A Trust based Clustering Routing Scheme to Enhance the Security of WSNs

Lakshmisree Panigrahi

ABSTRACT: ***Because of the nature of efficiency and load balancing, LEACH based hierarchical routing protocols mixed with trust management techniques can be one of the good choices to design a trustable and secured wirelesssensornetwork where each node can trust highly on the next hop on their forwarding path.Trust management models can be used as much powerful while aimimg at designing a secured and attack-resistant protocol for routing in wireless sensor networks.In case of trust management models,there are various methodologies and ways exist for computing trust value of a normal sensor node and/or that of a cluster head node and afterwards the resulted trust value can be used in different ways to find a secure routing path.This paper aims to provide a trust management scheme to address the packet drop attack or blackhole attack made by a compromised sensor node inside WSNs.Alongwith the security feature against the above attack,we have implemented DIJKSTRA shortest path algorithm to regain the speed efficiency which may have been degraded due to trust computation in various phases of the routing inside and outside of clusters in the network.***

Index Terms:DIJKSTRA shortest path,LEACH, multi-hop,WwirelessSsensorNetwork,Blackhole attack,Trust Management

I. INTRODUCTION

Prior to routing information about the events,if a trust model will be designed which will show the trustworthiness of the neighbourhood of nodes,then when a event takes place,the nodes has not to calculate the trusting score of neighbour nodes,they will just use the priorly calculated trusted scores of their neighbour nodes and decide the route in which they have to forward their packets with maximum trust.In adherence to the priorly computed trusted model ,the routing will be very faster ,also that will be very much secure.So,we can have a very efficient,secure,faster network which will be the very necessity of networks like WSNs where in many of the instances it will be needed to route correct information about events in a very faster rate with consideration of limited memory,processing,battery powers in between event nodes and base stations.Hence,it is of great importance to build trust models in passive stage of WSNs (when event does not occur) and use those trust model and routing strategy in active stage whenever an event occurs.In this proposed model we have calculated trust values in between nodes of a WSN during passive (offline) stage and have tried to use an efficient routing algorithm at the active(online)stage.In that sense,tried to build a very efficient and trustable WSN both for small and moderate-scale networks. In WSNs,the main role of trust model is that of identification of the node which misbehaves in the network and also the modules helps in the collaboration among the trustable nodes.

Revised Manuscript Received on June 05, 2019

Lakshmisree Panigrahi, Assistant Professor and a PhD student in Computer Science & Engineering Department of Siksha O Anusandhan Deemed to be University, Bhubaneswar, India.

Another positive feature of the model is that it improves the lifetime of networks because of the communication among only honest nodes, disregarding inclusion of dishonest nodes and usage of feedback for the
guidance of future decisions taken by nodes for deciding the correct trustable routing path for communication.There are different categories of trust classified in many different ways based on different features.:

Feature	Categories of TRUST
Based on observation	• Direct Trust
	• InDirect Trust
Based on property	○ Social TRUST
	○ QOS TRUST
Based on the place of usage	• Behavioural TRUST
	• Computational TRUST
Based on cooperation	○ Communication TRUST
	○ Data TRUST

The basic requirements of WSN are:

(i)**Reliability**- A WSN should be trustable and reliable for the users.
(ii)**Scalability**- Upon demand,a WSN should easily be upgradable or expandable.
(iii)**Power efficiency**-A WSN should be operable with minimum power.
(iv)**Mobility**- A WSN should be capable to move from place to place in an easy manner.
(v)**Responsiveness**-A WSN should react quickly i.e A wsn should be responsive[1].

Performance matrics of a wsn includes Scalability,energy efficiency,prolongation of stability period,network lifetime prolongation,efficient datadelivery,average routing overhead ,average end-to-end delay,how easily to be deferred from nodes of faulty nature,Quality of service ,time constraints etc[2].

Applications of sensor networks can be our day to day life as well as in other fields like military applications.Varieties of methods can be used to compute the trust value of a WSN node. The trust management methods can be event-based,reputation-based ,agent-based and collaborative trust management etc.In event-based trust management models,at a specific time event the trust rate will be calculated or that can be done at a periodic basis. In case of trust management models based on reputation,a node will store count of packets those has been transferred from that of a node and then rate of packets transferred from it's successive node will be computed.

An agent node is used for storing information of transferred packet from that of a cluster of nodes In case of agent-based trust models.Business models will be used to calculate trust In the case of collaborative trust management models[3].

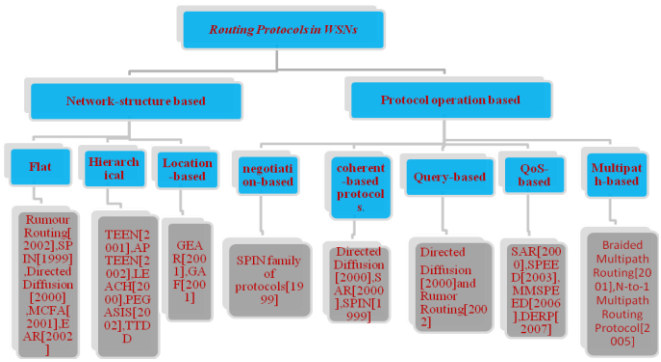
This paper discusses the various works those have been done till date for designing trust models for the security of WSNs as well provides a new idea to develop trust amomg the various nodes of a wsn which further can help for the development of an efficient light weight protocol for the above network.First of all,In section II.A,discussion is on the various works of routing protocols done for wsns.Then in the next section II.B, the LEACH variant routing protocols, in section II.C, Dijkstra algorithm and in Section II.D, some of the important trust and reputation models for wsns has been discussed. After going through the various works on routing and trust management models of wsns, in Section III.A, we have proposed DI-TRUST, a trustable model for secure routing in WSNs.Section III.C comprises of the result of the proposed model.

