DOI 10.12694/scpe.v18i3.1301
Scalable Computing: Practice and Experience ISSN 1895-1767
Volume 18, Number 3, pp. 207–218. http://www.scpe.org © 2017 SCPE

AN ENERGY EFFICIENT AND TRUST AWARE FRAMEWORK FOR SECURE ROUTING IN LEACH FOR WIRELESS SENSOR NETWORKS

ARZOO MIGLANI[*], TARUNPREET BHATIA[†], GAURAV SHARMA[‡] AND GULSHAN SHRIVASTAVA[§]

Abstract. Wireless Sensor Network (WSN) is an advanced technology and has been used widely in many applications such as health monitoring, environment monitoring, military purpose etc. Nature of this network is that they are often placed in an open environment and are susceptible to various attacks. Traditional cryptography methods are not supportable in WSNs as they have high energy and resource constraints. Trust management has been proved to be an effective measure to enhance security as well as to handle threats for WSNs. Trust can be defined as level of reliableness in a node. Low Energy Adaptive Clustering (LEACH) is a cluster based routing protocol for WSN which is superior to direct communication protocol and known for its minimum transmission energy. However, LEACH itself has some limitations related to security. In this paper, an energy efficient and trust aware framework for secure routing in LEACH (EETA-LEACH), has been proposed that improves LEACH protocol by introducing trust to provide secure routing, while maintaining originality of LEACH protocol. This approach is a combination of trust-based routing module and trust management module that works together to select trusted Cluster Head (CH). The simulation results demonstrate that proposed scheme is better in terms of network lifetime and Packet Delivery Ratio (PDR). It is verified that malicious nodes will not be selected as CH and trust value of a malicious node decreases with time.

Key words: WSNs: Wireless Sensor Networks, Trust Management, Cluster-Based WSNs, LEACH.

AMS subject classifications. 68M12

1. Introduction.

Wireless sensor network is an infrastructure less network that consists of large number of sensor nodes distributed over an area to monitor and to collect a certain amount of data. However, WSNs are placed in an open environment and hence are susceptible to various kind of attacks. A node may get attacked by adversary and disrupt normal working of sensor network. Moreover, other security mechanism such as asymmetric cryptographic algorithm depends upon high computational capacity, power and resource [1, 2] and it is easy for an adversary to steal keys. Other mechanism such as authentication, message integrity, confidentiality has also being proposed to solve security issues but all these methods are only helpful in providing assurance towards outsider attacks. Therefore, trust management is an efficient solution for a compromised network and preventing internal attacks. Trust can be explained as a belief in reliableness of other node that is how much a node has confidence in establishing a secure communication with other node. Trust algorithm proposed in this paper is an extension of [3]. The motive of this paper is also same that is to remove flaws in LEACH by introducing secure cluster based selection. LEACH [4] is clustering based approach where nodes arrange themselves into local area called clusters. After every round a new cluster head is selected to balance energy load. Every new round starts with Set-up phase proceeded by Steady-state phase. In Set-up phase clusters are formed based on some threshold value which is given as below in Eq. 1.1.

$$T(n) = \left(\frac{p}{1 - p \times rmod(\frac{1}{p})} \right) \tag{1.1}$$

After this sensor nodes will decide which cluster head to choose based on signal strength. Next based on strength of sensor in a cluster, cluster head will form a TDMA schedule and each node is supposed to transmit within their allotted slot. After collecting data from every cluster members, CH aggregates data and then forwards data to BS.

But there are some problems associated with LEACH. Though cluster head selection procedure ensures that all nodes would get an equal chance to become cluster head but energy factor is not considered while selecting cluster head. After a time period, it is likely that a node with low energy may get selected as cluster head [5]. Another problem is that different cluster head elected would have different distance to base station,

[*] Department of Computer Science and Engineering, Thapar University, India (arzoomiglani4@gmail.com)
[†] Department of Computer Science and Engineering, Thapar University, India (tarunpreetbhatia@gmail.com)
[‡] Départment d'Informatique, Université Libre de Bruxelles, Belgium (sharmagaurav86317@gmail.com)
[§] Department of Computer Science and Engineering, National Institute of Technology Patna, India (gulshanstv@gmail.com)

so their energy needs would also be different [6]. In addition, in large network, CH which is located at more distance from BS has to adopt multipath which consumes high energy. Moreover, energy demands for intra cluster communication are less than inter cluster communication. LEACH is completely dependent on cluster head for transmission and aggregation of data and a compromised cluster head would drop packets and may not perform task assigned to it thus making an unsecure network. Thus it is very important to choose a trusted CH. In this paper an improvement in LEACH protocol has been proposed, while maintaining the routing of original LEACH protocol.

In section 2, related work is discussed for enhancing lifetime of sensor network as well as some cluster based trust management schemes has been described. Proposed algorithm is presented in section 3. Section 4 presents simulation results followed by conclusion and future scope in section 5.

2. Related Work. Traditional methods of cryptography such as TinySec [7] can be used in prevention of external attacks in WSNs but they cannot block internal attacks. Watchdog and pathrater [8] were the initial work for enhancing security by means of trust. LEACH has inspired design of other cluster based protocol. As LEACH relies completely on selected cluster head for aggregation and transmission of data, so it is important to elect a reliable cluster head. Trust-based Low Energy Adaptive Clustering Hierarchy (T-LEACH) [9] designed by Song, Fei et al. proposed a trust based leach protocol that contains two components that is monitoring module and trust evaluation module. Routing part is same as original protocol; cluster head selection is dependent on trust value of cluster heads. With help of trust update slots new trust value are calculated and shared among cluster members. T-LEACH helps in less data loss than LEACH.

