An Efficient Trust based Routing Model using Ant-Colony Optimization for the Security of WSNs

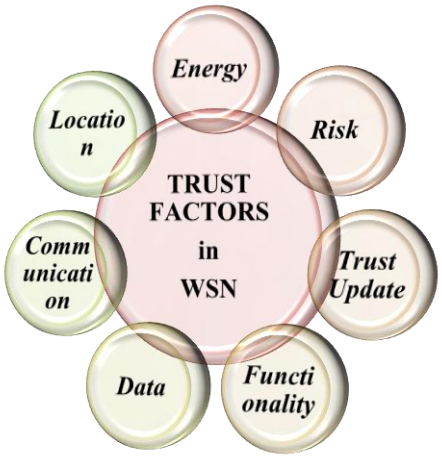
Lakshmisree Panigrahi

Abstract: ***Trust-based leach variant routing protocols mixed with ant colony optimization techniques can be one of the good choices to design a trustable and secured wsn. Many optimization techniques like Genetic Algorithms, Fuzzy Logics, Swarm Intelligence have been utilized by researchers to develop efficient routing protocols for wsns.if we discuss about Swarm Intelligence, then Lots of research work has been done already and also lots others are going to be done mainly on 2 colonies.one is bee-colony-optimization(BCO) and another one is ant-colony- optimization(ACO) .This paper proposes ACOTRUST, a trustable leach-based routing method using ACO algorithm to optimize routing with maintaining other parameters like distribution of energy dissipation evenly throughout the sensors, energy efficiency, throughput, security of wsns.***

IndexTerms: ***LEACH protocol, wireless sensor network, blackhole attack, Trust Management, Ant-Colony Optimization***

I. INTRODUCTION

This paper discuss the various works those have been done till date for designing trust models for the security of WSNs as well as providing a new idea to develop trust amomg the various nodes of the same which further can help for the development of an efficient light weight protocol for the above net work.The following trust factors are applicable in wsns[14]:



[Fig1.Trust Factors in WSNs]

In section II-A,the various works of routing protocols done for wsns have been discussed and section II-B discuss the Qos based routing protocols, Since now-a-days for many real time application areas of wsn,Qos is one of the important performance measures and ACOTRUST emphasizes the Qos performance metrics along with others .Sectional-C will discuss various ACO-based routing techniques since for our knowledge Computational Intelligence techniques are one of the best ways to design an efficient QoS-based routing technique in case of a WSN and Ant-colony optimization is a good Computatinal Intelligence technique.Since ACOTRUST implements trust with the Aco-Based routing ,Section II-D provides information about some of the important trust and reputation models for wsns.After going through the various works on Aco-based, QOS emphasized, and trust management models of wsn, Section 3,discuss ACOTRUST, the proposed ACO-implemented trustable model for secure routing in WSNs. And section 4 comprises simulation 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 for events, accordingly that 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.[12]

A.Routing Protocols in WSNs

There are many routing protocols designed and implemented by many researcers till date.As discussed In [5],there are 3 broad types of routing protocols:
-> routing protocols on the basis of network structure,
->routing protocols on the basis of routing paradigms and
->routing protocols on the basis of initiator of communication.

The authors also has listed out and compared various routing protocols w.r.t the above three types. The above paper has given advantageous,disadvantageous features and problems of many routing protocols like VM-LEACH,EEICCP,ECHERP,HSEP,MqoSP,LFCP-MWSN,RPFS-MP,ASLBRP,WB_TEEN,WBM-TEEN,LIEMRO,EFRP-ED,HCBQRP,EECBR-RP etc.In Another survey work[6] on routing in wsns stated **Taxonomy of Routing Protocols in WSN as (7 categories),they are:**

1.Hierachical − TEEN, LEACH and APTEEN
2.Data Centric −Rumor Routing and Directed Diffusion
3.Location Based −GEAR and GAF
4.MultiPath − Disjoint Path Routing
5. Negotiation − SPIN

Revised Manuscript Received on June 05, 2019

akshmisree Panigrahi, is currently a PhD student under Sikshya 'O' Anusandhan University ,Bhubaneswar, INDIA

6.Mobility − Joint Mobility and Routing
7.QOS Based − Sequential Assignment Routing

TEEN and APTEEN performs well as compared to LEACH (Low Energy Adaptive Clustering Hierarchy). performance of APTEEN is found to be in between LEACH and TEEN w.r.t the measures of network lifetime and energy dissipation.TEEN will not be recommendable for applications requiring periodic reporting of data.

B. Qos based routing protocols in wsns

For WSN routing,QoS requirements can be considered in terms of delay,reliability and fault tolerance in addition to energy consumption minimization.The reliability and fault tolerance need additional sensors deployment so that the network can be continued as function properly and there can be an accurate data deliver of the sensed events to the sink in the presence of failures of some sensor nodes[7].For WSNs,Sequential Assignment Routing,SAR is a good Qos-based routing which is table-driven and multipath routing aiming at energy efficiency and fault tolerance. QoS based routing are advantageous in real time applications like tracking targets tracking battle fields.But QoS requirements handling energy efficiently now-a-days is an open research issues.

In a survey work[8] for routing in wsn using computational intelligent techniques,the various intelligent techniques has been discussed.The various routing schemes for computation intelligent based routing are:fuzzy logic, neural networks, genetic algorithm, reinforcement learning, ant colony optimization.