II. RELATED WORK

This section starts with the discussion of various routing protocols. Routing is an essential activity in case of any wsn since how fast and correct manner a base station can listen to the originate nodes or events will give a profound impact on performance of the wsn and the above can be achieved only if we are using an efficient routing protocol.The different research challenges for routing in wsn are:Diverse topologies,Multiple sources/destinations, Multi-objective routing,QoS with multiple constraints, Security routing,Energy demand,Network applications,Development platforms etc.[4]

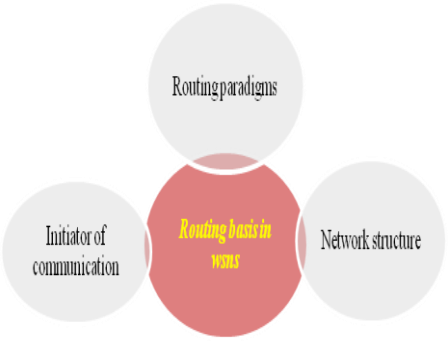
A.Routing Protocols in WSNs

Wireless communication technologies advancement and manufacturing of cost effective wireless devices,these are the two main reason for the widespread use of wireless sensor networks. In each application,the sensor nodes transmit their collected information to the sink nodes or base stations for processing purposes after sensing the target area.Design of efficient routing protocols with respect to different performance parameters of different applications is an important issue in case of wireless networks,particularly wsns.The traditional routing protocols exist in wireless sensor networks are single-path routing in which route discovery performed with minimum resource utilization and computational complexity,But a single path routing approach has limited capacity due to which the achievable network throughput highly reduces. To deal with the above single-path routing technique limitations, routing approach such as multipath routing has been used in case of wireless sensor and *ad hoc* networks. multipath routing approach construct multiple number of paths in between individual sensor nodes to the destination.Utilization of different paths can be concurrently done for providing sufficient network resources in heavy traffic situations.Every source node alternatively uses one path for transmission of data and switches to another different path in the presence of failure(of a node or of a link).The above routing approach is known as alternative path routing and mainly used for the purpose of fault-tolerance.Multipath routing schemes are used in case of different network management purposes like improving Quality of Service (QoS),fault-tolerant support,data transmission,reliability and providing congestion control for wired and also for wireless networks.In[2],Al-Karaki *et al* classified the routing protocols in case of wireless sensor networks as in Fig1.



[Fig1. Hierarchy of Routing protocols in wsns]

The survey paper discussed advantageous,disadvantageous features and problems of many routing protocols like VM-LEACH,EEICCP,ECHERP,HSEP,MqoSP,LFCPMWSN,RPFS-MP,ASLBRP,WB_TEEN,WBMTEEN,LIEMRO,EFRP-ED,HCBQRP,EECBR-RP etc.Also the above paper categorize routing protocols in wsns into 3 types w.r.t 3 basis as shown in fig2.



[Fig2. Types of Routing in WSNs]

According to another survey[5],there are 7 categories of routing models in wsns as shown in Fig3.

[Fig3. Categories of Routing in WSNs]

B. Leach Protocol And Its Variant

LEACH(Low Energy Adaptive Clustering Hierarchy) by Heinzelman, W. R.,et al[6] is a cluster based,distributive routing protocol.In LEACH,periodically cluster heads are elected randomly.Leach works in 4 steps:

- Advertisement step
- Setup step of clusters
- Creation of schedule step and
- Data Transmission step

Every sensornode of the network generates a random number with value ranges between 0 to 1.If the above random number is smaller than *T(n)* which is the threshold value as shown in the following equation(1) ,the corresponding sensornode becomes the cluster head in the current round.The threshold value:

$$T(n)=\begin{cases} p/(1-p*\mathbf{mod}\left(r,\left(\frac{1}{p}\right)\right) & ,\text{if } n\in G \\ 0 & ,\text{otherwise} \end{cases} \quad \text{----------(1)}$$

The process start again after l/p rounds.Each node which has been selected as cluster head at present round will send advertisement message.All remaining non-clusterhead(non-CH) nodes in the network, after receiving the above will take the decision about their clusterhead for the current round. Once cluster heads has been selected, steady-state step starts in which the sensor nodes starts sensing and transmits sensed data to their cluster-heads on basis of TDMA schedule .

There is a huge list of works done as the variant of the LEACH[33,7] to overcome some of the weakholes of the said protocol and to build very good and efficient routing in wsns.Some weakholes of Leach protocols are:

- Maintaining the fixed number of cluster heads at each round with a restriction that each node can become CH within every 1/p rounds exactly once can be difficult at all times.
- The threshold value *T(n)* which is used to select cluster heads at each round.In our proposed scheme ,modifications has been done in the threshold value and is seen better result in terms of different parameters.
- Leach assumes that each of cluster heads created in a round are at same distance from that of the sink or base station and cluster heads will directly send the aggregated information collected from their members to the base station without any intermediaries.But,practically,it may not be true in many applications.In reality,the cluster heads nearer to base station uses less power to send message as compared to remote ones.Many variant works on LEACH has been done to resolve the above issue.
- Energy utilized in unbalanced manners if cluster heads those are created in a round are not distributed evenly,thus decreasing network-lifetime[20].
- Security features is missing in the Original LEACH protocol.

Till date,there are lots and lots of research has been conducted resulting in a huge list of LEACH-Variant protocols.

The objective of many of the above protocols is to overcome one or multiple number of problems of original LEACH with keeping basic steps of routing protocol similar to that of original LEACH protocol.Section II.B.1 to II.B.3 discuss some of LEACH-variants protocols from 3 perspectives as follows.

Section II.B.1 discuss some LEACH-variant protocols based on random numbers,section II.B.2 and section II.B.3 discuss LEACH-VARIANT energy efficient protocols and some trust based LEACH protocols respectively.