With a similar motive an improvement of LEACH Routing Protocol Based on Trust for Wireless Sensor Networks [10] (TM-LEACH) is proposed by Wang Weichao et al. where a cluster head adjusting procedure is introduced that create multipath with elected cluster head acting as routers. TM-LEACH ensures reliability of data transmission. Rather than relying on optimal solutions Dhulipala et al. proposed A Heuristic Approach Based Trust Worthy Architecture [11]. This model has taken mobility of nodes into account for better trust aggregation. Distributed trust is calculated within a cluster where every node calculates trust of every other node and centralized trust is calculated based on overall cluster performance. If more than 80% of nodes are trusted then cluster will be declared as a secure for communication There are many improvements in LEACH which has been proposed in literature, [12, 13, 14] proposed schemes for energy efficient LEACH, [15, 16] proposed work for better cluster head selection

CONFIDANT [17] is available with several versions, it is proposed with a trust manager along with a reputation system which analyzes the events described by the watchdog, then detecting and removing misbehaving nodes from network. J. Manickam. et al. [18] proposed another fuzzy based solution in 2014. This scheme has less overhead with respect to energy and memory consumption. Trust is calculated at both intra-cluster and inter-cluster level. Inside a cluster to reduce communication overhead only direct trust is calculated. At inter-cluster level both of direct as well as indirect trust is calculated. Direct trust is calculated using a sliding time window scheme. For calculating indirect trust recommendation are considered, for requesting a recommendation a trust request (TREQ) message is broadcasted to all neighbours whosoever comes in transmission range. For deciding final trust fuzzy if and then rules are applied to three parameters that are: direct trust, Recommendation inconsistency and number of fluctuations.

In 2011, Senthilkumar [19] et al. introduced Honey Bee Mating algorithm to select cluster head but security issues in cluster head selection were not considered. Sahoo et al.[20] in 2015 proposed a energy efficient cluster based model. The crux of the paper is to prevent malicious nodes of the network to be a cluster head. The proposed algorithm uses a light weight dynamic trust algorithm in addition with Honey Bee Mating algorithm to elect most eligible member as cluster head. To implement the routing part, LEACH is used as base protocol. Trust calculated by sensor nodes can be used by can be used by secure localization as proposed by Peng Li et al. [21] in 2017. The approach introduced has improvised security by identifying malicious nodes and detecting Sybil attack. In 2015 wei Luo et al. [22] proposed a scheme to detect internal as well as external attack. In order to detect external attack SHA-1 hashing algorithm is used, to differentiate normal nodes from noxious nodes and to detect internal attack trust values of nodes are used. In addition to this, to maintain confidentiality the message between nodes are encrypted using asymmetric or symmetric key cryptography. Several Routing Framework using key management protocols over past years. Secure trust based key management(STKF) [23] is such a protocol for secure routing of data from source to destination using trust values of nodes. In this protocol, global trust value of routing path is computed by considering multiplication of trust values of nodes in route. Source node will select its authentic neighboring node to securely forward the data and neighbor selection will be done taking distance and trust relation between nodes.However,to avoid hacking of data and to maintain privacy data transmitted will be locked wit common pair of key. Another approach is proposed by yuxin liu et al.[24] to avoid black hole attack by using trust values. Source node will select its neighbour as next hop that has less distance with sink node and has trust values above the predefined threshold.

3. Proposed Model. For executing trust mechanism for sensor networks environment, following assumptions have been made:

- There are some malicious nodes present in the network
- BS has unlimited source of energy and it is free from any kind of attack
- If a node is performing some malicious activity then it will be penalized and its trust value will decrease.
- If a node is showing good behaviour, it will be rewarded and its trust value will be increased.
- Malicious nodes present in network are consuming more energy and dropping more packets than normal nodes.

Aim of this protocol is to choose trusted CH i.e. nodes with less trust value or less energy should not be selected as CH. Proposed work can be divide into two main modules that is trust management module and trust based routing module [9]. Figure 3.1 represents overall architecture of proposed algorithm.

- **Trust Management Module**: This module calculates trust based upon remaining energy, PDR and distance.
- **Trust-Based Routing Module**: It is almost same as basic LEACH protocols with some changes in it. Trust-based routing module uses trust management module to perform secure routing.

An improvement in LEACH protocol has been proposed, while maintaining the routing of original LEACH protocol. The scheme used to calculate trust is described below: Inputs

- Network area
- Number of nodes

Nodes will be randomly distributed in given area. Every node runs with an energy watcher, PDR calculator, distance estimator and trust supervisor [25, 26, 27]. Energy Watcher will calculate remaining energy of neighbour nodes and CHs, PDR calculator will calculate PDR of every node based upon number of packets dropped by node, Distance Manager will calculate and maintain distance between node and neighbours node along with CH distance with node.Trust Supervisor will maintain trust level of neighbouring nodes and CHs elected. For calculating trust value three factors will be considered that are remaining energy, PDR and distance i.e. nodes with high remaining energy, high PDR, and less distance between subject node and evaluated node will have more trust value and thus have high chances of becoming CH as compared to those nodes with low trust value, low PDR and high distance between nodes.

The four components of a node will work as follows:

- **Energy Watcher:** It will keep track of remaining energy of nodes. Energy model for the network is discussed as: To transmit a k-bit message with a distance of d, energy consumption can be calculated by Eq. 3.1:

  $$E_t = E_e(k,d) + E_a(k,d) \tag{3.1}$$

  where E_t is the transmitting energy, E_e is energy required to run transmitter and receiver circuitry, Ea is transmitter amplifier energy and energy required to receive any packet can be calculated by Eq. 3.2:

  $$E_r = k * E_e \tag{3.2}$$

  Hence energy will be consumed while transmitting or receiving packets in the network. As sensor networks are deployed in area where it is not possible to charge these nodes timely, so protocol designed should be energy efficient to save energy of these nodes and increasing network lifetime.
- **PDR Calculator:** This component will keep track of PDR. From the past records PDR calculator will maintain total number of packets sent to BS and how many of them are actually received by BS.