Technique of Computational Intelligence	*Routing Protocols*
NN based	Sensor intelligence routing (SIR)
FL based	Cluster head election using fuzzy logic (FCH) Fuzzy multi-objective routing (FMO)
RL based	Q-learning based routing(Q-Routing) Adaptive routing (AdaR)
GA based	Genetic algorithm based routing(GA-Routing) Genetic algorithm based energy-efficient clustering protocol (GA-EECP)
ACO based	Energy-efficient ant based routing (EEABR) Sensor-driven cost-aware ant routing (SC) Basic ant routing (BAR) Flooded piggybacked ant routing (FP) Flooded forward ant routing (FF)

RL-based techniques(ex:Q-Routing:,AdaR) for routing in wsn are highly flexible to topology changes.easy to implement and is suitable to solve distributed routing in WSNs.The limitation is that trade-off between exploitation (adoptation for experienced pairs of state–action with good reward) and exploration (new knowledge groping).Fuzzy Logic techniques(ex:FCH,FMO) are suitable to achieve multiple objectives by routing optimization and clustering heuristics.But the problem of fuzzy system is that it will not generate optimal solutions, and need re-learnt of fuzzy rules with changes in topology.ACO based techniques(Ex:SC-FF-FP,BAR,FF,FP,EEABR) approaches to the global shortest even though they seems to achieve local shortest.A search frontier needs to be maintain by that of GA-based techniques seeking for global optima as well as solving multi-criteria based optimization problems. It has its ability for permutation-based,rule-based representation with constructive solutions which can be applied to many machine learning and pattern recognition problems [11].In WSNs, GA based techniques (Ex:GA-Routing,GA-EECP)is suited for clustering when the clustering schemes can be pre-deployed. But it requires high processing,usually with a centralized solution.NN based techniques (Ex:SIR) improves WSN performance,But require high processing demands with that of centralized solutions.

C.LEACH AND IT'S VARIANTs

Low Energy Adaptive Clustering Hierarchy,LEACH (Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000, January)[3] is a cluster based routing protocol which has put the base of cluster-based routing in wsns and given the researchers of the above field a new interesting concept to do research in the said direction. LEACH offers an efficient way to minimize the power consumption in sensor networks.Some of the important assumptions of LEACH protocol are:

- The base station is assumed to be positioned at the center of the deployment area of the whole network which is having huge amount of energy,possibly infinite energy.
- Sensor nodes of the network are of homogeneous nature and each node will have their own unique identifiers.
- Every sensor is assumed to be statically positioned at deployment time and they will not change their position after deployment.
- Unlike base station or sink,all sensor nodes have uniform and finite energy,
- Energy consumption and distribution of cluster heads inside the network is uniform.
- Links of communication are symmetric from any sender to receiver inside network.
- There is always available data to be sent by the sensor nodes so that at every iteration the cluster head has to do the aggregation of data received from associated members.
- Various phases of LEACH are.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

I.	Advertisement phase
II.	Cluster setup phase
III.	Schedule creation phase(Generally TDMA)
IV.	Data transmission phase

LEACH protocol has some weak holes which can be improved.The improvements has been done in several LEACH variants and also can further improved in near future are:

- The threshold value *T(n)* which is used to select cluster heads at each round.In our proposed scheme ,we have done modifications in the threshold value and seen better result in terms of different parameters.

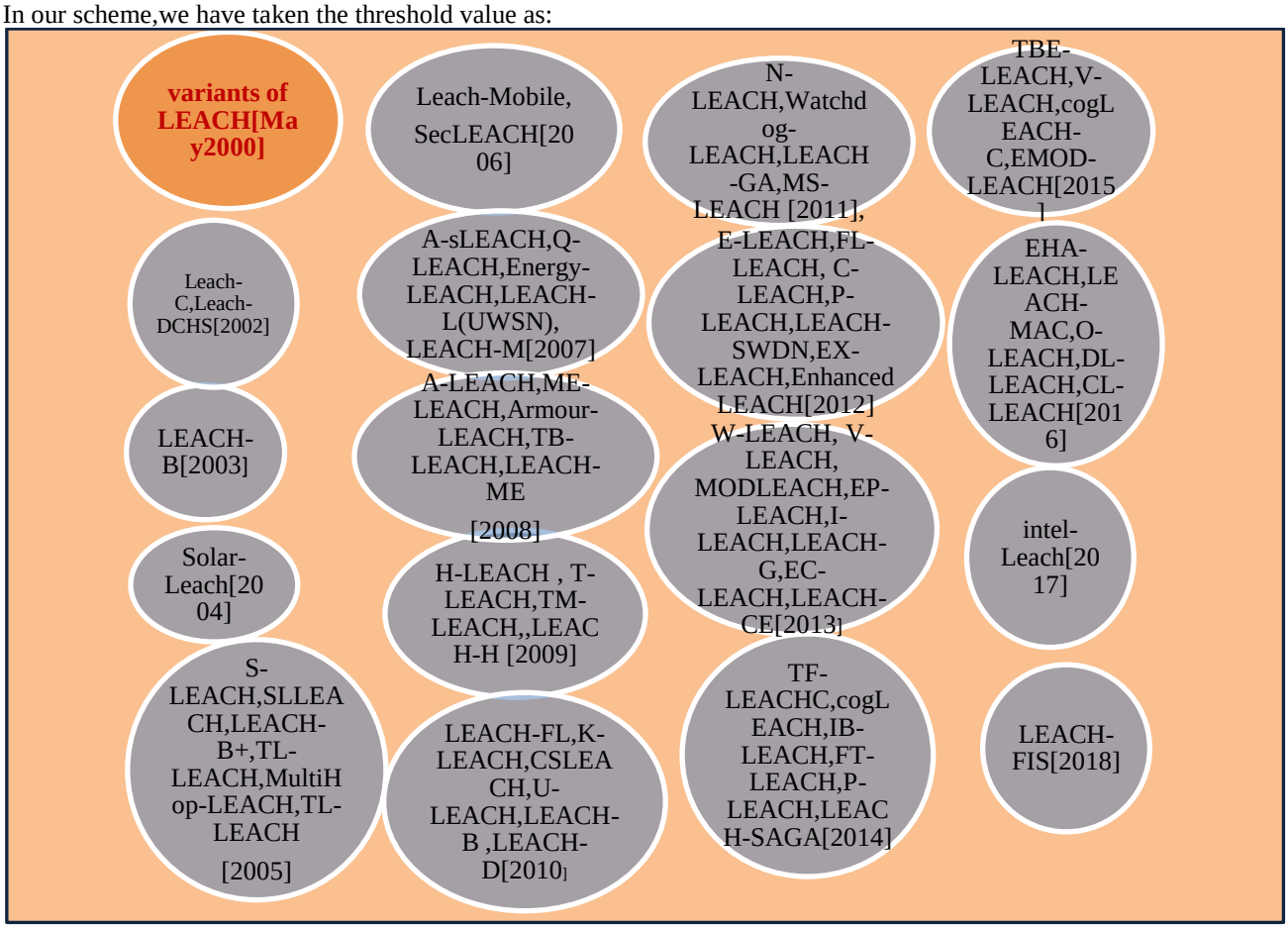
In case of original LEACH,In every round,a uniformly distributed pseudo random number between 0 and 1will be generated.If the above random number is less than or equal to T(n),then the particular node will be selected as Cluster Head,otherwise,the node will act as a normal cluster member node.