B.1. LEACH improvements based on Random Numbers

Many improvement works in the direction of above has been done during years.

- In one Improved LEACH work known as **Gaussian LEACH protocol**[8],authors have suggested Gaussian distribution of random numbers for selection of random numbers(between 0 and 1)which will be done at the beginning of each round.The measurement of network time is done using the following performance parameters:FND(First Node Dies or 99% of total nodes alive),HNA or HND(Half of the Nodes Alive or 50% of total nodes Die) and LND(Last Node Dies or 90% node dies).Results in the above paper shows that Gaussian LEACH outperforms original in terms of many parameters.

- In another work known as **AL-LEACH**[10],the random number has been generated as per the following equation:

  RND= *rnd* ∗ ((*N* − *Dead*)/N)

  During Cluster Setup Phase, each node assumes a random number,*rnd*, between 0 and 1, and it is weighted as per the above Equation; where *N* is the total nodes deployed in the network and *Dead* is the number of dead nodes during a particular round. A node becomes CH, if RND is less than *T*(*n*),where T(n) is the threshold equation. Simulation results showed AL-LEACH attains the highest value of FND, HNA and LND for 11.11%, 16.66% and 100% times respectively.

B.2. Energy-efficient Leach Improved Protocols

In one energy-efficient work[20], QOS parameters like energy spent, end to end delay, throughput, packet delivery ratio is computed retaining the wireless topology and transmission mechanism of LEACH SCHEME. MODLEACH [22] tends to minimize network energy consumption by selecting same cluster heads for next round/s with a condition that node have energy greater than threshold energy.In case of Energy efficient hierarchical clustering (EEHC)[23], formation of clusters in network is done properly and there is an

improvement in the storage level of energy at individual node.Also,there is decrease in energy consumption. S-LEACH[24] protocol used SPIN method within LEACH setup stage to decrease redundancy between identical or similar packets and gives better results as compared to LEACH in terms of energy efficiency, network lifetime and other parameters. Low-energy consumption unequal clustering protocol(LCUCR)[30], adopts multi-hop communication in between clusters and selection of clusterheads(CHs) and sub-clusterheads(sub-CHs) is done by taking distance and energy factors into the fitness function.forming an optimal path between cluster head and base station. Communication between cluster head and that of base station has done via sub-cluster heads. To minimize the problem of intra-cluster communication and hot spot problems, in uneven clustering, a intra-cluster multi-hop technique, has been proposed in[34].After completion of every round, the BS is checking cluster head's and their one hop child node's residual energy and If it is less than or equal to total energy's p fraction, then the BS will start new CH selection process. The above scheme saves energy by minimizing intra-cluster distance of communication avoiding CH rotation per round,In another paper[35] by the above author, a grid-based, unequal, fixed cluster strategy with an advanced data collection strategy has been proposd.Selection of CH is done based on member node's minimal cumulative transmission distance. The above paper has optimizes time value or round number of CH change and establishes relationships in between clusters of different size with the use of a factor(r).In LEACH-C[37],selection of CHs is done by using node energy and location awareness knowledge. In another improved version of LEACH protocol,known as LEACH-E[38], to select CHs, residual energy based minimum spanning tree technique is used. In IBLEACH[39], to minimize the energy consumption of the network,a pre-stage phase defined in between the setup and the steadystate phase. LEACH-EX[40] is a variant of LEACH-E protocol with a modified threshold function and selection of CHs is done through node's energy.LEACH-GA[9] defines a preparation phase along with the setup and steady state phases at the very beginning of first round. Election of CHs is done using optimal probability and genetic algorithm.

B.3. LEACH Protocols based on Trust Factors

There are many security vulnerabilities present in the LEACH protocol[7].Some of the security loopholes which can be created in the set up phase by the attackers are listed as follows:

- An attacker wants to create a wrong TDMA schedule by availing a false member list to the CH
- By broadcasting advertisement message, A malicious node may declare itself as ClusterHead
- From the clustering process, attackers are able to achieve information about cluster members and clusterheads
- By jamming or DoS attacks, attackers can try to disrupt the clustering process
- Attackers prevents some node for joining cluster or they themselves join cluster in setup phase

Since performance of important functions like data aggregation and data routing etc. are done by the cluster heads in case of a hierarchical protocol, unauthotized and inappropriate cluster head selection is one of the dangerous attack in case of LEACH. The proposed DI-TRUST model restricted the malicious nodes (with –ve trust value) to become the cluster head, hence gurantees to have non-malicious nodes as cluster heads.In Research paper[19],it has been considered a versatile trust based secure communication scheme using low-energitic,centralised cluster head(TF-LEACH C) in case of wireless sensor networks. This work uses trust parameters upon **LEACH-C(LEACH-Centralised)** protocol .**LEACH-C** is in basically the same as LEACH protocol with minor changes. Original LEACH is somewhat distributed in the sense that during SET-UP phase, decision about cluster head will be done at node level. But LEACH-C uses centralized approach for selection of cluster heads in each round. All sensor nodes communicate energy level and their position-related information to the base station, providing all necessary information for calculation of the average node energy. The protocol functioning of each round is consisting of four phases.They are:
(i) Advertisement phase (ii) Cluster setup phase (iii) Schedule Creation (iv) Data Transmission.
Evaluation of trust value of a wireless sensor network node is usually done by trust factors like data, communication, Functionality, Energy,Location, Trust update, Risk etc. All seven trust factors are evaluated and combined together to know the trustfulness of sensor nodes. Trust calculation in TF-LEACH C is done as follows: Every node's information is maintained by the cluster heads in a table with 5field entries(NODEID,A,B,R,S). Here, NODEID represents the id of the node for which trust value is calculated, A,B are the number of successful operations and unsuccessful operations respectively(upto last TDMA schedule), R,S are the number of successful operations and unsuccessful operations respectively(in the current TDMA schedule). S value of the trust factor of node N in the table is incremented by 1, if node id of N is specified in the malicious list sent by cluster head,otherwise R value of the above node is incremented. The A and B values of a node is updated by equations detailed in[19]. TLEACH is a WSN trust protocol by Song *et al*.[21]. It is the LEACH with trust component addition.Nodes as cluster heads,select the highest trust value known from their neighbors. The distributed algorithm in the above scheme has high convergent speed, but trust management with reputation may be vulnerable to collusion attacking. Two main components in TLEACH are:the Trust Evaluation Module and the Monitoring Module. A Neighbor Situational Trust Table (NSTT) is maintained by each sensor node filling with trust value entries for each pair of nodes(ids,situational operations). Since nodes may or may not behave maliciously for all the operations.Situational operations have an individual trust value such as data sensing and routing.LEACH-TM[25]selects cluster head based on the trust and the malicious nodes are detected.but it consumes more energy and involves communication overhead.