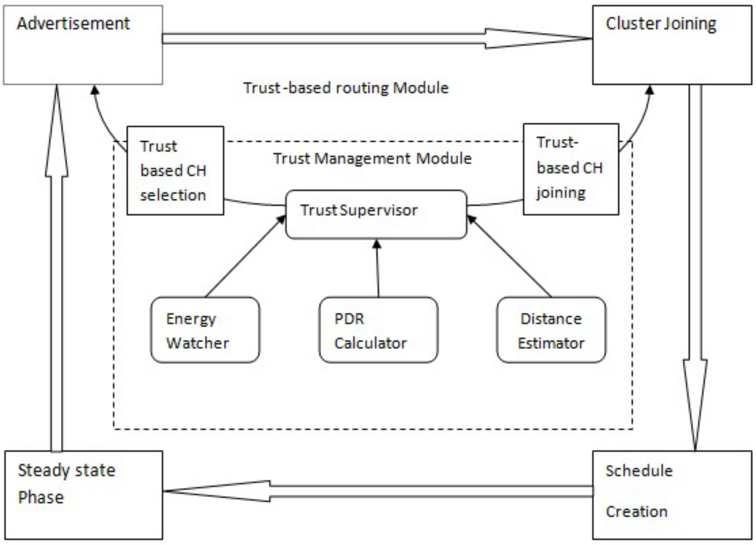

Fig. 3.1. *System Architecture*

Packets may be intentionally dropped by malicious node. Another reason for packets drop may be poor network connectivity. Nodes with high PDR will have high trust value and node with low PDR will have less trust value. Formula for PDR can be given by Eq. 3.3:

$$Packet\_Delivery\_Ratio = \frac{Packets\_Rcvd}{Packets\_To\_BS} \tag{3.3}$$

where Packets_Rcvd are total number of packets received by BS and Packets_To_BS are total number of packets sent to BS.

- **Distance Estimator:** This component will keep track of distance between nodes. If distance between evaluated node and subject node is less, a high trust value will be assigned to evaluated node otherwise if distance between subject node and evaluated node is high, then low trust value will be assigned to node. Hence trust value is inversely proportional to distance between nodes. Also this component will keep track of distance between nodes and CH.
- **Trust Supervisor:** This component will maintain trust values of nodes that will be used by routing module for trusted CH election and secure routing. The working of trust supervisor is being discussed in trust management module.

3.1. Trust Management Module. For calculating trust, trust supervisor will calculate both direct and indirect trust and final trust will be calculated by aggregating both trust values [28]. Direct trust is that trust which is calculated by nodes itself without scanning opinion of other nodes. Direct trust will be calculated based on past and present interactions of nodes. In order to save energy, sometimes it is not possible for a node to calculate direct trust of other nodes; in that case nodes will take recommendations from other nodes which will result in indirect trust. Indirect trust is also called second hand trust. In this model trust is calculated by considering energy, distance and PDR as trust metric. Nodes with high remaining energy, high PDR, less distance between nodes will have more trust value as compared to those nodes with less remaining energy, less PDR, more distance between nodes. As shown in Fig. 3.2 a subject node is one which wants to calculate trust of other node, evaluated node is one whose trust value is to be calculated, recommendation nodes are those whose opinions are considered for calculating indirect trust. Total trust of evaluated node will be computed by using both direct as well as indirect trust.

An initial trust of 0.5 is assigned to every node.The trust value of nodes can range between[0,1], where 1 represents that node is fully trustworthy, 0 represents complete distrust, 0.5 represents a normal trust value which

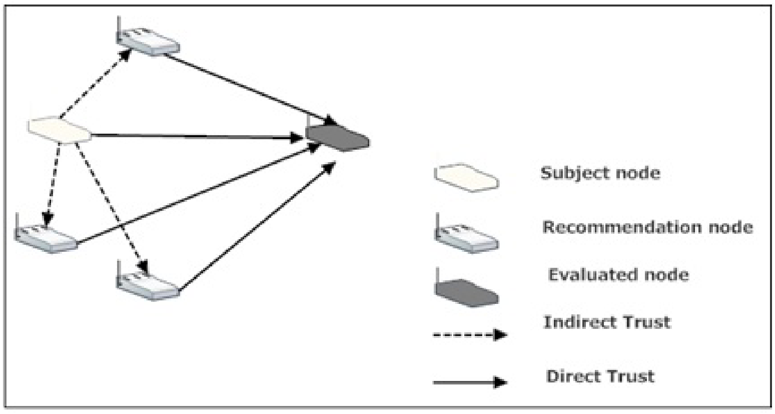

FIG. 3.2. *Trust Relationship*

can be ignored. For calculating direct trust, trust supervisor will interact with energy watcher, PDR calculator and distance estimator. For calculating direct trust, first trust supervisor will check remaining energy, and then a series of if-then rules will be applied to remaining energy, by comparing remaining energy with threshold value trust values will be assigned to nodes. Threshold values are selected by analyzing remaining energy after a particular round. Nodes will be awarded or penalized based upon the results after comparing remaining energy with threshold value. A node will be rewarded if its remaining energy is high after a particular round and if at the same round node is having less energy as compared to threshold then it will be penalized.

Once remaining energy has been checked, next trust supervisor will check PDR of nodes. PDR of nodes is compared with thresholds and then accordingly reward or penalty will be given. A node with high PDR will be rewarded and the nodes which drop more number of packets will have less PDR and hence penalized.

