Hindawi
Journal of Computer Networks and Communications
Volume 2017, Article ID 1630673, 8 pages
https://doi.org/10.1155/2017/1630673

Research Article

Energy Efficient Secure Trust Based Clustering Algorithm for Mobile Wireless Sensor Network

Eid Rehman, Muhammad Sher, Syed Hussnain Abbas Naqvi, Khan Badar Khan, and Kamran Ullah

Department of Computer Science and Software Engineering and Department of Electrical Engineering, International Islamic University, Islamabad, Pakistan

Correspondence should be addressed to Eid Rehman; eidrehmanktk@gmail.com

Received 22 April 2017; Accepted 12 June 2017; Published 28 August 2017

Academic Editor: Liansheng Tan

The main benefit of selecting a suitable node as cluster head (CH) in clustering for wireless mobile sensor networks (MWSNs) is to prolong the network lifetime. But the safe selection of CH is a challenging task by taking security into account. Mostly CH selection algorithms in MWSN do not consider security when selecting CH. We have proposed secure CH selection algorithm by calculating weight of each node to deal with secure selection using minimum energy consumption. The weight of node is a combination of different metrics including trust metric (behaviors of sensor node) which promotes a secure decision of a CH selection; in terms of this, the node will never be a malicious one. The trust metric is definitive and permits the proposed clustering algorithm to keep away from any malignant node in the area to select a CH, even if the rest of the parameters are in its favor. Other metrics of node include waiting time, connectivity degree, and distance among nodes. The selection of CHs is completed utilizing weights of member nodes. The preparatory outcomes acquired through simulation exhibit the adequacy of our proposed scheme as far as average rate of avoiding malicious node as a CH, energy efficiency, and some other performance parameters are concerned.

1. Introduction

With the rapid and historic advancement in communication technologies over the last two decades, the wireless sensor networks are matured enough as a capable tool for monitoring the physical world [1]. These networks consist of hundreds or even thousands of autonomous microdevices called motes or simply sensor nodes with sensing, processing, and communication capabilities. A typical wireless sensor network consists of a collection of static, mobile, or a mixture of static and mobile sensor nodes which can communicate with each other for exchanging data efficiently. The wireless sensor networks whose all or some sensors have the capability of movement around the deployed area are called Wireless Mobile Sensor networks (WMSN) [2].

The sensor networks are ideally used in commercial, civil, and military applications for continuous event detection and location sensing. WMSN has vast variety of applications including environmental monitoring, observing industry production, oil exploration, acoustic information processing patient monitoring, monitoring of natural or man-made crises like severe weather, earthquakes, volcanic activities, and battle field monitoring [3]. The nodes are limited in the sense of computational power, buffer storage space, and most importantly the energy resources. Grouping sensor into gathering of comparative nature to shape a cluster and select one node as lead to oversee group called cluster head (CH). The CH is dependable to gather information from member nodes and send to the base station for further processing. But due to mobility and frequently change in network topology, the selection of CH is a challenging task. This is because of the way that CHs complete additional work and thus devour more energy contrasted with member nodes during the system operations and this will prompt less than ideal demise causing network partition and in this way disappointment in communication [4].

Similarly because of wireless nature, sensor nodes are more vulnerable to attacks. The typical attacks in MWSNs include replay attack, data forwarding attack, and sinkhole attacks. Unfortunately, the current complex security

algorithms are inadmissible for MWSN in view of the limited capacities of minimal power of node. Trust administration is central to recognize danger, selfish, and unauthorized nodes. Trust in MWSN is the level of a conviction about the behavior of different nodes. Nodes communication with each other, that is, data and control data stream, is the source of getting the proof of trust in a large portion of trust management algorithms [4].

Numerous CH selection algorithms have been proposed for MWSN [5–10]. Most of these CH selection algorithms focus only on energy efficient CH selection. The security aspect of CH nodes is not considered when designing CH selection algorithm. So these algorithms should be designed in such a way which safely chooses CHs by perceiving the bargained hubs and denying them of their CH candidacy in MWSN.

This paper presents energy efficient and secure CH selection algorithm based on member nodes trust and some other metrics. The trust metric is unequivocal and permits the proposed CH selection algorithm to maintain a strategic distance from any danger or compromised nodes in the member node to end up noticeably a CH, regardless of the possibility that the rest of the parameters are to support it. Through trust, nodes behavior can be monitored. Remaining metrics include waiting time, connectivity degree of node, and relative mobility of nodes. The waiting time enables all nodes to hold up before transmitting CH declaration messages to stay away from extreme impact and conflict among the nodes. The connectivity of node degree is the amount of nodes in their communication range and relative mobility shows the nodes relative movement with CH. The CH is selected on the basis of weights of member nodes which are calculated based on these parameters. So this strategy ensures the selection of legitimate CHs with high weights.