TBE-LEACH[26] has been proposed for energy efficient routing.

C. Trust and Reputation Models in WSNs

Attacks those may be done by malicious nodes in wsns are:

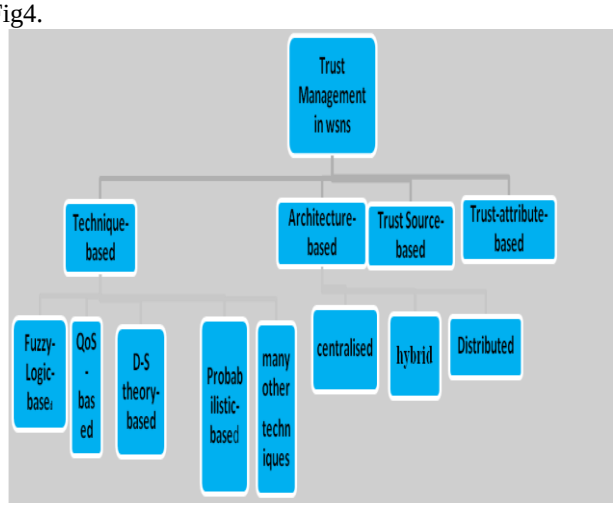
- **False data attack:** To mislead base station's process of decision-making,a malicious node reports false reading.
- **False energy attack:** False energy reporting of a malicious node to become cluster head.The malicious node drops all received data packets after being selected as cluster head.
- **Black-hole attack:** The malicious node drops all received packets.
- **Gray hole attack:** Selectively forwarding,dropping and tampering integrity the data packets by a malicious node.
- **Packet delay attack:** Other than the given time schedule, the malicious node will send data packets to cluster head and the later, discard the data packet by assuming it is old .
- **Badmouth attack**: False trust value reporting of a well-behaved sensor node is done by a malicious node. The false report will damage the reputation of the well-behaved node.

While evaluating the trust degree on the node N by node M,mainly following trust factors are analyzed[32]:

(1)Successfully sending packets rate: Node N's successful rate of sending packets in a period T.
(2) Received packets rate: Change of node N's received packets rate in a period T.
(3)Packets forwarding rate : Rrelation between sent packets and received packets of node N in a period T.
(4) Node availability: Relativity between hello packets sent and ACK feedbacks received by node M.
(5)Time frequency: Time relativity of context content in period T.
(6) Data consistency: Degree of difference for sending data packets between node N and its neighbor nodes.
(7) Security grade: Security requirements in accordance of different application fields of the network like Battle field, emergency response *etc*.
A neighbor node can be malicious or not can be determined by their trust value. By using above concept,paper[11] detect jamming, hello flood and selective forwarding attacks for a sensor network.
A resource-friendly and simple trust model,known as AEMP model has been presented in[12]. Data and communication trust has been used in[13] and reputation based trust is in [14]. Survey works on trust factors and trust models has been done in[15,17]. In another work[16] on trust models in wsns, data and communication trust has been computed for discrete and continuous events. Behaviour trust, historical trust, weighted trust, comprehensive trust, energy trust, locational trust can also have a role for constructing secure routing path of wsns.According to[18],there are three ways for using trust In routing decisions.The three ways are:

i. Trust-centric next hop selection
ii. Shortest Distance to Destination considered First(SDDF) and
iii. Weighted Routing Cost Function,

Trust Management models in wsns can be structured as in Fig4.



[Fig4. Trust Management in Wsns]

D. DIJKSTRA's Algorithm

Dijkstra's algorithm for the shortest path Problem,from the point of view of Dynamic programming is a successive approximation scheme which solves the above problem by the Reaching method. In this case, Dijkstra's explanation paraphrases the logic of the Bellman's principle of optimality in the context of shortest path problem which states as follows:
"In the problem of finding the shortest path in between 2 nodes, say A and B,if C is one of the node In the minimal path from A to B ,then minimal path knowledge of A to C can be obtained from that of the minimal path knowledge of A to B". Even though there are many variants of Dijkstra algorith present,in our proposed model we have used the original Dijkstra algorithm which finds the shortest path between two nodes of a graph with positive weighted edges. There are many works made in the literature with routing protocols in wsns. Since LEACH has motivated many researchers to further investigate the said protocol, no need to say, LEACH has been improved by many refinements using DIJKSTRA's ALGORITHM alongwith other shortest path algorithms. Since,our proposed work uses DIJKSTRA's ALGORITHM to find the shortest path in between message source node(non-cluster-head or non-clusrter-member) to the sink, listed below some works of implementation of DIJKSTRA's ALGORITHM within wsn, particularly within the LEACH routing protocol.
The algorithm[27] generates shortest hop braided multipath in order to be used for fault-tolerance or load-balancing. It guarantees the BFS tree and generates near optimal paths in O(V.D+V) message complexity and $O(D^2)$ time complexity regarding the communication costs towards the sink after termination of algorithm. The improved LEACH-DT(LEACH-Dynamic threshold[28] algorithm has balanced energy consumption of various nodes in network, reduced average energy consumption of the nodes, postponed death time of the first node in network, extended the life time of network, and increased the network throughput. LEICP (low energy intelligent clustering protocol)[29], an improvement of the LEACH protocol is proposed to overcome the shortcomings of LEACH. LEICP aims at balancing the energy consumption in every