Further trust is dependent on another factor that is distance between nodes. If distance between nodes is high then corresponding trust of the node will be more and vice-versa. Hence direct trust can be calculated based upon aggregation of three factors.

Next, indirect trust will be calculated based on recommendations considered from other nodes. Indirect trust is the sum of trust values calculated by other nodes and given by Eq. 3.4:

$$IT^{C}_{A\to B} = \sum_{C} DT_{A\to C} \times DT_{C\to B} \tag{3.4}$$

where, $IT^{C}_{A\to B}$ is indirect trust of B calculated by A considering recommendation from C and C $\neq$ A; and are the direct trust value calculated by A for$C$ and C for B. For calculating final total trust both of direct and indirect trust will be aggregated as given below by Eq. 3.5:

$$TT_{A\to B} = wDT_{A\to B} + (1-w)IT^{C}_{A\to B} \tag{3.5}$$

$TT_{A\to B}$ is the total trust of node A on node B, w is the weight associated with direct and indirect trusts. A higher value of w signifies that sensor nodes relies more on its own judgment whereas a lower value of w signifies that sensor nodes has more trust on recommendations provided by other nodes. Final trust values of nodes will be stored by Trust Supervisor.

3.2. Trust-Based Routing Module. Routing module consists of two main phases: Set-up phase and Steady-state phase. In Set-up phase clusters are arranged and selected followed by .steady-state phase where nodes will transmit data to BS.

1. Set-up phase

a) Advertisement phase

This phase is same as in original LEACH protocol but for increasing lifetime of network energy factor is considered while selecting CH, so that the nodes with less energy should not get selected as CH. The number

Table 3.1
Neighbour CH Information

Attribute	**Description**
ID	ID of neighbouring CH
E_{REM}	Remaining energy of CH
T_{node}	Final trust of neighbouring CH
D_{Bs}	Minimum distance of neighbouring CH from BS
EC	How many times Neighbouring CH is elected as CH
$N_{nearest}$	Whether nearest neighbour or not

of nodes elected as CH with low energy will be less thus increasing network lifetime. To start procedure of CH election, node will select a random number between 0-1. If the number chosen is less than threshold value of node, node will be selected as CH otherwise not. The threshold value can be given by Eq. 3.6:

$$T(n) = \left(\frac{p}{1 - p \times rmod(\frac{1}{p})} \times \frac{E_{REM}}{E_{INT}}, n \in G \right). \tag{3.6}$$

where p is the desired percentage of CHs, G is set of nodes that have not been elected as cluster-heads in the last $1/p$ rounds and r is the current round, E_{REM} is remaining energy of node and E_{INT} is initial energy of node. After this phase, nodes has list of all eligible CH members.

Trusted CH Arranging Procedure

After CH has been elected, now elected CH will find all its CH neighbours [10, 29] and all information regarding CH neighbour will be collected from energy watcher, trust supervisor and distance manager. CH will maintain information of neighbour CH in form of a table. Each node will maintain an entry corresponding to every attribute mentioned in Table 3.1.

Now CH will examine whether neighbour is nearest neighbour or not and this will be decided by comparing distance of nodes with D. Equation 3.7 gives the value of D. Distance between CHs will be calculated with signal strength. If distance calculated is less than D then $N_{nearest} = 1$ else it is 0.

$$D = \text{å} \times \sqrt{\frac{1}{\pi K}} \times L \tag{3.7}$$

where L is the side length of the square area where sensor nodes are deployed, K is the number of cluster-heads, åis an adjusting factor. This will uniformly cover whole area CHs. If number of nearest neighbour CH is greater than 0 then CH will calculate trust weight associated with every nearest neighbour CH and trust weight, W_T is calculated by Eq. 3.8:

$$W_T = \alpha \times \frac{E_{REM}}{E_{INT}} + \beta \times \frac{T_{node}}{\sum T_{node}} + \gamma \times \frac{d(CH, BS)}{AD_{c\text{ß}BS}} + EC \tag{3.8}$$

where, α, β, γ are the weight factors selected accordingly. As for this paper energy is already considered as attribute for trust calculation, so for simulation a lower value of is considered. If some other attribute is selected then a higher value for α should be considered otherwise β can have higher value and EC is number of times node is selected as CH. T_{node} is the trust value of neighbouring CH obtained from trust management module. $\sum T_{node}$ is aggregation of trust of all nearest neighbour CH. CH with heaviest trust weight value is selected as new CH and will broadcast this information to other nodes and CH selected earlier will vanish. In addition, minimum distance of node from BS is also considered. CH distance to BS is compared with other nodes CH distance to BS and if difference between CH and BS is greater than predefined value, node will not be selected as CH. d(CH, BS) is distance calculated between CH and BS and $AD_{c\text{ß}BS}$ is the acceptable distance between CH and BS. Hence CH selected with this procedure will be trusted, with better energy and will help in saving energy as transmitting energy cost will be less.

b) Cluster Joining

In original protocol non-CH nodes join cluster based on signal strength received from CH but here nodes will select their CH based on trust values of cluster nodes.

c) Schedule Creation

CH receives all messages from nodes that would like to join cluster. Based upon strength of nodes in the cluster, CH begins to create a TDMA schedule and assign slots to non-cluster nodes to send data as well as to calculate trust value.

2. Steady State Phase

In steady state phase nodes will transmit sensed data to CH along with calculating trust. This phase can be divided into two slots data slots and trust slots [9] . After end of this phase every other round begins with set-up phase.

