# Energy Aware and Trust Based Cluster Head Selection for Ad-hoc Sensor Networks

Zhe Wei[1] and Shuyan Yu[2]
(Corresponding author: Zhe Wei)

School of Computer Science, Civil Aviation Flight University of China[1]
46 Nanchang Rd 4th Section, Guanghan 618300, China
(Email: findwei@foxmail.com)
College of Management and Information, Zhejiang Post and Telecommunication College[2]

(Received May 1, 2017; revised and accepted July 5 & Aug. 20, 2017)

## Abstract

Clustering provides an efficient management method and energy balancing scheme for ad-hoc sensor networks. Cluster head is the most important role in a cluster and it acts as a local data coordinator and maintains cluster information. Once malicious nodes or lower energy nodes are selected as cluster heads, the system would be greatly affected. Thus selection of trusted cluster heads with proper residual energy becomes critical for the overall network performance. In this research, we propose an energy aware and trust based cluster head selection method for ad-hoc sensor networks. The proposed method relies on an effective distributed trust model for cluster head selection and it also considers the residual energy in the selection process. Simulations show that more trusted nodes with proper residual energy are selected as cluster heads, which in turn provides a higher packet delivery ratio from the cluster member nodes to the base station and a better balanced energy consumption of the network.

*Keywords: Ad-hoc Sensor Network; Cluster Head Selection; Energy Aware; Trust*

## 1 Introduction

Ad-hoc sensor networks normally consist of spatially distributed devices using wireless sensor nodes to collaboratively collect, process, and transmit physical or environmental parameters [21]. In practice, individual sensor nodes collet data of interest, process them locally for certain purposes, and send the processed data to the base station directly or indirectly with the help of intermediate nodes [15]. Autonomy is one of the most important characteristics of ad-hoc sensor networks where each node is self-configured without the centralized administration. Further, ad-hoc sensor networks are instant in that no pre-established infrastructure is needed for the network deployment, so they have been used for a variety of applications such as security surveillance, intrusion detection, disaster management, animal tracking and so on.

To ensure the full functioning of the various applications, security is an important issue to be addressed for the autonomous and unattended ad-hoc sensor networks [14]. This is because sensor nodes are vulnerable to attacks such as selective forwarding attack, Sybil attack and wormhole attack. Most security solutions like cryptography are software based and they are designed to mainly deal with the outside attacks for traditional networks, but such soft security is hard to be implemented in sensor nodes to counter the attacks especially from inside malicious nodes. To solve this problem, trusted computing [4] has been adopted to tackle the malicious nodes within the network. Trust is essentially a stimulating mechanism for nodes' cooperation and its computing is based on a node's action or behavior such as delivering or dropping data packets upon request. Under trust mechanism, higher trust nodes will receive more services from its peers and less trust nodes get fewer or no services from the others. Sensor nodes are also featured with limited power supply and they are usually disposed when their batteries are exhausted. Clustering techniques [22] provide an efficient energy balancing method for the sensor network. In a clustering scheme, all the nodes in the network are virtually partitioned into sub networks called clusters. In each cluster, member nodes have one or more elected Cluster Heads (CHs). CH is the most important element in a cluster and it acts as a local coordinator for data transmission within the cluster and maintains the cluster members and topology information [20].

However, once the malicious nodes are selected as CHs, the system performance would be greatly affected since all the member nodes depend on CHs for packet transmission to their respective destinations. In addition, some CHs with high trust value will be repetitively selected, which drains their energy faster. In this context, selection of trusted CHs with proper residual energy becomes critical for the overall network performance. In this research, we propose an Energy Aware and Trust (EAT) based CH selection method for ad-hoc sensor networks. The proposed method relies on an effective distributed trust model and it also considers the residual energy in the process of CH selection.

The rest of this article is organized as follows. Section 2 discusses the related work about the classical node clustering algorithm and the trust computing, Section 3 describes the proposed CH election method, simulation tests are carried out in Section 4, and the conclusions and the future research are discussed in Section 5.

