
William W. Guo, and Mark Looi
School of Information and Communication Technology, Central Queensland University, Rockhampton, Australia
Email: {w.guo, m.looi}@cqu.edu.au

Abstract—The adoption of clustering network has extended the lifetime of wireless sensor networks, but it also brings new issues to the network management, including cluster head selection. A number of cluster head selection algorithms have been proposed based on either sensor energy efficiency or sensor trust assessment. The energy-based cluster head selection algorithms assume that all sensors in a cluster are trustworthy. Thus the cluster head selected by such an algorithm is the most powerful node within the cluster but may not be trustworthy in practice. Conversely, the cluster head selected by a trust-based algorithm is the most trustworthy node within the cluster but may not have sufficient power supply. This paper presents a new framework and some reasoning schemes that incorporate the candidates chosen by trust-based cluster head selection algorithms with their energy capacities in different ways for determining a new cluster head. The proposed framework and schemes are easy to implement with a little extra computing cost. Therefore, it has a great potential in wide applications in the future.

Index Terms—Clustering network, cluster head selection, wireless sensor networks, trust-energy balanced scheme

I. INTRODUCTION

Wireless sensor networks (WSNs) have been widely used in monitoring real time changes of physical and chemical conditions in scientific experiments, military, engineering, manufacturing, health care, traffic control, security monitoring and so forth. A wireless sensor is a small and cheap device equipped with sensing, data processing and radio transmission functions powered by low-energy battery for economic viability. However, due to its inability in power replenishment, such sensor has limited capacity in computation, bandwidth and memory [1-3]. WSNs are constructed using such wireless sensors cooperatively and hence also inherit the limitations possessed by individual sensors.

Clustering network is one of the mostly adopted practices in prolonging the life span of WSNs [4-6]. Sensors in a clustering network are grouped into several clusters and each cluster consists of a cluster head and many members. The cluster head is responsible for managing the cluster, allocating jobs to individual members, collecting processed results within the cluster, and communicating with coordinators outside the cluster. Cluster members process tasks assigned by the cluster head, but members can be idle when no task is assigned and thus consume less energy in the expenses of the cluster head that should be running all the time. Although the cluster head consumes more energy than individual cluster members do, a clustering network actually saves the network energy to a large extent overall [7-9].

The adoption of clustering network has extended the lifetime of WSNs, but it also introduces two new problems to the management of the network. The first one is how to select a new cluster head in the event of the current cluster head fading out due to a higher level of energy consumption. The second issue is how to guarantee that the newly selected cluster head has not been compromised due to either malicious temperance or natural alteration of physical properties of sensors deployed in open environment. In the past several years, a number of cluster head selection algorithms have been proposed based on either sensor energy efficiency [2, 3, 9] or sensor trust assessment [1, 5, 10, 11]. However, no result has been reported in combining the two factors together during determining the new cluster head. This paper aims to fill this gap by proposing a new framework and some reasoning schemes that incorporate the candidates chosen by trust-based cluster head election algorithms with the energy status of these candidates in different ways for determining a new cluster head.

In the rest of this paper, a review of both the energy-based and trust-based cluster head selection algorithms proposed in recent literature is presented first. It is followed by a description of our proposed framework and schemes for determining a new cluster head based on the outcomes of the trust-based cluster head election algorithm with considerations of the energy status. Discussions are then incorporated with simulation results, followed by a brief conclusion.

II. REVIEW OF CLUSTER HEAD SELECTION STRATEGIES

A. Energy-based Cluster Head Selection

Cluster routing in WSNs was first proposed in LEACH (low-energy adaptive clustering hierarchy) in order to balance the energy dissipation of individual sensors in a cluster [4]. Since a cluster head consumes more power than members do, the role of cluster head in a cluster is
randomly assigned to any members periodically over time. LEACH has become one of the most popular cluster routing algorithms in WSNs due to its computational simplicity and easy implementation. However, its random selection mechanism cannot guarantee that all members maintain a well-balanced level of energy consumption over time. A number of cluster head selection algorithms based on or modified from LEACH have then been devised since 2000 [2, 3, 9, 12-16].

Although achieving the highest possible level of energy balance in a cluster is desirable when a cluster head is selected every time in theory, the process must be compensated by the computing cost in selecting such a cluster head. Complicated computation may lead to achieving the highest possible level of energy balance in a cluster, but it also consumes more power every time when a selection is called. Therefore, a simple and adaptive cluster head selection strategy should be preferred.