- **Data Slots:** Nodes will keep their transmitter on during their time slot only and will sense the data in the same time slot and send sensed data to CH selected meanwhile other nodes transmitters are off in order to save energy. It is assumed that CHs are having more energy than normal nodes so they keep their receivers always on to receive data from non-CH nodes of the cluster.
- **Trust Slots:** During this slot trust supervisor will calculate trust associated with their neighbors and CH based upon considered factors. Nodes update their trust value regularly. In addition, CH will calculate trust of neighbour CHs in this slot and updates their table.
  For communication within a cluster i.e. an intra-cluster communication, amplification energy must be less than a inter-cluster communication that is a communication between CH and BS [6]. The reason behind this is within a cluster distance between nodes is less, so less of energy is needed to transmit a message as compared to inter-cluster communication. Therefore more energy could be saved.

4. Simulation Results. The proposed algorithm EETA-LEACH has been designed in MATLAB [30]. It is considered that 100 nodes are randomly distributed over area of 100 × 100 m^2.

4.1. Selection of CH. Figure 4.1 shows random distribution of sensor nodes in an area of 100*100 sq. units and LEACH protocol is simulated for routing purpose. There are some malicious nodes present in the network. Malicious nodes are represented by a plus (+) sign, normal nodes are represented with a circle (o). In addition selection of CH in particular round is also presented in Fig 4.1, nodes that are selected as cluster head are represented with dark blue asterisk. It can be easily analyzed that if no security practises are adopted, malicious nodes present in network could be selected as CH. Hence as a result, malicious CH selected would drop packets received from cluster members witch in result reduce network performance.

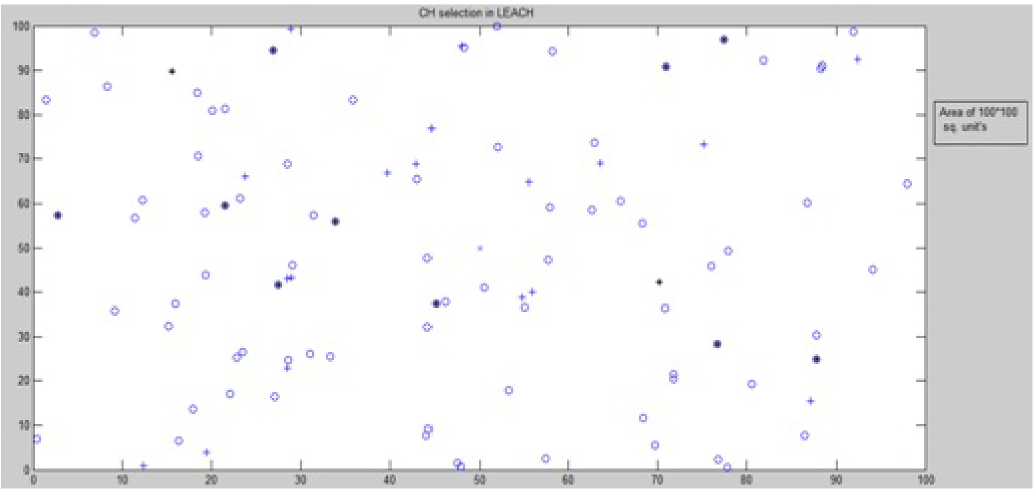

Fig. 4.1. *CH selection in LEACH*

After implementing EETA-LEACH, it is verified that chances of selecting malicious nodes as CH are almost negligible. In EETA-LEACH, CH is selected based upon trust values of nodes. Therefore selected CH will not be malicious. The whole scenario is represented in Fig 4.2. Trusted CH selected is represented by Green asterisk.

Algorithm 1 Trust Calculation Algorithm

```
procedure TRUST CALCULATION
input: Remaining energy, Packet_delievery_ratio,Distance between nodes
Every node is assigned with initial direct trust of 0.5
  if(R.E >Th1)
  DT= DT+5% of DT
  elseif(Th2 <R.E <Th1)
  DT=DT
  elseif(R.E <Th2)
  DT= DT-5% of DT
  End
  if(PDR >Th3)
  DT=DT+5% of DT
  elseif(Th4<PDR <Th3)
  DT=DT
  elseif(PDR <Th4)
  DT= DT-5% of DT End
  if(DS.N $\rightarrow$ E.N >Th5)
  DT=DT+5% of DT
  elseif(Th6 <DS.N $\rightarrow$ E.N <Th5)
  DT=DT
  elseif(DS.N $\rightarrow$ E.N <Th6)
  DT= DT-5% of DT
  end
Indirect trust will be calculated from recommendation nodes
  TT= w *DT + (1-w)*IT
 Notations:
  DT= Direct Trust
  IT= Indirect Trust
  TT= Total Trust
  Th=Threshold Value
  DS.N$\rightarrow$ E.N = Distance between subject node and evaluated node
```

