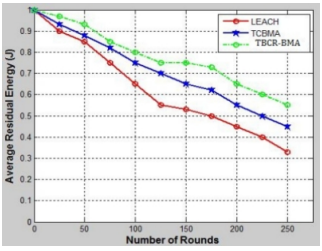

Fig. 5. No. of Alive Nodes

C. Total Energy Consumption From $fig.7$ it is clear that proposed TBCR-BMA has consumed less energy as it deprives the malicious node to become a CH. Also, TBCR-BMA forms the cluster only once. So, TBCR-BMA performs better in 250 rounds as compared to LEACH [5] and TCBMA [6].

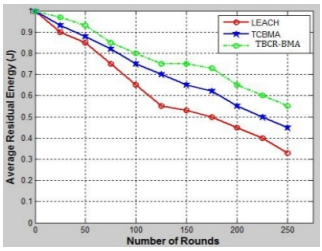

Fig. 6. Average Residual Energy

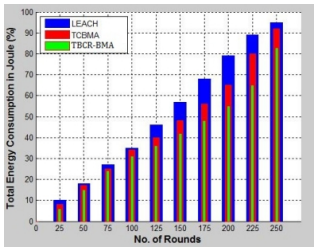

Fig. 7. Total Energy Consumption

5 Conclusion

We have implemented TRUST mechanism to select a benign CH. Malicious node may inject false packet, change destination address or drop data packets. This benign CH will not absorb any harmful activities and prolongs network life time. Furthermore, for balancing the energy consumption among CH_s, we also ensure that the clusters closer to the BS have smaller sizes than those farther away from it. Thus CH_s closer to the BS can also preserve some energy.

References

1. Yick, J., Mukherjee, B., Ghosal, D.: Wireless Sensor Network Survey. Computer Networks 52(12), 2292–2330 (2008)
2. Liu, X.: A Survey on Clustering Routing Protocols in Wireless Sensor Networks. Sensors, 11113–11153 (2012)
3. Abbasi, A.A., Younis, M.: A survey on clustering algorithms for wireless sensor networks. Computer Commununication 30, 2826–2841 (2007)
4. Rajagopalan, R., Varshney, P.K.: Data-aggregation techniques in sensor networks: A survey. IEEE Communication Survey Tutorial 8, 48–63 (2006)
5. Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: Energy- Efficient Communication Protocol for Wireless Microsensor Networks. In: IEEE Proceedings of the Hawaii International Conference on System Sciences, pp. 1–10 (January 2000)
6. Senthilkumar, J., Chandrasekaran, M., Suresh, Y., Arumugam, S., Mohanraj, V.: Advertisement timeout driven bee's mating approach to maintain fair energy level in sensor networks. Applied Soft Computing 12(7), 1884–1890 (2012)
7. Sahoo, R.R., Panda, R., Behera, D.K., Naskar, M.K.: A trust based clustering with Ant Colony Routing in VANET. In: Proceedings of IEEE International Conference on Computing Communication & Networking (ICCCNT), pp. 1–8 (July 2012)
8. Sahoo, R.R., Singh, M., Sardar, A.R., Mohapatra, S., Sarkar, S.K.: TREE-CR: Trust based secure and energy efficient clustering in WSN. In: Proceedings of IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), March 25-26, pp. 532–538 (2013)