The threshold value

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

In this equation p is the desired percentage to become a cluster head, r is the current round and G is the set of nodes that have not been selected as a cluster head in the last 1/P rounds.

In our scheme,we have taken the threshold value as:



[Fig2.Leach protocol variants]

T(n)= (p/**(1-p*mod(r,(1/p)))×(**E_{Si}-E_{mp})we have also added the another criteria for validation of trust value for that sensor node which we have discussed elaborately in section 3.1. Here, E_{Si} refer to the Energy at the sensor node Si and E_{mp} is the Multi-path Fading Energy.

In addition to the above criteria,we

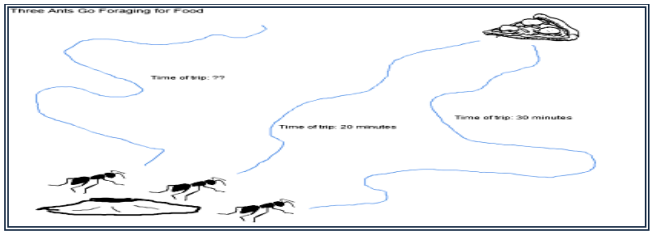
- LEACH uses a stochastic algorithm at each round.Each sensor node uses that algorithm to determine whether to become a cluster head or not.In the above case, LEACH assumes each node with powerful radio to reach directly to the base station or to the nearest cluster head, Using the radio of sensor node at full power all the time may waste energy.
- When number of cluster heads is 5% of total number of nodes,LEACH will give optimal performance.But,maintaining this number with a constraint that each node can become CH exactly once within every 1/p rounds i.e Nodes that have been cluster heads cannot become cluster heads again for *P* rounds, where *P* is the desired percentage of cluster heads.We have assumed p value to be 0.03 i.e.3%
- LEACH uses a random principle for selection of cluster head. Any node at random is elected as the CH and all the others are then turn by turn selected to be the CH. This leads to balanced energy consumption of all nodes, which in turn increases the lifetime of the network. If the CHs are unevenly located then it will lead to unbalanced energy utilization and decreases the lifetime of the network [1].

D. Traditional Optimization Algorithm of Ant-Colonies

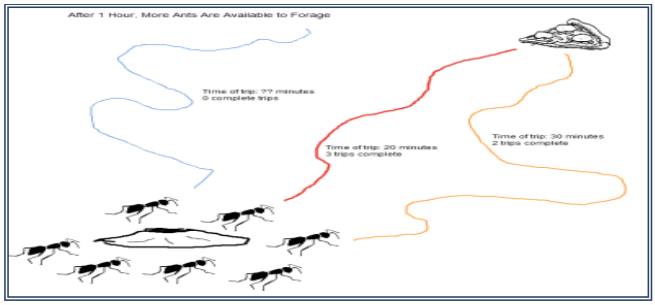
Optimization Algorithm of Ant-Colonies has taken the inspiration of that of the general behaviour by ants to find optimal and shortest routing path.The basic mechanism will be as follows:

When an ant move from nest to food source,it deposits pheromone which helps other ants to follow their path.While coming back it will also deposit pheromone.The next ant will be attracted towards that path which has more pheromone deposited.In this way,all ants will follow the shortest path at last and that is the global maxima path.