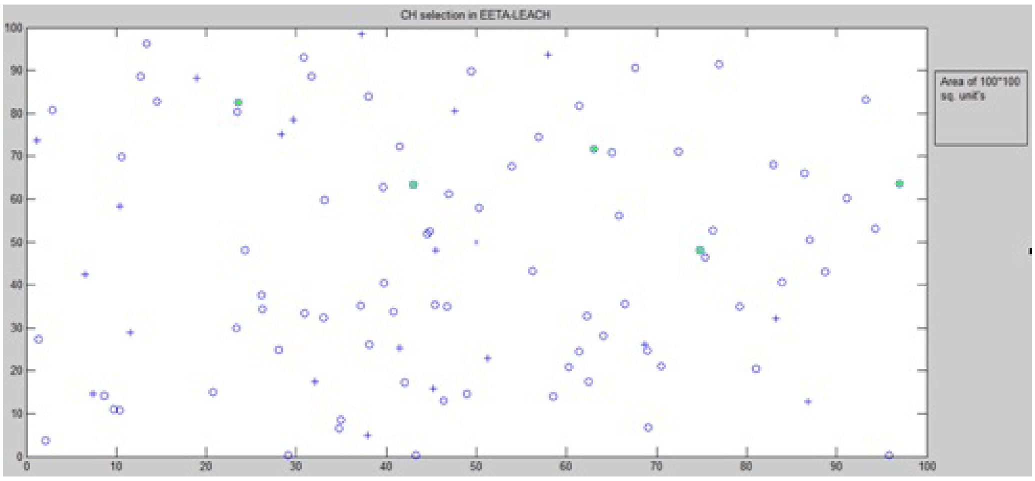

FIG. 4.2. *CH selection in EETA-LEACH*

4.2. Trust Evolution. Figure 4.3 plots trust value of a malicious node. Trust value of a malicious node decreases as time increases. The value of w1 and w2 is chosen to be 0.5 and 0.5 respectively in Eq. 3.5, which concludes that node is equally considering direct trust as well as recommended trust. At very first round node will have direct trust of 0.5, no indirect trust will be considered at first round, hence total trust will constitute to 0.5. Similarly at 10th round direct trust is 0.4800, indirect trust is 0.2438 and thus total trust is 0.3619 for this round. In the proposed model calculated trust is directly proportional to remaining energy and PDR, as malicious node consumes more energy, drops more packets therefore its trust value decreases as number of round increases.

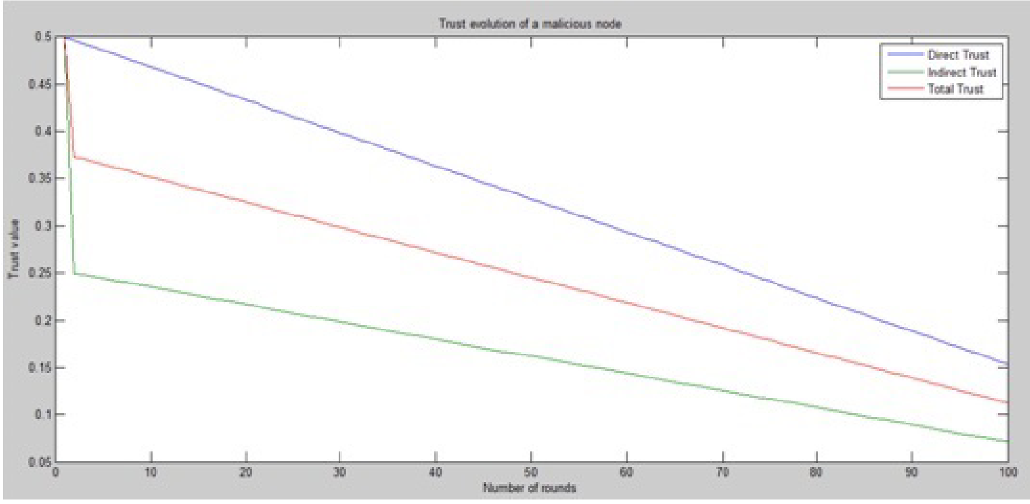

Fig. 4.3. *Trust evolution of a malicious node*

4.3. Analysis of Packet Delivery Ratio. Figure 4.4 shows number of malicious node versus average PDR. It could be observed that average PDR is 96% in EETA-LEACH and 91% in LEACH when there are no malicious node present in the network. There would be some packet loss because of poor network connectivity. Therefore PDR would not be 100% even if no malicious node present in the network. With presence of 5 malicious nodes in network EETA-LEACH network has PDR value of 0.9400 and LEACH has 0.8390, hence after implementing EETA-LEACH PDR increases by 12%. Similarly when 15 malicious nodes are present PDR is increased by 14% and with presence of 25 malicious nodes PDR increases by 21.5%. Hence it could be concluded that after implementing EETA-LEACH average PDR ratio is increased by 15.8%. EETA-LEACH has high average PDR as compared to leach because malicious nodes are not selected as CH and hence there is less packet drop in the network. Moreover EETA-LEACH can help in avoiding selective forwarding attack.

4.4. Network Lifetime Comparison. While comparing network lifetime it has been observed that EETA-LEACH has better lifetime when compared to LEACH as in LEACH there are many retransmissions as compared to EETA-LEACH. In addition in EETA-LEACH less of malicious nodes would be selected as CH so less consumption of energy as it is assumed that malicious nodes are consuming more energy. Moreover, consumption of less energy while intra-cluster communication as compared to inter-cluster communication and consideration of energy factor while selecting CH makes EETA-LEACH more energy efficient. It could be verified from figure 4.5 that in LEACH first node dies near 700th rounds as compared to EETA-LEACH where first node dies at 1100th round. Figure 4.5 shows network lifetime comparison.