cluster and prolonging the network lifetime. A fitness function is defined to balance the energy consumption in every cluster according to the residual energy and positions of nodes. In every round the node called auxiliary cluster-head calculates the position of the clusterhead using Bacterial Foraging Optimization Algorithm (BFOA). After aggregating the data received, the cluster-head node decides whether to choose another cluster-head as the next hop for delivering the messages or to send the data to the base station directly, using Dijkstra algorithm to compute an optimal path. The performance of LEICP is compared with that of LEACH.LEICP had prolonged the lifetime of the sensor network by about 62.28% compared with LEACH and acquire uniform number of cluster-heads and messages in the network.In Unequally Clustered Multihop Routing (UCMR)[31] protocol where each cluster has a different cluster size, based on its distance with reference to base station. In order to minimize the energy consumption of network and to improve the overall network performance the multi-hop routing with using Dijkstra's shortest path algorithm is used for intracluster and intercluster transmission.

III. PROPOSED TRUST MODEL

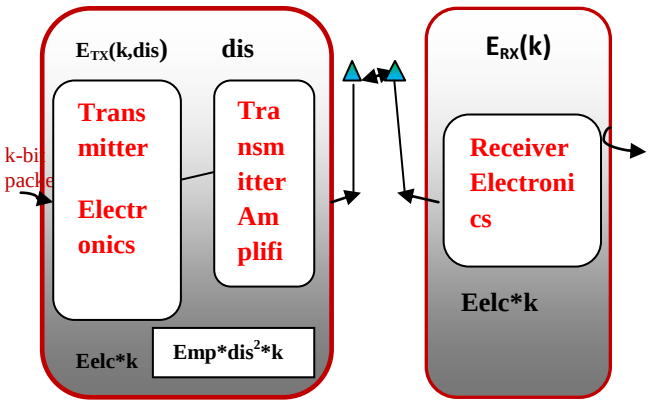
In DI-TRUST model, a new 2-tier clustering routing procedure have been proposed. From hierarchical routing procedure point of view,the above model is same as LEACH model. But internal procedures with regard to security and energy efficiency is different.

A. Energy Model

Energy model has a profound role on the lifetime of a wsn. Generally,two types of energy models are suitable for wsns.[9]

Two types of Energy Models in case of WSNs
a) First Order Radio Energy Model
b) Realistic Radio Model

LEACH protocol uses First-Order Radio energy model whose working model is as shown in Figure5.



[Fig5. First Order Radio Energy Model]

The dissipation energy of a radio for transmission of a k-bit message over a distance **dis** with an acceptable Signal-to-Noise Ratio (SNR) is as given in equation2.

$$E_{RX}(k,dis)=\begin{cases} k*Eelc+k*Efs*dis*dis, & \text{if } dis < d0 \\ n*Eelc+k*Emp*dis*dis*dis*dis, & \text{if } dis \geq d0 \end{cases} \quad \text{------(2)}$$

where **Eelc=** Energy dissipated per bit to run the transmitter or the receiver circuit

Efs and **Emp=E**nergy of transmitter amplifier models

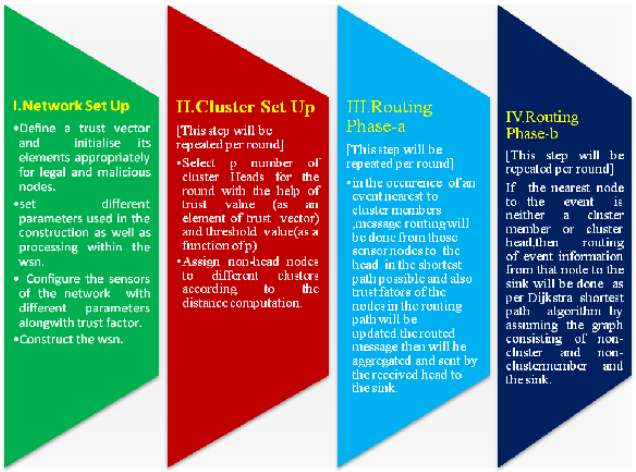
dis=The distance between the communicating nodes

Cross Over distance(d_0)=$\sqrt{Efs/Emp}$.

For the receive of a k-bit message,the energy expenditure by the radio(E_{RX})=**k*Eelc.**

B. Overall Construction of Proposed Model

Overall construction of the proposed scheme is in Fig6.



[Fig 6. Steps of proposed DI-TRUST model]

In the proposed DI-TRUST model,it has been assumed that the sink node will send multiple number of dummy packets to each of the nodes of the network initially. Since ,our model's underlying network uses TCP protocol, it has assumed that there should have been acknowledgement (ACK)packets transmmittd from the receiver back to the sender end. Hence, with respect to the above, the sink node should receive the acknowledgement (ACK)packets in response to each of the data(dummy) packets which it has sent from itself to each of the nodes of the sensor network. We have taken a universal trust vector for the whole sensor network, each entry of which will be set integer values(-ve or +ve integers) representing trustworthiness of the nodes of the network. The next issue is how the values of the above vector will be set . To resolve this issue,in our model, we have taken the parameter of the number of acknwoledgement received by the sink node from each of the nodes of the sensor network to which it already has sent multiple (say N) dummy packets.Initially,let us assume that all entries of the trust vector as 0's.After a successful receive of ACK packet from a particular node, the trust entry for that particular node in the trust vector will be increased by 1 whereas the inverse will be done (i.e. trust value will be decreased by 1)after the sink will not receive the ACK packets within a stipulated time. The trust vector will be updated at each step and after finishing all the above dummy-ACK packet transfer and corresponding updation of trust vector, the sink node will deselect all nodes with -ve trust entries in the trust vector to become the cluster head. All the above steps will be performed prior to the set-up and steady-state phase of hierarchical routing protocol.