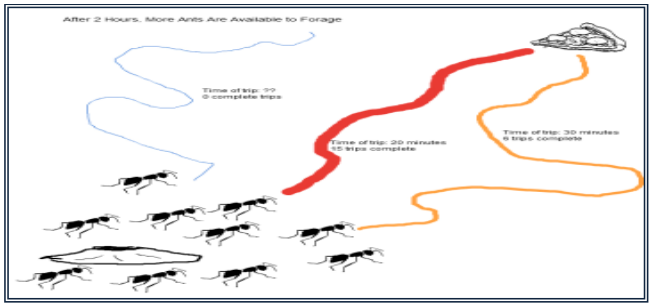
The General behaviour of the ants is as follows:



[Fig3a.At initial time]



[Fig3b.After some time]



[Fig3c.At final time]

At final time,all ants will follow thick red colored route which has more pheromone deposited on the path.The above procedure has been applied in Ant colony optimization applications.Ant colony optimization is basically a metaheuristic search technique which externally seems as if always it will aim to achieve local maxima,but ultimately it will end up with a global optima.This type of searching techniques,inspired by those of ants behaviour has given most fruitful results in many of searching and optimal path/route finding applications like Binary Knapsack,Travelling Salesperson,Quadratic Assignment problems,routing in networks etc.

The Basic steps of Ant-Colonies optimization algorithm are given as following :

step1:ACO parameter initialization
step2:Using probabilistic distribution,construct solution(temp) (use randomization and pheromone trail)
step3:Updation of pheromone
step4:if all ants has visited all nodes,go to step 5.otherwise gotostep 2.
step5:calculate optimal path length and update pheromone amount of that path.
Step6:if termination condition satisfy,output those values with maximum pheromone,otherwise goto step2.

E. ACO-Based Routing protocols for wsns

In one of the latest survey paper on wsn network routing protocols using Ant -colony optimization[9],the authors have stated that out of many of the techniques of swarm intelligence for routing in wsn,ant-colony and bee-colony techniques are highly efficient with respect to the important measurable parameters like robustness,scalability and energy etc.They have discussed various challenges which has to face by a routing technique aimed to be designed for a wsn.At the instance of routing,one sensor node will loose energy,computing power and bandwidth and in most of the cases,they may have to do this in a dynamic environment.Summarizing the above,the authors have mentioned the important challenges for routing protocols in wsn as, Connectivity, Latency, QoS, Deployment, Power, Mobility, Data Aggregation, Localization, Security, Congestion, Cost etc. The survey paper also discusses Some of the important Wsn routing work using ACO like “Energy Efficient Ant Based Routing”(EEABR)[year 2006],”Flooded Forward Ant Routing”(FF)[year 2004] ,”Flooded Piggyback Ant Routing”(FP)[year 2004],”Sensor Driven and Cost-Aware Ant Routing”(SC)[year 2004],”Energy-Delay Ant Based routing”(E-D Ants)[year 2008],”Basic Ant Based Routing for WSNs(BABR)“[year 2016],”Ant Colony Based Reinforcement Learning Algorithm “(AR and IAR)[year 2007],”Ant Based Quality of Service Routing “(ACO-QoSR)[year 2006],”Ant Colony Optimization based Location-aware Routing” (ACLR)[year 2008].In another survey work[13],there is a very good list of ACO based routing techniques(ARA,EEABR,Advance EEABR,AMQRA,FACO,E&D Ants,ARO,AntHocNet,ANT-E,E-ARA) and information about them has provided by the authors.According to the above paper,EEABR and it's variants are energy-aware and maintains maximum lifetime of wsn.

ACO-Based trust routing in WSN:

MPASR[15] and DPMA-MD algorithm[10] improves network security and minimises consumption of energy,which in turn can prolong lifetime of the network.

F. Trust and reputation models in wsns

Trust management models can be used to avail various security aspects and to keep the wsn safe Against various attaks.There are different types of attacks those can be made on WSNs like false energy,false data,black-hole,gray-hole,packet-delay,badmouth attacks etc.Trust Management models to prevent against various attacks in wsns can be structured in various ways like technique-based,trust source-based,architecture-

based and trust-attribute based etc.In case of a trust-based IDS, each and every node is observing their neighbour node's trust level.Depending on the above trust level values,neighboring nodes can be assumed as malicious,risky or trustworthy.For packet forward purpose,Only trustworthy sensor nodes will be recommended to the forward engine.The above trust scheme detect successfully various attacks like jamming attack,Hello flood attack and selective forwarding attacks by doing analysis of sensor network,statistics and behavior of malicious nodes[16].AEMP models can increase ability of a WSN network to work against inside-network attacks[17].AEMP requires fewer resources and simple calculations. It discusses also various influence parameters values for evaluating performance of nodes as well as the network and then integration of direct and indirect trust value has been done by the authors which is used for quick identification of a bad node.The disadvantage of AEMP models is that they may create the malicious evaluation problems. In spite of research on the role of trust in wireless sensor networks there still need examination of the trust associated with message routing between nodes of a WSN. But since dealing with both continuous and discrete report data by wireless sensor networks.development of new trust models can address combinely,data trust and the communication trust to infer the total trust[18].In[19]an overview of reputation and trust has been very well been explained.The trust updation factors has been summarised and examples of some systems implemented by usage of the above factors has discussed by another survey work[20].Various methods used to model trust and reputation systems has been surveyed w.r.t various domains with more details for ad-hoc and sensor networks since both the above networks are related closely with each other.Even though researchers have done works on the issue of trust in wireless sensor networks,associated with routing messages in between nodes,there is still need examination of this issue. So,for both continuous and discrete data monitor events and for reporting in wsns,new trust models should be addressed for above two types of data issue and combining data and communication trust inferring total trust[21].In[22],a survey about different trust models for wsns has been presented. The models have been discussed w.r.t adopted applications,network architectures,applied trust computation methodologies and trust management schemes.The paper also done comparisons among these models using a set of criterias and has evaluated their strengths and weaknesses.The behavior trust can be computed based on the node's behaviour in the process of sensing and forwarding.The historical trust's initial value will be set to maximum and updation done with comprehensive trust.By weighted calculation, Comprehensive trust is obtained, and then the construction of the trust list is done which in turn will guide the data fusion process.Using the above procedure.To avoid the posiibility of bad load balancing as a result of choosing the most trustable nodes frequently,energy and location criteria can be applied while choosing the next node in a routing path.In [23],the authors has defined three different ways to use trust information during routing decisions, each of them focusing either on legacy routing or on trust information.For routing,it uses three metrics.