We can enumerate the contributions of our paper as follows:

(i) Safely choosing CHs in cluster by perceiving the malicious node and denying them of their CH nomination

(ii) Energy efficient CH selection which maximizes the lifetime of the global network

(iii) Selecting stable CH in cluster which decreases frequency of CH role of change

The rest of the paper is organized as follows. Section 2 provides the literature review of some well-known cluster head selection algorithms for MWSNs. Section 3 describes the proposed scheme. Section 4 presents the energy consumption model and Section 5 discusses mobility model of our scheme. Section 6 describes the simulation results of our proposed scheme.

2. Literature Review

Abbasi and Younis [11] exhibited scientific categorization and order of common bunching plans, then outlined distinctive grouping calculations for WSNs in light of arrangement of variable converge time conventions and consistent converge time, and highlighted their objective, components, complexity, and so forth. LEACH-Mobile (low energy adaptive clustering hierarchy for mobile), in short LEACH-M [6], is a variation of LEACH (low energy adaptive clustering hierarchy), which support node mobility. In LEACH-M, clusters are progressively framed each time the sensor moves, offering high risk of overhead in the cluster setup, but it does not consider the trustworthiness of nodes when clustering.

Wang et al. [12] have proposed LEACH-TM (low energy adaptive clustering hierarchy trust transmission). The authors have formed LEACH-TM tradition by utilizing trust diagrams in which CH sets up multiroute with interchange CHs which are going about as switches. The performance of this scheme was discovered to be superior to LEACH as for energy utilization and number of nodes alive in the network but has no concern about node mobility. Watfa et al. [13] have proposed Battery Aware Reliable Clustering (BARC) protocol. This scheme utilizes trust variable and battery recuperation plan for the determination of CH which makes the system more reliable but does not consider the node mobility of node.

The author [14] proposed a distributed clustering algorithm for mobile wireless sensor networks shortly called ALM, improving the network stability and saving the energy consumption while keeping the network connectivity, but the security of CH gains no attention. Koucheryavy and Salim [15] exhibited the distributed clustering algorithm (DCA) calculation which utilizes satisfactory basis for CH determination in conjunction with heuristic indicators to create unfaltering and adjusted cluster, but clustering the nodes without the trust of nodes.

Trust management system based on neighbor monitoring is proposed [16] for MWNW. In the trust management framework, the trust quality is computed by the neighbor monitoring mechanism and the immediate trust esteem and the roundabout trust quality are consolidated to set up the appropriated trust model to recognize the malevolent nodes. This scheme does not focus on node clustering and CH selection.

Dahane et al. [17] presented an algorithm shortly called TCM, which is completely decentralized and goes for making a virtual topology with the reason to minimize regular reelection of the CH and evade by and large rebuilding of the whole network. This scheme chooses the most powerful and safe CHs with the obligation of checking the node in their cluster and maintaining clusters locally. In spite of the fact that the CH selection algorithms utilizing diverse methodology permit guaranteeing the determination of a CHs construct just in light of their high weights registered from the distinctive metrics, lamentably they do not guarantee that the chosen CHs are legitimated node, which is to say if the decision procedure of CHs is protected or not. The execution of this scheme was discovered superior to the LEACH convention concerning the measurements, for example, percentage of node alive, load balancing, and lifetime of the system. Table 1 shows the comparative analysis of these described schemes.

In this paper, our point is to build up a completely disseminated clustering algorithm with a specific end goal to enhance the energy efficiency, stability in cluster, and safe CH selection in a versatile domain. The most important is

Table 1: Comparative analysis of different schemes.

Scheme	CH selection parameter	Trust	Mobility	CH security
LEACH-M [6]	Random number and remoteness	No	Yes	No
LEACH-TM [12]	Random number and trust value	Yes	No	No
[13]	Battery awareness	Yes	No	No
ALM [14]	Weight	No	Yes	No
DCA [15]	Multiparameters	Yes	Yes	No
[16]	No	Yes	Yes	No
TCM [17]	Weight	Yes	Yes	No

the secure CH selection by observing the behavior of node using node trust management. The trust metric is decisive and allows the proposed CH selection algorithm to avoid any malicious node in the neighborhood to become a CH, even if the remaining metrics are in its favor.

3. Proposed Scheme

The proposed scheme is based on different parameters. So the below following subsections describe these parameters definition and calculation.