After set-up phase will begin , our model will first of all check the trust entries in the trust vector and if it is -ve, then we have assumed for that node to be discarded for being a cluster head. After finishing set-up phase, (the sensor network now has found it's clusters and associated cluster heads for that particular round) the network will be in steady-state phase in which actual data transmission will begin within nodes of clusters
in response to an event. At the instance of an event, the nearby sensor nodes will forward the information regarding the event to the cluster head through intermediate route and cluster head after doing suitable refinements and aggregation will forward the same directly to the sink. During the above intracluster routing process also, we have implemented trust vector. We have defined separate trust vectors for different clusters. Here, the size of intracluster trust vector is as per the size (no of member nodes)of a cluster. Suppose, no of clusters in a round of hierarchical routing protocol is NS, then for NS different clusters, we have defined NS number of trust vectors(let us name them asT1,T2,...Tns). The no of members of each of these clusters is not uniform. Hence trust vector size for them is not same. For example, if number of nodes in the cluster T1 is N1, then trust vector for that cluster is T1(N1) and correspondingly trust vector for the cluster k, of size Nk is Tk(Nk) and so on.. The different trust vectors will be updated differently since data routing will occur within the nodes of a particular cluster at any instance of event occurence.

In every round after the SET-Up phase, the network may left with some nodes which do not belong to any cluster. By taking those isolated nodes,a weighted graph will be defined. Also, the sink node will be defined as one of the above graph. Out of all those isolated nodes, some may be nearby sink and some may be far away. That is the only reason to consider the sink as one of the nodes of the above graph. Now, in the instance of sensing the presence of an event by an isolated node, the information will be sent from the above node to the sink by using Dijkstra Shortest Path algorithm. In this case, the source node is the sensed node and destination is the sink node. If, out of every nearby neighbour, sink node is the nearest node, message will directly flow to sink, otherwise, the best cost route will be choosen from source node to that of the sink.
If nearby node of an event is a cluster member, then message will flow from that node to the cluster head using either MultiPath routing or 3-Phase routing depending on a probability value similar to that of the LEACH protocol. While routing within a cluster, the suitable entries in the trust vector will be checked and if trust entry is permittable, then only routing takes place to the cluster head and trust vector will be updated appropriately.

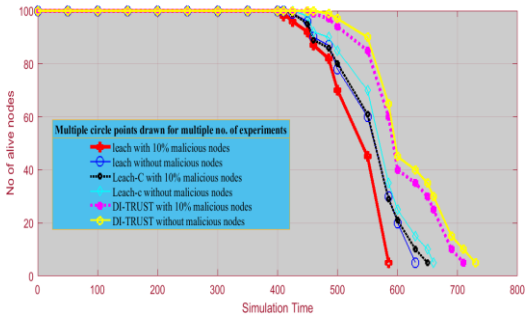
C. Simulation Results

DI-TRUST has been simulated in MATLAB[36].The different parameters for the simulation is as given in following table1 .

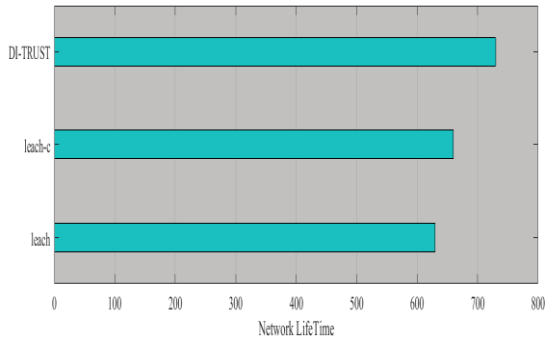
Parameter Name	Value
Simulation tools used	MATLAB
Node Deployment Area	100m X 100m
Simulation Stopping Criteria	Till number of dead nodes=5
Initial Energy/Node) (in Joules)	1.0
Energy for Data Aggregation(*EDA*)	5 nJ/bit/message
Multi-path Fading (Emp)	
Transmitter Electronics (*ETx−elec*) Receiver Electronics (*ERx−elec)* (*ETx−elec* = *ERx−elec* = *Eelec*)	50 nJ/bit
Free Space (E_*fs*)	10 pJ/bit/*m*2
Percentage of Cluster Heads	5%
Relative Position of BS	(50,50)
Packet Size	4000
Number of Nodes (Excluding BS)	3 to 100(randomly deployed)
Proposed Approach Compared with :	LEACH,LEACH-C

[Table1. Simulation Parameters]

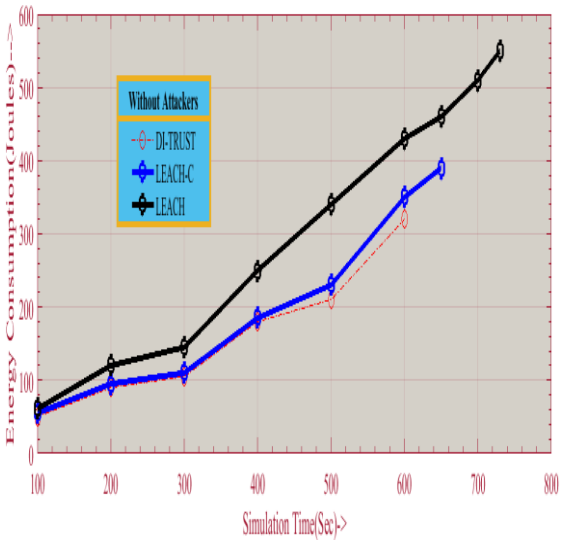
The simulation results are as shown in Fig7 to Fig9.As can be seen from the results shown in figures, DI-TRUST shows better performance in terms of energy savings, network lfetime, no of alive nodes per round etc. alongwith maintaining security against blackhole attacks by using trust vectors. Hence, the proposed model can be considered as an improved energy efficient trust managed version of LEACH for wsns.