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

III. PROPOSED MODEL

The aim of the proposed algorithm is to achieve efficient secure routng alongwith satisfying Qos requirements so that the proposed routing scheme can be applied successfully in real time sensor applicatons.

A. A.Overall construction of proposed ACOTRUST Scheme

ACOTRUST follows the basic steps of leach routing protocols with some variations.As in case of leach protocol,mainly there are 4 steps: Advertisement phase, Cluster setup phase, Schedule Creation and Data Transmission.Just like the LEACH protocol ,ACOTRUST uses the First Order Radio Energy Model. According to the above energy model, the dissipation energy of a radio to transmit an n-bit message over a distance **di** with an acceptable Signal-to-Noise Ratio (SNR) is as follows:

$$E_{RX}(n,di)=\begin{cases} n * Eelec + n * Efs * di * di, & \text{if di} < d0 \\ n * Eelec + n * Emp * di * di * di * di, & \text{if di} \geq d0 \end{cases}$$

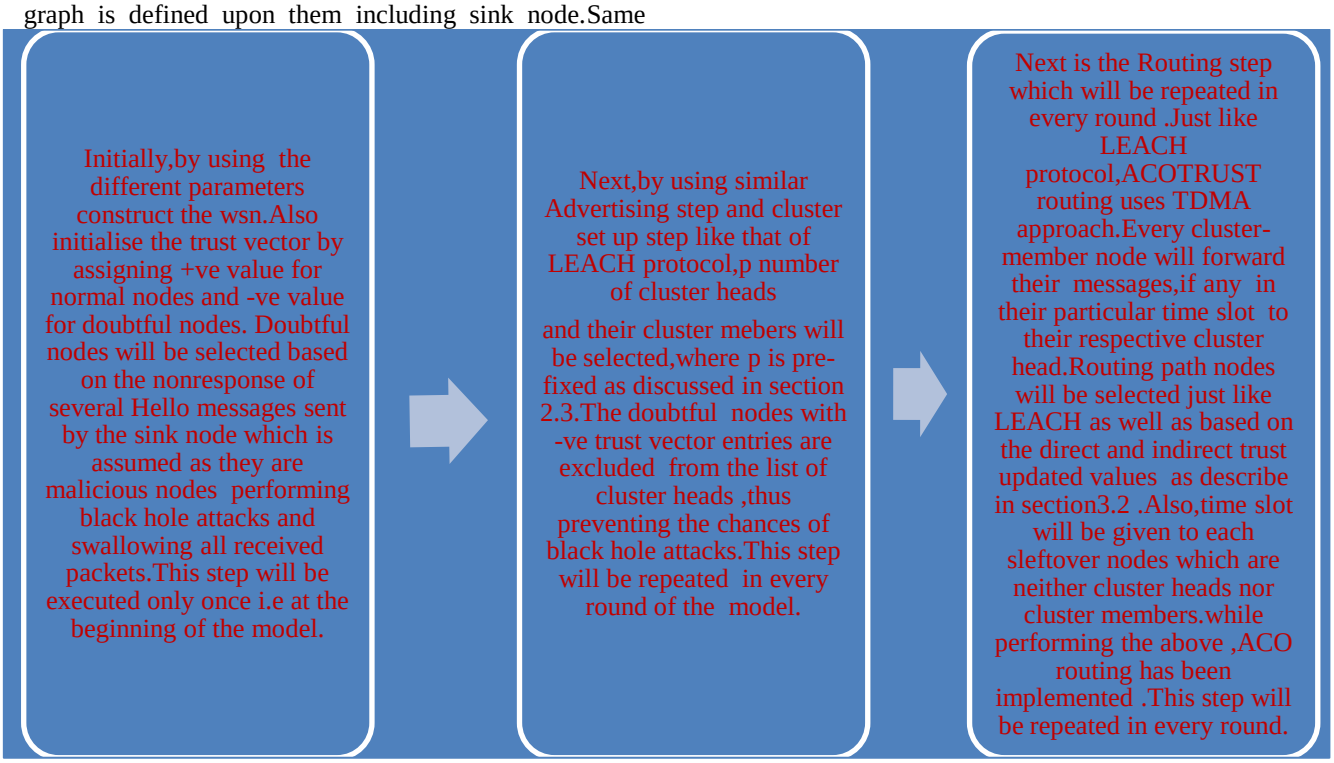
where **Eelec** is the energy dissipated per bit to run the transmitter or the receiver circuit,**Efs** and **Emp** depend on the transmitter amplifier models used for the experiments,and **di** is the distance between the communicating nodes Cross Over distance(d0)=$\sqrt{Efs \div Emp}$.For receiving n-bit message,the energy expenditure by the radio is:E_{RX}=n***Eele.**Within these 4 steps we have added trust management model(for achieving security against black hole attacks) and Ant-colony optimization for routing information from those sensor nodes which are neither cluster heads nor cluster members.