## 2 Related Work

LEACH (Low Energy Adaptive Clustering Hierarchy protocol) [9] is a classical hierarchical clustering algorithm for wireless sensor networks (WSNs) and many clustering algorithms such as C-LEACH [18], P-LEACH [12], A-LEACH [2], H-LEACH [3], N-LEACH [16], K-LEACH [24], E-LEACH [26], T-LEACH [11], W-LEACH [23], V-LEACH [1], LEACH-FL [8], and LEACH-ERE [13] have derived from LEACH by either modifying the threshold criteria or optimizing the algorithm parameters.

In LEACH, clustering is based on the signal strength and CHs are randomly selected. The operation process for LEACH is split into rounds and each round consists of the setup phase and the steady phase. In the setup phase, each sensor node that has not been selected as CH chooses a random number between 0 and 1 to decide whether it will become a CH or not for the current round. The decision of a node to be a CH is independent of other nodes. If the number of a sensor node is less than the predefined threshold value $T(n)$, this sensor node will convert from an ordinary node into a CH for the current round. The threshold $T(n)$ is defined by

$$T(n) = \begin{cases} \frac{p}{1-p*(r\,mod\,\frac{1}{p})} & if\; n \in G \\ 0 & otherwise \end{cases}$$

Where $r$ denotes the current round, $G$ represents the set of nodes that have not been selected as CHs in the last $\frac{1}{p}$ rounds, $p$ is a pre-determined percentage of CHs in the round, and $n$ is the number of nodes in the network. After a node is elected, it informs the member nodes about its election as CH through advertisement packet. Upon receiving the advertisement packet, the member node sends its ID in the join packet to the CH. In the steady phase, member nodes collect and transmit data to their CHs which aggregate the received data and forward these data to the BS. After a given period of time, the algorithm returns to the setup phase and enters into a new round of CH selection. LEACH balances the energy consumption of cluster members by rotating the CH, but the drawback of LEACH is that the CH selection is random without considering node's residual energy.

Trust and reputation mechanisms [7, 19, 25] have been gradually studied by researchers. In the trust computing, trust is defined as the degree of beliefs about the behaviors of others and it can help to identify the malicious nodes, predict the future behavior of a node, and select trustworthy nodes under certain trust strategies. The basis of trust mechanism is that its calculation is either directly based on the historical behaviors of participating nodes or indirectly based on the references from other nodes. Among these models, Bayesian theory that attempts to discover the behavior patterns through historical actions fundamentally complies with the procedure of trust evaluation. Bayesian based trust computing first calculates the prior probability of an event, then applies the prior probability into the binomial distribution, and finally modifies or updates such probability by using a posterior inference according to the relevant evidences [25].

RFSN (Reputation based Framework for high integrity Sensor Networks) [7] is a representative application of Bayesian theory for the trust computing. In RFSN, each sensor holds trust metrics representing past behaviors of other nodes in order to predict these nodes' future behaviors. According to the trust metrics built for other nodes by the behavior monitoring, a sensor node can rate them as *positive* or *negative* and evaluate the trustworthiness of these nodes. RFSN uses a completely decentralized management manner and can run on each sensor node, the latter of which in RFSN only interacts with nodes within its wireless communication range and thus only maintains the reputation of nodes in its vicinity. In RFSN, a transaction is defined as two nodes making an exchange of information or participating in a collaborative process. After each transaction, one partner will rate the other as *cooperative* or not. Let $\Theta$ represent the probability that a certain node will cooperate when asked to exchange information in RFSN, and a prior distribution that reflects the probability that a node would cooperate with another one is defined by

$$P(\Theta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\Theta^{\alpha-1}(1-\Theta)^{\beta-1}$$

where $0 \leq \Theta \leq 1, \alpha \geq 0$, and $\beta \geq 0$. $\Theta$ can be used as the success probability in Bernoulli observations. For example, let $T \in [0,1]$ be the node *i's* rating for node $j$ in one transaction, then

$$P(T|\Theta) = \Theta^{T}(1-\Theta)^{1-T}$$

After the transaction the posterior of $\Theta$ is:

$$P(\Theta|T) = \frac{P(T|\Theta)P(\Theta)}{\int P(T|\Theta)P(\Theta)d\Theta} \sim Beta(\alpha+T, \beta+1-T)$$

