EETCA: Energy Efficient Trustworthy Clustering Algorithm for WSN

T. Senthil[1] and Dr. B. Kannapiran[2]
[1] Assistant Professor, Kalasalingam University, Krishnankoil, India
[2] Associate Professor, Kalasalingam University, Krishnankoil, India
*Corresponding author: T. Senthil

Received March 15, 2016; revised July 19, 2016; revised September 20, 2016; accepted October 15, 2016; published November 30, 2016

Abstract

A Wireless Sensor Network (WSN) is composed of several sensor nodes which are severely restricted to energy and memory. Energy is the lifeblood of sensors and thus energy conservation is a critical necessity of WSN. This paper proposes a clustering algorithm namely Energy Efficient Trustworthy Clustering algorithm (EETCA), which focuses on three phases such as chief node election, chief node recycling process and bi-level trust computation. The chief node election is achieved by Dempster-Shafer theory based on trust. In the second phase, the selected chief node is recycled with respect to the current available energy. The final phase is concerned with the computation of bi-level trust, which is triggered for every time interval. This is to check the trustworthiness of the participating nodes. The nodes below the fixed trust threshold are blocked, so as to ensure trustworthiness. The system consumes lesser energy, as all the nodes behave normally and unwanted energy consumption is completely weeded out. The experimental results of EETCA are satisfactory in terms of reduced energy consumption and prolonged lifetime of the network.

Keywords: WSN, network lifetime, clustering, trust, energy efficiency

1. Introduction

Wireless Sensor Networks (WSN) has gained substantial research interest, owing to the advancement of wireless communications. A WSN consists of numerous interconnected sensor nodes without any physical medium [1, 2]. With this captivating capability, WSN can be effectively deployed, even in human inaccessible areas. Thus, WSN is the popular solution for creating emergency network, all at once. Some of the major applications of WSN are emergent networks, combat ground monitoring, healthcare monitoring and so on [3, 4].

The sensor nodes are responsible for sensing, processing the data and communicating with other sensor nodes. These sensor nodes work in an orchestrated fashion to achieve common goal. All the tasks to be achieved depend solely on the energy or battery of the sensor nodes. As the WSN mainly serves for emergent situations, it is impossible to replace or recharge the batteries of the sensors. WSNs are energy constrained and thus, the available energy must be utilized efficiently.

Energy consumption of a network is indirectly proportional to the lifetime of the network. Energy consumption and lifetime of the network are interrelated to each other. The poorer the energy utilization, the shortest is the lifetime of the network. In this case, the goal of the network cannot be achieved, as the network is short-lived. This is the serious threat to be addressed. There are several ways to reduce energy consumption in WSN, such as radio optimization, data reduction, sleep cycle scheduling and energy efficient clustering.

A short-lived network cannot yield the fruit to the society. On realizing the aforementioned fact, this paper deals with the energy efficient clustering technique, in order to preserve energy and thereby improvising the lifetime of the network. The central theme of clustering is to accumulate certain number of nodes and a node with greater capability is elected as the cluster head.

The cluster head manages all the operations of its constituent nodes. By this way, the cluster head preserves the energy of all its constituent nodes and the overall energy consumption is minimized. The cluster head takes charge of allocating resources to the cluster member nodes and reduces the communication overhead also. Besides this, a clustering algorithm improves the throughput, scalability and stability of the network. Several factors are needed to be kept in mind, while designing a clustering algorithm. For instance, forming many small clusters overcrowds the space and large cluster formation depletes the energy of cluster head.

This paper presents a trustworthy clustering algorithm namely Energy Efficient Trustworthy Clustering Algorithm (EETCA), which designates the cluster head based on the trust score. The trust score determines the cluster head and the trust score is computed by packet delivery ratio and battery backup of the node. In order to have control over the size of the cluster, a threshold is fixed. This is because of realizing the fact that small or large sized clusters will not serve the purpose effectively.

This work focuses on two different aspects of trust such as cluster member and cluster head trust. The cluster member trust involves the member and the cluster head. On the other hand, cluster head trust involves cluster head and base station. This algorithm is very efficient in terms of energy utilization and lifetime improvement. The work contributions of this research are highlighted below.

The major contribution of this work is a clustering algorithm for WSN which ensures energy efficiency. Besides this, the presented algorithm overthrows the malicious nodes from the network.

- The chief node of the proposed clustering algorithm is selected by the trust score of two neighbourhood nodes. By this way, the most eligible node is elected as the chief node.
- The chief node is vigilant against the misbehaviour and computes trust score for all of its constituent nodes. In case of a poor trust score, the chief node blocks the node.
- The trust score computation of this work does not rely on a single node. For a constituent node, two scores are computed by the neighbourhood constituent node and the chief node. Thus, the trust score is more reliable.
- When it comes to chief node, the trust score is computed by the neighbourhood chief nodes and the base station.
- It is recognized that a single chief node must not be overburdened. Hence, the chief node is recycled as soon as the energy drops below energy threshold.
- By incorporating trust mechanism, the trustworthy nodes alone can participate in the system and this considerably reduces the energy consumption by the nodes.
- The computed trust score need not to be broadcasted to all the nodes, such that the communication overhead of the proposed algorithm is minimal.

Most of the existing algorithms in the literature are not based on trust. When the trust based algorithms are taken into account, the energy consumption is found to be maximum. Besides this, most of the existing algorithms show communication overhead. Motivated by these existing algorithms, the proposed work aims to present a new trust based clustering algorithm with minimal energy consumption and communication overhead.