The proposed trusted scheme working steps has been shown in fig4.Basically,there are 3 steps:

- ✓ First of all,The WSN network is constructed by using different initialized parameters. A Trust vector is also initialize with a size similar to the number of nodes in the wsn.The sink node broadcast "hello" message in the network and each of the nodes are receiving that message.Assuming support of a underlying handshaking mechanism and "hello" message has been received error-free by every node of the network,the sink should receive acknowledgement from each of the nodes.If there is any deviation i.e sink does not receive response from a node,it is assumed as the node is malicious one and swallowing every message it receives.Thus,they will be considered doubtful nodes with a possibility of black-hole attacks.They are assumed as doubtful nodes,not fully malicious nodes since it may be due to any other factors,the acknowledgement may not have been reached to the sink.But,as a safety measure,they should be avoided to be selected as cluster head since if cluster head is itself performing blak–hole attack by-chance,then that is much more harmful as compared to other attacks on wsns.Hence,these doubtful nodes will be excluded from the selection process of cluster heads by defining –ve entries(-1) in the trust vector .All

remaining nodes is initialized with +ve(+1) trust vector entries.

- ✓ Next, Following the steps similar to that of Advertising and cluster set up,'p' number of cluster heads is selected in every round.The total number of rounds executed by the model depends on the no of alive nodes.Many of LEACH variant protocols has executed till the number of alive nodes would be 10%(90% dead nodes) or 5%(95% dead nodes), ACOTRUST assumes the stopping criteria as 0% alive nodes(100% dead nodes).Experimenting in stopping criteria with 5% or 10% alive nodes can be done as a future scope of this model. After the selection of cluster heads,cluster set up is done following similar steps to that of LEACH protocol with a little-bit variation.It is assumed that after all 'p' number of clusters and their members is set,there may have some leftover nodes which neither are cluster-heads nor cluster members.(This may not happen in each and every round of the model,but it may happen in many of the rounds since we have taken the percentange number of cluster heads as 3% and there is a maximal threshold distance to be assumed between a cluster head and it's members)
- ✓ and if these leftover nodes is present in the network ,a graph is defined upon them including sink node.Same timeslot as given to every cluster member node will be provided on a regular basis to these leftover nodes.if these nodes have sensed some event ,they can send information about the event only in their respective timeslot only just like the normal cluster member nodes.
- ✓
- ✓ Next,comes the important step of the model,*routing phase* in which actual routing of messages,(*if any*) about events takes place and is forwarded to the sink node ultimately. If source node is a cluster member,messages are send from that node(in its time slot only) to it's respective cluster head by following steady state phase routing of LEACH protocol as well as trust updated values and then aggregated messages is forwarded directly from the cluster head to the sink .But,if the node is a leftover node(as discussed above),then ACO algorithm is executed on the graph of leftover nodes(including sink) as well as trust updated values is consulted to select the best path.The above routing steps is repeated for every cluster-member node as well as leftover nodes(if any).Updation of trust values done in the proposed model by using either direct or indirect trust has been discussed elaborately in section B.



[Fig4.Steps of proposed ACOTRUST]

ACOTRUST uses ACO-QoSR[15] protocol approach to implement ACO based routing in the aim of achieving efficiency in four QoS metrics:packet delivery ratio, routing overhead,end-to-end delay, and energy residual ratio in addition to satisfying the time constraints of the real-time applications. It find paths from sensor to sink nodes.routing table of nodes checked while sending information from source to sink,alongwith checking of direct and indirect trust values.

B .Trust value Computation of ACOTRUST

To calculate Intracluster trust in between the nodes of network,one of the best way is to use QoS (Quality of Service) parameters.One of the critical aspect of QoS routing in WSNs is security.So,if trust will be computed as per QoS routing ,then it can be guaranted to many extent that the data transmission in between the nodes of a cluster will be secure;i.e the data routing will be prevented from the misbehaviour of malicious nodes to great extent.The question is how we can calculate QoS trust values in between the nodes of a cluster in a wireless sensor network.In the proposed ACOTRUST model,a new Aco-based procedure with an introduction of trust value computation for the efficient routing of Wireless sensor networks has been

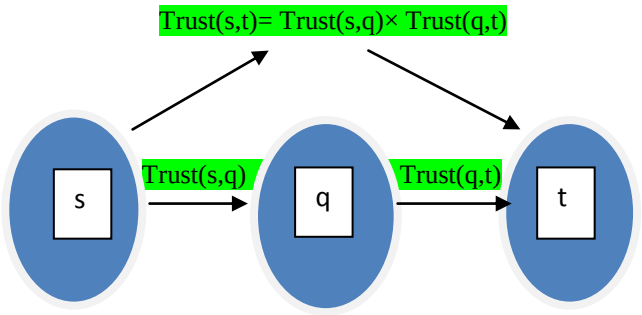
discussed.Paper[24] summarizes various trust evaluation methods.In the proposed model,final trust computation updated value is calculated as direct trust and if in case direct trust computation fails,the trust between nodes is calculated by indirect trust as follows.

✓ **Direct Trust Computation:**

Suppose node s wants to decide about trust worthiness of another node t,then if node s has been available enough information to compute trust value of t from previous communication experiences,then trust(s,t) is calculated directly as the no of previous interactions done by t with that of s.Also,if node s has available trust information about node t transitively,then transitive trust(s,t) is calculated as follows:

trust(s,t)=trust(s,q)×trust(q,t)

Where 'q' is the intermediate friend node of s with trust information available about t.The above has been picturized in fig 5.



