LSR PROTOCOL BASED ON NODES POTENTIALITY IN TRUST AND RESIDUAL ENERGY FOR WSNS

Shaik Sahil Babu[#1], Arnab Raha[#2], M.K. Naskar[#3]

[#] Department of Electronics and Telecommunication Engineering,

Jadavpur University, Kolkata – 700 032, West Bengal, India

[1]sksahilbabu419@gmail.com, [2]arnabraha1989@gmail.com,
[3]mrinalnaskar@yahoo.co.in

ABSTRACT

In Wireless Sensor Networks (WSNs), all the nodes selected for packet routing must be trustworthy, and at the same time energetic too. Smooth conservation of nodes energies and the trust levels, are an important issues in WSN because they directly affects the life span and reliability of the nodes as well as the entire network. The energy utilization at every node must be very smooth and at the same time, packets should be forwarded via trusted nodes only. In this paper, we propose an Energy Efficient Link State Routing Protocol (EELSRP) using the potential nodes selected by applying the fuzzy logic on the trust and residual energy levels. This routing protocol finds the best route by balancing the nodes residual energies and trust levels, and protects the WSN against routing attacks by eliminating the un-trusted nodes before the creation of route.

KEYWORDS

Wireless Sensor Network (WSN); Fuzzy Logic; Geometric Mean (GM); Direct Trust; Indirect Trust; Route Trust (RT); Base Station (BS); Benevolent Node; Packet Latency.

1. INTRODUCTION

As Wireless Sensor Networks (WSNs) are highly application oriented, these various applications bring various security needs. In WSN, sensor nodes have limited communication bandwidth, processing resources, memory space and battery capacity [1]. Though the cryptographic security methods are playing major role for providing security, they are not suitable for WSNs, due to resource constraints like memory, processing and energy at node. Cryptographic security is more complex and the overhead is high. Hence, a new way of security called "Trust" came into picture and has become new area for researchers. Trust, a degree of reliability of a node on any other neighbour node of WSN, can be formed from the track record of past transactions made with the node. By maintaining a record of the transactions with other nodes, directly as well as indirectly, trust value will be established [2]. Trust is dependent on time; it can increase or decrease with time based on the available evidence through direct interactions with the same node or recommendations from other trusted nodes [3].

Similarly, energy of a node is another constraint in WSN, because all the nodes operate on battery, which can't be replaced in their life time. Hence, energy efficiency has become another challenging issue in WSN applications. Any type of processing at node should not consume much energy as it affects the node's life, in-turn the life span of the WSN. The life time of any network, can evaluated from the trustworthy relations among the nodes and from the number of route from source node to destination. As a matter of fact, for routing any packet in WSN, all the nodes of routing path from source to sink must be both, energetic as well as trustworthy. Otherwise, the packet may not be reached or captured. There is much literature for WSN routing protocols, but routing protocol with potential nodes like, trustworthy as well as energetic, is out

DOI : 10.5121/ijnsa.2012.4202

of literature. Hence, a routing protocol with the integration of trust and node's residual energies is very much required. Integration of Trust in routing protocols of WSNs gives high security for packet routing from the Source node to reach the Base Station. Integration of energetic node in routing protocols of WSNs gives high guarantee in packet reaching to the Base Station.

In DTLSRP [4], trust using direct interactions only is incorporated. Trust aware routing framework for WSNs is proposed by [5], to secure multi-hop routing in WSNs against intruders exploiting the replay of routing information. With the idea of trust management, their proposal enables a node to keep track of the trustworthiness of its neighbours and thus to select a reliable route. Their proposal can also be implemented for large-scale WSNs deployed in wild environments. Many security attacks have been presented in ([6], [7]) with a significant subset targeting the routing process [8]. If an adversary force manages to capture the node, it participates in the network, and it can damage the routing process by simply dropping the packets it receives for forwarding. Another attack easy to implement is packet modification. In [9] an approach that the human society follows proposed to defend against the majority of routing attacks. Although the design of mechanisms to enhance security at all layers of the networking protocol stack has attracted the interest of the research community (e.g. [10], [11]), very limited implementation effort has been reported. In [12], the implementation of link-layer security architecture is presented, while in [13] experience regarding the implementation of hash-based encryption schemes in TinyOS operated sensor nodes is reported. In [14], the efficiency of a set of routing protocols is compared based on real test-bed experiments. In [15], very limited information regarding the implementation of a trust model is provided. Finally, in [16] presented results and experience gained through the implementation of a location-based trust-aware routing solution. A distributed trust model is incorporated in the routing solution which relies on both direct and indirect trust information.

In this paper, we propose a new energy efficient link state routing protocol based on potential nodes found by applying fuzzy logic on node's residual energy and trustworthiness by eliminating the malicious nodes from the network, and presented simulated results. This protocol incorporates a trust computational model [17] with direct and indirect experiences based on geometric mean approach on the QoS characteristics such as packet forward, data rate, power consumption reliability, etc. To find the potentiality of the node, a Fuzzy Logic is applied on node's trust and residual energy. Finally, routing path will be formed with potential nodes only.