The remainder of this paper is systematized as follows. The review of literature with respect to existing algorithms in WSN is presented in section 2. Section 3 presents the problem description and assumptions of this work. The proposed clustering algorithm is presented in section 4. The performance of EETCA is evaluated and the experimental results are presented in section 5. Finally, the concluding remarks are presented in section 6.

2. Related Work

This section reviews the existing literature with respect to trust based clustering algorithms.

2.1 Trust based clustering algorithms

Several trust based clustering algorithms are presented in the literature for WSN [5-10]. However, these works face certain issues with respect to energy constraints. A Group based Trust Management Scheme (GTMS) is presented in [11] for WSN. This algorithm computes the trust value for a group of nodes and it results in the reduction of memory consumption. However, GTMS consumes more energy while broadcasting feedbacks.

In [12], a Hierarchical dynamic Trust Management Protocol (HTMP) is presented. This algorithm focuses on two different aspects of trust such as social trust and quality of service trust. However, this algorithm involves computational complexity which results in increased energy consumption.

A trust based cluster head election algorithm is presented in [13]. However, this algorithm does not focus more on trust. A trust based mechanism is presented in [14] to elect cluster head. This algorithm employs probability value for cluster head selection. The ordinary nodes join the cluster with respect to the trust value of the cluster head. This process is continued until all the nodes find their cluster head. However, this algorithm spares more energy. The improvised version of Low Energy Adaptive Clustering Hierarchy (LEACH) algorithm [15] is presented as LEACH-TM, which is based on trust [16]. This work selects cluster head based on the trust and the malicious nodes are detected. However, this algorithm consumes more energy and involves communication overhead.

In [17], a secure and trustable routing scheme namely ActiveTrust is proposed for WSN. The major goal of this work is to combat against black hole attacks, which show impact over data collection. ActiveTrust deals with black hole attacks by creating several detection routes and the trust of nodes is measured. This work is proved to be energy efficient. A Trust and Energy Aware Routing Protocol (TERP) is presented in [18], which exploits a distributed trust scheme in order to identify and exclude the suspicious nodes. The routes are computed by taking the trust, energy and hop counts into account. This strategy provides a way to use the available energy in a balanced fashion and thereby increasing the network lifetime.

The work proposed in [19] presents a trust derivation scheme by utilising game theoretic approach and is claimed as energy efficient. Initially, a risk strategy model is developed to study the cooperation of the sensor nodes, followed by which the trust is derived. It is claimed that this work provides security and is efficient. A trust management system is proposed in [20], which exploits fuzzy logic to compute the trust value of the path. In order to compute the trust value of the nodes, graph theory is utilized in association with the fuzzy logic. Additionally, a filtering algorithm is also proposed against attacks such as slandering, harbouring and so on.

A trust based routing protocol namely E-STAR for WSN is proposed in [21]. The trust system computes multidimensional trust values for the nodes. These trust values are combined with the public key certificates of the nodes and are used to select the routes. This protocol improves packet delivery ratio and the stability of routes. In [22], an Efficient Distributed Trust Model (EDTM) is presented, which computes direct and indirect trust. The direct trust takes communication, energy and data trust into account, whereas the indirect trust considers the reliability and familiarity of trust into account. This work guarantees security by preventing several security attacks.

Motivated by the above works, this paper intends to present a new clustering algorithm based on trust, which mainly focuses on energy conservation. The cluster head is elected by trust based mechanism and for every time interval, the trustworthiness of the nodes is checked. Though there are several works which intend to utilize trust concept for clustering, this work highlights itself in the following ways. Most of the existing trust based solutions consume more energy for trust value computation. Taking this as a challenge, this work aims to minimize the energy consumption by considering important trust metrics into account and thus, the trust score computation is made simpler. Besides this, the nodes are blocked whenever the trust score falls below the threshold. This improves the performance of EETCA further.

3. Preliminaries

3.1 Assumptions

This paper presents a clustering algorithm that is based on trust score. The trust score is computed by the packet delivery ratio, battery backup and the count of neighbour nodes. Packet delivery ratio can determine the forwarding tendency of the node and thus the behaviour of the node can be judged effectively. Battery backup is the primary requirement of any task to be accomplished.

This algorithm takes battery backup into account, as an energy drained node cannot serve its purpose. A node is considered healthy, when it is surrounded by many neighbour nodes. Thus, neighbour node count is also considered in the computation of the trust score. This work assumes the following.

- Only one base station with high energy backup is present in this network and is mobile.
- The sensor nodes of this network are immobile and static.
- Every node knows its location information, however they are not equipped with Global Positioning System (GPS)
- A node in the network can be either cluster head or cluster member.
- This paper denotes cluster head as the chief node and the cluster member as constituent node.
- A constituent node can forward the packet to the chief node directly.
- The chief node forwards the data to the base station via other chief nodes.

The proposed algorithm well-suits the energy constrained WSN. The chief node recycling process, further improves the energy conservation. The communication overhead of the proposed work is very low. In substance, the overall energy consumption of the system is low, which in turn prolongs the lifetime of the network.

4. Proposed Approach

4.1 Overview of the work

This paper intends to present a clustering algorithm, which aims at electing a chief node with respect to the trust score. As the chief node election banks on trust score, the most qualified node is selected. A threshold is fixed to control the size of the cluster. This is to prevent numerous small clusters and limited large clusters. Numerous small clusters overcrowd the network and introduce communication overhead. On the other hand, limited large clusters overburden the chief node and maximize the energy consumption.