[Fig5.Transitive trust Computation]

In these cases,direct trust value computation is sufficient and indirect trust computation is skipped.

✓ **InDirect Trust Computation:**In case if direct trust can not be calculated,for trust(s,t),node s is calculating trust about t by consulting all of its neighbor trustable friends who has available enough information($\geq$ min) about t to help s for computing trust(s,t).In this case,Trust(s,t) will be evaluated as weighted average of all trust values of neighbours of s summarizing as a trust chain in following equation:

$$\text{trust}(s,t) = \frac{\sum(\text{trust}(s,q)\times\text{trust}(q,t))}{\sum\text{trust}(s,q)} \quad \text{,such that} \quad qcadj(s)\text{trust}(q,t) \geq \min$$

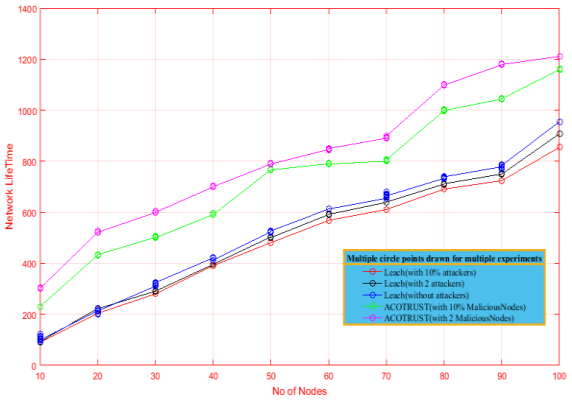
In the above equation,'adj(n)' is interpreted as adjacent node of node 'n' with respect to a given threshold distance and 'min' refers to minimum threshold trust value one node should have about the other node(for whom trust value is going to be calculated) .

IV. Simulation Results

The different parameters for our simulation is as given in following table .Since we have taken a randomly deploymed WSN,we have experimented multiple number of times(25 to 100 times) to get the resulted graphs (fig 6 to fig9) shown below.With respect to various parameters,from the graphs,irrespective of 100 experiments ACOTRUST gives better results in terms of energy efficiency,network lifetime etc as compared to LEACH alongwith maintaining security of the network.

Parameter Name	Value
Simulation tools used	MATLAB
Deployment Area	100metre X 100metre
Simulation Stopping Criteria	Till number of alive nodes=0
Number of experiments Done/graph result	25 to 100
Initial Energy/Node) (in Joules)	0.5
Data Aggregation Energy =(/message)	5 nJ/bit
Multi-path Fading Transmitter Electronics = Receiver Electronics	50 nJ/bit
Free Space Energy	10 pJ/bit/*m*2
Percentage of Cluster Heads	3%
Base Station Position(Relative)	(50,50)
Packet Size	4000 bits
Number of Nodes (Excluding BS)	10 to 100(randomly deployed)
Proposed Approach Compared with :	LEACH

[Table1.Simulation Parameters]



[Fig6.Network LifeTime(sec) Vs No of Nodes]

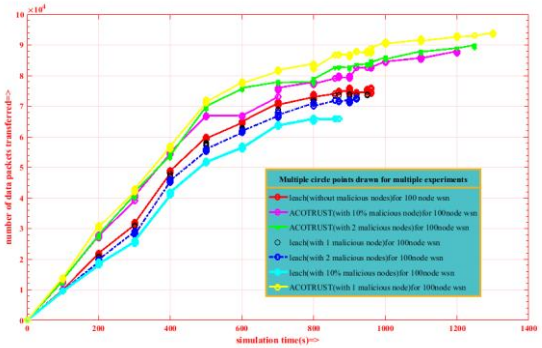
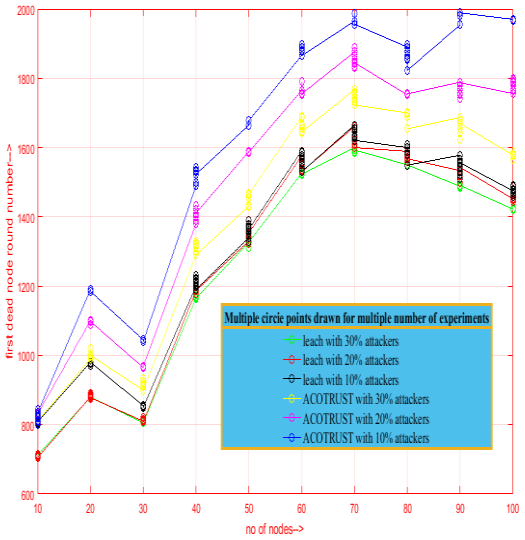
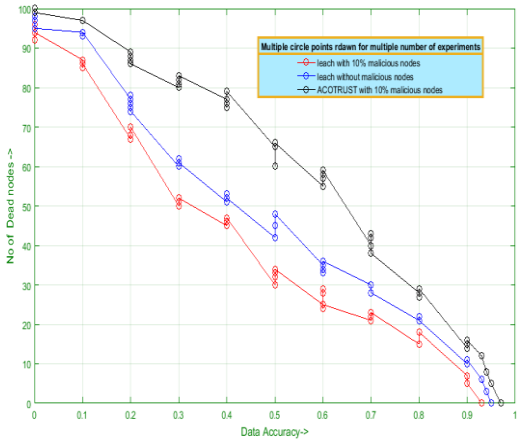


Figure 7. No of Packets Transferred vs Simulated Time]



[Fig8.Round number of first node dead vs no of nodes]



[Fig9 .Data Precision Vs No. of Nodes]

V. CONCLUSION

In this proposed work,a robust,reliable and scalable routing technique with the use of ACO has been proposed with taken care of few QOS parameters like security,energy consumption etc.For security various parameter point of view,it is shown that AOTRUST gives good results as compared to LEACH protocol.So,the above trustable technique can be used to design a secure wsn. ACOTRUSTachieves baseline security by adapting trustable computation and depending on its various parameter values,this approach is efficient and secure .The overhead of ACOTRUST is manageable.ACOTRUST preserves the original LEACH protocol structure,including data aggregation method.We have experimented the proposed work against blackhole attack and it successfully defense the above attack.In future,we can extend this work to deal with many insider as well as outsider attacks in wsns.Since we have confined our work for wsns consisting of 100 nodes,our technique can be experimented for large wsns.