The mathematical expectation of $\Theta$ is:

$$E(\Theta) = \frac{\alpha+T}{\alpha+T+\beta+1-T} \quad (1)$$

In Equation (1), $E(\Theta)$ can be regarded as the trust value of a node, and the shape parameter ($\alpha$, $\beta$) can be interpreted as the observed number of positive outcomes (cooperation) and the observed number of negative outcomes (non-cooperation) in one transaction respectively. According to Equation (1), the limitation of the trust calculation in RFSN is that trust has to be computed after each transaction so as to update the trust values.

# 3 EAT Based CH Selection

## 3.1 Energy Model

In the proposed method, the information of remaining energy about each sensor node is exchanged periodically among one-hop neighbors and based on [10], when $k$-bit data packet is transmitted within distance $d$ in ad-hoc sensor networks, the transmitter energy consumption $E_t(k, d)$ is defined by

$$E_t(k,d) = \begin{cases} kE_{elec} + k\varepsilon_{FS}d^2 & d < d_0 \\ kE_{elec} + k\varepsilon_{MP}d^4 & d \geq d_0 \end{cases}$$

where $E_{elec}$ is the electronics energy such as signal coding and spreading, $\varepsilon_{FS}d^2$ and $\varepsilon_{MP}d^4$ are the amplifier energy in the free space fading channel with $d^2$ power loss and multi path fading channel with $d^4$ power loss respectively. If the distance $d$ is less than the predefined threshold $d_0$, the power loss can be modeled as the free space model, or else, if $d$ is greater than or equal to $d_0$, the power loss is modeled as the multi path model. After receiving this $k$-bit data packet, the receiver energy consumption $E_r(k)$ is defined by

$$E_r(k) = kE_{elec}$$

Thus the remaining energy of a certain node $i$ is

$$E_{remaining} = E_{initial} - E_t(k,d) - Er(k)$$

In practice, the free space model is used and a threshold $E_{threshold} = 0.00005J$ is set so as to check whether a node has enough remaining energy to work as a CH.

## 3.2 Trust Calculation

Unlike the binomial distribution based trust method in RFSN, *negative* binomial distribution based method is more flexible and with more applications. In our previous work [25], we proposed a negative binomial distribution based trust that can well be applied in WSNs. The definition is as follows.

$$E(\Theta) = \frac{\alpha + r}{\alpha + \beta + r + s} \tag{2}$$

where $r$ and $s$ are the corresponding increments, $E(\Theta)$ and the shape parameter ($\alpha$, $\beta$) has the similar meanings to those in Equation (1), but the increment in Equation (2) can be 2 or more and neighboring nodes need not update the trust of the monitored node every time. For example, many newly designed MAC protocols such as SW-MAC [17] and ASS-MAC [5] support sleep mode in sensor networks where sleep-wake scheduling is set to achieve the energy efficiency in communications and the energy consumption can be significantly reduced by putting nodes into sleep state when their services are not needed for certain period of time [17]. It means that nodes in sleep mode cannot respond to the requests from others. Assume node $j$ makes a series of requests within a fixed period of time $\Delta T$ from node $i$ and $i$ works alternatively between sleep and wake mode during the requests. If $j$ receives $r(\Delta T)$ positive outcomes and $s(\Delta T)$ negative outcomes from $i$ within $\Delta T$, then the trust value of $i$ maintained by $j$ is defined by

Table 1: Algorithm of EAT based CH selection

**Algorithm**

```
//Use LEACH to form clusters in the sensor network.
//In each round, the CH is selected as follows.
Input:  Cluster members
Output: CH of a cluster
Begin
loop1: for(i=1;i<=ClusterNumber;i++)
            if (MaxTrust < Trust[i]){
                MaxTrust=Trust[i];
                j=i;}
          if ($E_{remaining}(j)$ >= $E_{threshold}$)
                Node j is selected as CH;
            else {
              ClusterNumber−−;
              remove Node j from the ClusterNumber;
              goto loop1; }
End
```

$$E_{i,j}(\Theta) = \frac{\alpha_{i,j} + r_{i,j}(\Delta T)}{\alpha_{i,j} + \beta_{i,j} + r_{i,j}(\Delta T) + s_{i,j}(\Delta T)}$$