The energy of the chief node is monitored by the base station and in case of energy drop below the energy threshold, the chief node is recycled. As an added advantage, this work follows bi-level trust with respect to constituent and the chief node. All the aforementioned points justify that the energy consumption of this work is significantly reduced and the network is trustworthy. The effective utilization of energy paves way for improvisation of the network lifetime. The entire flow of the proposed algorithm EETCA is decomposed into three phases. They are

1. Chief node selection
2. Chief node recycling phase

3. Bi-level trust estimation

The first phase of this work aims at electing the chief node, based on the computed trust score by Dempster-Shafer theory. The second phase is responsible for recycling the chief node, when the energy drops below the energy threshold. The third phase is concerned with the computation of trust score, so as to verify the trustworthiness of the nodes. The third phase computes the trust score for both constituent and chief nodes. The overall trust score depends on the trust metrics such as forwarding rate factor, packet consistency factor, battery backup and number of neighbours.

4.2 Cluster establishment

This work enforces a constraint that a cluster must possess twenty nodes only. A threshold to limit the cluster size is fixed as 20. This threshold is chosen based on the trial and error method. These optimal sized clusters utilize the energy effectively. The clustering algorithm chooses a node randomly and encircle around it, so as to enclose twenty nodes. This is followed by the computation of the trust score by employing Dempster-shafer theory, based on which the chief node is elected.

4.2.1 Chief node selection

The chief node of a cluster is selected with respect to the computed trust score. The proposed algorithm does not rely upon the trust assessment provided by a single node. Instead, two neighbourhood nodes calculate the trust score of each node and the computed trust scores are combined together. The value of this combined trust score is normalized between 0 and 1.

The trust score of the nodes is computed by the Dempster-Shafer theory, which is also called as evidence theory. This theory was proposed by Arthur P. Dempster [23]. The main advantage of this theory is that it does not require any knowledge about the probabilistic theory. This theory is employed to club the trust scores computed by the two neighbourhood nodes of every node.

A node can be claimed as trustworthy, not trustworthy and either of these [24]. This can be represented as

$$q: \delta = \{TW, \overline{TW}\} \tag{1}$$

The above presented equation states that the node q can be trust worthy or not trustworthy. The same equation can be explained by the rationale as below.

$$R = \{TW\} \tag{2}$$

$$\bar{R} = \overline{\{TW\}} \tag{3}$$

$$D = \delta \tag{4}$$

Equation 2 states that the node is trustable, whereas the $\overline{TW}$ states that the node is not trustable. Finally, D is a rationale that expresses the uncertainty that a node can be trustable or not. Consider that the probability function of reliability and unreliability of a node q is denoted by β and it is represented by the following equations.

$$\begin{cases} P1(R) = \beta \\ P1(\overline{R}) = 0 \\ P1(D) = 1 - \beta \end{cases} \tag{5}$$

$$\begin{cases} P1(R) = 0 \\ P1(\overline{R}) = \beta \\ P1(D) = 1 - \beta \end{cases} \quad (6)$$

This is followed by the summation of trust scores being computed by the neighbourhood nodes of every node. The rationale takes all the three cases into account and presented in the equations between 7 and 9.

$$P1(R) \oplus P2(R) = \frac{1}{K}[P1(R)P2(R) + P1(R)P2(D) + P1(D)P2(R)] \quad (7)$$

$$P1(\overline{R}) \oplus P2(\overline{R}) = \frac{1}{K}[P1(\overline{R})P2(\overline{R}) + P1(\overline{R})P2(D) + P1(D)P2(\overline{R}) \quad (8)$$

$$P1(D) \oplus P2(D) = \frac{1}{K}P1(D)P2(D) \quad (9)$$

Where K is given by

$$K = P1(R)P2(R) + P1(R)P2(D) + P1(D)P2(R) + P1(\overline{R})P2(\overline{R}) + P1(\overline{R})P2(D) + P1(D)P2(\overline{R}) + P1(D)P2(D) \quad (10)$$

The first case symbolizes that both the neighbourhood nodes claim that a particular node is trustable. The second case illustrates the scenario in which both the neighbourhood nodes decide that the node is not trustable. The last case shows a scenario in which the node can either be claimed as trustable or not trustable. **Fig. 1** presents the process of chief node selection.

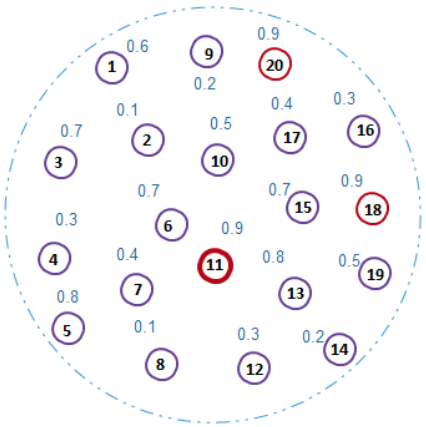

Fig. 1. Chief node selection

The value of the summation of trust scores being computed by two neighbourhood nodes range from 0 and 1. The value of 1 notifies that the node is completely trustworthy. On the other hand, value 0 represents that the node is completely untrustworthy. The value of 0.5 indicates that the node is partially trustworthy. In **Fig. 1**, it can be observed that there are three nodes with 0.9 as the trust score. In this case, the node with maximum number of neighbours is chosen as the chief node. The algorithm for chief node selection is presented below.

EETCA - Chief node election algorithm

Input: Set of nodes
Output: Clusters
Begin
Select a node in a random fashion;
Draw a circle to enclose 20 nodes;
Calculate P1 and P2;
Ts=P1+P2;
Pick the node with highest Ts;
Declaration of chief node by BS;
End;

The attractive theme of chief node election is that the trust score computation does not rely upon a single node. Suppose, if the trust score computation is done by a single node then the computation is not reliable. This is because the node which computes the trust score may be untrustworthy. Thus, the trust score computation is done by two different neighbourhood nodes of a node. By this way, the trust score is computed for every node. The node with highest trust score is elected as the chief node.