3.1. Trust Evaluation. In order to detect misbehaving nodes, each node monitors one or more behavioral aspects of its neighbor nodes. Each behavioral aspect is mapped to define trust metric, while trust metrics are combined into aggregated value called trust value. The value which is based only on nodes self-observations is called direct trust. Nodes may rely on recommendations provided by the neighbors to form an opinion on other nodes trustworthiness, which is called indirect trust. Then, both direct and indirect trust values are combined into the total trust value. The trust calculation is done in specific time interval which is called rounds. In particular, node i will compute total trust of node j as follows in the given equation.

The direct trust of node j is evaluated by node i at time t if these nodes are one-hope neighbor. The proposed cluster scheme is one hope, so node i uses its direct observation toward node j during the periodic trust evaluation round. The following specific detection mechanism has been applied by node i to collect direct observation to evaluate node j, while nodes i and j are one-hop neighbor at time t.

A node's trust worthiness can be evaluated by making qualitative and quantitative analysis of various factor which effect direct trust values. In the proposed scheme, sender is acknowledged (ACK) for sending packets. These factors include the following:

(1) if node i monitors node j, then ratio of received packets is the confirmed amount of acknowledgments (ACK) sent by node j. This ratio will never be larger than node j ratio. According to the change of the ratio, node I can know whether node j has response forging behavior. If the received packets ratio changes in the consecutive time interval (t_i, t_{i-1}) and does not have big difference, then node j works normally [18]. Equation (1) calculates the received packet rate ratio.

$$\mathrm{RP}_{i,j}(t) = \frac{\mathrm{RP}_{ij}(t) - \mathrm{RP}_{ij}(t-1)}{\mathrm{RP}_{ij}(t) + \mathrm{RP}_{ij}(t-1)}. \quad (1)$$

This factor protects from replay ACK attack by monitoring receiving node acknowledged at specific time.

(2) Sending successfully packets rate ($\mathrm{SPF}_{i,j}(t)$): because of wireless nature, it is possible that the same packets are received from different sources, that is, one time directly from sender, and the same packet is also received from another node for further forwarding. Its realized that each packet transmit by node contains a period stamp and can be recognized efficiently regardless of the possibility that the packets have a similar substance. Equation (2) [18] calculates successful sending of packet rate of node j by node i.

$$\mathrm{SPF}_{i,j}(t) = \frac{\mathrm{SP}_{ij}(t)}{\mathrm{SP}_{ij}(t) + \mathrm{SF}_{ij}(t)}, \quad (2)$$

where $\mathrm{SF}_{ij}(t)$ is the requiring number of sent packets and $\mathrm{SF}_{ij}(t)$ is the redundant number of sent packets. This factor effects data forward attack by observing the packets of neighbor nodes.

(3) Rate of data forwarding ($\mathrm{PF}_{i,j}(t)$): it is possible that node j forwards data packets of another node, that is, k, and broadcasts 4 ACK. At that point, node i can gather these ACK packets of node j to acquire the quantity of sending packets. Equation (3) [18] calculates the number of data transmission packets.

$$\mathrm{SF}_{i,j}(t) = \frac{\mathrm{SF}_{ij}(t) - \mathrm{SF}_{ij}(t-1)}{\mathrm{SF}_{ij}(t) + \mathrm{SF}_{ij}(t-1)}. \quad (3)$$

The change rate of $\mathrm{SF}_{i,j}(t)$ effectively protects from Sinkhole attack and additionally determine malicious activity of node.

(4) Factor of availability ($\mathrm{FAV}_{i,j}(t)$): node i transmits HELLO packet for the recognition whether this packet can be gotten by j. On the chance that i gets

the ACK-HELLO from j, it is demonstrated that j is accessible. Equation (4) calculates factor availability of neighboring nodes. Equation (4) calculates factor availability of neighboring nodes.

$$\mathrm{FAV}_{i,j}(t) = \frac{\mathrm{PAV}_{ij}(t)}{\mathrm{PAV}_{ij}(t) + \mathrm{NFAV}_{ij}(t)}, \tag{4}$$

where $\mathrm{PAV}_{ij}(t)$ is the quantity of packets that has been acknowledged and $\mathrm{NFAV}_{ij}(t)$ show the number of packets which has not been acknowledged.