The rest of this paper is organized as follows: first in section 2 we present the related work on WSN routing protocols based on trust and traditional trust evaluation method, and in section 3 the designated EELSR Protocol based on nodes potentiality derived from the Fuzzy logic application on trust and residual energy, while in section 4 Simulation results. Finally, section 5 gives the conclusions and future scope.

2. RELATED WORK

Routing methods based on Trust: Routing related protocols based with trust integration have been widely addressed in the literature. The following are the most important research results in this direction:

2.1 Trusted GPSR

The Greedy Perimeter Stateless Routing [18] is modified to take trust levels of node into account. Each time a node sends out a packet it waits until it overhears its neighbouring node forwarding it. Based on this correct and prompt forwarding information it maintains a trust value for its neighbours. This information is then taken into account in the routing decisions.

2.2 ARIADNE

It is very efficient protocol, using highly efficient symmetric cryptographic primitives and per-hop hashing function [19]. It prevents the attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents a large number of types of Denial-of-Service attacks.

2.3 ATSR (Ambient Trust Sensor Routing)

A fully distributed Trust Management System is realized in ATSR [1] in order to evaluate the reliability of the nodes. Using this approach, nodes monitor the behaviour of their neighbours in respect to different trust metrics and finds direct trust value per neighbour. It also, takes into account indirect trust information, i.e. trust information from its neighbours, also called reputation. Direct and indirect trust information is combined to reach the Total Trust information. Finally, the routing decisions are based on geographical information (distance to the base-station) and Total Trust information. The trust model presented has been integrated with a location-based routing protocol. If no malicious node exists in the network, i.e. the Total Trust is almost equal to 1, the ATSR behaves simply the Greedy Perimeter Stateless Routing (GPSR) protocol.

2.4 SPINS (A suite of security protocols optimized for sensor networks)

This [20] has been designed to provide data authentication, data confidentiality and evidence of data freshness. In this protocol two security blocks SNEP and µTESLA are involved. The first block introduces overhead of 8 bytes and maintains a counter for achieving semantic security. µTESLA provides authentication for data broadcasting. Though SPINS claim to provide trusted routing ensuring data authentication and confidentiality, but it does not deal with Denial of Service Attacks.

2.5 Trust- aware DSR:

The watchdog and Pathrater modules has been designed and incorporated in the Dynamic Source Routing protocol for security [21]. The watchdog module is responsible for detecting selfish nodes that do not forward packets. For this, each node in the network buffers every transmitted packet for a limited period. During this period each node enters into promiscuous mode in order to overhear whether the next node has forwarded the packet or not. And based on the feedback that Pathrater receives from the watchdog, it assigns different ratings to the nodes. These ratings are then used to select routes consisting of nodes with the highest forwarding rate.

2.6 CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad-hoc Networks)

This [22] protocol adds reputation system and a trust manager to the Watchdog and Pathrater scheme. The trust manager evaluates the events reported by the Watchdog and issues signals to other nodes regarding malicious nodes. The signal recipients are maintained in a friends-list. The reputation system maintains a black-list of nodes at each node and shares them with friends-list nodes. In one way it is a punishment based scheme by not forwarding packets of nodes whose trust level drops below the certain threshold.

2.7 TRANS (Trust Routing for Location Aware Sensor Networks)

TRANS [23] routing protocol selects routes based on trust information not on hop count to avoid the insecure locations. This protocol assumes that the sensors know their locations and

that geographic routing is used. A sink sends a message only to its trusted neighbours for the destined location. Those corresponding neighbours forward the packet to their trusted neighbours that have the nearest location to destination. Thus the packet reaches the destination along a path of trusted sensors. Here the important feature of TRANS, the sink identifies misbehaviour by observing replies, probes potential misbehaving locations, and isolates insecure locations. On discovery of such locations, the sink records and advertises to the neighbouring nodes.

2.8 Traditional weighting approach for Trust evaluation [3]

He introduced one algorithm for trust calculation and risk assessment based on trust factors and dynamic aspects of trust. He assumed that trust is computed using traditional weighting approach of the QoS characteristics such as packet forward, data rate, error rate, power consumption, reliability, competence, etc. A traditional weighing approach to calculate Trust and asses Risk (Risk assessment algorithm) is introduced. These weights W_A, W_B can be assigned using different approaches. Some nodes might give more weight to direct trust, others might give more weight to recent indirect trust.

3. Energy Efficient Link State Routing Protocol based on Nodes Potentiality in Trust and Residual Energy for WSNs

Our proposed model is extended and modified version of routing protocol DTLSRP [4] and geometric mean based Trust Management System [17]. In GMTMS [17], we proposed a new trust model suitable for many practical applications of the Wireless Sensor Networks (WSNs). In [4], we proposed LSR Protocol for WSNs based on Direct Trust of a neighbour node only. In this proposal, we are evaluating the Trust from both direct and indirect trusts. As in [17], Trust of a node on any neighbour node is a function of both direct and indirect trusts. Similarly, LSR Protocol proposed in [4], based on only Direct Trusts. In this proposed LSR Protocol, Indirect Trust also integrated for reliability, and for the smooth conservation of energies of nodes, and balancing between trust and residual energy, the selection of nodes for routing is performed by applying Fuzzy logic on node's trustworthiness and residual energy. There are five steps to find the best route from source node to Base Station that gives equal importance to residual energy and trust level at every node of the entire route.