[Fig7. No.of Alive nodes Vs Simulation Time]



[Fig8. Execution Time comparison of Leach,Leach-C,DI-TRUST]



[Fig9. Total Energy Consumption Vs time]

IV. CONCLUSION

In the proposed model,DIJKSTRA ALGORITHM have been implemented within the traditional steady-state phase to compromise the delay introduced due to trust calculation at various steps of the routing process. It is found that after introducing trust computation step also,the algorithm gives efficient routing results. Hence,the DI-TRUST model can be used as an efficient trust-based routing model retaining the security of the network.It has assumed that all cluster head will send their aggregated data directly to the sink. But, this may not be suitable for all cases. The cluster head which is nearer to the sink can send faster comparatively with that of the remote cluster heads. Also,the proposed model is cofined upto 100 nodes.In future, the above can be experimented for a large network consisting of more than 100 nodes. With the exclusion of above cases,the model gives efficient results in terms of various parameters(w.r.t routing as well as security) in comparison to that of the LEACH protocol.

REFERENCES

1. S.Natarajan,Dr.H.Abdul Rauf,Dr.S.P.Victor,"Virus Threat Identification in WSN based Networks",*International Journal of Technology in Computer Science & Engineering* ISSN 2349 – 1582 ,Volume 4, No 2, June 2017.
2. Al-Karaki, J.N.; Kamal, A.E. Routing Techniques in Wireless Sensor Networks: A Survey. *IEEE Wirel. Commun.* **2004**, *11*, 6–28.
3. Yenumula B. Reddy,"TRUST-BASED APPROACH IN WIRELESS SENSOR NETWORKS USING AN AGENT TO EACH CLUSTER",*International Journal of Security, Privacy and Trust Management (IJSPTM)*, Vol.1, No.1, February 2012.
4. Amit Sarkar and T. Senthil Murugan,"Routing protocols for wireless sensor networks: What the literature says?",lexandria Engineering Journal (2016) 55, 3173–3183.
5. Mallanagouda Patil and Rajashekhar C. Birada,"A Survey on Routing Protocols in Wireless Sensor Networks",*ICON* 2012,pp 86-91.
6. Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan," Energy-Efficient Communication Protocol for Wireless Microsensor Networks", t *2000 IEEE. Published in the Proceedings of the Hawaii International Conference on System Sciences*, January 4-7, 2000, Maui, Hawaii.
7. Mohammad Masdari, SadeghMohammadzadehBazarchib, MoazamBidaki," Analysis of Secure LEACH-Based Clustering Protocols in Wireless Sensor Networks", *Journal of Network and Computer Applications* 36 (2013) 1243–1260.
8. Ankit Thakkar1, Ketan Kotecha2," A NEW ENHANCED LEACH ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORK BASED ON GAUSSIAN DISTRIBUTION OF RANDOM NUMBERS", *International Journal of Advanced Research in Engineering and Technology (IJARET)*, Volume 4, Issue 7, November – December (2013).
9. Banerjee, Joydeep & Mitra, Swarup & Naskar, M. (2011). Comparative Study of Radio Models for data Gathering in Wireless Sensor Network. *International Journal of Computer Applications.* 27. 49-57. 10.5120/3433-4480.
10. Thakkar A., Kotecha K , AL-LEACH (2014) Alive Nodes Based Improved Low Energy Adaptive Clustering Hierarchy for Wireless Sensor Network. In: Kumar Kundu M., Mohapatra D., Konar A., Chakraborty A. (eds) Advanced Computing, Networking and Informatics- Volume 2. Smart Innovation, Systems and Technologies, vol 28. Springer, Cham.pp51-58.
11. Syed Muhammad Sajjad,Safdar Hussain Bouk,Muhammad Yousaf,"Neighbor Node Trust Based Intrusion Detection System for WSN",Procedia Computer Science 63 (2015) 183 – 188.
12. Gu Xiang,Qiu Jianlin,Wang Jin,"Research on Trust Model of Sensor Nodes in WSNs", Procedia Engineering 29 (2012) 909 – 913.
13. Momani M. (2010) Trust Models in Wireless Sensor Networks: A Survey. In: Meghanathan N., Boumerdassi S., Chaki N., Nagamalai D. (eds) *Recent Trends in Network Security and Applications. CNSA 2010. Communications in Computer and Information Science*, vol 89. Springer, Berlin, Heidelberg
14. G.Edwin Prem Kumar et al,"A Comprehensive overviem on Application of trust and reputation in Wireless sensor network",Procedia Engineering 38 (2012) 2903 – 2912.
15. Mohammad Momani, and Subhash Challa,"Survey of Trust Models in Different Network Domains,"in International Journal of Ad Hoc, Sensor & Ubiquitous Computing, 2010
16. Yenumula B. Reddy,"TRUST-BASED APPROACH IN WIRELESS SENSOR NETWORKS USING AN AGENT TO EACH CLUSTER",International Journal of Security, Privacy and Trust Management (IJSPTM), Vol.1, No.1, February 2012.
17. Zhenguo Chen,Liqin Tian and Chuang Lin,"Trust Model of Wireless Sensor Networks and Its Application in Data Fusion",sensors 2017,17,703.
18. S. Voliotis, H.C. Leligou and Theodore Zahariadis,"Incorporating trust in location-based routing protocols",51 International Symposium ELMAR-2009, 28-30 September 2009, Zadar, Croatia.
19. Geetha V, K. Chandrasekaran, "Trust Factor based LEACH-C protocol for wireless sensor networks". *International Journal of Computer Applications* (0975 8887) Volume 105 - No. 18, November 2014.
20. MS. WAJEDA PATHAN,DEEPAK.C.MEHETRE," SECURE ENERGY EFFICIENT cOMMUNICATION IN CLUSTERING FOR WIRELESS SENSOR NETWORKS", *International Journal of Advanced Computational Engineering and Networking*, ISSN: 2320-2106, Volume-5, Issue-3, Mar.-2017.
21. Song, F.; Zhao, B.H. Trust-Based LEACH Protocol for Wireless Sensor Networks. In *Proceedings of the Second International Conference on Future Generation Communication and Networking*, Volume 01,Yokohama,Japan, 13–15 December 2008;. FGCN. IEEE Computer Society, Washington, DC,pp.202-207,IEEE,2008.
22. D.Mahmood,N.Javaid,S.Mahmood,S.Qureshi,A.M.Memon,T.Zaman, " MODLEACH: A Variant of LEACH for WSNs", 2013 Eighth International Conference on Broadband, Wireless Computing, Communication and Applications,IEEE.
23. Dr. M. Kezia Joseph1, Shafia Tasneem," Energy Efficient Hierarchical Clustering (EEHC) Protocol using Apply Trust Based Concept for Securing Cluster-Based Sensor Networks", *International Research Journal of Engineering and Technology* (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 07 | July-2016.
24. Ali F. Marhoon,Mishall H. Awaad,"Reduce Energy Consumption by Improving the LEACH Protocol", IJCSMC, Vol. 3, Issue. 1, January 2014, pg.01 – 09.
25. 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.