The chief node manages all the activities of its' constituent nodes and hence the chief node must be qualified and trustworthy. In order to choose the most appropriate node as the chief node, this work employs a trustworthy scheme. The node with highest trust score is declared as the chief node.

The chief node declaration is done by the base station. The base station is mobile and it starts to move for every time period. The base station checks for the trust scores of all the participating nodes and officially confirms the chief node. This is followed by the process of forwarding $JOIN$ requests by the chief node to the neighbourhood nodes.

4.2.2 Chief node recycling phase

The objective of this phase is not to overburden the chief node, such that the energy of the chief node may get dropped suddenly. The chief node must have sufficient energy in order to perform all its tasks effectively. Hence, it is recognized that the same node cannot be retained as the chief node; if at all the node has got super power. However, this is not the case of this work. The chief node is one among all nodes but with greater trust score. Thus, the battery of the node may start to deplete than other nodes.

The proposed chief node selection algorithm holds a threshold for min_erg (minimum energy) and the tl (time to live). The threshold for min_erg and tl is set as 0.6 and 60 seconds. For every sixty seconds, the battery backup of the chief node is verified. In case, if the battery backup is more than the min_erg, then the chief node stays in the same position. The algorithm for chief node recycling process is presented below.

ECTMRA - Chief node recycling procedure

Input : Chief nodes
Begin
Do check
if (current energy $\leq \boldsymbol{min\_erg}$)
Get approval from BS;
Recycle the node;
End;
End;

On the other hand, suppose the battery backup gets to diminish before the expiry of tl, then the chief node has to recycled all at once. Thus, the chief node is recycled if either of the conditions satisfy. This concept saves much energy as no single node is overloaded and a balanced energy sharing technique is followed.

4.2.3 Bi-level trust computation

This phase relies on two different aspects of trust, which focuses on the constituent node and chief node's trust. The first phase elects the most trustworthy node as the chief node. However, any node can be compromised at any point of time by the adversary. Thus, it is mandatory to keep an eagle-eye over the network, so as to prevent the malicious activities of the node.

To achieve this, the proposed algorithm computes the trust score of each node (constituent and chief node) for every period of time. The EETCA is claimed as trustworthy because it does not pay attention only towards chief node selection, but also maintains the trustworthiness of the entire network. The trust score is computed by the aggregation of several essential trust metrics and it is shown in **Fig. 2**.

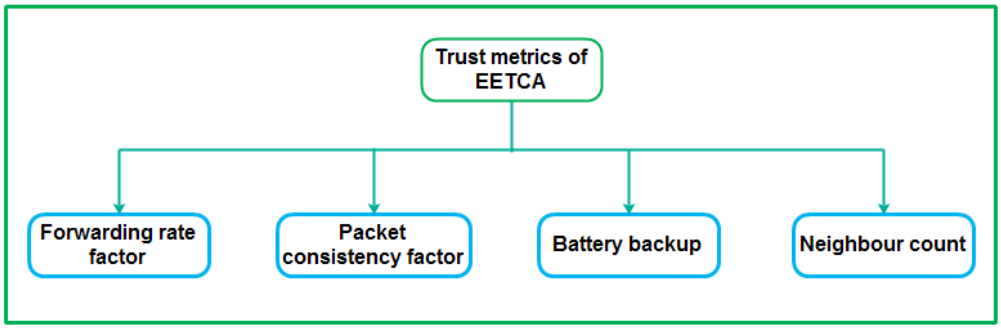

Fig. 2. Trust metrics of EETCA

The trust score of constituent node is computed by the neighbourhood node and the chief node. Both these trust scores are summed up and normalised to determine the nature of the node. Similarly, the trust score of the chief node is calculated by the neighbourhood chief node and the base station. These computed trust scores are added and normalized. In both cases, if the computed trust score is too low then that particular node will be blocked.

The chief node is given the authority to block its constituent node, in case of poor trust score. In case, if the trust score of the chief node is low then the base station blocks the chief node. In this scenario, the process of chief node election happens immediately.

As an added advantage, this algorithm does not rely upon a single node for the trust score computation. Instead, two different nodes are engaged in the computation of the trust score and the computed trust scores are aggregated. The aggregated trust score is normalized at last, so as to maintain the standard. The trust metrics considered by EETCA is presented below.

4.2.3.1 Trust metrics of EETCA

The proposed clustering algorithm relies on the trust score of the nodes. The trust score is computed by the blending significant trust metrics such as forwarding rate factor, packet consistency factor, battery backup and the number of surrounding neighbours.

Forwarding rate factor decides the forwarding tendency of the node. Packet consistency factor checks for the consistency of the packet, being forwarded by the node. This is checked by comparing the packets of neighbour nodes. Battery backup is the lifeblood of all tasks in the network. A node is considered as healthy when it is surrounded by many neighbouring nodes.

Thus, the proposed algorithm incorporates all the aforementioned trust metrics to compute the trust score and the node with greatest trust score is picked up. It is obvious that the most qualified node is chosen as the chief node. The sample trust metrics table is presented in **Table 1.**

- **Forwarding rate factor**

Forwarding rate factor determines the real forwarding tendency of a node. To illustrate the concept, three different cases are presented below. For instance, if a node forwards all the packets in a stipulated period of time, then the behaviour of the node is normal. In certain cases, the malicious nodes attempt to forward the packets in a repetitive fashion, so as to shatter the network. This type of attack is termed as replay attacks. Finally, a node may not show any interest in forwarding packets, which means that the node is completely selfish. Hence, a single trust metric can figure out the normal, selfish or malicious nodes.