Step 1: Every node in the network finds the neighbour nodes and evaluates their trust and residual energy levels.

Step 2: Every node applies Fuzzy Logic on nodes listed above and finds their routing potential levels. Based on minimum qualification for participation in routing, some neighbour nodes will be listed as potential nodes.

Step 3: Source node runs Link State Routing Protocol using potential nodes only, assuming Base Station as a destination, and gets the routing information.

Step 4: Source node extracts the different routes to the Base Station, from the information given by the neighbour nodes. Also, Source node calculates route potential levels for each of the discovered routes.

Step 5: Source node uses the highest potential level route for routing.

3.1. Trust and Residual Energy Evaluation

Every node uses trust evaluation method [17] and knows the trust levels of its neighbours of one radio range (*m* with respect to node **S**) as shown in Figure 1. It finds the trustworthy neighbour nodes (say A, B, C) based on the trust threshold t_{TH}. If no node is found trustworthy or only few trustworthy nodes are present in its radio range then it increase the radio range from *m* to *n,* and finds the new trustworthy nodes again (nodes D, E, F, G, H, I may be added), which is an energy consuming operation.

Every node in WSN maintains a database that contains the history related to their neighbours, i.e., trust metrics of each neighbour node, direct trusts, indirect trusts, trusts at different times, and residual energies of neighbours. Every node gets residual energy levels of its neighbour nodes in every reply transaction performed to find the trust, and will be stored in the database of the node. These residual energies received, maintained by the trust management system of the node.

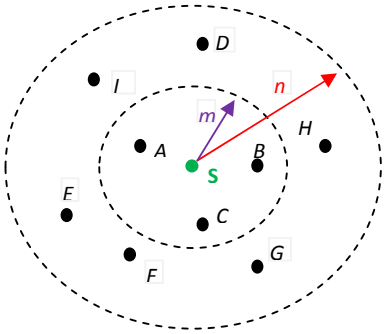

Fig.1 Node S radio range

In trust management system [17], the direct trust is geometric mean of all different trust metrics for different events occurred in the network. Every node will be having a separate record of data of every surrounding node in different trust metrics for different events occurred in the network. From these records, Direct Trust (DT) is calculated based on geometric mean of the QoS characteristics as given in the below equations.

$$\mathrm{DT} = \text{geometric mean of trust metrics}$$

$$\mathrm{DT} = [\prod(\mathrm{m}_1, \mathrm{m}_2, \dots, \mathrm{m}_\mathrm{k})]^{1/\mathrm{k}}$$

$$\mathrm{DT}_{\mathrm{N}_1}(\mathrm{N}_2) = \left[\prod_\mathrm{n}\left(\mathrm{m}_{\mathrm{N}_1,\,\mathrm{N}_2,\mathrm{n}}\right)\right]^{\frac{1}{\mathrm{k}}}$$

Here, $\mathrm{m}_1, \mathrm{m}_2, \dots, \mathrm{m}_\mathrm{k}$ are the trust metrics of node. The $\mathrm{DT}_{\mathrm{N}_1}(\mathrm{N}_2)$ in the above equation is the Direct Trust value of node N_1 on node N_2, calculated for K different type of trust metrics (for n=1 to k).

The Indirect Trust on node N_2 with respect to N_1 can be calculated from the direct trusts (DTs on N_2 with respect to its neighbours) sent by the neighbour nodes of N_2.

$$\mathrm{IT} = \text{geometric mean of trust information given by neighbour nodes.}$$

$$\mathrm{IT}_{\mathrm{N}_1}(\mathrm{N}_2) = \left[\prod_\mathrm{p}\left(\mathrm{DT}_\mathrm{p}(\mathrm{N}_2)\right)\right]^{\frac{1}{\mathrm{L}}} \quad \text{for p = 1 to L}$$

Here, $DT_1, DT_2, \ldots, DT_L$ are the DTs given by the neighbour nodes. The $IT_{N_1}(N_2)$ is the Indirect Trust value of node N_1 on node N_2, calculated for indirectly given information by L neighbours of N_2.

As shown in following equation, DT is direct trust (experience), IT is indirect trust (recommendations), T is total trust.

$$\text{total trust } T = F(DT, IT)$$

$$T = DT * W_a + IT * W_b$$

The weights W_a is weightage given to DT and W_b to the IT where $W_a + W_b = 1$. Weights can be assigned using different approaches. Sometimes DT may be given more weight, and IT may be given less weight i.e. $W_a > W_b$.

$$T_{N_1}(N_2) = DT_{N_1}(N_2) * W_a + IT_{N_1}(N_2) * W_b$$

Hence, every node of the network finds the neighbour nodes and evaluates their trust and residual energy levels. If no neighbour node found in the radio range, then it increases the radio range and gets the new neighbour nodes if any, and evaluates their trust. Based on minimum *trust threshold* (t_{TH}) and minimum *residual energy threshold* (re_{TH}), some nodes will be filtered out and they are not allowed in routing. Hence, every node prepares a list of their neighbour nodes with different trust levels and residual energies.