REFERENCES

1. Ms. Wajeda Pathan,And Deepak.C.Mehetre,"Energy Efficient Communication In Clustering For Wireless Sensor Networks,"*International Journal of Advanced Computational Engineering and Networking*., volume.5, Issue-3, Mar.-2017.
2. Mohammad.Masdari,Sadegh.Mohammad,zadeh.Bazarchib,and Moazam.Bidaki,"Analysis of Secure LEACH-Based Clustering Protocols in Wireless Sensor Networks," *Journal of Network and Computer Applications 36.*, (2013) 1243–1260.
3. Wendi.Rabiner.Heinzelman,Anantha.Chandrakasan,andHari..Balakrishnan,"Energy-Efficient Communication Protocol for Wireless Microsensor Networks,"*IEEE. Published in the Proceedings of the Hawaii International Conference on System sciences*.,January 4-7, 2000, Maui, Hawaii.
4. Singh.Sunil Kumar, Kumar. Prabhat, and Singh.Jyoti,"A Survey on Successors of LEACH Protocol,"*IEEE Access*.,PP. 1-1. 10.1109/ACCESS.2017.2666082.
5. Najm-us-Sama,Kartinah Zen and Atiq-Ur-Rahman,"An Extensive Survey on Performance Comparison of Routing Protocols in Wireless Sensor Network,"*Journal of Applied Sciences.*, ISSN 1812-5654 DOI: 10.3923/jas.2017.238.245.
6. Mallanagouda Patil and Rajashekhar C. Birada,"A Survey on Routing Protocols in Wireless Sensor Networks",*ICON*., 2012,pp 86-91.
7. D.Mahmood,N. Javaid,S.Mahmood,S.Qureshi,A.M.Memon,T.Zaman," MODLEACH:A Variant of LEACH for WSNs," *Eighth International Conference on Broadband, Wireless Computing, Communication and Applications,IEEE.,2013.*
8. Hemant.Munot and P.H.Kulkarni,"Survey on Computational Intelligence Based Routing Protocols in WSN," *International Research Journal of Engineering and Technology (IRJET)*.,volume. 03 Issue: 09 | Sep -2016.
9. Anand.Nayyar and Rajeshwar.Singh,"Ant Colony Optimization (ACO) based Routing protocols for Wireless Sensor Networks (WSN): A Survey," *International Journal of Advanced Computer Science and Applications.*, Vol. 8, No. 2, 2017.
10. Zhang.L,Yin.N.Wang, R.C,"Research of malicious nodes identification based on DPAM-DM algorithm for WSN.," *J. Commun*., 2015, 36, 53–59.
11. 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*.,Volume.4, No 2, June 2017.
12. Amit.Sarkar and T. Senthil Murugan,"Routing protocols for wireless sensor networks:What the literature says?,",*lexandria Engineering Journal*., (2016) 55, 3173–3183.
13. Sudarshan. D. Shirkande and Rambabu. A. Vatti,"ACO Based Routing Algorithms for Ad-hoc Network (WSN,MANETs):A Survey,",*2013 International Conference on Communication Systems and Network Technologie.s*,pp.230-235.
14. Geetha.V,and 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.
15. Lin. Zhang, *et al*,"A Multi-Attribute Pheromone Ant Secure Routing Algorithm Based on Reputation Value for Sensor Networks,"*Sensors* 2017, 17, 541.
16. Syed.Muhammad Sajjad,Safdar Hussain Bouk,Muhammad Yousaf,"Neighbor Node Trust Based Intrusion Detection System for WSN,"*Procedia Computer Science* 63., (2015) 183 – 188.
17. Gu.Xiang,Qiu. Jianlin,and Wang.Jin,"Research on Trust Model of Sensor Nodes in WSNs,",*Procedia Engineering., 29* (2012) 909 – 913.
18. 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
19. 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.
20. Mohammad Momani, and Subhash Challa,"Survey of Trust Models in Different Network Domains,"in International Journal of Ad Hoc, Sensor & Ubiquitous Computing, 2010
21. 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.

22. Zhenguo.Chen,Liqin.Tian and Chuang.Lin,"Trust Model of Wireless Sensor Networks and Its Application in Data Fusion,"*sensors.*, 2017,17,703.
23. 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.
24. Aminu.Bello.Usman, Jairo.Gutierrez,"Toward trust based protocols in a pervasive and mobile computing environment: A survey," *Ad Hoc Networks 81*.,(2018) 143–159.

AUTHORS PROFILE

Lakshmisree Panigrahi is currently a PhD student under Sikshya 'O' Anusandhan University ,Bhubaneswar, INDIA She has done M.Tech in Computer Science and Engg in the same University.Her Research intrest includes Computer Networking,Security and Bioinformatics.