Two simple strategies have been proposed to deal with cluster head selection in different circumstances of request processing in WSNs in [2]. If the request processing requires involvement of all members in a cluster, the sensor with the maximum energy in the cluster should be selected as the cluster head. Otherwise, the sensor with the lowest number of previous selection as the cluster head should be selected as the new cluster head if the request processing requires involvement of only a few members in a cluster. This process is illustrated in Fig. 1.

![Figure 1. An energy-based cluster head selection procedure](image1)

B. Trust-based Cluster Head Selection

Energy-based cluster head selection algorithms assume that all sensors are trustworthy and the selection of a cluster head is only determined by the energy level of a sensor alone. Without input from other members in a cluster in this selection process, a compromised (malicious or faulty) sensor has an equal chance to be selected as the cluster head. To overcome this potential problem in WSNs, a few trust-based algorithms for cluster head election have been proposed [1, 10, 11].

A framework of trust-based cluster head election was proposed in [1], which is illustrated in Fig. 2. In an established cluster, each sensor stores and maintains a trust table of its neighbours based on its observation on and record of the behaviour of all other nodes in its neighbourhood. When the power level of the current cluster head is below a predetermined threshold or the serve of the current cluster head reaches a predetermined period of time, it broadcasts an election message within the cluster. Each node then votes for a new cluster head by replying to the current head with its choice of. The candidate is the top pick in the trust table of a particular node candidate using the pairwise secret key with the cluster head. The current cluster head counts the votes and then decides the winner based on simple majority. The node with the second highest number of votes is selected as the vice cluster head. The purpose of the vice cluster head is to assume cluster head function in the event that the newly elected cluster head fails before taking over the duty from the current head. Simulation shows that this selection mechanism almost never selects a compromised node as the new cluster head in the presence of no more than 15% of compromised nodes in the cluster, much more reliable than the election of cluster head in a similar cluster that doesn’t employ the trust-based election mechanism [1].

![Figure 2. A trust-based cluster head election procedure](image2)
modified for selecting the trust cluster head [11]. Simulations show that both the trust table based and ACS-based algorithms produce almost identical results in trust cluster head election. However, ACS-based applications normally require a high computing cost.

III. A FRAMEWORK OF TRUST-ENERGY BALANCED PROCEDURE (FTEBP) FOR CLUSTER HEAD SELECTION

A. Outline of FTEBP

The cluster head selected by an energy-based algorithm is the most powerful node within the cluster but may not be trustworthy due to the lack of trust assessment during the process. On the other hand, the cluster head selected by a trust-based algorithm is the most trustworthy node within the cluster but may not have sufficient power supply. Thus we propose a framework of trust-energy balanced procedure (FTEBP) for cluster head selection to fill the gap between the trust-based and energy-based selection algorithms. This framework is illustrated in Fig. 3.

![Figure 3. Framework of trust-energy balanced procedure (FTEBP)](image)

Once a new cluster head (CH) election is triggered by whatever a predefined clause, a trust-based election algorithm, preferably adopting a less complicated computational process, is called to select the top $m$ trustworthy sensors as the candidates, rather than only one or two mostly trustworthy nodes in traditional trust-based election algorithms. The energy level of each candidate is then checked by its residual capacity. By doing so, it means that we regard trust more important than energy capacity of any sensor in a cluster. The candidates may not be the most energetic nodes within the cluster, but will be among the most trustworthy ones within the cluster.

The new cluster head is ideally the most powerful node with the highest trust, but this happens rarely. Therefore, a balance must be made between the trust and energy levels of these candidates. In this paper, we propose some trust-energy balanced schemes (TEBS) to achieve this goal, which will be described in the next section in detail. The purpose of TEBS is to select the most capable node from all trustworthy candidates in terms of their Capability that is a capped production of both the trust and energy indexes in different ways for different types of network communications. The top two sensors out of all candidates ranked using TEBS in terms of Capability will be selected to be the new cluster head and its back-up, respectively.

B. Trust-energy Balanced Schemes (TEBS)

TEBS is represented by Capability ($C$) of a sensor, which takes the following general form:

$$C(i) = \alpha t(i)^u e(i)^v,$$  

(1)

where $t(i)$ is the trust index and $e(i)$ is the energy index of sensor $i$; $\alpha$ is a positive constant depending on the nature of the cluster; $u$ and $v$ are positive real values determined according to the types of cluster communications. Capability of any sensor is capped below 1.0, or 100% because both the trust and energy of any sensor cannot be higher than 100%. Using this as the selection criterion, the new cluster head should be the node with the highest Capability, i.e.,

$$CH = \text{Max}[C(i)] = \text{Max}[\alpha t(i)^u e(i)^v], \ (i = 1, \ldots, m) \quad (2)$$

Relative weighting of either trust or energy in capability evaluation can be adjusted by assigning different values to $u$ or $v$ or both in Formula (1). Since $t$ is below 1.0, a $u$ value between 0 and 1.0 will increase the weight of trust in capability evaluation whereas a $u$ value greater than 1.0 will decrease the weighting of trust in the evaluation. The similar effect occurs for energy by changing the $v$ value.