- **Packet consistency factor**

Packet consistency factor scrutinizes the original behaviour of the node. To exemplify this concept, consider a node A wants to forward a packet to node D, through intermediate nodes B and C. In this scenario, the node B may tamper the original packet and is a serious issue to be considered. As far as this scenario is concerned, there are two intermediary nodes B and C. Hence, the packet tamper can be done by either of these nodes. The packet consistency of node B and C are checked by nodes A, C and A, B respectively. Thus, the severity of packet tamper is considerably reduced.

Table 1. Sample trust value table

Trust metrics	Value assignment (Ts)	Description
Forwarding rate factor	1	Normal
	0.5	Either normal or abnormal
	0	Malicious
Packet consistency factor	1	Normal
	0.5	Tolerable level of tamper
	0	Severe data tamper
Battery Backup	1	Energy packed node
	0.5	Moderately energized node
	0	Zero energized

Neighbour count	1	Healthy node
	0.5	Fit node
	0	Weak node

- **Battery backup**

Battery backup is the heart of the node. A node can serve its purpose only when it has required energy. A node with low battery backup can die at anytime and thus, the intended task may not be achieved. Thus, battery backup is the most important trust metric.

- **Neighbour count**

The final trust metric being considered by this work is the neighbour count. A node is considered as healthy, when it is surrounded by more number of neighbours. Hence, it is worthwhile to select a node with greater number of neighbours as the chief node.

4.2.3.2 Trust score of constituent node

The trust score of the constituent node is computed for every minute by a neighbourhood and the chief node. The value of the trust score of any node ranges from 0 to 8, as the two different trust scores are clubbed together. The computed value is normalized between 0 and 1, to improve the readability and to maintain the standard. The normalization of values is computed by the following equation.

$$Norm = \frac{(x-ac_l)\times(n_h-n_l)}{ac_h-ac_l} \tag{11}$$

Where x is any value ranging from 0 and 8, ac_l and ac_h is the lower and upper limit of actual value which is 0 and 8 respectively. n_h and n_l is the upper and the lower limit of the normalized value, which is 0 to 1. By this way, the trust score of the constituent node is determined and the value is stored in the trust table of the chief node. In case, if the computed trust score falls below 0.3, then the node is blocked by the chief node. The bi-level trust score computation is presented below.

EETCA – Bi-level trust computation procedure

Input: Constituent nodes, chief nodes
Output : Trust scores
Begin
Case 1: Constituent nodes
Declare neighbour node trust score computation as i;
Declare chief node trust score computation as j;
For every 60 seconds
Ts=i+j;
if (Ts$\leq \mathbf{0.3}$*)*
Notify chief node;
Block the node;
Else
Store Ts in chief node;
End;
Case 2: Chief nodes
Declare chief node trust score computation as i1;

```
Declare BS trust score computation as j1;
For every 60 seconds
  Ts1=i1+j1;
 if (Ts1≤ 0.4)
  Notify BS;
  Block the node;
Else
  Store Ts1 in BS;
End;
```

4.2.3.3 Trust score of chief node

The node with greatest trust score is elected as the chief node by the base station. However, it is not a good idea to eliminate chief nodes from trust score computation, as the node may get compromised by the adversary at any period of time. The trust score of the chief node is computed by the neighbourhood chief node and the base station for every period of time. The so computed trust scores are summed up together and normalised by the eqn.11. In case, if the trust score of the chief node is below 0.4, then the base station blocks the chief node. The process of chief node happens immediately and is initiated by the base station. The trust scores of all the chief nodes are maintained by the base station itself.

5. Experimental Analysis

The performance of the proposed algorithm is analysed by several experiments. The experimental area of the proposed work is set as 200 by 200 metres. The number of sensor nodes is 200. Certain malicious nodes are randomly distributed. The malicious nodes show less interest in forwarding packets and affect the consistency of packets. The malicious nodes can either be constituent or chief nodes. This work detects these sorts of malicious nodes and blocks them.

The malicious nodes can be tracked when the threshold of trust score reached 0.3 in case of constituent nodes and 0.4 in case of chief nodes. Initially, all the nodes deployed in the network are trustworthy with trust score 1. However, the trust score starts to deteriorate when certain nodes involve in malicious activities. Thus, these malicious nodes can easily be figured out, as the trust score drops down.

The most important trust metrics of this work are considered and the graphs are presented in figures 3 to 6. The malicious node detection with respect to trust score (Ts) is presented in **Fig. 3**. In **Fig. 4**, the average forwarding ratio of nodes is tested with respect to the varying rounds. It can be observed that the average forwarding ratio drops, as the trust score decreases. The consistency of the packets is evaluated by varying the number of rounds. The average packet forwarding ratio is evaluated in **Fig. 5**. All these trust metrics drop initially and grows afterwards.