Further, trust from the third parties should be added as indirect references. According to the *D-S* belief theory [6], suppose $j$ receive the trust about $i$ from $h$. Let $(\alpha_i^h, \beta_i^h)$ denote such indirect trust and $j$ has the past trust values about $i$ and $h$ that are denoted by $(\alpha_i, \beta_i)$ and $(\alpha_h, \beta_h)$ respectively. Thus combined with indirect trust from $h$, the shape parameters are redefined by

$$\alpha_i^{'} = \alpha_i + \frac{2\alpha_h\alpha_i^h}{(\beta_h + 2) + (\alpha_i^h + \beta_i^h + 2) + 2\alpha_h}$$

$$\beta_i^{'} = \beta_i + \frac{2\alpha_h\beta_i^h}{(\beta_h + 2) + (\alpha_i^h + \beta_i^h + 2) + 2\alpha_h}$$

where $\alpha_i^{'}$ and $\beta_i^{'}$ are the direct-indirect integrated trust parameters about node $i$ respectively. The proposed CH selection algorithm is presented in Table 1 and in case no qualified CH is selected in the current round, a random node within the cluster is designated as the acting CH.

# 4 Simulations

The problem that this study deals with is to select CHs with descent trust value and proper residual energy so as to effectively prevent malicious nodes from becoming CHs and efficiently balance the energy consumption of the network. Although LEACH can balance the energy consumption of cluster members by rotating the CH, the drawback is that the CH selection is random without considering node's residual energy and trust values. Thus both malicious nodes and nodes with low residual energy can become CHs in LEACH, which could deteriorate the system performance. In this section, to test the performance of the proposed method, NS-2 is used for the simulation and LEACH is selected for comparison.

## 4.1 Settings

Assume that 500 sensor nodes are randomly deployed in a $400m$*$400m$ square region. The BS is set at the center of the area and all the CHs can directly communicate with the BS. When requested by the BS, all cluster members send fixed 200-sized data packets containing node ID and meaningful information directly to the CH through which these packets are transmitted to the BS. Suppose that there are 10% evenly deployed malicious nodes, and when working as cluster members they selectively send void data packets to the CH in order to drain the network energy, and when these malicious nodes are selected as CHs, they randomly drop some or all the data packets sent by the cluster members. It is also assumed that new round of CH selection is carried out in every 20 requests from the BS. Other settings are as follows: the initial reputation of each node is 0.5; 802.11 protocol with TDMA and sleep mode is implemented in MAC; $EI = 0.5J$, $E_{elec} = 50nJ/bit$, $d = 1m$, and $\varepsilon_{fs}d^2 = 10pJ/bit/m^2$; the channel bandwidth is set to 1 Mb/s; sensor nodes are capable of bidirectional communication on every link and they work in the promiscuous mode so that nodes can over hear the ongoing packets from its neighbors.

## 4.2 Test 1

Under ideal conditions, CHs are the trusted entities for packet transmission and data packets from the cluster member nodes should be completely transmitted by the corresponding CHs to the BS. But due to the existence of malicious nodes or malicious CHs, not all the CHs are trusted and some packets may not be delivered by malicious CHs and eventually cannot reach the BS. In this part, CH average trust value and the packet delivery ratio are tested and results are presented in Figure 1 and Figure 2 respectively.