5. Conclusion and Future Scope. In this paper an energy efficient trust based approach has been proposed which is combination of trust-based routing module and trust management module. In trust management module, trust supervisor calculates trust for nodes as well CH that can be used for trusted CH selection and secure routing. Total trust value is a combination of direct trust that is calculated by node itself and indirect

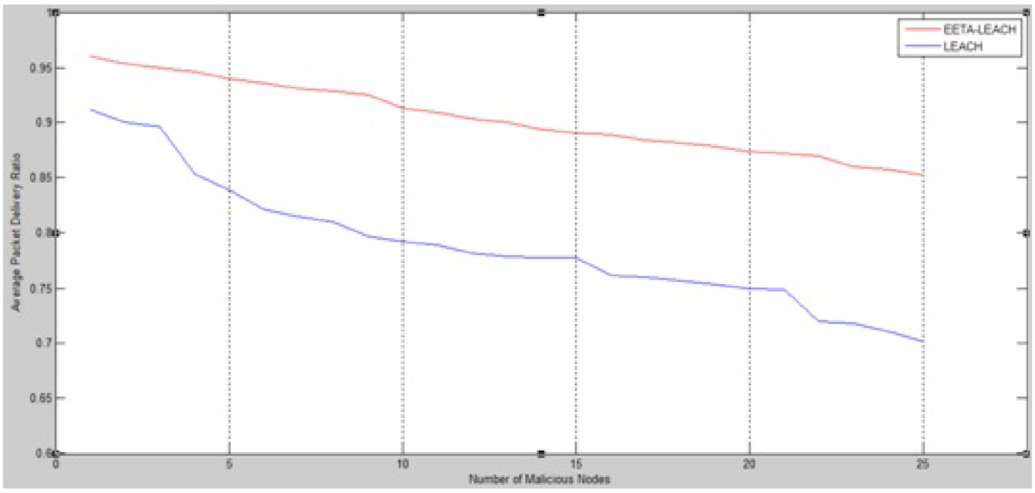

Fig. 4.4. *Packet Delivery Ratio versus number of malicious node*

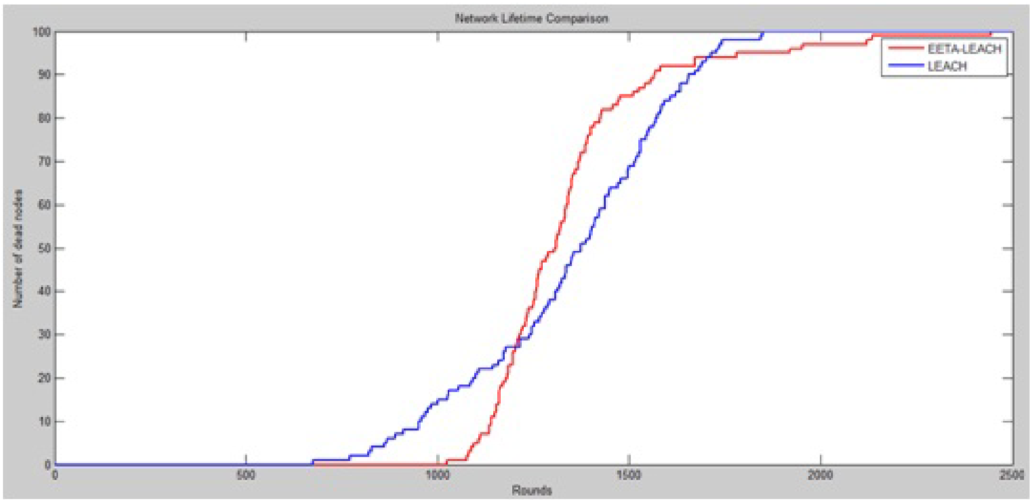

Fig. 4.5. *Network Lifetime Comparison*

trust which is trust from recommendation nodes. Trust-based routing module modifies original LEACH. Routing module comprises of further four phases that are advertisement phase, cluster joining, schedule creation and steady state phase. Nodes that are malicious in nature will have less PDR and consumes more energy. So these malicious nodes will not be selected as CH because their computed trust value will be less. In addition, routing module uses less energy for intra-cluster communication as compared to inter-cluster communication which would help in improving network lifetime. Protocol performance is verified using MATLAB simulator. It is verified that malicious nodes will not be selected as CH and trust value of a malicious node decreases with time. Simulation results proved that proposed algorithm consumes less energy and improves PDR as there are less number of retransmission. Average PDR is improved by 15.8%. In addition with implementation of EETA-LEACH, network lifetime improves as first node dies at 1100th round in EETA-LEACH as compared to LEACH where first node dies at 700th round. In future, this work could be extended by considering other types of WSNs e.g. dynamic WSNs, heterogeneous WSNs. Other social trust attributes such as privacy, intimacy, number of interaction could be considered in future to extend this work. Beside this trust model could be further extended to develop lightweight algorithm to further reduce energy consumption. Memory requirement for this protocol are bit high as past records has to be stored by energy watcher, trust supervisor, PDR calculator. So challenging problem is to reduce memory requirements. In this paper, nodes that have less PDR are considered as malicious without considering the fact that less PDR could be less because of poor network connectivity, this also motivates future work.

REFERENCES

[1] Garcia-Luna-Aceves, J. J., and Spohn, M., *Source-tree routing in wireless networks*, In Network Protocols, 1999.(ICNP'99) Proceedings. Seventh International Conference on, pp. 273-282. IEEE, 1999.

[2] Cordasco, Jared, and Susanne Wetze, *Cryptographic versus trust-based methods for MANET routing security*, Electronic Notes in Theoretical Computer Science 197.2 (2008): 131-140.

[3] A. Miglani, Tarunpreet Bhatia, and Shivani Goel , *TRUST based energy efficient routing in LEACH for wireless sensor network*, In Communication Technologies (GCCT), 2015 Global Conference on, pp. 361-365. IEEE, 2015.

[4] Heinzelman, Wendi Rabiner, Anantha Chandrakasan, and Hari Balakrishnan , *Energy-efficient communication protocol for wireless microsensor networks* , In System sciences, 2000. Proceedings of the 33rd annual Hawaii international conference on, pp. 10-pp. IEEE, 2000.

[5] Naregal, Keerti, and Anand Gudnavar , *Improved cluster routing protocol for wireless sensor network through simplification* , In Advanced Computing and Communications (ADCOM), 2012 18th Annual International Conference on, pp. 1-3. IEEE, 2012.