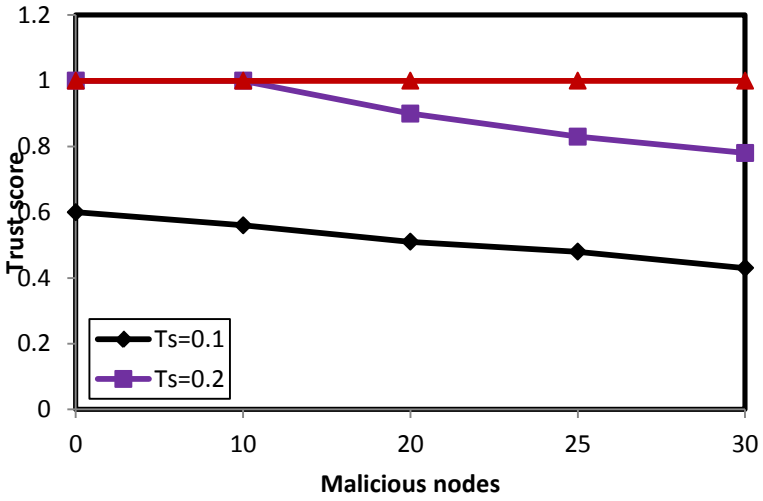

Fig. 3. Malicious node detection wrt trust score

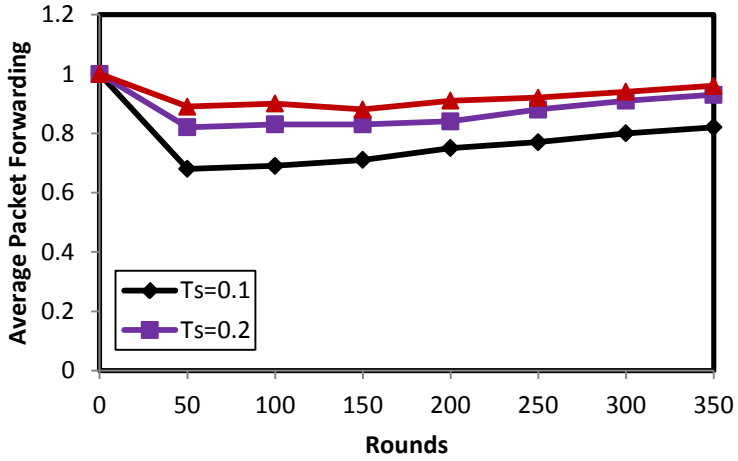

Fig. 4. Average forwarding ratio wrt trust score

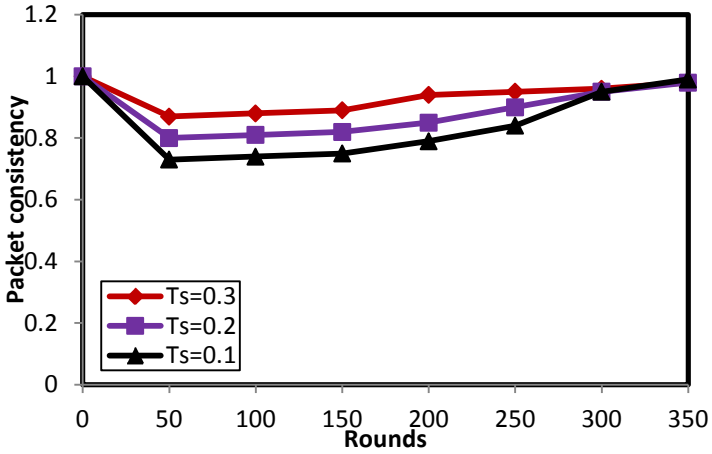

Fig. 5. Average packet consistency wrt trust score

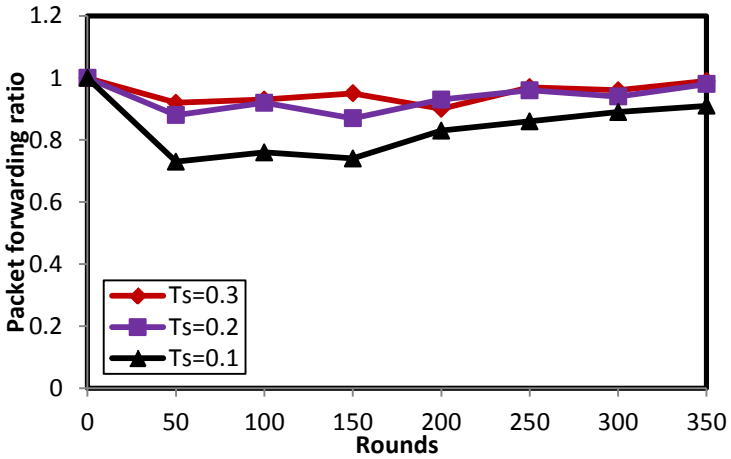

Fig. 6. Average packet forwarding ratio wrt trust score

The energy consumption of EETCA is compared with the standard LEACH-TM protocol [16], Group based Trust Management Scheme (GTMS) [11] and Trust aware Low Energy Secure protocol TLES [25]. The energy consumption of nodes can be observed in **Fig. 7**. From the experimental results, it is evident that the energy consumption of EETCA is minimal. The reason for minimum energy consumption is that the proposed algorithm employs clustering technique, which consumes lesser energy. Besides this, the energy consumption is reduced, as the communication overhead of this work is found to be minimal. The communication overhead of EETCA is presented in **Fig. 8**. Whenever the trust score goes below the threshold, the corresponding nodes are blocked immediately. Thus, all the nodes present in the network are trustworthy and thus the energy consumption is reasonable.