Direct trust ($\mathrm{DT}_{i,j}(t)$) of node i for node j is calculated as in (5) by combining these trust factors.

$$\begin{aligned}\mathrm{DT}_{i,j}(t) = {} & w_1 * \left(1 - \left|\mathrm{RP}_{i,j}(t)\right|\right) + w_2 * \left|\mathrm{SPF}_{i,j}(t)\right| \\ & + w_3 * \left(1 - \left|\mathrm{PF}_{i,j}(t)\right|\right) + w_4 * \left|\mathrm{FAV}_{i,j}(t)\right|.\end{aligned} \tag{5}$$

After the trust calculation, node i classified the behavior of node j based on the trust value. Equation (6) classified the behavior level (BL) of node as normal and malicious node. When node behavior is greater than or equal to .8, then the node is declared as malicious and does not take part in CH selection process.

$$\mathrm{Bl}_j = \frac{1}{\mathrm{DT}_{i,j}(t)}. \tag{6}$$

It is a normal node if $0 \le \mathrm{Bl}_j \le 0.7$.
It is a malicious node if $0.8 \le \mathrm{Bl}_j \le 1$.

3.2. Waiting Time of Node. All sensor nodes calculate the weighting time to decide whether the node itself should be a cluster head or not for themselves. All nodes need to hold up before broadcasting CH declaration messages to evade extreme crash and conflict among the nodes. The waiting time (WI) [19] for node is calculated as follows:

$$\begin{aligned}\mathrm{WT} = {} & \mathrm{WT}_{\max} * \alpha \left[1 - \frac{E_{\mathrm{Residual}}}{E_{\mathrm{initial}}}\right] \\ & * \beta \left[\left|\mathrm{Avg}\left(v_i^k\right) - v_n\right|\right],\end{aligned} \tag{7}$$

where $\mathrm{WT}_{\max}$ is a predefined maximum waiting time. E_{Residual} and E_{initial} mean the amount of residual energy of a node and the amount of initial energy, respectively. $\mathrm{Avg}(v_i^k)$ and v_n indicate the average velocity of the surrounding nodes and the velocity of each node. A higher remaining energy node with the littlest deviation is probably going to be a CH since its waiting time is shorter.

3.3. The Degree of Connectivity D_v of Node i at Time (t). Find the neighborhood of each node v (i.e., nodes communication range) which defines its [20] degree, as in

$$D_v = \left[\left|N_i\right|\right] = \left[\frac{n_i}{\mathrm{dist}(i,j)} < tx_{\mathrm{rang}}\right], \tag{8}$$

where $i \neq j$, tx_{rang} is the communication rang of node, and $\mathrm{dist}(i, j)$ shows the distance between nodes i and j.

3.4. Relative Mobility of Node. Relative mobility (R_m) of nodes represents the relative mobility among sensor nodes and CH, not the sum of vector of velocities. Main purpose is to form stable clusters. So we have to select nodes with low relative mobility as CHs. Relative mobility can be calculated as [21] in

$$R_m = \max_{k=1\cdots k}\left\{\sum_{\forall n_i \in c_k}\sqrt{v_{ni}^2 + v_{ck}^2 - 2v_{ni}^2 v_{nk}^2 \cos\left(\frac{\theta_{ni} - \theta_{ck}}{2}\right)}\right\}, \tag{9}$$

where v_{ck} is the velocity of the CH, v_{ni} is the moving velocity of member sensor nodes, θ_{ni} shows the movement angle of sensor nodes, and θ_{ck} is the movement angle of the CH.

3.5. Cluster Head Selection Algorithm. This section focuses only on the CH selection phase. In order to avoid malicious node selection as a CH that frequently changes its status, it is necessary to select a CH that does not move very quickly and is trusted. The cluster head selection is based on node weight and weight consists of a number of parameters including trust computation, waiting time, degree of connectivity, and relative mobility nodes. Equation (10) has been used for the calculation of node weight.

$$W_i = \mathrm{Bl} * \alpha_1 + \mathrm{WT} * \alpha_2 + D_v * \alpha_3 + R_v * \alpha_4, \tag{10}$$

where $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 1$. The node with the highest weight is selected as a CH in cluster for specific round. The benefit of such an algorithm is to the point that the weight parameters ($\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$) can be adjusted as per the network requirements. The estimations of coefficients α_i ought to be picked relying upon the premise of the significance of every metric in the considered MWSNs applications. The computed weight for every sensor depends on the above parameters ($\mathrm{Bl}, \mathrm{WT}, D_v, R_V$). For instance, it is conceivable to assign a greater value to the metric BL contrasted to other metrics if we promote the safety aspect in the clustering mechanism. It is additionally conceivable to dole out the same worth for every coefficient α_i for the situation where all metrics are considered as having the same significance. Initially, nodes are not associated with any clusters. In order to establish a cluster, each sends "'Hello'" message to its neighboring nodes. When node receives this message, it updates the information which includes the value of its weight metric. Then receiving node compares its metric with others; if its values are smaller, then it waits for an "'INVITE'" message which is sent by another CH for inviting it to join its cluster.