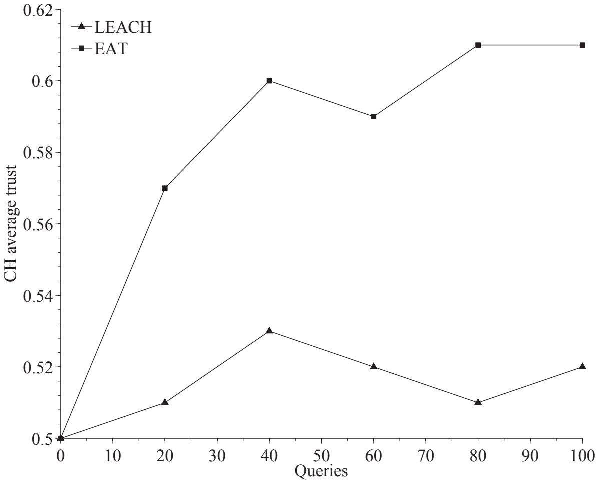

Figure 1: CH average trust

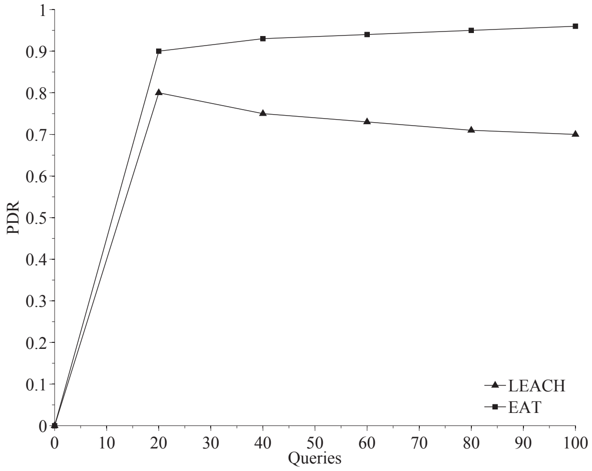

Figure 2: Packet delivery ratio

In LEACH, malicious nodes can be selected as CHs without any prevention, thus the CH average trust in LEACH fluctuates around 0.52 during the queries as can be noticed in Figure 1. It indicates that some selected CHs have lower trust values than 0.5 and these CHs could present malicious behaviors such as dropping the packets sent from the member nodes in the current scenario. While in EAT, the CH average trust increases steadily and reach about 0.61 on the 100th query meaning that more and more trusted nodes are selected as CHs.

**Definition 1.** *Packet deliver ratio, or PDR is the number of packets received by the BS to the number of packets sent by the member sensor nodes.*

In Figure 2, as the query number increases, the PDR in LEACH reaches its maximum value around 0.8 on the 20th query and then drops constantly and reaches around 0.7 on the 100th query. This is because in LEACH malicious nodes can be selected as CHs without any precautions. Once malicious nodes become CHs, they can do considerable damage to the network such as dropping some or all the received packets from the cluster member nodes in this case. On contrast, EAT can maintain