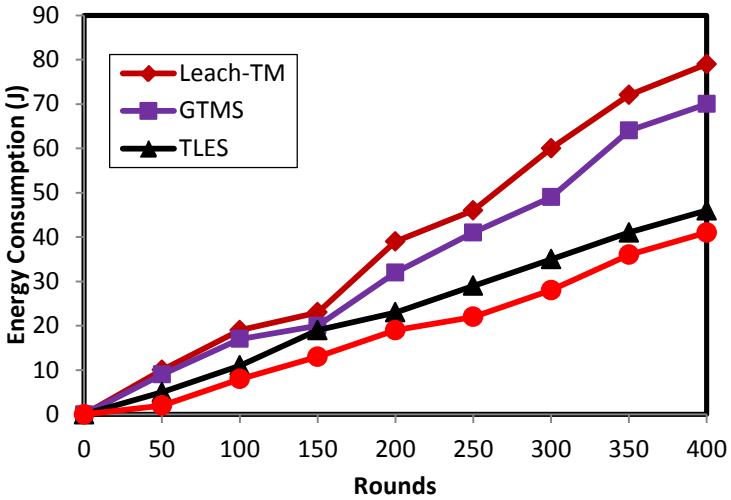

Fig. 7. Energy consumption analysis

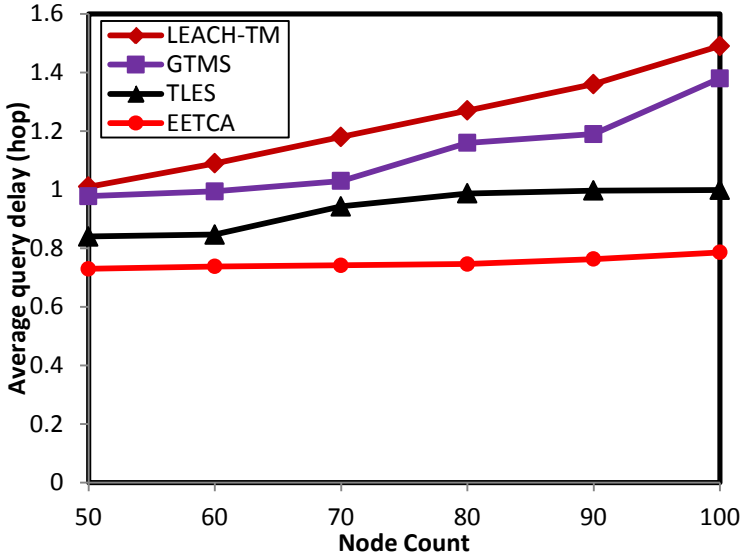

Fig. 8. Communication cost analysis

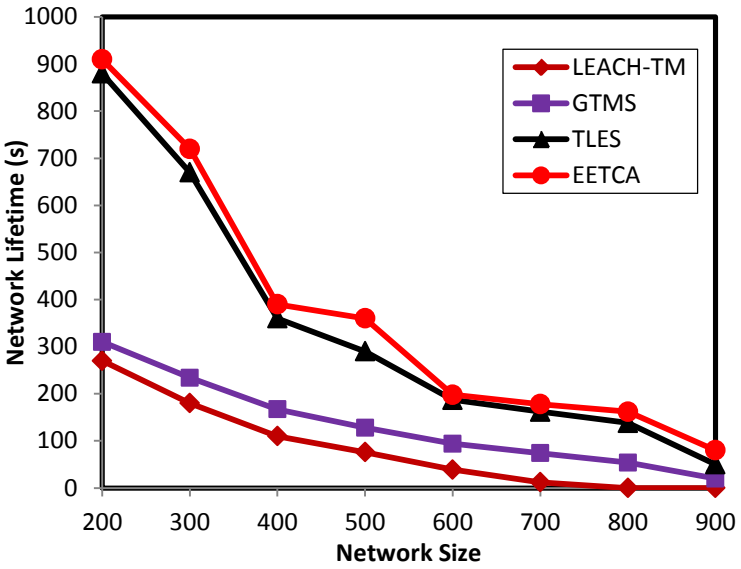

Fig. 9. Network lifetime analysis wrt to first node death

Finally, the lifetime of the network is measured by varying the network size and is presented in **Fig. 9**. The lifetime of the network is calculated with respect to the death of the first node of the network. As the distance between the nodes increases, the power requirement of nodes increases. This leads to the reduction of the lifetime of the network. Comparing to LEACH-TM, GTMS and TLES, the lifespan of EETCA is longer. Besides this, lesser energy consumption improves the lifetime of the network. Thus, the proposed EETCA justifies itself by efficient energy utilization by incorporating a novel trust model and thereby improves the lifetime of the network.

6. Conclusion

This paper proposes a new clustering algorithm namely Energy Efficient Trustworthy Clustering Algorithm (EETCA), which minimizes the energy consumption and thereby improves the lifetime of the network. WSN is energy constrained and it is impossible to replace to recharge the batteries of sensors all the time. For this sake, the available energy has to be utilized in an effective manner. Thus, a clustering algorithm based on trust metrics is presented for effective utilization of energy. The experimental results show that the proposed work is better than the LEACH-TM algorithm. In future, this work can be enhanced by focussing on mobile sensor network.

References

[1] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E., "Wireless sensor networks: A survey," *Comput. Netw*, Vol.38, pp.393–422, 2002. Article (CrossRef Link)

[2] Yick, J., Mukherjee, B., Ghosal, D., "Wireless sensor network survey," *Comput. Netw.*, vol.52, pp. 2292–2330, 2008. Article (CrossRef Link)

[3] H. Chan, A. Perrig, "Security and privacy in sensor networks," *IEEE Computer*, vol.36, no.10, pp.103–105, 2003. Article (CrossRef Link)

[4] Y.M. Huang, M.Y. Hsieh, H.C. Chao, S.H. Hung, J.H. Park, Pervasive, "Secure access to a hierarchical-based healthcare monitoring architecture in wireless heterogeneous sensor networks," *IEEE Journal on Selected Areas of Communications*, vol. 27, no.4, pp.400-411, 2009. Article (CrossRef Link)