3.2 Fuzzy Logic for neighbour nodes routing potential levels

To increase the life of the node, as well as the entire network, every node in the network must utilize their energy properly. All the time, neither only energetic nodes nor the only trustworthy nodes may be selected for routing. If only energetic nodes, without considering trustworthiness are selected for routing, then the packet may not reach the Base Station. Similarly, if only trustworthy nodes, without considering residual energy are selected for routing, then the life span of most trustworthy nodes will be fall down. Hence, trustworthy node may die, and entire lifespan of network decreased. In this proposed method, we are giving same priority to the two parameters, because we are applying this fuzzy logic on nodes whose trust and residual energy levels are greater than the minimum threshold level. The relation between trust management system, routing protocol, neighbour node's database and the fuzzy logic controller is shown in Figure 2. The trust management system periodically finds the neighbour nodes trust metrics including residual energy, in its radio range, evaluates their trust levels and stores them into the database. As shown in Fig. 2, the inputs to the FLC come from the database module. The inputs are trust and residual energy levels. The output of FLC is routing potential level. The routing protocol collects the routing potential levels of the entire neighbour nodes for routing operations. The inputs and outputs for the FLC and their minimum and maximum values are shown in Table 1.

An important function of trust management system is, it gets the neighbour node's residual energy levels. All the gathered data maintained in the node's database. Whenever routing protocol wants to form a new route to send some packet to the BS, it first instructs the trust management system to update the database. Then the TMS in turn, initiates the Fuzzy Logic Controller to find the neighbour nodes routing potential levels from the available information of the database and update the database. Then the routing protocol collects the nodes routing potential level information and take appropriate decision for routing in that moment.

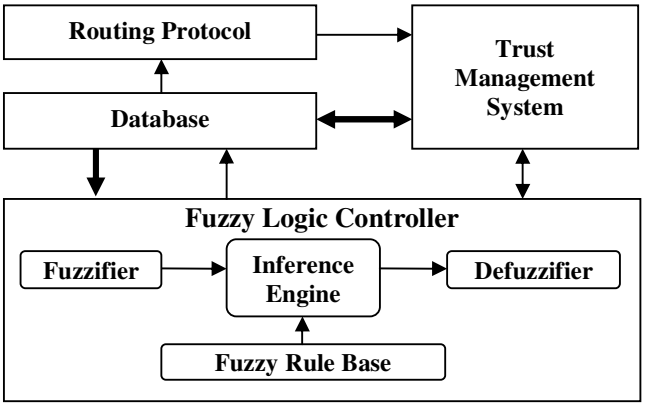

Fig. 2 Relationship of FLC with database

Hence, every node applies Fuzzy Logic on nodes listed in Step 1, and finds their routing potential levels, i.e., *node routing potential levels* (***nrpl***). So, every node will be having neighbour nodes list with their qualifying *node routing potential levels*. Based on minimum qualifying *node routing potential level threshold* (***nrpl*** $_{TH}$), some nodes may be filtered out again. All other nodes are listed, are called potential nodes, and they are only eligible for participating in routing.

3.3 LSRP execution at Source node using potential nodes

Link state routing protocols are the most widely used static routing protocols. Here, we are only interested in the basic features of the LSRP and are not mentioning the wide details of it or whether OPSF, IS-IS, MOPSF,MLSRP etc. are used in this case. Applying anyone of these LSRPs are possible depending upon other network needs.

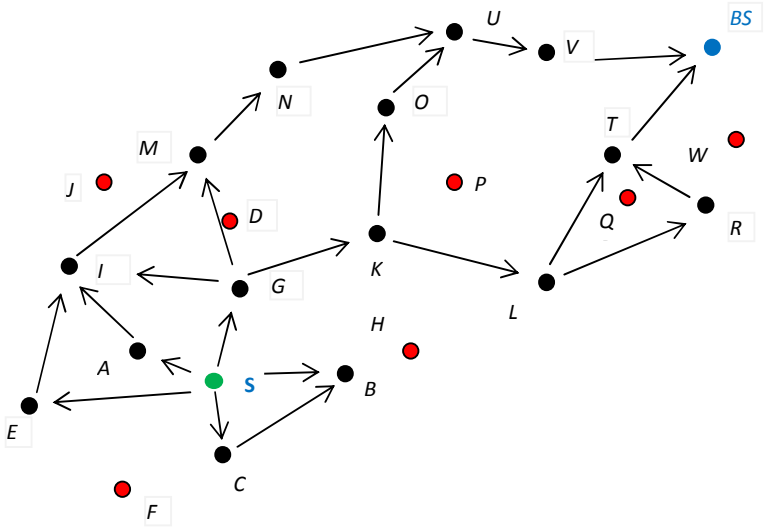

Fig. 3 LSR Protocol via potential nodes

The basic features of LSRP in brief are:

a) Discovery of the neighbors of the nodes and learning their network addresses
b) Measurement of the delay or cost to each of its neighbors.
c) Construction of a packet telling all the information learnt by it.
d) Transmission of this packet to all the router nodes.