Every node is shown by a state of vector including $N_i d$, weight, and N status. Since the CH has performed different tasks at the same time such as controlling cluster members, data aggregation, and transmission of this data to base station, so CH selection should be periodical after each round because the CH rapidly exhausts their battery. At the beginning of each round, every sensor calculates its weight and broadcasts a hello message to its neighboring nodes. The hello messages consist of two parts weight and node ID and weight and node CH, where node CH is set to zero. A node

Output: CH is Selected with CH-ID;
Data: **Input**: Node-id, Weight
Result: CH Selection
Step 1 N Deploy all the nodes;
Step 2 for $i = 1 \rightarrow N$ **do**
  if $E_i > 0$ && $r \bmod (1/p) \neq 0$ **then**
    Compute Behavior Level (Bl) // given by (6);
    if (Bl ≥ 0.8)
    then
    Declare as Malicious node and not allow then to take part in CH selection
    Else
    Compute Waiting Time // given by (7);
    Compute Degree of Connectivity // given by (8);
    Compute Relative Mobility // given by (9)
  end
end
Step 3 Compute Weight W_i for current round // given (10);
Step 4 for $i = 1 \rightarrow N$ **do**
  If (weight$_i \geq$ weight$_{i+1}$) // if weight of ith node is greater
  $CH_i \equiv$ true;
  else
  $CH_i \equiv$ false // node ith not be a CH
end
Step 5 if $CH_i \equiv$ true **then**
  BC(ADV) $\leftarrow$ broadcast an advertisement message
  //non-CH node i join into the closest CH;
end

Algorithm 1: The proposed CH selection algorithm.

having the greatest weight has been selected as CH for the current round. The selected CH broadcasts an advertisement message (ADV$_C H$) including its state vector to its neighboring nodes requesting them to join it. Each neighboring sensor node receives this message and if it does not belong to any cluster, then it compares its weight to the CH weight. If weight is less than CH weight, then this node accepts request as a CH. Algorithm 1 shows the CH selection process.

4. Energy Consumption Model

Transmission and receiving cost for a distance of d for k-bit can be calculated as follows: transmitting cost for k-bit as

$$E_t = \left(\text{Cic}_{\text{En}} * N_B\right) + \text{Amp}_{\text{EN}} + \text{Dist}^2$$
$$R_E = \left(\text{Cic}_{\text{En}} * N_B\right) n \quad (11)$$
$$\text{Agr}_{\text{EN}} = \left(\text{Cic}_{\text{En}} * N_B * n\right),$$

where E_t is the transmitting cost and Cir_{En} is the energy consumption to run the transmitter circuit. Amp_{EN} is the energy dissipation for the transmission amplifier. The cost of data aggregation is Agr_{EN} and N_B denotes the number of transmitted data bits

Table 2: Simulation parameters.

Mobility model	Random way point
Number of sensor nodes	100
Length of data packet	512 bytes
Length of control packet	50 bytes
Initial energy	.1 joule
Interface queue types	Drop tail
Communication model	Bidirection
Simulation area	100 * 100
Speed	1–10 m/s

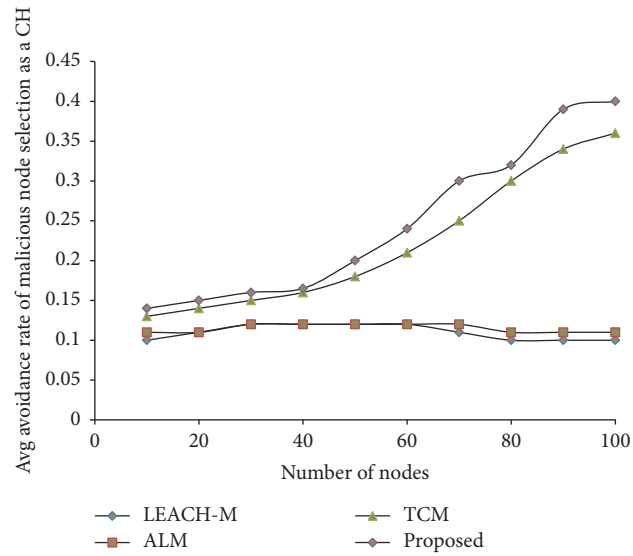

Figure 1: Average avoidance rate of malicious node selection as a CH versus number of nodes.