[5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 3, pp. 1–37, May 2008. Article (CrossRef Link)

[6] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," *IEEE Trans. Depend. Secure Comput.*, vol. 9, no. 2, pp. 184–197, Apr. 2012. Article (CrossRef Link)

[7] E. Aivaloglou and S. Gritzalis, "Hybrid trust and reputation management for sensor networks," *Wireless Netw.*, vol. 16, no. 5, pp.1493–1510, Jul. 2010. Article (CrossRef Link)

[8] A.Rezgui andM. Eltoweissy, "$\mu RACE$: A reliable adaptive service driven efficient routing protocol suite for sensor-actuator networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 5, pp. 607–622, May 2009. Article (CrossRef Link)

[9] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proc. of ACM Workshop Security of ad hoc and Sensor Networks (SASN'04)*, pp. 66–67, Oct. 2004. Article (CrossRef Link)

[10] Z. Yao, D. Kim, and Y. Doh, "PLUS: Parameterized and localized trust management scheme for sensor networks security," in *Proc. of Third IEEE Int. Conf. Mobile Ad-Hoc and Sensor Systems (MASS'06)*, pp. 437–446, Oct. 2006. Article (CrossRef Link)

[11] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. Lee, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp.1698–1712, Nov. 2009. Article (CrossRef Link)

[12] F. Bao, I. Chen,M.Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Trans. Netw. Service Manag*., vol. 9, no. 2, pp. 169–183, Jun. 2012. Article (CrossRef Link)

[13] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," in *Proc. of Second IEEEWorkshop on Dependability and Security in Sensor Networks and Systems*, pp. 10–22, 2006. Article (CrossRef Link)

[14] R. A. Raje and A. V. Sakhare, "Routing in wireless sensor network using fuzzy based trust model," in *Proc. of the 4th International Conference on Communication Systems and Network Technologies (CSNT '14)*, pp. 7–9, 2014. Article (CrossRef Link)

[15] W. R. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, “Energy-efficient communication protocol for wireless microsensor networks,” in *Proc. of the 33rd International Conference on System Sciences*, pp. 1–10, Maui, Hawaii, USA, 2000. Article (CrossRef Link)
[16] W. Wang, F. Du, and Q. Xu, “An improvement of LEACH routing protocol based on trust for wireless sensor networks,” in *Proc. of the 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM ’09)*, pp. 1–4, Beijing, China, September 2009. Article (CrossRef Link)
[17] Yuxin Liu, Mianxiong Dong, Kaoru Ota, Anfeng Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks,” *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 9, pp. 2013-2027, 2016. Article (CrossRef Link)
[18] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb, Abdul Waheed Khan, “TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network,” *IEEE Sensors Journal*, Vol. 15, No. 12, pp.6962-6972, 2015. Article (CrossRef Link)
[19] Junqi Duan, Deyun Gao, Dong Yang, Chuan Heng Foh, Hsiao-Hwa Chen, "An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications,” *IEEE Internet of Things Journal*, Vol.1, No.1, pp. 58-69, 2014. Article (CrossRef Link)
[20] Shuaishuai Tan, Xiaoping Li, Qingkuan Dong, "A Trust Management System for Securing Data Plane of Ad-Hoc Networks,” *IEEE Transactions on Vehicular Technology*, Vol.35, No.9, pp. 7579-7592, 2015. Article (CrossRef Link)
[21] Mohamed M.E.A. Mahmoud, Xiaodong Lin, Xuemin (Sherman) Shen, "Secure and Reliable Routing Protocols for Heterogeneous Multihop Wireless Networks,” *IEEE Transactions on Parallel and Distributed Systems*, Vol.26, No.4, pp.1140-1153, 2013. Article (CrossRef Link)
[22] Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, Mohsen Guizani, "An Efficient Distributed Trust Model for Wireless Sensor Networks,” *IEEE Transactions on Parallel and Distributed Systems*, Vol.26, No.5, pp. 1228-1237, 2015. Article (CrossRef Link)
[23] Dempster, A. P., “Upper and lower probabilities induced by a multivalued mapping,” *The Annals of Mathematical Statistics*, vol.38, No.2, pp.325–339, 1967. Article (CrossRef Link)
[24] Thomas M. Chen and Varadharajan Venkataramanan, "Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks,” *IEEE Internet Computing*, Vol.9, pp.35-41, 2005. Article (CrossRef Link)
[25] Zuo Chen, Min He, Wei Liang, and Kai Chen, "Trust-Aware and Low Energy Consumption Security Topology Protocol of Wireless Sensor Network,” *Journal of Sensors*, vol.2015, pp. 1-10, 2015. Article (CrossRef Link)

T.Senthil works as a Senior Assistant Professor of Electronics and Communication Engineering Department at Kalasalingam University, Tamil nadu, India. He received his B.E and M.E degree from MK University, India with specialization in Electronics and communication engineering and Microwave & optical engineering in 1988 and 1997 respectively. He has more than twenty years of teaching experience and has published papers in National/International conferences and Journals. His current research focus is on energy efficient protocols in wireless sensor networks. He is the life member of ISTE.

B. Kannapiran was born in 1980. He obtained his Bachelor degree in Instrumentation and Control Engineering from Madurai Kamaraj University, India in 2001 and Master degree in Applied Electronics from Madurai Kamaraj University, India in 2002. He also obtained hid Ph.D degree from Anna University Chennai, India in 2013. Presently he is working as Associate Professor in the Department of Instrumentation and Control Engineering, Kalasalingam University. He has published papers in International journals, National and International Conferences. His research topics include soft computing, Fault Diagnosis.