If both trust and energy of a candidate are treated equally as in the natural way without manipulation in capability evaluation, we can define our first trust-energy balanced scheme (Scheme 1) as

$$C(i) = t(i)e(i).$$  

(3)

Since the trust index of a candidate is resulted from the collective assessment given by all its neighbours, we prefer not to manipulate the trust index in capability evaluation. Energy index of a sensor is actually the residual power of the node alone, so we choose to
manipulate the $v$ value to adjust the relative weighting of both the trust and energy in capability evaluation.

If we assign 0.5 and 1.0 to $v$ and $\alpha$ in Formula (1) respectively and keep trust as being, a new trust-energy balanced scheme (Scheme 2) that enlarges the energy term in capability evaluation is defined as

$$C(i) = t(i)\sqrt{e(i)}.$$ (4)

An increase in the energy term means an actual increase in capability even though the trust term remains unchanged. Therefore, this scheme may be more useful when the power consumption of cluster head is usually very low.

If we assign 2.0 and 1.0 to $v$ and $\alpha$ in Formula (1) respectively and keep trust as being, another trust-energy balanced scheme (Scheme 3) that decreases the energy term in capability evaluation is defined as

$$C(i) = t(i)e(i)^2.$$ (5)

A decrease in the energy term means a decrease in capability even though the trust term remains unchanged. Since the energy index is below 1.0, the quadratic operation applied to the energy term accelerates its reduction even further. Therefore, this scheme may be more useful when the power consumption of cluster head is usually very high. In such circumstances, the selection of cluster head moves towards the nodes with a satisfactory level of trust but a higher energy index. This avoids frequently calling for cluster head election.

IV. SIMULATION AND DISCUSSION

Simulation results of the three schemes presented earlier are illustrated in Figs. 4-6, respectively. We are only interested in the outcomes confined within the range of 0.5-1.0 for both trust and energy. Values labelled on contours are Capability values produced by individual schemes.

Scheme 1 is a standard evaluator that treats both trust and energy equally so the distribution of Capability is diagonally symmetric (Fig. 4). Once a minimum satisfactory level of Capability is chosen (i.e., $C \geq 0.7$), the new cluster head should be the candidate whose Capability is the highest among the candidates and graphically within the confined top-right area in Fig. 4. Note that a node with a minimum value of 0.7 for either trust or energy may satisfy a Capability of 0.7 under Scheme 1.

Scheme 2 treats energy more highly than trust so the distribution of Capability is flatter than that of Scheme 1 (Fig. 5). If choosing the same minimum satisfactory Capability of 0.7, the new cluster head will be the candidate whose Capability is the highest among the candidates and graphically within the top one-third area in Fig. 5. This implies that the enlargement of the energy term actually relaxes the requirement on the trust level so that a trust level of 0.5 may still satisfy the threshold of Capability. Therefore, this scheme should be better used when all nodes have a high level of trust. Even this condition is not met, the process of firstly selecting the most trustworthy nodes as candidates should ensure that one of the most trustworthy sensors is selected as the new cluster head eventually.
On the contrary, Scheme 3 reduces weighting of energy in capability evaluation and thus the distribution of Capability is much steeper than that of Scheme 1 (Fig. 6). If choosing the same minimum satisfactory Capability of 0.7, the new cluster head will be the candidate whose Capability is the highest among the candidates and graphically within only a triangular area on the top-right corner in Fig. 6, much smaller than that of Scheme 1 in Fig. 4. This implies that the decrease of the energy term in the evaluation demands an increase in either the trust level or energy index so as to meet the threshold of Capability. Therefore, this scheme should be better used when a highly trustworthy node with sufficient energy supply is needed to coordinate the cluster that may require a huge amount of internal and external communications. Scheme 3 is the most restricted criterion on cluster head selection among the three schemes. Note that no node may satisfy a predefined threshold of Capability against Scheme 3.
We use the following two cases to further illustrate the differences among the three schemes in selecting a new cluster head. Assume that the minimum satisfactory Capability is 0.7 and all sensors have a unique trust level of 0.8; the three reasoning schemes produce different minimum requirements on the energy term accordingly (Fig. 7). Scheme 1 would qualify a node with an energy capacity of >0.875 as a candidate for the cluster head whereas Scheme 2 would pass a sensor with an energy capacity of >0.766 as a candidate for the cluster head. The highest threshold is set by Scheme 3 that demands a minimum energy capacity of 0.935 for a sensor to be considered as a candidate for cluster head.