5. Performance Analysis

The proposed solution has been validated through simulation using Table 2 parameters and comparing its performance with the LEACH-M, ALM, and TCM algorithms. The proposed scheme aims to preserve as less energy as possible by selecting secure CH and consumes less energy. The result comparison among proposed schemes and LEACH-M, ALM, and TCM has been carried out using the following simulation parameters shown in Table 1.

The main objective of the proposed scheme is to secure the CH selection process with minimum energy consumption, so that to avoid malicious nodes selection as a CH. Because CH carries the whole member data, the selection of malicious node as a CH will definitely waste the network resources and data. Figure 1 shows the avoidance rate of malicious nodes selection as a CH. We have deployed 10 nodes as malicious nodes in the whole network to see the avoidance rate of malicious nodes selection. It is clear from Figure 1 that the proposed scheme avoids the malicious node

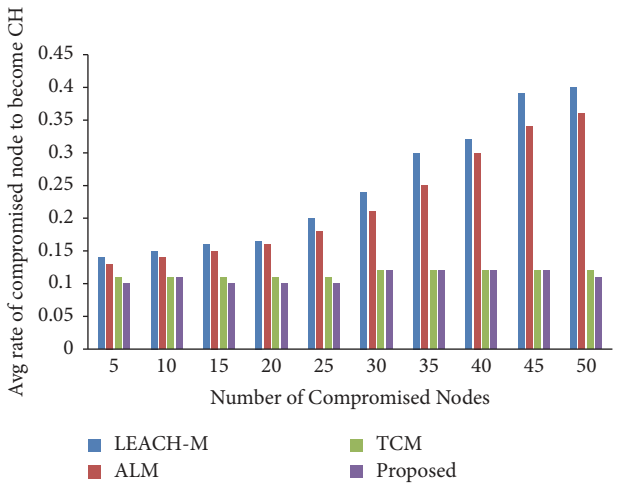

Figure 2: Average rate of compromised node become CH versus number of compromised nodes.

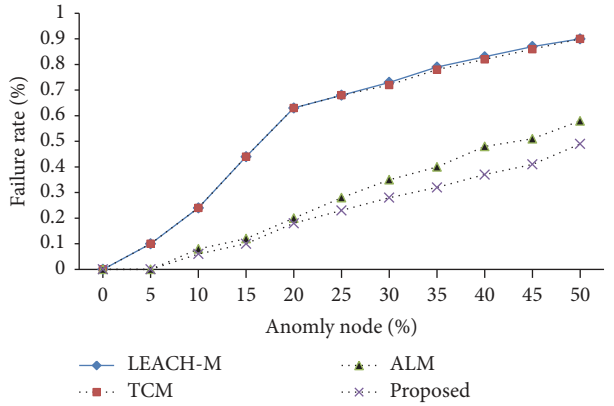

Figure 3: Percentage of failure rate versus anomaly node in parentage.

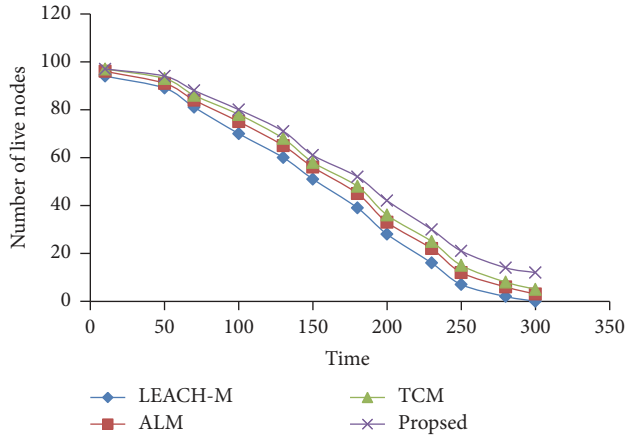

Figure 4: Alive number of nodes versus time.

selection as a CH more efficiently because of node behavior measurement through trust management and also avoidance of unauthorized node to join any cluster.

Average rate that a compromised node turns into a CH is figured by excluding the CH from the entire cluster which was a compromised node and independent from anyone else. This metric represents how well a cluster formation scheme expels compromised nodes. LEACH-M and ALM have no defense mechanism against compromised node and that is why the average rate of compromised node to become CH is too high. Figure 2 shows how many compromised nodes become a CH when the number of compromised nodes increases. It is clear from Figure 2 that our scheme outperforms ALM in spite of the fact that the segregation rate of compromised node is by all accounts too small, and its performance is fairly great in light of the fact that the majority of bargained separators are detached.