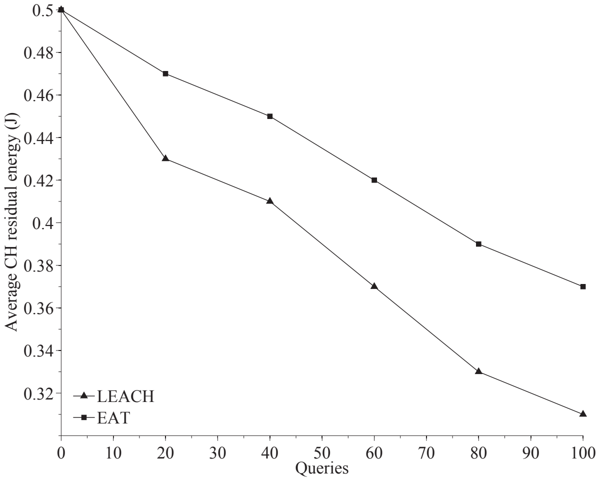

Figure 3: Average CH residual energy

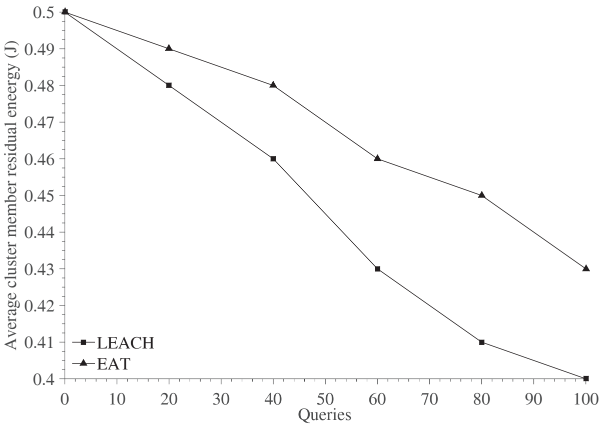

Figure 4: Average cluster member residual energy

a higher PDR during the queries by incorporating trust mechanism and avoiding malicious nodes becoming CHs and hence can obtain PDR about 0.95 on the 100th query. Compared to LEACH, EAT has an average of 19.8% improvement in PDR.

### 4.3 Test 2

In this part, the average CH residual energy and the average cluster member residual energy are tested and results are shown in Figure 3 and Figure 4 respectively.

In Figure 3, the average CH residual energy in both methods declines as the query goes on, but EAT always maintain a higher average residual energy than LEACH, e.g., about 0.46J and 0.41J respectively on the 40th query. It indicates that by considering the node residual energy during the CH selection, EAT can choose the potential candidate CH with more residual energy. By contrast, LEACH rotates the CH and randomly selects the CH without taking the remaining energy into consideration resulting in lower average CH residual energy than EAT. It can also be found in Figure 1 and Figure 3 that EAT can not only maintain a higher CH trust value but also keep a higher average CH residual energy than LEACH.

The similar result can be found in Figure 4 that in EAT, the average cluster member residual energy is always higher than LEACH, e.g., about 0.46J and 0.43J respectively on the 60th query. It indicates that EAT can better balance the energy consumption within the clusters. Compared to LEACH, EAT has an average of 4.2% improvement regarding the average CH residual energy and 2.2% improvement on the average cluster member residual energy.

## 5 Conclusions

Improper CH selection could severely degrade the performance of the clustered ad-hoc sensor networks especially when malicious nodes or low-energy nodes are selected and become CHs. In this study, with the help of trust mechanism and by considering nodes' residual energy, an energy aware and trusted CH selection method is proposed aiming to select CHs with descent trust value and proper residual energy. Simulation tests have confirmed that the proposed method can effectively prevent malicious nodes from becoming CHs and efficiently balance the energy consumption of the network. But due to the random behavior of malicious nodes, some malicious nodes can still be elected as CHs in the proposed method as can be seen the PDR test. Thus how to further enhance the PDR and better spot the malicious nodes with more different random misbehaving patterns will be our future work.

## Acknowledgment

This work is partially supported by the National Science Foundation of China under grant No. 61073177, the Scientific Research Program of CAFUC under grant Nos. J2018-03, F2017KF02, J2013-41, and Q2014-053. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which has improved the presentation.

## References

[1] A. Ahlawat and V. Malik, "An extended vice-cluster selection approach to improve LEACH protocol in WSN," *International Conference on Advanced Computing & Communication Technologies*, pp. 236-240, 2013.

[2] M. Ali, T. Dey and R. Biswas, "ALEACH: Advanced LEACH routing protocol for wireless microsensor networks," in *Proceedings of the International Conference on Electrical and Computer Engineering*, pp. 909-914, 2008.

[3] A. Azim and M. Islam, "Hybrid LEACH: A relay node based low energy adaptive clustering hierarchy for wireless sensor networks," in *Proceedings of IEEE Malaysia International Conference on Communication*, pp. 911-916, 2009.

[4] D. Challener, K. Yoder, and R. Catherman, "A practical guide to trusted computing," *Pearson Education*, 2007.

[5] I. Dbibih and *et al.*, "ASS-MAC: adaptive sleeping sensor MAC protocol designed for wireless sensor networks," in *International Conference on Information Technology for Organizations Development*, pp. 1-5, 2016.

[6] A. Dempster, "Upper and lower probabilities induced by multivalued mapping," *The Annals of Mathematical Statistics*, vol. 38, no. 2, pp. 325-339, 1967.

[7] S. Ganeriwal, *et al.*, "Reputation based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 3, pp. 15-37, 2008.