One of the main advantages in our algorithm is that it doesn't require the LSRP to apply Dijsktra's algorithm or any other algorithm to find the shortest path from the source to the sink. It gets automatically evaluated from determination of Route potential levels.

For example, the WSN shown in Fig. 3, A to W, are nodes in which S is a Source node, and BS is Base Station. Nodes with Black colour are potential nodes and Red marked, are not qualified nodes for routing, because they may be either not trustworthy or low residual energy or both.

TABLE 1 Universe of Discourse for Inputs and Output.

Name	Input/ Output	Min. Value	Max. Value
*Node's Trust (**T**)*	**I**	0	1.0
*Node's Residual Energy Level (**E**)*	**I**	0	1.0
*Node's routing potential level (**nrpl**)*	**O**	0	1.0

Hence, Source node gets the different routes information from neighbour nodes. This information contains different nodes those are eligible to participate in routing and their *node routing potential levels* with respect to their neighbour nodes.

3.4 Routes and their potential levels extraction

Source node calculates the different routes, from the information given by the neighbour nodes. Also, Source node calculates *route potential levels* (***rpl***) for each of the discovered routes from Source to Base Station, by applying geometric mean on all the ***nrpl***s of the nodes those are falling in the route. Each route will be having its own *route potential level*. Upon the completion of the LSRP protocol, the different routes that are found out are listed in Table 2.

Table 2. Different routes from Source (S) to Base Station (BS)

Rt no.	Route	Rt no.	Route
1	S→G→I→M→N→O→K→L→T→BS	13	S→A→I→M→N→O→U→V→BS
2	S→G→I→M→N→O→K→L→R→T→BS	14	S→A→I→M→N→U→V→BS
3	S→G→I→M→N→O→U→V→BS	15	S→A→I→M→N→O→K→L→T→BS
4	S→G→I→M→N→U→V→BS	16	S→A→I→M→N→O→K→L→R→T→BS
5	S→G→M→N→O→K→L→T→BS	17	S→A→E→I→M→N→O→U→V→BS
6	S→G→M→N→O→K→L→R→T→BS	18	S→A→E→I→M→N→U→V→BS
7	S→G→M→N→O→U→V→BS	19	S→A→E→I→M→N→O→K→L→T→BS
8	S→G→M→N→U→V→BS	20	S→A→E→I→M→N→O→K→L→R→T→BS
9	S→G→K→L→T→BS	21	S→E→I→M→N→O→K→L→T→BS
10	S→G→K→L→R→T→BS	22	S→E→I→M→N→O→K→L→R→T→BS
11	S→G→K→O→U→V→BS	23	S→E→I→M→N→O→U→V→BS
12	S→G→K→O→N→U→V→BS	24	S→E→I→M→N→U→V→BS

Route potential levels:

rpl = geometric mean (nodes routing potential levels in the route)

The route potential level of route n that has k-hops is given by the following equation.

$$\boldsymbol{rpl_{R_n}} = [\prod_{l=1\ to\ k}(\textbf{node routing potential level}_{\ l})]^{\frac{1}{k}}$$

For example, as shown in Table 2, route 9 has 5 hops and its routing potential level is:

$$\boldsymbol{rpl_{R_9}} = [\prod_{l=1\ to\ 5}[(\mathbf{S} \rightarrow \mathbf{G}), (\mathbf{G} \rightarrow \mathbf{K}), (\mathbf{K} \rightarrow \mathbf{L}), (\mathbf{L} \rightarrow \mathbf{T}), (\mathbf{T} \rightarrow \mathbf{BS})]]^{\frac{1}{5}} \quad ...(1)$$

3.5 Routing using route with highest routing potential level

In the fifth and final step, data will be routed only through that path whose routing potential level value is the highest. The highest routing potential level route may or may not be the minimum number of hop route. If all the nodes in the minimum number hop route are energetic and trustworthy then only that route will be selected as highest potential route. And if any one of the nodes in the minimum number hops route is neither energetic nor trustworthy nor both then that route may get lower potential than other routes.

4. SIMULATION RESULTS

We have designed the FLC system; it is shown as a block in the Figure 2. The inputs to the FLC come from the database module. The inputs are trust and residual energy level of node. The output of FLC is potential level of the node. The Universe of Discourse for Inputs and Output are shown in Table 1.

Fuzzifying of Inputs and Outputs: We have used triangular membership functions to fuzzify the inputs. For different inputs the fuzzy variable and its crisp input ranges are shown below in Fig. 4. The optimization of these assignments is often done through trial and error method for achieving optimum performance of the FLC.