26. Arzoo Miglani,Tarunpreet Bhatia,Shivani Goel,,"TRUST based energy efficient routing in LEACH for wireless sensor network", *Proceedings of 2015 Global Conference on Communication Technologies(GCCT 2015)IEEE.*
27. Onur Yilmaz a, Sercan Demirci a, Yagiz Kaymakb,∗, Serkan Erguna, Ahmet Yildirim," Shortest hop multipath algorithm for wireless sensor networks", *Computers and Mathematics with Applications 63* (2012) 48–59.
28. Yong Lu, Xingwen liu, and Ming li," Study on Energy-Saving Routing Algorithm Based on Wireless Sensor Network",*Journal of Computers* Vol. 28, No. 4, 2017, pp. 227-235.
29. Li, L. Cui, B. Zhang and Z. Fan, "A low energy intelligent clustering protocol for wireless sensor networks," *2010 IEEE International Conference on Industrial Technology*, Vina del Mar, 2010, pp. 1675-1682.
30. Changjiang Jiang,Yun Ren,Yuwei Zhou,Hancheng Zhang," Low-energy Consumption Uneven Clustering Routing Protocol for Wireless sensor Networks", 2016 8th *International Conference on Intelligent Human-Machine Systems and Cybernetics.*
31. U. Hari, B. Ramachandran and C. Johnson, "An Unequally Clustered Multihop Routing protocol for Wireless Sensor Networks," *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI),* Mysore, 2013, pp. 1007-1011.
32. Renjian Feng,Xiaofeng Xu,Xiang Zhou and Jiangwen Wan,"A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory", *Sensors* 2011, *11*, 1345-1360.
33. Singh, Sunil Kumar & Kumar, Prabhat & Singh, Jyoti. (2017). A Survey on Successors of LEACH Protocol. *IEEE Access. PP. 1-1. 10.1109/ACCES*S.2017.2666082.
34. Singh, Sunil Kumar & Kumar, Prabhat & Singh, Jyoti & Alryalat, Mohammad. (2017). An energy efficient routing using multi-hop intra clustering technique in WSNs. 381-386. 10.1109/*TENCON.2017*.8227894.
35. Singh, Sunil Kumar & Kumar, Prabhat & Singh, Jyoti. (2018). An Energy Efficient Protocol to Mitigate Hot Spot Problem Using Unequal Clustering in WSN. Wireless Personal Communications. 10.1007/s11277-018-5716-3.
36. https://www.mathworks.in/products/matlab.
37. Heinzelman.W, Chandrakasan.A and Balakrishnan.H. (2002) "An Application-Specific Protocol Architecture for Wireless Microsensor Networks", *IEEE Transactions on Wireless Communications* **1(4)**: 660-670.
38. Xu.J, Jin.N, Lou.X, Peng.T, Zhou.Q, and Chen.Y. (2012) "Improvement of Leach protocol for WSN", In IEEE sponsored *9th International conference on fuzzy systems and knowledge discovery*: 2174 – 2177.
39. Salim.A, Osamy.W, and Khedr.A.M. (2014) "IBLEACH: Intra-balanced Leach protocol for Wireless Sensor Networks", *Wireless Network* **20 (6)**: 1515 – 1525
40. Anand.G and Balakrishnan.R. (2013) "Leach-Ex protocol – A comparative performance study and analysis with Leach variants of Wireless Sensor Networks", *National Conference on Frontiers &Advances in Information Science & Technology*: 192 – 196.

AUTHORS PROFILE

Lakshmisree Panigrahi is currently an Assistant Professor and a PhD student in Computer Science & Engineering Department of Siksha O Anusandhan Deemed to be University, Bhubaneswar, INDIA. She has done M.Tech in Computer Science and Engg in the same University. Her Research interest includes Computer Networking, Security and Bioinformatics.