[8] R. Ge, H. Zhang and S. Gong, "Improving on LEACH protocol of wireless sensor networks using fuzzy logic," *Journal of Information & Computational Science*, vol. 7, no. 3, pp. 767-775, 2010.

[9] W. B. Heizelman, A. P. Chandrakasan and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Sensor Communications*, vol. 1, no. 4, pp. 660-670, 2002.

[10] W. B. Heinzelman, *et al.*, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660-670, 2002.

[11] R. Hou, W. Ren and Y. Zhang, "A wireless sensor network clustering algorithm based on energy and distance," in *Proceedings of the International Workshop on Computer Science and Engineering*, pp. 439-442, 2009.

[12] K. Jin, Y. Zhang and D. Tian, "Based on the improvement of leach protocol for wireless sensor network routing algorithm," in *Proceedings of the International Conference on Intelligent System Design and Engineering Application*, pp. 1525-1528, 2012.

[13] J. Lee and W. Cheng, "Fuzzy logic based clustering approach for wireless sensor networks using energy predication," *IEEE Sensors Journal*, vol. 12, no. 9, pp. 2891-2897, 2012.

[14] C. T. Li and M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks," *Information Sciences*, vol. 181, no. 23, pp. 5333-5347, 2011.

[15] C. T. Li, M. S. Hwang, C. Y. Liu, "An electronic voting protocol with deniable authentication for mobile Ad hoc networks," *Computer Communications*, vol. 31, no. 10, pp. 2534–2540, June 2008.

[16] Y. Li, L. Ding and F. Liu, "The improvement of LEACH protocol in WSN," in *Proceedings of the International Conference on Computer Science and Network Technology*, pp. 1345-1348, 2011.

[17] L. Liang and *et al.*, "SW-MAC: a low-latency mac protocol with adaptive sleeping for wireless sensor networks," *Wireless Personal Communications*, vol. 77, no. 2, pp. 1191-1211, 2014.

[18] R. Mehta, A. Pandey and P. Kapadia, "Reforming clusters using C-LEACH in wireless sensor networks," in *Proceedings of the International Conference on Computer Communication and Information*, pp. 1-4, 2012.

[19] P. Mukherjee and S. Sen, "Comparing reputation schemes for detecting malicious nodes in sensor networks," *The Computer Journal*, vol. 3, no. 54, pp. 482-498, 2011.

[20] R. Mylsamy and S. Sankaranarayanan, "A preference-based protocol for trust and head selection for cluster-based MANET," *Wireless Personal Communications*, vol. 86, no. 3, pp. 1611-1627, 2016

[21] Y. B. Sailed and A. Olivereau, "A lightweight threat detection system for industrial wireless sensor networks," *International Journal of Network Security*, vol. 18, no. 5, pp. 842-854, 2016.

[22] T. Sanu and M. Thomaskutty, "Lossless address data compression using quadtree clustering of the sensors in a grid based WSN," *Ad Hoc Networks*, vol. 56, pp. 84-95, 2017.

[23] C. So-In, *et al*, "Performance evaluation of LEACH on cluster head selection techniques in wireless sensor networks," in *Proceedings of the International Conference on Computer and Information Technology*, pp. 51-61, 2013.

[24] M. Thein and T. Thein, "An energy efficient cluster-head selection for wireless sensor networks," in *Proceedings of the International Conference on Intelligent System, Modeling and Simulation*, pp. 287-291, 2010.

[25] F. Wang, *et al.*, "SONR: A reliable reputation system of self organized network," *Journal of Network and Computer Applications*, vol. 35, pp. 914-926, 2012.

[26] J. Xu and *et al.*, "Improvement of LEACH protocol for WSN," in *Proceedings of the International Conference on Fuzzy System and Knowledge Discovery*, pp. 2174-2177, 2012.

# Biography

**Zhe Wei** received his Ph.D. degree in computer science and technology in 2015. Now he is a lecturer in Civil Aviation Flight University of China. His main research includes WSN security and applications.

**Shuyan Yu** received her master degree in software engineering in 2006. Now she is an associate professor in Zhejiang Post and Telecommunication College. Her main research includes computer security and applications.