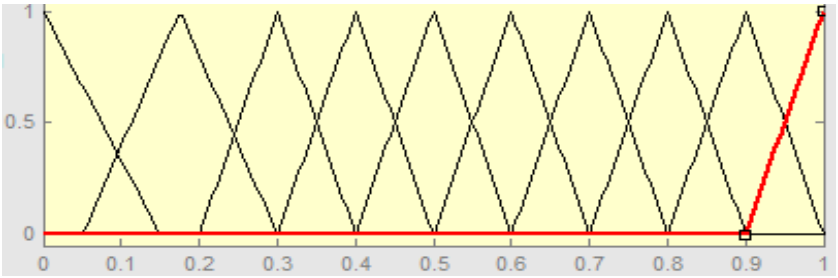

Fig. 4 Crisp ranges for Inputs and Output

We have just only one output, which is node's routing potential level, and assigned fuzzy memberships as we did for inputs.

The Fuzzy Inference Technique available of MATLAB is used in our node election method. The so-called mamdani method is applied. Fuzzy rule base for defuzzification is shown in Figure 5.

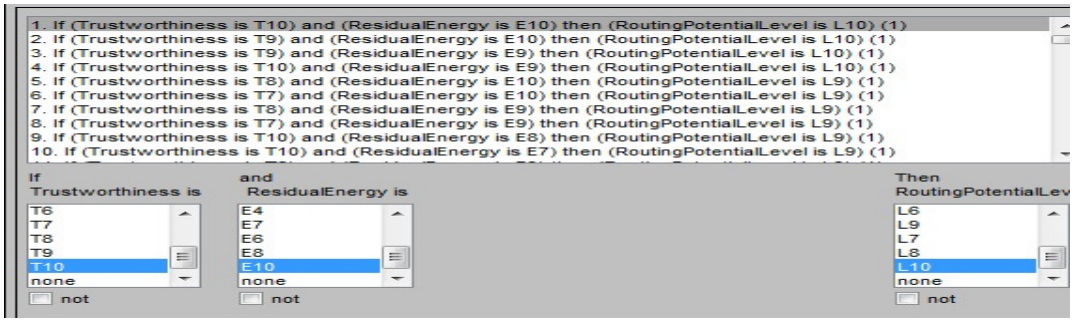

Fig. 5 Fuzzy rule base

The output which is node's potential level for different inputs, i.e., none's residual energy level and trust levels is shown in Figure 5. Defuzzification of node's potential level output is evaluated using the centroid approach: overlap and additive composition.

The Fig. 6, shows how smooth the energy as well as trust level of node can be balanced to find the node's routing potential level. We have chosen a symmetric square field area with random distribution of nodes as shown in Fig.3. The assignment of node's routing potential levels with respect to their neighbour nodes has taken randomly and is shown in Table 3.

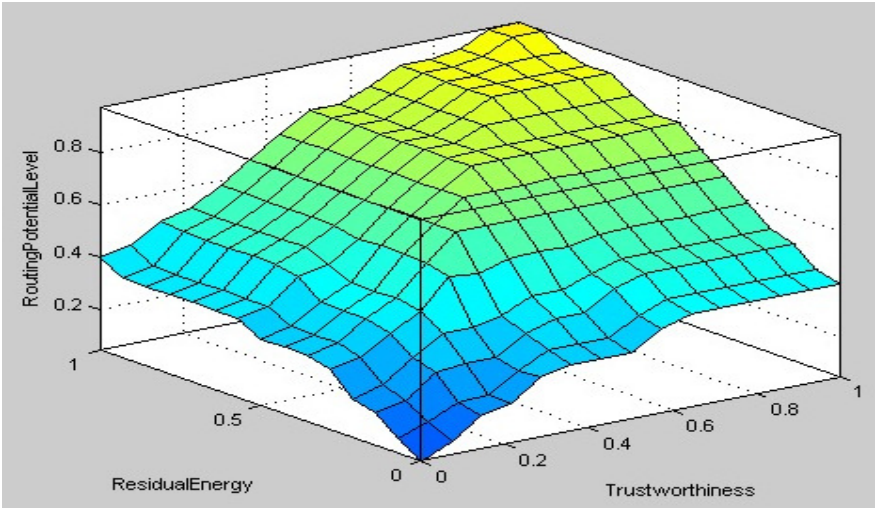

Fig. 6 Fuzzy Output for node routing potential level

As per the Fig. 3, as a result of the execution of our routing protocol at node S, there will be 24 routes from Source node (S) to Base Station. Hence, the nose S lists the all 24 routes with node's routing potential level at every hop in all the routes. Route potential levels (***rpl***s) of all the routes listed in Table 2, are found by applying the equation (1) and are given below in the respective order from route 1 to 24.

Route Potential Levels are $rpl_{R_1} = 0.50$, $rpl_{R_2} = 0.54$, $rpl_{R_3} = 0.48$, $rpl_{R_4} = 0.44$, $rpl_{R_5} = 0.49$, $rpl_{R_6} = 0.54$, $rpl_{R_7} = 0.47$, $rpl_{R_8} = 0.43$, $rpl_{R_9} = 0.52$, $rpl_{R_{10}} = 0.59$, $rpl_{R_{11}} = 0.54$, $rpl_{R_{12}} = 0.51$, $rpl_{R_{13}} = 0.52$, $rpl_{R_{14}} = 0.46$, $rpl_{R_{15}} = 0.53$, $rpl_{R_{16}} = 0.57$, $rpl_{R_{17}} = 0.47$,

$rpl_{R_{18}} = 0.42$, $rpl_{R_{19}} = 0.48$, $rpl_{R_{20}} = 0.52$, $rpl_{R_{21}} = 0.51$, $rpl_{R_{22}} = 0.56$, $rpl_{R_{23}} = 0.50$, $rpl_{R_{24}} = 0.44$.