We define one failure as an anomaly node selected to be CH; failure rate is to compute coordinate influence of one malicious node, likewise called unsuccessful anomaly detection rate. Generally, when anomaly node rate is low (5), failure rate is 0. As rate goes up, failure rate additionally goes higher. LEACH-M and TCM are schemes with no trust and authentication mechanism, so it performs worse than ALM and the proposed schemes. In contrast, the proposed scheme is a converged model (trust supervision) with a strong defense to anomaly nodes, so it shows the highest robustness. Figure 3 shows the percentage of failure rate of anomaly nodes.

The network lifetime is the time interval from initial deployment of the network until the death of all the live nodes. It can be, for instance, the moment when the remaining sensors die, a percentage of sensors die, the network is partitioned, or the loss of coverage occurs. In the simulation, the proposed scheme measured the time span of the network in which none of the nodes can perform the designated tasks and compared these results with the other approach. Figure 4 shows the comparison of the proposed scheme with other schemes in number of nodes that are alive in network in simulation time. As shown in Figure 4, the lifetime of network increases in the proposed scheme because the reselection of CH cannot occur frequently and is also secure.

Figure 5 shows that nodes died more slowly in the proposed scheme because of stable and trusted nodes selection as a CH. The proposed scheme extends the stability period by selecting suitable CH on the basis of calculated weight using relative trust, less energy consumption ratio, and high success factor. The slow node death rate of the proposed scheme reflected in Figure 5 is to secure efficient and high stability among member and CH.

The average energy consumption ratio of the entire topology is the average distinction between the initial energy and the final level of remaining energy of network. This metric is important because the energy level of the network used is proportional to the networks lifetime. The lower the energy consumption ratio, the longer the networks lifespan. Figure 6 shows energy consumption ratio comparison of the proposed scheme with other schemes. From this chart, it can be seen that the average energy consumption ratio of the proposed scheme is less than LEACH-M, ALM, and TCM, because the proposed scheme first selects most stable and secure CH in cluster.

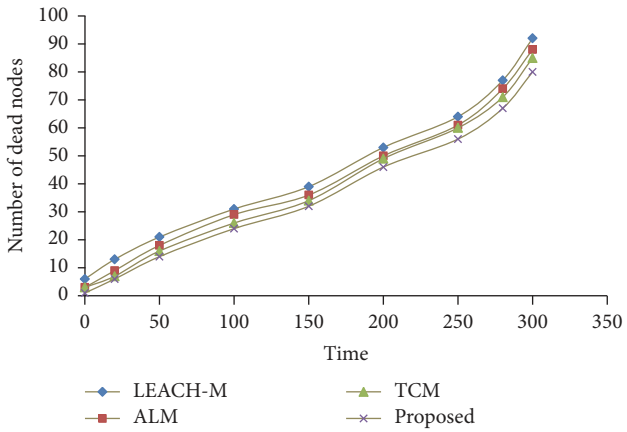

Figure 5: Number of dead nodes and time.

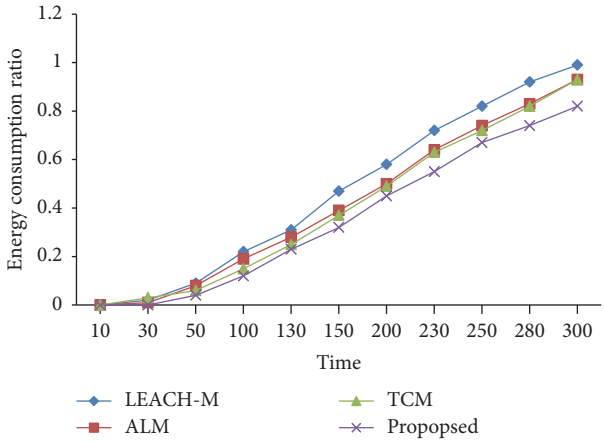

Figure 6: Average energy consumption ratio and time.

6. Conclusion

This paper presented secure CH selection algorithm for minimizing the energy consumption ratio. Most of the CH selection algorithms in MWSN do not consider security when selecting CH. We have proposed secure CH selection algorithm by calculating weight of each node to deal with secure selection using minimum energy consumption. The weight of node is combination of different metrics including trust metric (behaviors of sensor nodes) which allowed a secure CH decision of a CH in the sense where this last node will never be a malicious one. The trust metric is decisive and secure and allows the proposed clustering algorithm to avoid any danger malicious node in the neighborhood to become a CH, even if its remaining metrics are in its favor. Other metrics include waiting time of node, node connectivity degree, and distance among nodes. The simulation demonstrates that the proposed scheme is greatly improved when contrasted with LEACH-M, ALM, and TCM as far as various measurements and energy consumption ratio of network are concerned.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[2] Q. Dong and W. Dargie, "A survey on mobility and mobility-aware MAC protocols in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 88–100, 2011.