[6] Mahmood, Danish, Nadeem Javaid, Sajjad Mahmood, Shaima Qureshi, Atif M. Memon, and Tariq Zaman , *MOD-LEACH: a variant of LEACH for WSNs* , In Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013 Eighth International Conference on, pp. 158-163. IEEE, 2013.

[7] Karlof, Chris, Naveen Sastry, and David Wagner , *TinySec: a link layer security architecture for wireless sensor networks* , In Proceedings of the 2nd international conference on Embedded networked sensor systems, pp. 162-175. ACM, 2004.

[8] Marti, Sergio, Thomas J. Giuli, Kevin Lai, and Mary Baker , *Mitigating routing misbehavior in mobile ad hoc networks* , In Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255-265. ACM, 2000.

[9] Song, Fei, and Baohua Zhao, *Trust-based LEACH protocol for wireless sensor networks* ,In Future Generation Communication and Networking, 2008. FGCN'08. Second International Conference on, vol. 1, pp. 202-207. IEEE, 2008.

[10] Wang, Weichao, Fei Du, and Qijian Xu , *An improvement of LEACH routing protocol based on trust for wireless sensor networks* , In Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on, pp. 1-4. IEEE, 2009.

[11] Dhulipala, V. R. Sarma, N. Karthik, and R. M. Chandrasekaran , *A novel heuristic approach based trust worthy architecture for wireless sensor networks*, Wireless personal communications (2013): 1-17.

[12] Kim, Jin-Mook, Hyeon-Kyu Joo, Seong-Sik Hong, Woo-Hyun Ahn, and Hwang-Bin Ryou *An efficient clustering scheme through estimate in centralized hierarchical routing protocol*, In Hybrid Information Technology, 2006. ICHIT'06. International Conference on, vol. 2, pp. 145-152. IEEE, 2006.

[13] Chang, Ruay-Shiung, and Chia-Jou Kuo *An energy efficient routing mechanism for wireless sensor networks* , In Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Conference on, vol. 2, pp. 5-pp. IEEE, 2006.

[14] Xiangning, Fan, and Song Yulin *Improvement on LEACH protocol of wireless sensor network* In Sensor Technologies and Applications, 2007. SensorComm 2007. International Conference on, pp. 260-264. IEEE, 2007.

[15] Lijuan, Yu, and Li Simin *Design and simulation of an improved LEACH algorithm in wireless sensor networks* ,Study of Optical Communications 5 (2008): 67-70.

[16] WU, Chun-tao, and Yan-jun HU *Improvement of LEACH in wireless sensor networks* ,Computer Technology and Development 3 (2009): 023.

[17] Buchegger, Sonja, and Jean-Yves Le Boudec, *Performance analysis of the CONFIDANT protocol*, In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking and computing, pp. 226-236. ACM, 2002.

[18] Anita, X., M. A. Bhagyaveni, and J. Manickam, *Fuzzy-based trust prediction model for routing in WSNs*, The Scientific World Journal 2014 (2014).

[19] Senthilkumar, J., M. Chandrasekaran, Y. Suresh, S. Arumugam, and V. Mohanraj *Advertisement timeout driven bee's mating approach to maintain fair energy level in sensor networks*, Applied Soft Computing 11, no. 5 (2011): 4029-4035.

[20] Sahoo, Rashmi Ranjan, Abdur Rahaman Sardar, Moutushi Singh, Sudhabindu Ray, and Subir Kumar Sarkar *A bio inspired and trust based approach for clustering in WSN* , Natural Computing 15, no. 3 (2016): 423-434.Natural Computing 15, no. 3 (2016): 423-434.

[21] Li, Peng, Xiaotian Yu, He Xu, Jiewei Qian, Lu Dong, and Huqing Nie *Research on Secure Localization Model Based on Trust Valuation in Wireless Sensor Networks* , Security and Communication Networks 2017 (2017).

[22] Luo, Wei, Wenping Ma, and Qiang Gao *A dynamic trust management system for wireless sensor networks* , Security and Communication Networks 9, no. 7 (2016): 613-621.

[23] Kaur, Jugminder, Sandeep S. Gill, and Balwinder S. Dhaliwal *Secure trust based key management routing framework for wireless sensor networks*, Journal of Engineering 2016 (2016).

[24] Liu, Yuxin, Mianxiong Dong, Kaoru Ota, and Anfeng Liu *ActiveTrust: secure and trustable routing in wireless sensor*

networks , IEEE Transactions on Information Forensics and Security 11, no. 9 (2016): 2013-2027.

[25] Zhan, Guoxing, Weisong Shi, and Julia Deng , *Design and implementation of TARF: A trust-aware routing framework for WSNs* ,IEEE Transactions on dependable and secure computing 9, no. 2 (2012): 184-197.

[26] Raje, Radhika A., and Apeksha V. Sakhare , *Routing in wireless sensor network using fuzzy based trust model* , In Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on, pp. 529-532. IEEE, 2014.

[27] Sakthidevi, I., and E. Srievidhyajanani , *Secured fuzzy based routing framework for dynamic wireless sensor networks* , In Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on, pp. 1041-1046. IEEE, 2013.

[28] Fei, Xiong, and Xu Qi Jian *Active trust transmission mechanism for wireless sensor network*, In Intelligent Information Technology Application, 2008. IITA'08. Second International Symposium on, vol. 1, pp. 626-632. IEEE, 2008.

[29] Zhang, Y. *On The Improvement In LEACH Protocol of Wireless Sensor Networks*, Micro Computer Information, 2006,Vol.22(4-1), pp.183-185.

[30] `https://www.mathworks.in/products/matlab`.

Edited by: Kavita Sharma
Received: May 25, 2017
Accepted: Aug 2, 2017