Though the route 9 has least hops, it is not selected as because node routing potential level of node L on node T is 0.3 only as shown in Table 3. Similarly, in all other routes except the route 10, any one or many node/s routing potential level is/are less.

Table 3. Random assignment of routing potential levels to the node's neighbours.

Node and its neighbours with ***node routing potential levels (nrpl**s)*			
S	B = 0.5, C = 0.9, A = 0.4, E = 0.7, G = 0.5	**L**	T = 0.3, R = 0.6, K = 0.7
A	I = 0.7, S = 0.8, E = 0.5	**M**	I = 0.6, G = 0.7, N = 0.5
B	S = 0.6, C = 0.7	**N**	M = 0.3, U = 0.4, O = 0.6
C	S = 0.9, B = 0.5	**O**	K = 0.7, U = 0.8, N = 0.7
D	Un-trusted node	**P**	Un-trusted node
E	S = 0.8, I = 0.3	**Q**	Un-trusted node
F	Un-trusted node	**R**	T = 0.6, L = 0.4
G	S = 0.8, I = 0.3, M = 0.3, K = 0.7	**T**	L = 0.5, BS = 0.7
H	Un-trusted node	**U**	N = 0.9, O = 0.4, V = 0.3
I	E = 0.4, A = 0.5, G = 0.7, M = 0.5	**V**	U = 0.7, BS = 0.5
J	Un-trusted node	**W**	Un-trusted node
K	G = 0.4, O = 0.6, L = 0.5	**BS**	T = 0.6, V = 0.6

The other results are represented in the following two plots. Fig.7 shows the Packet delay, and Fig. 8 shows Network life span.

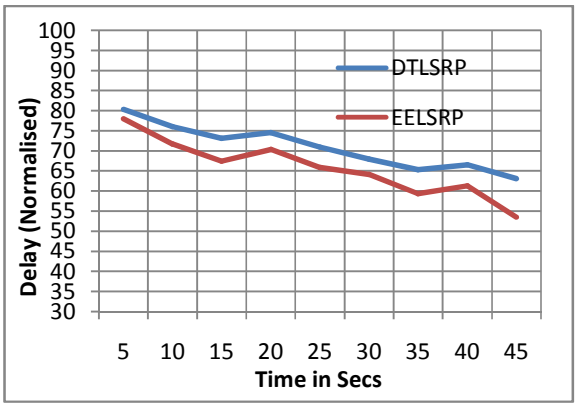

Fig. 7 Packet Delay

The simulation has been carried out in TOSSIM simulator based upon the TinyOS platform in IRIS motes. We have used a homogeneous noise model in our TOSSIM simulator. The Sources and the Sinks were selected randomly at regular intervals while doing the simulation. We have followed two trivial processes while doing our simulation:

i. In the first case we have assigned uniform trust values and the results were obtained using the original network behavior which changed with time.
ii. In the second case, we have assigned some pre-evaluated trust values to the nodes and all the network characteristics like, were taken to be proportional to those values.

This plot shows the advantage of our protocol as compared with the (LSRTP denotes DRTLSRP). Although in a few cases the performance of both are quite similar but in others our model scores over the ATSR one.

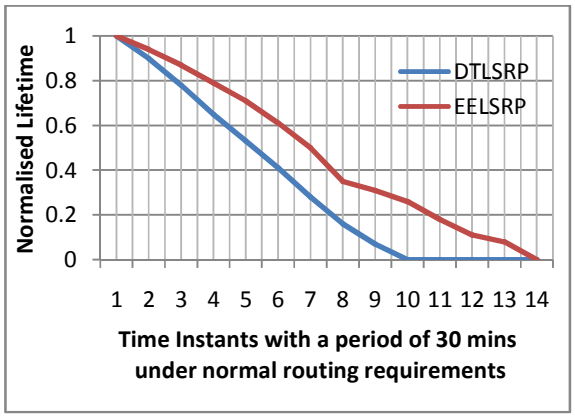

Fig. 8 Network Life Span

This plot shows the plot of transmission latency with random trust assignment. Although we can't clearly decide which one is better, it's possible to conclude that in the long run our model behaves better than their one especially in the case of equal trusts and when the number of nodes in the network is very large.

It is evident from the graph, that our proposed algorithm EELSRP enables us to send packets with reduced delay compared to DTLSRP [04].

5. CONCLUSION AND FUTURE WORK:

It can be ultimately concluded from this simulation results that our model EELSRP performs better with respect to the DTLSRP protocol [04] using only direct trusts. Due to smooth conservation of the nodes residual energies and trustworthiness, the network life span also increases. This increment in the network life time saves the WSN in many practical data/packet transmission situations. The increased connectivity among the nodes helps the routing protocols to make routing for a longer time. Future work includes implementation of this protocol and extracting energy efficiency in practical environment.