[3] H. J. Visser and R. J. M. Vullers, "RF energy harvesting and transport for wireless sensor network applications: principles and requirements," *Proceedings of the IEEE*, vol. 101, no. 6, pp. 1410–1423, 2013.

[4] C. Zhu, L. Shu, T. Hara, L. Wang, S. Nishio, and L. T. Yang, "A survey on communication and data management issues in mobile sensor networks," *Wireless Communications and Mobile Computing*, vol. 14, no. 1, pp. 19–36, 2014.

[5] C.-M. Liu, C.-H. Lee, and L.-C. Wang, "Distributed clustering algorithms for data-gathering in wireless mobile sensor networks," *Journal of Parallel and Distributed Computing*, vol. 67, no. 11, pp. 1187–1200, 2007.

[6] K. Poulose Jacob, V. Paul, and G. Santhosh Kumar, "Mobility metric based leach-mobile protocol," 2008.

[7] M. Lehsaini, H. Guyennet, and M. Feham, "Ces: cluster-based energy-efficient scheme for mobile wireless sensor networks," in *Wireless Sensor and Actor Networks II*, pp. 13–24, Springer, 2008.

[8] M. H. Anisi, A. Hanan Abdullah, and S. Abd Razak, "Efficient data gathering in mobile wireless sensor networks," *Life Science Journal*, vol. 9, no. 4, pp. 2152–2157, 2012.

[9] R. U. Anitha and P. Kamalakkannan, "Energy efficient cluster head selection algorithm in mobile wireless sensor networks," in *Proceedings of the 2013 3rd International Conference on Computer Communication and Informatics, ICCCI 2013*, pp. 1–5, January 2013.

[10] A. Ahmed and S. Qazi, "Cluster head selection algorithm for mobile wireless sensor networks," in *Proceedings of the 2013 7th International Conference on Open Source Systems and Technologies, ICOSST 2013*, pp. 120–125, December 2013.

[11] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer Communications*, vol. 30, no. 14-15, pp. 2826–2841, 2007.

[12] W. Wang, F. Du, and Q. Xu, "An improvement of LEACH routing protocol based on trust for wireless sensor networks," in *Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '09)*, pp. 1–4, Beijing, China, September 2009.

[13] M. K. Watfa, O. Mirza, and J. Kawtharani, "BARC: A Battery Aware Reliable Clustering algorithm for sensor networks," *Journal of Network and Computer Applications*, vol. 32, no. 6, pp. 1183–1193, 2009.

[14] F. D. Tolba, W. Ajib, and A. Obaid, "Distributed clustering algorithm for mobile wireless sensors networks," in *Proceedings of the 12th IEEE SENSORS 2013 Conference*, pp. 1–4, November 2013.

[15] A. Koucheryavy and A. Salim, "Prediction-based clustering algorithm for mobile wireless sensor networks," in *Proceedings of the 12th International Conference on Advanced Communication Technology*, pp. 1209–1215, February 2010.

[16] B. Liu and Y. Wu, "A secure and energy-balanced routing scheme for mobile wireless sensor network," *Wireless Sensor Network*, vol. 07, no. 11, pp. 137–148, 2015.

[17] A. Dahane, N.-E. Berrached, and A. Loukil, "Balanced and safe weighted clustering algorithm for mobile wireless sensor

networks," *IFIP Advances in Information and Communication Technology*, vol. 456, pp. 429–441, 2015.

[18] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory," *Sensors*, vol. 11, no. 2, pp. 1345–1360, 2011.

[19] H. Kim, "Cluster head selection scheme for minimizing the changes of the cluster members considering mobility in mobile wireless sensor networks," in *Proceedings of the 2013 15th International Conference on Advanced Communication Technology (ICACT)*, pp. 285–289, IEEE, 2013.

[20] S. Weber and L. Cheng, "A weighted clustering algorithm for mobile ad hoc networks," *Communications Magazine, IEEE*, 2004.

[21] Y. Zhang, W. Chen, J. Liang, B. Zheng, and S. Jiang, "A network topology control and identity authentication protocol with support for movable sensor nodes," *Sensors*, vol. 15, no. 12, pp. 29958–29969, 2015.