Assume that the minimum satisfactory Capability is still 0.7 and all sensors have a unique energy capacity of 0.8, correspondingly, the three reasoning schemes set different minimum requirements on the trust term (Fig. 8). Scheme 1 has the same level of demand on trust (>0.875) due to its symmetric nature to the energy term. Scheme 2 would qualify a node with a trust level of >0.783 as a candidate for the cluster head. However, by the standard of Scheme 3, no such sensor would qualify as the candidate for the cluster head. Either a lower Capability...
or higher energy capacity should be set for this scheme to be applicable.

Table 1 and Fig. 9 show an example how the new cluster head and its deputy are selected by applying these three schemes. Five candidates selected from a trust-based process are ranked in terms of the trust level. The corresponding energy index to each candidate is then obtained (Fig. 9a). These data items allow all three schemes to be applied to each case. Scheme 1 selects candidate #3 as the new cluster head and candidate #4 as its deputy (Fig. 9b). Scheme 2 chooses candidate #1 as the new cluster head and candidate #2 as its deputy. Scheme 3 picks candidate #4 as the new cluster head and candidate #3 as its deputy. In the last case, the super power of both candidates #3 and #4 balances off the super trust possessed by candidates #1 and #2. Candidate #5 has near perfect power but its relatively low trust (even though still trustworthy) is not enough to push up its selection.

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Trust (t)</th>
<th>Energy (e)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.95</td>
<td>0.80</td>
</tr>
<tr>
<td>2</td>
<td>0.90</td>
<td>0.85</td>
</tr>
<tr>
<td>3</td>
<td>0.85</td>
<td>0.95</td>
</tr>
<tr>
<td>4</td>
<td>0.80</td>
<td>0.98</td>
</tr>
<tr>
<td>5</td>
<td>0.75</td>
<td>0.99</td>
</tr>
</tbody>
</table>

Table 1. Example of Cluster Head Selection Using TEBS

<table>
<thead>
<tr>
<th>Scheme 1</th>
<th>Trust (t)</th>
<th>Energy (e)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.680</td>
<td>0.765</td>
<td>0.784</td>
</tr>
<tr>
<td>Scheme 2</td>
<td>0.850</td>
<td>0.830</td>
</tr>
<tr>
<td>Scheme 3</td>
<td>0.608</td>
<td>0.792</td>
</tr>
</tbody>
</table>

Note: Cluster head is in bold and its deputy is in italic bold.

V. CONCLUSION

The energy-based cluster head selection algorithms assume that all sensors in a cluster are trustworthy so the cluster head selected from such an algorithm is the most powerful node within the cluster but may not be trustworthy in practice. Conversely, the cluster head selected from a trust-based algorithm is the most trustworthy node within the cluster but may not have sufficient power supply. A framework of trust-energy balanced procedure (FTEBP) is proposed in this paper to combine the two selection strategies together for choosing a new cluster head. FTEBP determines the new cluster head based on the trust-energy balanced schemes (TEBS) that select the most capable sensor in terms of a new parameter Capability among the candidates chosen by a trust-based process in a cluster. Depending on the types of communications within a WSN, different schemes can be used to select the most appropriate sensor as the cluster head. The proposed framework and schemes are also easy to implement with a little extra computing cost. Therefore, it has a great potential in wide applications in the future.

REFERENCES


William W. Guo received his PhD from The University of Western Australia in 1999. After two years as postdoctoral research fellow at Curtin University and Edith Cowan University in Australia, he has been a faculty member at Edith Cowan University and then Central Queensland University since 2002. He is now a senior lecturer and Chair of ICT Postgraduate Programs Committee in the School of Information and Commmation Technology at Central Queensland University. His research interests include computational intelligence and applications, image processing, data mining and modelling, business intelligence and security. He has published more than fifty papers in international journals, edited books and conference proceedings in these areas. He is a member of IEEE, ACM, and ACS and a regular reviewer for many international journals.

Mark Looi received his PhD from Queensland University of Technology in Australia. He was a professor in security and Head of Computer Science Department at Queensland University of Technology for many years before joining Central Queensland University in 2011. He is now a professor and Dean of School of Information and Communication Technology. His research interests include network security, security audits and reviews, security policies, and smart cards. He has supervised many PhD students to completion and published many papers in these areas in international journals, edited books and conference proceedings. He is a member of IEEE and a Fellow of ACS.