REFERENCES:

[1] Theodore Zahariadis, Helen C. Leligou, Panagiotis Trakadas and Stamatis Voliotis, "Mobile Networks Trust Management in Wireless Sensor Networks", *European Transactions on Telecommunications*, 2010; 21:386-395.

[2] M. Momani, J. Agbinya, G. P. Navarrete and M. Akache, "A New Algorithm of Trust Formation in Wireless Sensor Networks", in AusWireless '06. Sydney, Australia, 2006.

[3] Mohammad Momani, Ph.D thesis on "Bayesian methods for modeling and management of Trust in Wireless Sensor Networks", University of Technology, Sydney, July, 2008.

[4] Shaik Sahil Babu, Arnab Raha, Mrinal Kanti Naskar, "A Direct Trust dependent Link State Routing Protocol using Route Trusts for WSNs (DTLSRP)", Wireless Sensor Network, International Journal for Scientific Research, 2011, 3, 125-134. doi:10.4236/wsn.2011.34015 Published Online April 2011.

[5] Guoxing Zhan, Weisong Shi, and Julia Deng, "TARF: A Trust-aware Routing Framework For Wireless Sensor Networks", Wayne State University, Detroit, MI 48202, USA.

[6] T.Kavitha, D.Sridharan, "Security vulnerabilities In Wireless Sensor Networks: A Survey" *Journal of Information Assurance and Security*, Vol. 5 (2010) 031-044.

[7] Jaydip Sen, "A Survey on Wireless Sensor Network Security", *International Journal of Communication Networks and Information Security* (IJCNIS) Vol. 1, No. 2, August 2009.

[8] Chris Karlof, David Wagner, "Secure routing in WSNs: attacks and countermeasures", *Ad hoc networks Journal*, Vol. 1, Issue 2-3, Sept. 2003, pp.293-315.

[9] Asad Amir Pirzada, Chris McDonald, and Amitava Datta "Performance comparison of Trust-Based Reactive Routing Protocols", *IEEE Transactions on mobile computing*, Vol. 5, No. 6, June 2006.

[10] Sencun Zhu, Sanjeev Setia, Sushil Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", *Proc. Of 10th ACM conf. on Computer and Communications Security*, 2003.

[11] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", *7th Annual International Conference on Mobile Computing and Networking* (MobiCom 2001), 2001.

[12] Chris Karlof, Naveen Sastry, David Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", SenSys'04, November 3-5, 2004, Baltimore, Maryland, USA.

[13] HangRok Lee, YongJe Choi, HoWon Kim, "Implementation of TinyHash based on Hash Algorithm for Sensor Network", *World Academy of Science, Engineering and Technology*, Vol. 10, 2005.

[14] Matthias Becker, Sven Schaust and Eugen Wittmann, "Performance of Routing Protocols for Real Wireless Sensor Networks", *10th Int. Symposium on Performance Evaluation of Computer and Telecommunication Systems* (SPECTS'07), San Diego, USA, 2007.

[15] Matthew J. Probst and Sneha Kumar Kasera, "Statistical Trust Establishment in Wireless Sensor Networks", *13th International Conference on Parallel and Distributed Systems*, 2007.

[16] Theodore Zahariadis, Helen Leligou, Panagiotis Karkazis, Panagiotis Trakadas, Ioannis Papaefstathiou, Charalambos Vangelatos, Lionel Besson, "Design and Implementation Of A Trust-Aware Routing Protocol For Large WSNs", *International Journal of Network Security & Its Applications* (IJNSA), Vol. 2, No. 3, July 2010, pp. 52-68.

[17] Shaik Sahil Babu, Arnab Raha, Mrinal Kanti Naskar, "Geometric Mean based Trust Management System for WSNs (GMTMS)", Proceedings of the International Conference "World Congress on Information and Communication Technologies 2011 (IEEE WICT- 2011)", Mumbai, December 2011, pp. 444-449.

[18] Asad Amir Pirzada and Chris McDonald, "Trusted Greedy Perimeter Stateless Routing", IEEE, ICON 2007.

[19] Y.C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Proc. Eighth Ann. Int'l Conf. Mobile Computing and Networking (MobiCom), pp. 12-23.

[20] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victorwen and David E. Culler, "SPINS: Security Protocols for Sensor Networks", ACM Journal of Wireless Networks, 8:5, September 2002, pp. 521 – 534.

[21] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks", in Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom), ACM Press, 2000, pp. 255 – 265.

[22] S. Buchegger and J. Boudec, " Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes – Fairness In Distributed Ad-hoc Networks", in proceedings of the 3rd ACM International Symposium on Mobile Ad-hoc Networking and Computing (MobiHoc), ACM Press, 2002, pp. 226-236.

[23] Sapon Tanachaiwiwat, Pinalkumar Dave, Rohan Bhindwale, Ahmed Helmy, "Location-centric Isolation of Misbehavior and Trust routing in Energy-constrained Sensor Networks", IEEE International Conference on Performance, Computing and communications, 2004.